DARKTRACE

Darktrace Threat Visualizer API Guide

Threat Visualizer v4.1

Last Updated: February 1 2021

Darktrace Threat Visualizer API Guide

Threat Visualizer v5.0

Getting Started with the API

The Darktrace API provides a method of accessing additional information about a particular alert or device in the Darktrace system. The API uses HTTP GET requests to return formatted JSON data containing the requested information and HTTP POST or DELETE requests to configure the system. The API can be an incredibly useful tool to integrate Darktrace with third-party SIEM or SOC environments, or perform bulk actions on devices and model breaches.

Requests are made in the format:

```
'https://[appliance-IP]/[endpoint]' -H "DTAPI-Token: [token]" -H "DTAPI-Date: [date]" -H "DTAPI-
Signature: [signature]"
```

Pseudocode example

The required headers are composed of a date-time within 30 minutes of the appliance server time (`DTAPI-Date`), a public token collected from the Threat Visualizer System Config page (`DTAPI-Token`), and a HMAC-SHA1 hash (`DTAPI-Signature`) of the public and private tokens on the System Config page, the date-time and the specific API endpoint and request parameters.

Acquiring the API Token Pair

Before any data can be queried, an API token pair is needed for each Master appliance. Creating the API token requires access to the Darktrace Threat Visualizer interface and a user account with appropriate permissions to access and modify the **System Config** page.

1. Navigate to the **System Config** page on the Threat Visualizer of the appliance you wish to request data from. Select “Settings” from the left-hand menu.

2. Locate the ‘**API Token**’ subsection and click ‘**New**’.

3. Two values will be displayed, a **Public** and **Private** token, the Private token will not be displayed again.

Both Tokens are required to generate the `DT-API Signature` value, which must be passed with every API request made to the appliance, so make sure you record them securely.

API Authentication

Building an API request

API Authentication requires the API request to be constructed in advance as the specific request with its parameters is used to generate the authentication value `[signature]` . In this example, the following GET request is used to retrieve model breaches from an appliance within a given timeframe.

```
https://<appliance-ip>/modelbreaches?starttime=[START_TIMESTAMP]&endtime=[END_TIMESTAMP]
```

Where:

- `[START_TIMESTAMP]` = UNIX timestamp in milliseconds (verify 13 digits)
- `[END_TIMESTAMP]` = UNIX timestamp in milliseconds (verify 13 digits)

Required Headers

Every API query requires three header values for authentication:

DTAPI-Token: `[public-token]` is the public token obtained when creating the API token pair.

DTAPI-Date: `[date]` is the current date and time, which must be within 30 minutes of the Darktrace system time. Any of the following formats are acceptable.

- YYYYMMDDTHHIISS, i.e. 20190101T120000
- YYYY-MM-DDTHH:ii:ss, i.e. 2019-01-01T12:00:00
- YYYY-MM-DD HH:ii:ss, i.e. 2019-01-01 12:00:00
- Mon, 01 Jan 2019 12:00:00
- Mon, 01 Jan 2019 12:00:00 [GMT/UTC]
- Mon Jan 1 12:00:00 2019

DTAPI-Signature: `[signature]` is determined by computing the HMAC-SHA1 construct of a specific string. This string is composed of the API query string created above, the private API token, the appliance public API token and the current date in any of the formats above, each separated by a newline character.

Generating the Signature

The `[signature]` value is calculated using an implementation of the following method. Note the `\n` newline characters between the request, API token and timestamp in the 2nd parameter passed to the function:

```
hmac-sha1("[private-token]","[api-request]\n[public-token]\n[date]");

hmac-sha1("7chbwad4hl4n5ok69e2edrs2ogpiqy8ldd5oozdb","/modelbreaches?
starttime=1514808000000&endtime=1514808060000\n118v8jecrbrtkucou5a34hsbzounohx6jce61dwy\n20200101T1
20000");
```

Pseudocode example

The above function outputs `5ec616dfeca52c3738c77041f99d89f2648de420` , the `[signature]` value, using the following example values.

```
[api-request]: /modelbreaches?starttime=1514808000000&endtime=1514808060000
[public-token]: 118v8jecrbrtkucou5a34hsbzounohx6jce61dwy
[private-token]: 7chbwad4hl4n5ok69e2edrs2ogpiqy8ldd5oozdb
[date]: 20200101T120000
```

Important Notes:

- Only the endpoint request is used to generate the signature, the IP address or hostname of the appliance should not be included.
- For POST requests, add each post parameter into the query string as `/postendpoint?param1=value&param2=value` or `/postendpoint?{"param1":"value","param2":"value"}` to generate the signature value, where `param1` and `param2` are the data fields to be edited.

Code Examples

Examples of the `[signature]` generation in Python3 and Bash using the sample parameters we have used thus far. More code examples in other languages, along with full authentication and connection scripts where available, may be requested from Darktrace support.

Ensure that the library or method used for signature generation uses the correct encoding for your environment, to prevent signature generation errors.

Python3

```
import hmac
import hashlib
sig = hmac.new('7chbwad4hl4n5ok69e2edrs2ogpiqy8ldd5oozdb'.encode('ASCII'),('/modelbreaches?
starttime=1514808000000&endtime=1514808060000' +'\n'+ '118v8jecrbrtkucou5a34hsbzounohx6jce61dwy'
+'\n'+ '20200101T120000').encode('ASCII'), hashlib.sha1).hexdigest()
print(sig)
```

Bash

```
time=$( date +"%Y-%m-%d %T" ) #Adjust as appropriate for time zone
privatetoken=7chbwad4hl4n5ok69e2edrs2ogpiqy8ldd5oozdb
publictoken=118v8jecrbrtkucou5a34hsbzounohx6jce61dwy
request="/modelbreaches?starttime=1514808000000&endtime=1514808060000"

authSig=$(printf '%s\n' "$request" "$publictoken" "$time")
hmac="$(echo -n "$authSig" | openssl dgst -sha1 -hex -hmac "$privatetoken" -binary | xxd -p )"
echo $hmac
```

This example uses the current time to generate the signature value. To recreate the example value above, replace the `date` function with `20200101T120000`

Making the API Query

Once the `[signature]` value is generated, all headers are now ready for authentication. The API call can now be made in the following format:

```
'https://[appliance-IP]/[request]' -H "DTAPI-Token: [public-token]" -H "DTAPI-Date: [date]" -H
"DTAPI-Signature: [signature]"
```

Pseudocode example

For example:

```
curl -k 'https://192.168.0.1/modelbreaches?starttime=1514808000000&endtime=1514808060000' -H
"DTAPI-Token: 118v8jecrbrtkucou5a34hsbzounohx6jce61dwy" -H "DTAPI-Date: 20200101T120000" -H "DTAPI-
Signature: 5ec616dfeca52c3738c77041f99d89f2648de420"
```

/advancedsearch/api/search

The `/advancedsearch` endpoint allows Advanced Search data to be queried and exported in JSON format from the Darktrace appliance programmatically. Advanced Search queries are Base64 encoded strings, composed of the query search terms. There are three extensions available:

- `/advancedsearch/api/search`
- `/advancedsearch/api/analyze`
- `/advancedsearch/api/graph`

The `search` extension provides the standard Advanced Search query functionality - see `graph` or `analyze` for more details on other extensions.

To familiarize yourself with what a query might look like, make a basic query in the Threat Visualizer version of Advanced Search and look at the URL - it will appear as a string of random characters. Copy the string of random characters found after the `#` in the URL. From the Threat Visualizer homepage, select Utilities from the main menu and then Base64 Converter. Paste the string into the pop-up and click ‘Decode’ - you can now see what an Advanced Search query is composed of.

For example, making a query in the Threat Visualizer Advanced Search for `@type:"ssl" AND @fields.dest_port:"443"` over the last 15 minutes will produce the URL:

```
https://<applianceIP>/advancedsearch/
#eyJzZWFyY2giOiIgQHR5cGU6XCJzc2xcIiBBTkQgQGZpZWxkcy5kZXN0X3BvcnQ6XCI0NDNcIiIsImZpZWxkcyI6W10sIm9mZn
NldCI6MCwidGltZWZyYW1lIjoiOTAwIiwiZ3JhcGhtb2RlIjoiY291bnQiLCJ0aW1lIjp7InVzZXJfaW50ZXJ2YWwiOjB9LCJtb
2RlIjoiIiwiYW5hbHl6ZV9maWVsZCI6IiJ9
```

Pasting the part after the `#` into the Base64 converter and clicking ‘Decode’ will produce:

```
{"search":" @type:\"ssl\" AND @fields.dest_port:\"443\"","fields":[],"offset":
0,"timeframe":"900","graphmode":"count","time":{"user_interval":0},"mode":"","analyze_field":""}
```

This is the basic structure of an Advanced Search query. Some of the parameters included in this request are not necessary when accessing Advanced Search programmatically. Please see the notes section for more details.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`interval`	numeric	A time interval in seconds from the current time over which to return results.
`search`	string	Optional Advanced Search search query to make. Ensure all double quotes are escaped.
`analyze_field`	string	The field to return aggregate stats for. Only used when making queries to the `/graph/mean` extension
`offset`	numeric	An offset for the results returned.

Notes

- Double quotes used in the search string must be escaped with a backslash before encoding. For example, `"search":" @type:\"ssl\" AND @fields.dest_port:\"443\""` .
- The query timeframe can either take a `starttime` / `endtime` or `to` / `from` value, or a `timeframe` interval of seconds since the current time.
  - If `starttime` / `endtime` or `to` / `from` is used, the timeframe value must be set to `"custom"` . Time parameters must always be specified in pairs.
  - If using `interval` , the `time: {}` object can be omitted from the query. It is important to note that the query response will not be the same every time as the `interval` time value is relative.
- By default, this endpoint will return 50 records at a time. The `size` parameter can be used to return up to 10,000 results. Returned data can be paginated by limiting the `size` value and making multiple requests, incrementing the `offset` value by the `size` value each time (e.g., `size=100` , multiple queries for `offset=0, offset=100, offset=200`).
- The empty `fields` array is required but the values contained within it do not change the API response. All fields will be returned when accessing advanced search programmatically.
- The parameters `graphmode` and `mode` appear in Advanced Search queries made in the Threat Visualizer. They are not required when accessing Advanced Search programmatically.
- The `analyze_field` parameter is only required when making queries to the `/advancedsearch/api/graph/mean` endpoint.

Example Request

1. `GET` HTTP/HTTPS unidirectional traffic seen over the last 12 hours:

```
https://<applianceIP>/advancedsearch/api/search/
eyJzZWFyY2giOiJAdHlwZTpjb25uIEFORCBAZmllbGRzLnByb3RvOnRjcCBBTkQgTk9UIEBmaWVsZHMuY29ubl9zdG
F0ZTpcIlMwXCIgQU5EIE5PVCBAZmllbGRzLmNvbm5fc3RhdGU6XCJSRUpcIiBBTkQgKEBmaWVsZHMub3JpZ19wa3Rz
OjAgT1IgQGZpZWxkcy5yZXNwX3BrdHM6MCkgQU5EIChAZmllbGRzLmRlc3RfcG9ydDpcIjQ0M1wiIE9SIEBmaWVsZH
MuZGVzdF9wb3J0OlwiODBcIikiLCJmaWVsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjQzMjAwIiwidGlt
ZSI6eyJ1c2VyX2ludGVydmFsIjowfX0=
```

Where the string

```
{"search":"@type:conn AND @fields.proto:tcp AND NOT @fields.conn_state:\"S0\" AND NOT
@fields.conn_state:\"REJ\" AND (@fields.orig_pkts:0 OR @fields.resp_pkts:0) AND
(@fields.dest_port:\"443\" OR @fields.dest_port:\"80\")","fields":[],"offset":
0,"timeframe":"43200","time":{"user_interval":0}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiJAdHlwZTpjb25uIEFORCBAZmllbGRzLnByb3RvOnRjcCBBTkQgTk9UIEBmaWVsZHMuY29ubl9zdG
F0ZTpcIlMwXCIgQU5EIE5PVCBAZmllbGRzLmNvbm5fc3RhdGU6XCJSRUpcIiBBTkQgKEBmaWVsZHMub3JpZ19wa3Rz
OjAgT1IgQGZpZWxkcy5yZXNwX3BrdHM6MCkgQU5EIChAZmllbGRzLmRlc3RfcG9ydDpcIjQ0M1wiIE9SIEBmaWVsZH
MuZGVzdF9wb3J0OlwiODBcIikiLCJmaWVsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjQzMjAwIiwidGlt
ZSI6eyJ1c2VyX2ludGVydmFsIjowfX0=
```

2. **GET** all identified files between 8am and 10am on February 1st 2020 with a computed SHA-1 hash:

```
https://<applianceIP>/advancedsearch/api/search/
eyJzZWFyY2giOiJAdHlwZTpmaWxlc19pZGVudGlmaWVkIEFORCBfZXhpc3RzXzpcIkBmaWVsZHMuc2hhMVwiIiwiZm
llbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJhbWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAx
VDA4OjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMVQxMDowMDowMFoiLCJ1c2VyX2ludGVydmFsIjoiMCJ9fQ==
```

Where the string

```
{"search":"@type:files_identified AND _exists_:\"@fields.sha1\"","fields":[],"offset":
0,"timeframe":"custom","time":
{"from":"2020-02-01T08:00:00Z","to":"2020-02-01T10:00:00Z","user_interval":"0"}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiJAdHlwZTpmaWxlc19pZGVudGlmaWVkIEFORCBfZXhpc3RzXzpcIkBmaWVsZHMuc2hhMVwiIiwiZm
llbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJhbWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAx
VDA4OjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMVQxMDowMDowMFoiLCJ1c2VyX2ludGVydmFsIjoiMCJ9fQ==
```

3. **GET** any SMB1 sessions seen in the last 7 days:

```
https://<applianceIP>/advancedsearch/api/search/
eyJzZWFyY2giOiJAdHlwZTpzbWJfc2Vzc2lvbiBBTkQgQGZpZWxkcy5wcm90b2NvbF92ZXI6XCJzbWIxXCIiLCJmaW
VsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjYwNDgwMCIsInRpbWUiOnsidXNlcl9pbnRlcnZhbCI6MH19
```

Where the string

```
{"search":"@type:smb_session AND @fields.protocol_ver:\"smb1\"","fields":[],"offset":
0,"timeframe":"604800","time":{"user_interval":0}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiJAdHlwZTpzbWJfc2Vzc2lvbiBBTkQgQGZpZWxkcy5wcm90b2NvbF92ZXI6XCJzbWIxXCIiLCJmaW
VsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjYwNDgwMCIsInRpbWUiOnsidXNlcl9pbnRlcnZhbCI6MH19
```

Example Response

Request:

```
  /advancedsearch/api/search/
eyJzZWFyY2giOiJAdHlwZTpjb25uIEFORCBAZmllbGRzLnByb3RvOnRjcCBBTkQgTk9UIEBmaWVsZHMuY29ubl9zdGF0ZTpcIlM
wXCIgQU5EIE5PVCBAZmllbGRzLmNvbm5fc3RhdGU6XCJSRUpcIiBBTkQgKEBmaWVsZHMub3JpZ19wa3RzOjAgT1IgQGZpZWxkcy
5yZXNwX3BrdHM6MCkgQU5EIChAZmllbGRzLmRlc3RfcG9ydDpcIjQ0M1wiIE9SIEBmaWVsZHMuZGVzdF9wb3J0OlwiODBcIikiL
CJmaWVsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjQzMjAwIiwidGltZSI6eyJ1c2VyX2ludGVydmFsIjowfX0=
{
  "took": 17,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 6900,
    "max_score": null,
    "hits": [
      {
        "_index": "logstash-dt-01-01-2020.02.24",
        "_type": "doc",
        "_id": "AXB4bgyXFqFpgk38klzi",
        "_score": null,
        "_source": {
          "@fields": {
            "orig_pkts": 2,
            ...
          },
          "@type": "conn",
          "@timestamp": "2020-02-24T18:20:31",
          "@message":
"1582568431.7656\tCNbx1P3gEMU3dZqS00\t10.0.56.12\t50518\t192.168.120.39\t443\ttcp\t-
\t2\t64\tOriginator SYN + FIN\tSH\ttrue\t0\t0\t1582568431.7656\t0\t104\tF\ttrue\t0"
        },
        "sort": [
          1582568431000
        ]
      },
      ...
      }
    ]
  },
  "darktraceChildError": "",
  "kibana": {
    "index": [
      "logstash-darktrace-2020.02.24"
    ],
    "per_page": 50,
    "time": {
      "from": "2020-02-24T06:27:23.209Z",
      "to": "2020-02-24T18:27:23.209Z"
    },
    "default_fields": [
      "@type",
      "@message"
    ]
  }
}
```

Response is abbreviated.

/advancedsearch/api/search Response Schema

Response Schema

Response Field	Type	Example Value	Description
`took`	numeric	`22`	The time the request took in milliseconds.
`timed_out`	boolean	`FALSE`	Whether the response timed out.
`_shards`	object		A system field.
`_shards.total`	numeric	`2`	A system field.
`_shards.successful`	numeric	`2`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`13123`	The total number of entries that matched the query.
`hits.max_score`	-	`null`	A system field.
`hits.hits`	array		An array of advanced search entries.
`hits.hits._index`	string	`logstash-dt-01-2020.03.23`	The index the entry was returned from.
`hits.hits._type`	string	`doc`	A system field.
`hits.hits._id`	string	`K18S2Iqiu7Wz1jaN`	The unique id for the entry in the database.
`hits.hits._score`	-	`null`	A system field.
`hits.hits._source`	object		An object describing the entry.
`hits.hits._source.@fields`	object		An object containing all the relevant fields for the protocol. A list of fields that may be returned for each protocol can be found at ▯.
`hits.hits._source.@type`	string	`conn`	The protocol or entry type.
`hits.hits._source.@timestamp`	string	`2020-03-23T11:59:09`	A timestamp for the insertion of the entry into advanced search logs.

`hits.hits._source.@message`	string	`1584964749.0817\tCT6zqD1qlMlhcAp00\t104.20.203.23\t54250\t172.`
		`\t2\t64\tMidstream traffic\t0TH\ttrue\t0\t0\t1584964749.0817\t`
			A unique string constructed from field values for the entry.

`hits.hits.sort`	array	`1586937600000`	A simplified timestamp for the record for sorting purposes.
`darktraceChildError`	string	`Factory Probe 1`	The name of a probe which did not respond to the request.
`kibana`	object		Details about the advanced search logs.
`kibana.index`	array		A system field.
`kibana.per_page`	numeric	`50`	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.
`kibana.time`	object		The time window specified in the request.
`kibana.time.from`	string	`2020-03-23T00:09:24.980Z`	The start of the time window specified in the request.

Response Field	Type	Example Value	Description
`kibana.time.to`	string	`2020-03-23T12:09:24.980Z`	The end of the time window specified in the request.
`kibana.default_fields`	array	`“@type”`	Default fields always returned at the highest level.

Example Response

Request:

```
  /advancedsearch/api/search/
eyJzZWFyY2giOiJAdHlwZTpjb25uIEFORCBAZmllbGRzLnByb3RvOnRjcCBBTkQgTk9UIEBmaWVsZHMuY29ubl9zdGF0ZTpcIlM
wXCIgQU5EIE5PVCBAZmllbGRzLmNvbm5fc3RhdGU6XCJSRUpcIiBBTkQgKEBmaWVsZHMub3JpZ19wa3RzOjAgT1IgQGZpZWxkcy
5yZXNwX3BrdHM6MCkgQU5EIChAZmllbGRzLmRlc3RfcG9ydDpcIjQ0M1wiIE9SIEBmaWVsZHMuZGVzdF9wb3J0OlwiODBcIikiL
CJmaWVsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjQzMjAwIiwidGltZSI6eyJ1c2VyX2ludGVydmFsIjowfX0=
```

```
{
  "took": 17,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 6900,
    "max_score": null,
    "hits": [
      {
        "_index": "logstash-dt-01-01-2020.02.24",
        "_type": "doc",
        "_id": "AXB4bgyXFqFpgk38klzi",
        "_score": null,
        "_source": {
          "@fields": {
            "orig_pkts": 2,
            ...
          },
          "@type": "conn",
          "@timestamp": "2020-02-24T18:20:31",
          "@message":
"1582568431.7656\tCNbx1P3gEMU3dZqS00\t10.0.56.12\t50518\t192.168.120.39\t443\ttcp\t-
\t2\t64\tOriginator SYN + FIN\tSH\ttrue\t0\t0\t1582568431.7656\t0\t104\tF\ttrue\t0"
        },
        "sort": [
          1582568431000
        ]
      },
      ...
      }
    ]
  },
  "darktraceChildError": "",
  "kibana": {
    "index": [
      "logstash-darktrace-2020.02.24"
    ],
    "per_page": 50,
    "time": {
      "from": "2020-02-24T06:27:23.209Z",
      "to": "2020-02-24T18:27:23.209Z"
    },
    "default_fields": [
      "@type",
      "@message"
    ]
  }
}
```

Response is abbreviated.

/advancedsearch/api/analyze

The `/advancedsearch` endpoint allows Advanced Search data to be queried and exported in JSON format from the Darktrace appliance programmatically. Advanced Search queries are Base64 encoded strings, composed of the query search terms.

The `analyze` extension can produce a `trend` , `score` , `terms` or `mean` (“stats” in the User Interface) analysis on a specific field. It requires a Base64 encoded query string as created in `/advancedsearch/api/search` as part of the request.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`interval`	numeric	A time interval in seconds from the current time over which to return results.
`search`	string	Optional Advanced Search search query to make. Ensure all double quotes are escaped.

Notes

- Double quotes used in the search string must be escaped with a backslash before encoding. For example, `"search":" @type:\"ssl\" AND @fields.dest_port:\"443\""` .
- The query timeframe can either take a `starttime` / `endtime` or `to` / `from` value, or a `timeframe` interval of seconds since the current time.
    - If `starttime` / `endtime` or `to` / `from` is used, the timeframe value must be set to `"custom"` . Time parameters must always be specified in pairs.
    - If using `interval` , the `time: {}` object can be omitted from the query. It is important to note that the query response will not be the same every time as the `interval` time value is relative.
- The parameters `graphmode` and `mode` appear in Advanced Search queries made in the Threat Visualizer. They are not required when accessing Advanced Search programmatically.
- The empty `fields` array is required but the values contained within it do not change the API response.

Example Request

1. `GET` the most used terms for `@fields.dest_port` between 2020-02-20 17:00:00 and 2020-02-20 17:15:00 for the query `@type:"dns" AND @fields.proto:"udp"` :

```
https://<applianceIP>/advancedsearch/api/analyze/@fields.dest_port/terms/
eyJzZWFyY2giOiIgQHR5cGU6XCJkbnNcIiBBTkQgQGZpZWxkcy5wcm90bzpcInVkcFwiIiwiZmllbGRzIjpbXSwib2
Zmc2V0IjowLCJ0aW1lZnJhbWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTIwVDE3OjAwOjAwWiIs
InRvIjoiMjAyMC0wMi0yMFQxNzoxNTowMFoiLCJ1c2VyX2ludGVydmFsIjoiMCJ9fQ==
```

Where the string

```
{"search":" @type:\"dns\" AND @fields.proto:\"udp\"","fields":[],"offset":
0,"timeframe":"custom","time":
{"from":"2020-02-20T17:00:00Z","to":"2020-02-20T17:15:00Z","user_interval":"0"}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiIgQHR5cGU6XCJkbnNcIiBBTkQgQGZpZWxkcy5wcm90bzpcInVkcFwiIiwiZmllbGRzIjpbXSwib2
Zmc2V0IjowLCJ0aW1lZnJhbWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTIwVDE3OjAwOjAwWiIs
InRvIjoiMjAyMC0wMi0yMFQxNzoxNTowMFoiLCJ1c2VyX2ludGVydmFsIjoiMCJ9fQ==
```

2. `GET` the Office 365 users (`@fields.saas_credential`) with the most frequent failed logins (`@type:office365 AND @fields.saas_event:"UserLoginFailed"`) over the last 7 days:

```
https://<applianceIP>/advancedsearch/api/analyze/@fields.saas_credential/score/
eyJzZWFyY2giOiJAdHlwZTpvZmZpY2UzNjUgQU5EIEBmaWVsZHMuc2Fhc19ldmVudDpcIlVzZXJMb2dpbkZhaWxlZF
wiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJhbWUiOiI2MDQ4MDAifQ==
```

Where the string

```
{"search":"@type:office365 AND @fields.saas_event:\"UserLoginFailed\"","fields":
[],"offset":0,"timeframe":"604800"}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiJAdHlwZTpvZmZpY2UzNjUgQU5EIEBmaWVsZHMuc2Fhc19ldmVudDpcIlVzZXJMb2dpbkZhaWxlZF
wiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJhbWUiOiI2MDQ4MDAifQ==
```

3. **GET** stats about the volume of bytes transferred from 192.168.120.39 to 10.0.56.12 on 2nd February 2020:

```
https://<applianceIP>/advancedsearch/api/analyze/@fields.orig_bytes/mean/
eyJzZWFyY2giOiIgQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbGRzLnNvdXJjZV9pcDpcIj
E5Mi4xNjguMTIwLjM5XCIgQU5EIEB0eXBlOlwiY29ublwiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJh
bWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAyVDAwOjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMl
QyMzo1OTo1OVoiLCJ1c2VyX2ludGVydmFsIjowfX0=
```

Where the string

```
{"search":" @fields.dest_ip:\"10.0.56.12\" AND @fields.source_ip:\"192.168.120.39\" AND
@type:\"conn\"","fields":[],"offset":0,"timeframe":"custom","time":
{"from":"2020-02-02T00:00:00Z","to":"2020-02-02T23:59:59Z","user_interval":0}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiIgQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbGRzLnNvdXJjZV9pcDpcIj
E5Mi4xNjguMTIwLjM5XCIgQU5EIEB0eXBlOlwiY29ublwiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJh
bWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAyVDAwOjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMl
QyMzo1OTo1OVoiLCJ1c2VyX2ludGVydmFsIjowfX0=
```

Example Response

Request:

```
/advancedsearch/api/analyze/@fields.dest_port/terms/
eyJzZWFyY2giOiIgQHR5cGU6XCJkbnNcIiBBTkQgQGZpZWxkcy5wcm90bzpcInVkcFwiIiwiZmllbGRzIjpbXSwib2Zmc2V0Ijo
wLCJ0aW1lZnJhbWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTIwVDE3OjAwOjAwWiIsInRvIjoiMjAyMC0wMi
0yMFQxNzoxNTowMFoiLCJ1c2VyX2ludGVydmFsIjoiMCJ9fQ==
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 8001,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "terms": {
      "doc_count_error_upper_bound": 0,
      "sum_other_doc_count": 0,
      "buckets": [
        {
          "key": 53,
          "doc_count": 6574
        },
        {
          "key": 5353,
          "doc_count": 1427
        }
      ]
    }
  },
  "darktraceChildError": "",
  "kibana": {
    "index": "logstash-darktrace-2020.02.20",
    "per_page": 50,
    "time": {
      "from": "2020-02-20T17:00:00.000Z",
      "to": "2020-02-20T17:15:00.000Z"
    }
  }
}
```

/advancedsearch/api/analyze Response Schema

Response Schema - `/mean`

Response Field	Type	Example Value	Description
took	numeric	406	The time the request took in milliseconds.
timed_out	boolean	FALSE	Whether the response timed out.
_shards	object		A system field.
_shards.total	numeric	2	A system field.
_shards.successful	numeric	2	A system field.
_shards.skipped	numeric	0	A system field.
_shards.failed	numeric	0	A system field.
hits	object		An object encapsulating the advanced search entries that matched the request.
hits.total	numeric	20573	The total number of entries that matched the query.
hits.max_score	numeric	0	A system field.
hits.hits	array		An array of advanced search entries.
aggregations	object		Aggregated values to use in graphical operations.
aggregations.stats	object		An object describing statistical analysis on the results within that interval.
aggregations.stats.count	numeric	10355	The number of results contained within the grouped interval.
aggregations.stats.min	numeric	0	For the field specified when making the request, the minimum value observed within the interval.
aggregations.stats.max	numeric	14651	For the field specified when making the request, the maximum value observed within the interval.
aggregations.stats.avg	numeric	310.263351	For the field specified when making the request, the average value observed within the interval.
aggregations.stats.sum	numeric	3212777	For the field specified when making the request, the sum of all values observed within the interval.
darktraceChildError	string	FactoryProbe_1	The name of a probe which did not respond to the request.
kibana	object		Details about the advanced search logs.
kibana.index	string	logstash-darktrace-2020.03.02	A system field.
kibana.per_page	numeric	50	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.
kibana.time	object		The time window which the data is grouped into.

Response Field	Type	Example Value	Description
`kibana.time.from`	string	`2020-03-02T00:00:00.000Z`	The start of the time window specified in the request.
`kibana.time.to`	string	`2020-03-02T23:59:59.000Z`	The end of the time window specified in the request.

Example Response

```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 25,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "stats": {
      "count": 25,
      "min": 97,
      "max": 308,
      "avg": 195.36,
      "sum": 4884
    }
  },
  "kibana": {
    "index": "logstash-darktrace-2020.04.17",
    "per_page": 50,
    "time": {
      "from": "2020-04-17T17:27:43.806Z",
      "to": "2020-04-17T18:27:43.806Z"
    }
  }
}
```

Response Schema - `/terms`

Response Field	Type	Example Value	Description
`took`	numeric	`171`	The time the request took in milliseconds.
`timed_out`	boolean	`FALSE`	Whether the response timed out.
`_shards`	object		A system field.
`_shards.total`	numeric	`4`	A system field.
`_shards.successful`	numeric	`4`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`5`	The total number of entries that matched the query.
`hits.max_score`	numeric	`0`	A system field.

Response Field	Type	Example Value	Description
`hits.hits`	array		An array of advanced search entries.
`aggregations`	object		An array of aggregated data about the field queried upon.
`aggregations.terms`	object		An array of aggregated data from the terms analysis performed.
`aggregations.terms.doc_count_error_upper_bound`	numeric	`0`	A system field.
`aggregations.terms.sum_other_doc_count`	numeric	`0`	A system field.
`aggregations.terms.buckets`	array		An array of values for the field which was analyzed.
`aggregations.terms.buckets.key`	string	`grayson.stone@holdingsinc.com`	A field value.
`aggregations.terms.buckets.doc_count`	numeric	`3`	The number of times the value appeared in the specified field.
`darktraceChildError`	string	`FactoryProbe_1`	The name of a probe which did not respond to the request.
`kibana`	object		Details about the advanced search logs.
`kibana.index`	string	`logstash-darktrace-2020.03.23`	A system field.
`kibana.per_page`	numeric	`50`	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.
`kibana.time`	object		The time window specified in the request.
`kibana.time.from`	string	`2020-03-16T16:34:45.211Z`	The start of the time window specified in the request.
`kibana.time.to`	string	`2020-03-23T16:34:45.211Z`	The end of the time window specified in the request.

Example Response

```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 8001,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "terms": {
      "doc_count_error_upper_bound": 0,
      "sum_other_doc_count": 0,
      "buckets": [
        {
          "key": 53,
          "doc_count": 6574
        },
        ...
      ]
    }
  },
  "darktraceChildError": "",
  "kibana": {
    "index": "logstash-darktrace-2020.02.20",
    "per_page": 50,
    "time": {
      "from": "2020-02-20T17:00:00.000Z",
      "to": "2020-02-20T17:15:00.000Z"
    }
  }
}
```

Response is abbreviated.

Response Schema - `/trend`

Response Field	Type	Example Value	Description
`took`	numeric	`83`	The time the request took in milliseconds.
`timed_out`	boolean	`FALSE`	Whether the response timed out.
`_shards`	object		A system field.
`_shards.total`	numeric	`2`	A system field.
`_shards.successful`	numeric	`2`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`20573`	The total number of entries that matched the query.
`hits.max_score`	NoneType	`null`	A system field.
`hits.hits`	array		An array of advanced search entries.

Response Field	Type	Example Value	Description
`hits.hits.id`	string	`SF`	The value of the specified field.
`hits.hits.count`	numeric	`6868`	The amount of times that value appeared in the entries that matched the query parameters.
`hits.hits.start`	numeric	`2707`	A system field.
`hits.hits.trend`	numeric	`41.61`	The increase or decrease of that value's occurrence over the time window specified.
`hits.count`	numeric	`10000`	The total number of entries analyzed.
`darktraceChildError`	string	`FactoryProbe_1`	The name of a probe which did not respond to the request.
`kibana`	object		Details about the advanced search logs.
`kibana.index`	array	`logstash-darktrace-2020.03.02`	A system field.
`kibana.per_page`	numeric	`50`	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.
`kibana.time`	object		The time window specified in the request.
`kibana.time.from`	string	`2020-03-02T00:00:00.000Z`	The start of the time window specified in the request.
`kibana.time.to`	string	`2020-03-02T23:59:59.000Z`	The end of the time window specified in the request.

Example Response

```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 26,
    "max_score": null,
    "hits": [
      {
        "id": "SearchAlert",
        "count": 3,
        "start": 3,
        "trend": 0
      },
      ...
    ],
    "count": 26
  },
  "kibana": {
    "index": [
      "logstash-darktrace-2020.04.17"
    ],
    "per_page": 50,
    "time": {
      "from": "2020-04-17T17:24:50.759Z",
      "to": "2020-04-17T18:24:50.759Z"
    }
  }
}
```

Response is abbreviated.

Response Schema - `/score`

Response Field	Type	Example Value	Description
`took`	numeric	`25`	The time the request took in milliseconds.
`timed_out`	boolean	`FALSE`	Whether the response timed out.
`_shards`	object		A system field.
`_shards.total`	numeric	`2`	A system field.
`_shards.successful`	numeric	`2`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`52`	The total number of entries that matched the query.
`hits.max_score`	NoneType	`null`	A system field.
`hits.hits`	array		An array of advanced search entries.
`hits.hits.id`	string	`benjamin.ash@holdingsinc.com`	For the field specified in the request, the value.
`hits.hits.count`	numeric	`19`	The frequency that that value appeared within the entries that matched the parameters.
`hits.count`	numeric	`52`	The total number of entries that matched the query.
`darktraceChildError`	string	`FactoryProbe_1`	The name of a probe which did not respond to the request.
`kibana`	object		Details about the advanced search logs.
`kibana.index`	array	`logstash-darktrace-2020.03.23`	A system field.
`kibana.per_page`	numeric	`50`	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.
`kibana.time`	object		The time window specified in the request.
`kibana.time.from`	string	`2020-03-16T16:33:00.615Z`	The start of the time window specified in the request.
`kibana.time.to`	string	`2020-03-23T16:33:00.615Z`	The end of the time window specified in the request.

Example Response

```
    "took": 0,
    "timed_out": false,
    "_shards": {
      "total": 2,
      "successful": 2,
      "skipped": 0,
      "failed": 0
    },
    "hits": {
      "total": 26,
      "max_score": null,
      "hits": [
        {
          "id": "Saas::Misc",
          "count": 23
        },
        {
          "id": "Saas::Login",
          "count": 3
        }
      ],
      "count": 26
    },
    "kibana": {
      "index": [
        "logstash-darktrace-2020.04.17"
      ],
      "per_page": 50,
      "time": {
        "from": "2020-04-17T17:26:24.603Z",
        "to": "2020-04-17T18:26:24.603Z"
      }
    }
  }
```

/advancedsearch/api/graph

The `/advancedsearch` endpoint allows Advanced Search data to be queried and exported in JSON format from the Darktrace appliance programmatically. Advanced Search queries are Base64 encoded strings, composed of the query search terms.

The `graph` extension returns data to create a timeseries graph of results, it can produce a `count` or `mean` graph. It requires a Base64 encoded query string as created in /advancedsearch/api/search as part of the request. When making a request to `mean` , a field must also be supplied to aggregate upon.

A request to the `graph` extension requires a graph interval. The graph interval is the time window that results will be grouped into for each 'bar' of the graph. It takes a value in milliseconds (seconds * 1000). The larger the value, the faster the query will be returned. Queries over a large timeframe with a low graph interval value will use significant resources and are strongly discouraged. At a minimum, the following values should be used:

Query Timeframe	Minimum Graph Interval
15m	10000 (10s)
60m	30000 (30s)
4h	60000 (1m)
12h	300000 (10m)
24h	300000 (10m)
48h	1800000 (30m)
7d	3600000 (1h)

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`interval`	numeric	A time interval in seconds from the current time over which to return results.
`size`	numeric	The number of results to return, default is 50 if unspecified. Maximum is 10,000
`search`	string	Optional Advanced Search search query to make. Ensure all double quotes are escaped.
`analyze_field`	string	The field to return aggregate stats for. Only used when making queries to the `/graph/mean` extension

Notes

- Double quotes used in the search string must be escaped with a backslash before encoding. For example, `"search":" @type:\"ssl\" AND @fields.dest_port:\"443\""` .

- The query timeframe can either take a `starttime` / `endtime` or `to` / `from` value, or a `timeframe` interval of seconds since the current time.
  - If `starttime` / `endtime` or `to` / `from` is used, the timeframe value must be set to `"custom"` . Time parameters must always be specified in pairs.
  - If using `interval` , the `time: {}` object can be omitted from the query. It is important to note that the query response will not be the same every time as the `interval` time value is relative.
- The `analyze_field` parameter is required when making queries to the `mean` extension. It must be provided in the Base64 encoded string.
- The `graphmode` parameter appears in Advanced Search queries made in the Threat Visualizer. When accessing Advanced Search programmatically, the type of data returned is controlled by the extension used - `/advancedsearch/graph/count` or `/advancedsearch/graph/mean` - rather than the `graphmode` field.
- The parameter `"mode":` appears in Advanced Search queries made in the Threat Visualizer. It is not required when accessing Advanced Search programmatically.
- The empty `fields` array is required but the values contained within it do not change the API response.

Example Request

1. `GET` the number of SSH connections (in half-hour segments) between 192.168.120.39 and 10.0.56.12 in the last 48 hours:

```
https://<applianceIP>/advancedsearch/api/graph/count/1800000/
eyJzZWFyY2giOiJAdHlwZTpzc2ggQU5EICgoQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbG
RzLnNvdXJjZV9pcDpcIjE5Mi4xNjguMTIwLjM5XCIpIE9SIChAZmllbGRzLnNvdXJjZV9pcDpcIjEwLjAuNTYuMTJc
IiBBTkQgQGZpZWxkcy5kZXN0X2lwOlwiMTkyLjE2OC4xMjAuMzlcIikpIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLC
J0aW1lZnJhbWUiOiIxNzI4MDAiLCJ0aW1lIjp7InVzZXJfaW50ZXJ2YWwiOjB9fQ==
```

Where the string

```
{"search":"@type:ssh AND ((@fields.dest_ip:\"10.0.56.12\" AND @fields.source_ip:
\"192.168.120.39\") OR (@fields.source_ip:\"10.0.56.12\" AND @fields.dest_ip:
\"192.168.120.39\"))","fields":[],"offset":0,"timeframe":"172800","time":{"user_interval":
0}}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiJAdHlwZTpzc2ggQU5EICgoQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbG
RzLnNvdXJjZV9pcDpcIjE5Mi4xNjguMTIwLjM5XCIpIE9SIChAZmllbGRzLnNvdXJjZV9pcDpcIjEwLjAuNTYuMTJc
IiBBTkQgQGZpZWxkcy5kZXN0X2lwOlwiMTkyLjE2OC4xMjAuMzlcIikpIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLC
J0aW1lZnJhbWUiOiIxNzI4MDAiLCJ0aW1lIjp7InVzZXJfaW50ZXJ2YWwiOjB9fQ==
```

2. `GET` the average data transfer (volume of bytes) transferred from 192.168.120.39 to 10.0.56.12 on 2nd February 2020:

```
https://<applianceIP>/advancedsearch/api/graph/mean/30000/
eyJzZWFyY2giOiIgQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbGRzLnNvdXJjZV9pcDpcIj
E5Mi4xNjguMTIwLjM5XCIgQU5EIEB0eXBlOlwiY29ublwiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJh
bWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAyVDAwOjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMl
QyMzo1OTo1OVoiLCJ1c2VyX2ludGVydmFsIjowfSwiYW5hbHl6ZV9maWVsZCI6IkBmaWVsZHMub3JpZ19pcF9ieXRl
cyJ9
```

Where the string

```
{"search":" @fields.dest_ip:\"10.0.56.12\" AND @fields.source_ip:\"192.168.120.39\" AND
@type:\"conn\"","fields":[],"offset":0,"timeframe":"custom","time":
{"from":"2020-02-02T00:00:00Z","to":"2020-02-02T23:59:59Z","user_interval":
0},"analyze_field":"@fields.orig_ip_bytes"}
```

has been Base64 encoded to

```
eyJzZWFyY2giOiIgQGZpZWxkcy5kZXN0X2lwOlwiMTAuMC41Ni4xMlwiIEFORCBAZmllbGRzLnNvdXJjZV9pcDpcIj
E5Mi4xNjguMTIwLjM5XCIgQU5EIEB0eXBlOlwiY29ublwiIiwiZmllbGRzIjpbXSwib2Zmc2V0IjowLCJ0aW1lZnJh
bWUiOiJjdXN0b20iLCJ0aW1lIjp7ImZyb20iOiIyMDIwLTAyLTAyVDAwOjAwOjAwWiIsInRvIjoiMjAyMC0wMi0wMl
QyMzo1OTo1OVoiLCJ1c2VyX2ludGVydmFsIjowfSwiYW5hbHl6ZV9maWVsZCI6IkBmaWVsZHMub3JpZ19pcF9ieXRl
cyJ9
```

Example Response

Request:

```
/advancedsearch/api/graph/count/10000/
eyJzZWFyY2giOiJAdHlwZTpjb25uIEFORCBAZmllbGRzLnByb3RvOnRjcCBBTkQgTk9UIEBmaWVsZHMuY29ubl9zdGF0ZTpcIlM
wXCIgQU5EIE5PVCBAZmllbGRzLmNvbm5fc3RhdGU6XCJSRUpcIiBBTkQgKEBmaWVsZHMub3JpZ19wa3RzOjAgT1IgQGZpZWxkcy
5yZXNwX3BrdHM6MCkgQU5EIChAZmllbGRzLmRlc3RfcG9ydDpcIjQ0M1wiIE9SIEBmaWVsZHMuZGVzdF9wb3J0OlwiODBcIikiL
CJmaWVsZHMiOltdLCJvZmZzZXQiOjAsInRpbWVmcmFtZSI6IjQzMjAwIiwidGltZSI6eyJ1c2VyX2ludGVydmFsIjowfX0=
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 217,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "count": {
      "buckets": [
        {
          "key": 1582536600000,
          "doc_count": 17
        }
        ...
      ]
    }
  },
  "darktraceChildError": "",
  "kibana": {
    "index": [
      "logstash-darktrace-2020.02.24",
      "logstash-darktrace-2020.02.23",
      "logstash-darktrace-2020.02.22"
    ],
    "per_page": 50,
    "next": 1
  }
```

Response is abbreviated.

/advancedsearch/api/graph Response Schema

Response Schema - `/graph/mean`

Response Field	Type	Example Value	Description
`took`	numeric	`8`	The time the request took in milliseconds.
`timed_out`	boolean	`FALSE`	Whether the response timed out.
`_shards`	object		A system field.
`_shards.total`	numeric	`2`	A system field.
`_shards.successful`	numeric	`2`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`20573`	The total number of entries that matched the query.
`hits.max_score`	numeric	`0`	A system field.
`hits.hits`	array		An array of advanced search entries.
`aggregations`	object		Aggregated values to use in graphical operations.
`aggregations.mean`	object		An object containing time series data for a mean graph.
`aggregations.mean.buckets`	array		An array of grouped data which can be represented as time series data.
`aggregations.mean.buckets.key_as_string`	string	`2020-03-02T00:00:00.000Z`	The timestamp for the grouped data interval in readable format.
`aggregations.mean.buckets.key`	numeric	`1586937600000`	The timestamp for the grouped data interval in epoch time.
`aggregations.mean.buckets.doc_count`	numeric	`131`	The number of results contained within the grouped interval.
`aggregations.mean.buckets.mean_stats`	object		An object describing statistical analysis on the results within that interval.
`aggregations.mean.buckets.mean_stats.count`	numeric	`131`	The number of results contained within the grouped interval.
`aggregations.mean.buckets.mean_stats.min`	numeric	`0`	For the field specified when making the request, the minimum value observed within the interval.
`aggregations.mean.buckets.mean_stats.max`	numeric	`2448`	For the field specified when making the request, the maximum value observed within the interval.
`aggregations.mean.buckets.mean_stats.avg`	numeric	`219.6946565`	For the field specified when making the request, the average value observed within the interval.
`aggregations.mean.buckets.mean_stats.sum`	numeric	`28780`	For the field specified when making the request, the sum of all values observed within the interval.
`darktraceChildError`	string	`FactoryProbe_1`	The name of a probe which did not respond to the request.

Response Field	Type	Example Value	Description
kibana	object		Details about the advanced search logs.
kibana.index	array	logstash-darktrace-2020.03.02	A system field.
kibana.per_page	numeric	50	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.

Example Response

```
{
  "took": 0,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 22,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "mean": {
      "buckets": [
        {
          "key_as_string": "2020-04-17T18:02:30.000Z",
          "key": 1587146550000,
          "doc_count": 1,
          "mean_stats": {
            "count": 1,
            "min": 144,
            "max": 144,
            "avg": 144,
            "sum": 144
          }
        },
           ...
      ]
    }
  },
  "kibana": {
    "index": [
      "logstash-darktrace-2020.04.17"
    ],
    "per_page": 50
  }
}
```

Response is abbreviated.

Response Schema - `/graph/count`

Response Field	Type	Example Value	Description
took	numeric	2	The time the request took in milliseconds.
timed_out	boolean	FALSE	Whether the response timed out.
_shards	object		A system field.
_shards.total	numeric	2	A system field.

Response Field	Type	Example Value	Description
`_shards.successful`	numeric	`2`	A system field.
`_shards.skipped`	numeric	`0`	A system field.
`_shards.failed`	numeric	`0`	A system field.
`hits`	object		An object encapsulating the advanced search entries that matched the request.
`hits.total`	numeric	`8921`	The total number of entries that matched the query.
`hits.max_score`	numeric	`0`	A system field.
`hits.hits`	array		An array of advanced search entries.
`aggregations`	object		Aggregated values to use in graphical operations.
`aggregations.count`	object		An object containing time series data for a count graph.
`aggregations.count.buckets`	array		An array of grouped data which can be represented as time series data.
`aggregations.count.buckets.key`	numeric	`1586937600000`	The timestamp for the grouped data interval in epoch time.
`aggregations.count.buckets.doc_count`	numeric	`39`	The number of results contained within the grouped interval.
`darktraceChildError`	string	`FactoryProbe_1`	The name of a probe which did not respond to the request.
`kibana`	object		Details about the advanced search logs.
`kibana.index`	array	`logstash-darktrace-2020.03.23`	A system field.
`kibana.per_page`	numeric	`50`	The number of results returned in the page. If the `size` value is changed, will continue to return a value of 50.

Example Response

```
{
  "took": 1,
  "timed_out": false,
  "_shards": {
    "total": 2,
    "successful": 2,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": 217,
    "max_score": 0,
    "hits": []
  },
  "aggregations": {
    "count": {
      "buckets": [
        {
          "key": 1582536600000,
          "doc_count": 17
        }
        ...
      ]
    }
  },
  "darktraceChildError": "",
  "kibana": {
    "index": [
      "logstash-darktrace-2020.02.24",
      "logstash-darktrace-2020.02.23",
      "logstash-darktrace-2020.02.22"
    ],
    "per_page": 50,
    "next": 1
  }
```

Response is abbreviated.

/aianalyst/incidents

The `/aianalyst/incidents` endpoint provides access to AI Analyst events - a group of anomalies or network activity investigated by Cyber AI Analyst that pose a likely cyber threat.

The Darktrace Cyber AI Analyst investigates, analyzes and reports upon threats seen within your Darktrace environment; as a starting point, it reviews and investigates all Model Breaches that occur on the system. If anomalies or patterns of activity are identified during this analysis process, an event is created.

AI Analyst incidents in the Threat Visualizer UI are comprised of one or more events, where an event is a tab within each incident.

- Where an incident in the UI is cross-network - involves multiple devices - it will be structured in the API response as a parent event containing a number of `children` . These are ids for separate events which AI Analyst has concluded are part of the same activity. These events are grouped by default and can be separated with the parameter `mergeEvents=false` - this is recommended when gathering alert data on a rolling basis.

- Where an incident is multiple events on the same device, the Threat Visualizer groups events by the device triggering the activity to create a device incident.

For users wishing to create alerts and construct incidents from the events returned by the API, important information about how events should be grouped are provided by the grouping and activity IDs. Each event returned by the API contains an `activityId` , one or more `groupingIds` , and a `groupByActivity` field which may be `true` or `false` . The `activityId` is an identifier for the specific activity detected by AI Analyst, and each entry in the `groupingIDs` array refers to a device that triggered the activity detection.

Where `groupByActivity=true` , events which are returned during the timeframe should be aggregated by the `activityId` to create cross-device incidents. Where `groupByActivity=false` , events which are returned during the timeframe should be aggregated by the `groupingIds` to create device-based incidents.

Please note, AI Analyst incidents are aggregations of events within a timeframe. Incidents as presented in the User Interface may not directly correlate with those constructed from the API due to differing time or scoring parameters.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`includeacknowledged`	boolean	Include acknowledged events in the data.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`locale`	string	The language for returned strings. Currently supported are `de_DE` (German), `en_GB` (English UK), `en_US` (English US), `es_ES` (Spanish ES), `es_419` (Spanish LATAM), `fr_FR` (French), `ja_JP` (Japanese), `ko_KR` (Korean) , “pt_BR” (Portuguese BR)
`uuid`	string	A unique identifier for an AI Analyst event. Takes multiple values comma-separated.
`mergeEvents`	boolean	True by default. Controls whether events containing multiple child events (such as cross-network incidents) are aggregated into a single event.

Notes

- A time window for the returned events can be specified using `starttime` / `endtime` and unix time in milliseconds.
    - Where only `endtime` is set, `starttime` will default to 1 week before `endtime`. Where only `starttime` is set, `endtime` will default to the current time.
    - Events that are pinned or part of pinned incidents will always be returned, regardless of the time period specified.
    - If no time parameters are specified, events from the last seven days (and pinned events) will be returned.
- Where `locale` is not specified or not supported in the current software version, strings will default to `en_GB`.
- Where the specified `locale` uses non-ascii characters, these will be returned in unicode format and must be parsed.
- The `uuid` of an event can always be found in the `children` field of the JSON response. Where an event is comprised of multiple combined events, all uuids in the `children` array should be requested in a comma-separated format to retrieve the entire event. Multiple entries in this array will only occur if `mergeEvents=true` (default).
    - The `id` field seen in the JSON response is a system field intended for use by the Threat Visualizer interface. Although for many event types the contents of the `children` field and the `id` field are consistent, some event types (such as cross-network events) utilize a pseudo-identifier in the `id` field which will not return data when used with the `uuid` parameter.
    - Links back to the Threat Visualizer can be constructed in the format `https://<appliance-ip>/#aiincident/<uuid>,<uuid>`.

Please see the response schema for a full breakdown of the `details` *array.*

Example Request

1. `GET` all AI Analyst events - including acknowledged events - for the 7 day period from 3rd to 9th July 2020:

```
https://<applianceIP>/aianalyst/incidents?
starttime=1593734400000&endtime=1594166399000&includeacknowledged=true
```

2. `GET` details of an AI Analyst event with `uuid=04a3f36e-4u8w-v9dh-x6lb-894778cf9633` in French:

```
https://<applianceIP>/aianalyst/incidents?uuid=04a3f36e-4u8w-v9dh-
x6lb-894778cf9633&locale=fr_FR
```

3. `GET` details of a cross-network AI Analyst event with three child events - `c0ec5c71-b4fb-429b-82a7-4d6a73cbcaed`, `ve9cpd8n-j8mh-fyh3-leev-sz8s8xwfwrs5` & `c5r8131w-yev6-if7b-7alc-b6jp1v8ewon2`:

```
https://<applianceIP>/aianalyst/incidents?uuid=c0ec5c71-
b4fb-429b-82a7-4d6a73cbcaed,ve9cpd8n-j8mh-fyh3-leev-sz8s8xwfwrs5,c5r8131w-yev6-if7b-7alc-
b6jp1v8ewon2
```

Example Response

Request: /aianalyst/incidents?uuid=04a3f36e-4u8w-v9dh-x6lb-894778cf9633&locale=en_US

```
[
  {
    "aiaScore": 100,
    "children": [
      "04a3f36e-4u8w-v9dh-x6lb-894778cf9633"
    ],
    "summary": "A chain of administrative connections were observed between multiple devices,
which occurred around the same time, and included workstation-local-82.",
    "id": "04a3f36e-4u8w-v9dh-x6lb-894778cf9633",
    "pinned": true,
    "acknowledged": false,
    "details": [
      [
        {
          "header": "First Hop",
          "contents": [
            {
              "type": "timestampRange",
              "key": "Time",
              "values": [
                {
                  "start": 1579710063121,
                  "end": 1579711920166
                }
              ]
            },
            {
              "type": "device",
              "key": "Source device",
              "values": [
                {
                  "sid": 12,
                  "mac": "56:2d:4b:9c:18:42",
                  "ip": "10.12.14.2",
                  "identifier": "Finance File Server",
                  "did": 532,
                  "hostname": null,
                  "subnet": null
                }
              ]
            },
            ...
          ]
        }
      ],
      [
        ...
          ]
        }
      ]
    ],
    "summariser": "LateralMovementCrawler",
    "relatedBreaches": [
      {
        "timestamp": 1579710173000,
        "threatScore": 19,
        "pbid": 252317,
        "modelName": "Anomalous Connection / Active SSH Tunnel"
      }
    ],
    "breachDevices": [
      {
      "sid": 10,
      "mac": "93:gb:28:g1:fc:g1",
      "ip": "10.0.18.224",
      "identifier": "workstation-local-82",
      "did": 230,
      "hostname": "workstation-local-82",
      "subnet": null
      }
    ],
    "periods": [
      {
        "start": 1579708374972,
        "end": 1579711920166
      }
    ],
    "attackPhases": [
      5
    ],
    "groupingIds": [
      "544a6ce7"
    ],
```

Response is abbreviated.

/aianalyst/incidents Response Schema

Understanding the `details` array

The details array and sub-arrays contain all contextual information and analysis output regarding the event. The outer array groups sections of information together which are related, and the inner array groups together subsections that make up that section. Each subsection has a header and one or more objects (in the contents array) containing relevant information - subsections are interrelated and should not be moved outside their parent section.

For example, an event concerns a suspicious SaaS activity. The details array contains two sub-arrays (sections), the first section concerns the SaaS account itself and contains only one subsection, the second section concerns the activity itself and contains three subsections. This would be structured as follows:

```
"details": [
  [ // Section 1
    {
      "header": "SaaS User Details", // Subsection 1.1
      "contents": [ // Information relevant to Subsection 1.1
        ...
      ]
    }
  ], // End of Section 1
  [ // Section 2
    {
      "header": "Agent Carrying out Suspicious Activity", // Subsection 2.1
      "contents": [ // Information relevant to Subsection 2.1
        ...
      ]
    },
    {
      "header": "Summary of Activity", // Subsection 2.2
      "contents": [ // Information relevant to Subsection 2.2
        ...
      ]
    },
    {
      "header": "Activity Details", // Subsection 2.3
      "contents": [ // Information relevant to Subsection 2.3
        ...
      ]
    }
  ]
], // End of Section 2
```

It is important to preserve the sectioning of information as it directly relates to one another, particularly where multiple actors or connections appear within the event. For example, if an event contained two connections - one with data transfer and one without - it is essential that the subsection concerning the data that was transferred stays with the information about the connection it was transferred over.

Response Schema - Single Event

Response Field	Type	Example Value	Description
`activityId`	string	`4c8c7d74`	An identifier for the specific activity detected by AI Analyst. If `groupByActivity=true` , this field should be used to group events together into an incident.
`summariser`	string	`SslC2Summary`	A system field.
`details`	array		An array of multiple sections (sub-arrays) of event information. Please see Understanding the `details` array" below. "

Response Field	Type	Example Value	Description
`details.header`	string	`Device Making Suspicious Connections`	A short title describing the section of information.
`details.contents`	array		An array of multiple objects describing relevant information for this subsection, such as involved devices, relevant external hosts, ports used and anomaly scorings.
`details.contents.key`	string	`Source device`	Assigns meaning to the values in the `values` field - a short description of the data.
`details.contents.type`	string	`device`	The type of information contained within the object. A full list of examples is available.
`details.contents.values`	array		One or more values that relate to the key. For example, a series of ports or hostnames. Full examples of all data types are available.
`details.contents.values.identifier`	string	`workstation-local-82`	An example value contained within the array. In this case, it relates to a source device. An identifier for the device used when constructing summaries or reports. May be the device label, hostname or IP, depending on availability.
`details.contents.values.ip`	string	`10.15.3.390`	An example value contained within the array. In this case, it relates to a source device. The IP associated with the device.
`details.contents.values.did`	numeric	`5649`	An example value contained within the array. In this case, it relates to a source device. The unique “device id” identifier for the device that triggered the breach. This field is used to group events into device-based incidents within the Threat Visualizer.
`details.contents.values.hostname`	string	`workstation-local-82`	An example value contained within the array. In this case, it relates to a source device. The hostname associated with the device, if available.
`details.contents.values.sid`	numeric	`111`	An example value contained within the array. In this case, it relates to a source device. The subnet id for the subnet the device is currently located in.
`details.contents.values.subnet`	string	`null`	An example value contained within the array. In this case, it relates to a source device. The subnet label for the corresponding subnet, if available.
`details.contents.values.mac`	string	`2g:d8:a2:a8:54:c6`	An example value contained within the array. In this case, it relates to a source device. The MAC address associated with the device.
`groupByActivity`	boolean	`FALSE`	Indicates whether the event should be aggregated by activity or by device to create an incident. When true, the event should be aggregated by activityID, and when false, aggregated by groupingID(s).

Response Field	Type	Example Value	Description
`groupingIds`	array	`bba29024`	Each entry in the `groupingIDs` array refers to a device that triggered the activity detection. In single events, should only contain one ID. If `groupByActivity=false` , this field should be used to group events together into an incident.
`attackPhases`	array	`2`	Of the six attack phases, which phases are applicable to the activity.
`periods`	array		An array of one or more periods of time where anomalous activity occurred that AI Analyst investigated.
`periods.start`	numeric	`1595380593276`	A timestamp for the start of the activity period in epoch time.
`periods.end`	numeric	`1596593374299`	A timestamp for the end of the activity period in epoch time.
`relatedBreaches`	array		An array of model breaches related to the activity investigated by AI analyst.
`relatedBreaches.timestamp`	numeric	`1595380593276`	The timestamp at which the model breach occurred in epoch time.
`relatedBreaches.modelName`	string	`Anomalous Connection / Repeated Rare External SSL Self-Signed`	The name of the model that breached.
`relatedBreaches.pbid`	numeric	`1468028`	The “policy breach ID” unique identifier of the model breach.
`relatedBreaches.threatScore`	numeric	`46`	The breach score of the associated model breach - out of 100.
`summary`	string	`The device workstation-local-82 was observed making multiple SSL connections to the rare external endpoint 172.217.169.36…`	A textual summary of the suspicious activity. This example is abbreviated.
`id`	string	`557eb412-4ccc-4b83-ad49-7ec5675062cc`	A system field.
`pinned`	boolean	`FALSE`	Whether the event, or an incident that the event is associated with, is pinned within the Threat Visualizer user interface. Pinned events will always return regardless of the timeframe specified.
`title`	string	`Possible SSL Command and Control`	A title describing the activity that occurred.
`acknowledged`	boolean	`FALSE`	Whether the event has been acknowledged.
`aiaScore`	numeric	`100`	The reportability of the event as classified by AI Analyst - out of 100.
`children`	array	`557eb412-4ccc-4b83-ad49-7ec5675062cc`	One or more unique identifiers that can be used to request this AI Analyst event via the UI or API. Where there is more than one uuid, requests can be made with comma-separated values.

Response Field	Type	Example Value	Description
`breachDevices`	array		An array of devices involved in the related model breach(es).
`breachDevices.hostname`	string	`workstation-local-82`	The hostname associated with the device, if available.
`breachDevices.identifier`	string	`workstation-local-82`	An identifier for the device used when constructing summaries or reports. May be the device label, hostname or IP, depending on availability.
`breachDevices.did`	numeric	`5649`	The unique “device id” identifier for the device that triggered the breach. This field is used to group events into device-based incidents within the Threat Visualizer.
`breachDevices.ip`	string	`10.15.3.390`	The IP associated with the device.
`breachDevices.mac`	string	`2g:d8:a2:a8:54:c6`	The MAC address associated with the device.
`breachDevices.subnet`	string	`null`	The subnet label for the corresponding subnet, if available.
`breachDevices.sid`	numeric	`111`	The subnet id for the subnet the device is currently located in.
`userTriggered`	boolean	`FALSE`	Whether the event was created as a result of a user-triggered AI Analyst investigation.
`externalTriggered`	boolean	`FALSE`	Whether the event was created as a result of an externally triggered AI Analyst investigation.

Example Response

```
[
  {
    "aiaScore": 100,
    "children": [
      "04a3f36e-4u8w-v9dh-x6lb-894778cf9633"
    ],
    "summary": "A chain of administrative connections were observed between multiple devices,
which occurred around the same time, and included workstation-local-82.",
    "id": "04a3f36e-4u8w-v9dh-x6lb-894778cf9633",
    "pinned": true,
    "acknowledged": false,
    "details": [
      [
        {
          "header": "First Hop",
          "contents": [
            {
              "type": "timestampRange",
              "key": "Time",
              "values": [
                {
                  "start": 1579710063121,
                  "end": 1579711920166
                }
              ]
            },
            {
              "type": "device",
              "key": "Source device",
              "values": [
                {
                  "sid": 12,
                  "mac": "56:2d:4b:9c:18:42",
                  "ip": "10.12.14.2",
                  "identifier": "Finance File Server",
                  "did": 532,
                  "hostname": null,
                  "subnet": null
                }
              ]
            },
            ...
          ]
        }
      ],
      [
        ...
          ]
        }
      ]
    ],
    "summariser": "LateralMovementCrawler",
    "relatedBreaches": [
      {
        "timestamp": 1579710173000,
        "threatScore": 19,
        "pbid": 252317,
        "modelName": "Anomalous Connection / Active SSH Tunnel"
      }
    ],
    "breachDevices": [
      {
      "sid": 10,
      "mac": "93:gb:28:g1:fc:g1",
      "ip": "10.0.18.224",
      "identifier": "workstation-local-82",
      "did": 230,
      "hostname": "workstation-local-82",
      "subnet": null
      }
    ],
    "periods": [
      {
        "start": 1579708374972,
        "end": 1579711920166
      }
    ],
    "attackPhases": [
      5
    ],
    "groupingIds": [
      "544a6ce7"
    ],
```

Response is abbreviated.

Response Schema - Cross-Network Event

Response Field	Type	Example Value	Description
`aiaScore`	numeric	`50`	The reportability of the event as classified by AI Analyst - out of 100.
`children`	array	`c0ec5c71-b4fb-429b-82a7-4d6a73cbcaed`	ve9cpd8n-j8mh-fyh3-leev-sz8s8xwfwrs5
`summary`	string	`Multiple actors were observed accessing documents that appear to contain sensitive information over a configured SaaS service.`	A textual summary of the suspicious activity.
`id`	string	`00b14e94-f744-5ecb-a35a-35a2dda23162`	A system field.
`pinned`	boolean	`TRUE`	Whether the event, or an incident that the event is associated with, is pinned within the Threat Visualizer user interface. Pinned events will always return regardless of the timeframe specified.
`acknowledged`	boolean	`FALSE`	Whether the event has been acknowledged.
`details`	array		An array of multiple sections (sub-arrays) of event information. Please see Understanding the `details` array" above. "
`details.header`	string	`SaaS User Details`	A short title describing the section of information.
`details.contents`	array		An array of multiple objects describing relevant information for this subsection, such as involved devices, relevant external hosts, ports used and anomaly scorings.
`details.contents.type`	string	`device`	The type of information contained within the object. A full list of examples is available.
`details.contents.key`	string	`SaaS account`	Assigns meaning to the values in the `values` field - a short description of the data.
`details.contents.values`	array		One or more values that relate to the key. For example, a series of ports or hostnames. Full examples of all data types are available.
`summariser`	string	`SaasPasswordSummary`	A system field.
`relatedBreaches`	array		An array of model breaches related to the activity investigated by AI analyst.
`relatedBreaches.timestamp`	numeric	`1592220000000`	The timestamp at which the model breach occurred in epoch time.
`relatedBreaches.threatScore`	numeric	`73`	The breach score of the associated model breach - out of 100.
`relatedBreaches.pbid`	numeric	`1430296`	The “policy breach ID” unique identifier of the model breach.

Response Field	Type	Example Value	Description
`relatedBreaches.modelName`	string	`SaaS / Possible Unencrypted SaaS Password Storage`	The name of the model that breached.
`breachDevices`	array		An array of devices involved in the related model breach(es).
`breachDevices.sid`	numeric	`-9`	The subnet id for the subnet the device is currently located in.
`breachDevices.mac`	string	`null`	The MAC address associated with the device.
`breachDevices.ip`	string	`null`	The IP associated with the device.
`breachDevices.identifier`	string	`SaaS::Office365: isabella.west@holdingsinc.com, An identifier for the device used when constructing summaries or reports. May be the device label, hostname or IP, depending on availability.`	
`breachDevices.did`	numeric	`11811`	The unique “device id” identifier for the device that triggered the breach. This field is used to group events into device-based incidents within the Threat Visualizer.
`breachDevices.hostname`	string	`SaaS::Office365: isabella.west@holdingsinc.com`	The hostname associated with the device, if available.
`breachDevices.subnet`	string	`null`	The subnet label for the corresponding subnet, if available.
`periods`	array		An array of one or more periods of time where anomalous activity occurred that AI Analyst investigated.
`periods.start`	numeric	`1591010000000`	A timestamp for the start of the activity period in epoch time.
`periods.end`	numeric	`1591010000000`	A timestamp for the end of the activity period in epoch time.
`attackPhases`	numeric		Of the six attack phases, which phases are applicable to the activity.
`groupingIds`	array	`544a6ce7`	Each entry in the `groupingIDs` array refers to a device that triggered the activity detection. For cross-network events, will contain multiple IDs due to multiple devices. When the parameter mergeEvents=false is used, only one groupingID should be present in the array but cross-network events will not be produced.
`activityId`	string	`ae463dc8`	An identifier for the specific activity detected by AI Analyst. If `groupByActivity=true` , this field should be used to group events together into an incident.

Response Field	Type	Example Value	Description
`groupByActivity`	boolean	`true`	Indicates whether the event should be aggregated by activity or by device to create an incident. When true, the event should be aggregated by activityID, and when false, aggregated by groupingID(s).
`title`	string	`Access of Probable Unencrypted Password Files by Multiple SaaS Actors`	A title describing the activity that occurred.
`userTriggered`	boolean	`FALSE`	Whether the event was created as a result of a user-triggered AI Analyst investigation.
`externalTriggered`	boolean	`FALSE`	Whether the event was created as a result of an externally triggered AI Analyst investigation.

Example Response

```
[
  {
    "aiaScore": 50,
    "children": [
      "c0ec5c71-b4fb-429b-82a7-4d6a73cbcaed",
      "ve9cpd8n-j8mh-fyh3-leev-sz8s8xwfwrs5",
      "c5r8131w-yev6-if7b-7alc-b6jp1v8ewon2"
    ],
    "summary": "Multiple actors were observed accessing documents that appear to contain sensitive
information over a configured SaaS service.",
    "id": "00b14e94-f744-5ecb-a35a-35a2dda23162",
    "pinned": true,
    "acknowledged": false,
    "details": [
      [
        {
          "contents": [
            {
              "key": "SaaS account",
              "values": [
                {
                  "hostname": "SaaS::Office365: isabella.west@holdingsinc.com",
                  "mac": null,
                  "sid": -9,
                  "identifier": "SaaS::Office365: isabella.west@holdingsinc.com",
                  "ip": null,
                  "subnet": null,
                  "did": 11811
                }
              ],
              "type": "device"
            },
            {
              "key": "Actor",
              "values": [
                "isabella.west@holdingsinc.com"
              ],
              "type": "string"
            },
            {
              "key": "Service product",
              "values": [
                "SharePoint"
              ],
              "type": "string"
            },
          ...
      ]
    ],
    "summariser": "SaasPasswordSummary",
    "relatedBreaches": [
      {
        "threatScore": 73,
        "timestamp": 1592224114000,
        "pbid": 1430296,
        "modelName": "SaaS / Possible Unencrypted SaaS Password Storage"
      },
      {
        "threatScore": 65,
        "timestamp": 1591007992000,
        "pbid": 1423708,
        "modelName": "SaaS / Possible Unencrypted SaaS Password Storage"
      },
      ...
    ],
    "breachDevices": [
      {
        "hostname": "SaaS::Office365: isabella.west@holdingsinc.com",
        "mac": null,
        "sid": -9,
        "identifier": "SaaS::Office365: isabella.west@holdingsinc.com",
        "ip": null,
        "subnet": null,
        "did": 11811
      },
      {
        "hostname": "SaaS::Office365: sofia.martinez@holdingsinc.com",
        "mac": null,
        "sid": -9,
        "identifier": "SaaS::Office365: sofia.martinez@holdingsinc.com",
        "ip": null,
        "subnet": null,
        "did": 11873
```

Response is abbreviated.

Example `details` entries

`"type": "string"`

```
{
  "type": "string",
  "key": "Application protocol",
  "values": [
    "SSH"
  ]
}
```

`"type": "device"`

```
{
  "type": "device",
  "key": "Source device",
  "values": [
    {
      "sid": 12,
      "mac": "93:gb:28:g1:fc:g1",
      "ip": "10.140.15.33",
      "identifier": "Workstation 12",
      "did": 57,
      "hostname": null,
      "subnet": null
    }
  ]
}
```

`"type": "externalHost"`

```
{
  "type": "externalHost",
  "key": "Endpoint",
  "values": [
    {
      "ip": null,
      "hostname": "stackoverflow.com"
    }
  ]
}
```

`"type": "timestamp"`

```
{
  "type": "timestamp",
  "key": "Hostname first observed",
  "values": [
    1593646723036
  ],
},
```

"type": "duration"

```
{
  "type": "duration",
  "key": "Median beacon period",
  "values": [
    30
  ]
}
```

"type": "integer"

```
{
  "type": "integer",
  "key": "Destination port",
  "values": [
    22
  ]
}
```

"type": "float"

```
{
  "type": "float",
  "key": "Latitude",
  "values": [
    12.46
  ]
}
```

"type": "percentage"

```
{
  "type": "percentage",
  "key": "Hostname rarity",
  "values": [
    100
  ]
}
```

"type": "dataVolume"

```
{
  "type": "dataVolume",
  "key": "Total data in",
  "values": [
    142271
  ]
}
```

"type": "ratio"

```
{
  "type": "ratio",
  "key": "Validation Statuses",
  "values": [
    {
      "percentage": 50
      "value": "ok",
    },
    {
      "percentage": 50
      "value": "Unknown",
    }
  ]
}
```

"type": "timestampRange"

```
{
  "type": "timestampRange",
  "key": "Time",
  "values": [
    {
      "start": 1579710063121,
      "end": 1579711920166
    }
  ]
}
```

"type": "integerRange"

```
{
  "type": "integerRange",
  "key": "Range of connections per hour",
  "values": [
    {
      "start": 1
      "end": 6,
    }
  ]
}
```

"type": "durationRange"

```
{
  "type": "durationRange",
  "key": "Range of periods",
  "values": [
    {
      "start": 30
      "end": 79,
    }
  ]
}
```

"type": "dataVolumeRange"

```
{
  "type": "dataVolumeRange",
  "key": "Range of data volumes sent per external connection",
  "values": [
    {
      "start": 717
      "end": 944,
    }
  ]
}
```

"type": "percentageRange"

```
{
  "type": "percentageRange",
  "key": "Rarity of all endpoints",
  "values": [
    {
      "start": 100
      "end": 100,
    }
  ]
}
```

"type": "stringRange"

```
{
  "type": "stringRange",
  "key": "Days of activity",
  "values": [
    {
      "start": "Wednesday"
      "end": "Sunday",
    }
  ]
}
```

/aianalyst/incident/comments

The `/aianalyst/incident/comments` endpoint returns current comments on an AI Analyst event. It requires the `uuid` of an event to be provided.

Request Type(s)

```
[GET]
```

Parameters

Parameter	Type	Description
`incident_id`	string	A unique identifier for the AI Analyst event to return comments for. Only one value is supported at a time.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- The `uuid` of an event can always be found in the `children` field of the JSON response from the `/aianalyst/incidents` endpoint. Where an event is comprised of multiple combined events, (multiple uuids in the `children` array), `mergeEvents=true` can be used when querying the `/aianalyst/incidents` endpoint to separate events into single uuids to be used against the `/aianalyst/incident/comments` endpoint.

Example Request

1. `GET` comments for an AI Analyst event with `incident_id=04a3f36e-4u8w-v9dh-x6lb-894778cf9633` :

```
https://<applianceIP>/aianalyst/incident/comments?incident_id=04a3f36e-4u8w-v9dh-
x6lb-894778cf9633
```

Example Response

Request: /aianalyst/incident/comments?incident_id=04a3f36e-4u8w-v9dh-x6lb-894778cf9633

```
{
  "comments": [
    {
      "username": "smartinez_admin",
      "time": 1595501000000,
      "incident_id": "04a3f36e-4u8w-v9dh-x6lb-894778cf9633",
      "message": "Assigned to Aidan Johnston for investigation."
    }
  ]
}
```

/aianalyst/incident/comments Response Schema

Response Schema

Response Field	Type	Example Value	Description
`comments`	array		An array of comments made against the incident events.
`comments.username`	string	`ecarr`	The user who made the comment.
`comments.time`	numeric	`1595501000000`	The time the comment was posted in epoch time.
`comments.incident_id`	string	`7d0c1dec-593e-4559-8a71-49847c3e53f5`	The unique identifier of the event against which the comment was posted.
`comments.message`	string	`Concerning behavior. Investigating possible compromise.`	The comment text.

Example Response

```
{
  "comments": [
    {
      "username": "ecarr",
      "time": 1595501000000,
      "incident_id": "04a3f36e-4u8w-v9dh-x6lb-894778cf9633",
      "message": "Concerning behavior. Investigating possible compromise."
    }
  ]
}
```

/antigena

The `/antigena` endpoint returns information about current and past Antigena Network actions. It can be used to retrieve a list of currently quarantined devices or Antigena Actions requiring approval.

If a time window is not specified, the request will return all current actions with a future expiry date and all historic actions with an expiry date in the last 14 days. Actions which were not activated will still be returned.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`includecleared`	boolean	Returns all Antigena actions including those already cleared. Defaults to false.
`needconfirming`	boolean	Filters returned Antigena actions by those that need human confirmation or do not need human confirmation.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`includeconnections`	boolean	Adds a connections object which returns connections blocked by an Antigena action.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- Time parameters must always be specified in pairs.
- When `fulldevicedetails=true` , actions will be contained in an `actions:` object and devices in a `devices:` object
- `active=true` means the action has been activated, either by human confirmation or automatically in active mode. If an Antigena Action is cleared manually, `active` will show `false` . If an Antigena action expires, it will continue to show `active=true` .
- Actions manually cleared by a user will have the value `cleared=true` , expired actions will have `cleared=false` . When an action is cleared manually, it will also set the `active` value to `false` .
- If `includeconnections=true` , a connections object will be added with details of all connections that were blocked by active Antigena actions.

Example Request

1. `GET` all Antigena Actions that require approval and retrieve full details for associated devices:

```
https://<applianceIP>/antigena?fulldevicedetails=true&needconfirming=true
```

2. `GET` all actions on January 10th 2020 (including cleared actions) and any blocked connections:

```
https://<applianceIP>/antigena?
from=2020-01-10T12:00:00&to=2020-01-10&includecleared=true&includeconnections=true
```

Example Response

Request: /antigena?includeconnections=true&fulldevicedetails=true

```
{
  "actions": [
      {
        "codeid": 4764,
        "did": 316,
        "ip": "10.0.18.224",
        "action": "quarantine",
        "label": "Quarantine device",
        "detail": "",
        "score": 0.3,
        "pbid": 442301,
        "model": "Antigena / Network / External Threat / Antigena Quarantine Example",
        "modeluuid": "d92d6f73-gc1b-cg96-d4g8-df8a79f2a3cd",
        "start": 1582038124000,
        "expires": 1582041724000,
        "blocked": true,
        "agemail": false,
        "active": true,
        "cleared": false
      },
      ...
    }
  ],
  "connections": [
    {
      "action": "quarantine",
      "label": "Quarantine device",
      "did": 316,
      "direction": "outgoing",
      "ip": "10.0.18.224",
      "port": 443,
      "timems": 1582033860000,
      "time": "2020-02-18 13:51:00"
    },
    ...
  ],
  "devices": [
    {
      "did": 316,
      "ip": "10.0.18.224",
       "ips": [
          {
            "ip": "10.0.18.224",
            "timems": 1581508800000,
            "time": "2020-02-12 12:00:00",
            "sid": 23
          }
        ],
       "did": 316,
       "sid": 23,
       "hostname": "Sarah Development",
       "firstseen": 1528807092000,
       "lastseen": 1581510431000,
       "os": "Linux 3.11 and newer",
       "typename": "desktop",
       "typelabel": "Desktop"
       "tags": [
          {
              "tid": 9,
              "expiry": 0,
              "thid": 9,
              "name": "Antigena All",
              "restricted": false,
              "data": {
                "auto": false,
                "color": 200,
                "description": ""
              },
              "isReferenced": true
            },
        ...
      ]
    },
    ...
  ]
}
```

Response is abbreviated.

/antigena Response Schema

Response Schema

`fulldevicedetails=false`

Response Field	Type	Example Value	Description
`codeid`	numeric	`4894`	A unique id for the Antigena action.
`did`	numeric	`532`	The “device id” of the device the action is applied against.
`ip`	string	`10.0.18.224`	The IP that the action is applied against.
`action`	string	`quarantine`	The type of action being performed.
`label`	string	`Quarantine device`	The readable label for the action being performed.
`detail`	string		Any additional detail about the action being performed.
`score`	numeric	`0.3`	The model breach score of the model breach that triggered the Antigena action.
`pbid`	numeric	`449854`	The model breach ‘policy breach id’ of the model breach that triggered the action.
`model`	string	`Anomalous File::Masqueraded File Transfer`	The name of the model that triggered the Antigena action.
`modeluuid`	string	`ee88d329-6cdd-8dd3-5baa-2e323g3fa833`	The unique identifier for the model that triggered the Antigena action.
`start`	numeric	`1586190000000`	The start time of the action in epoch time.
`expires`	numeric	`1586190000000`	The expiry time of the action in epoch time.
`blocked`	boolean	`FALSE`	Whether the action blocked any matching connections.
`updated`	string	`1585910000000`	When the action was last updated. For example, a user extending an action.
`agemail`	boolean	`FALSE`	Whether the action was triggered by Antigena Email.
`active`	boolean	`FALSE`	Whether the action has been activated at some point.
`cleared`	boolean	`FALSE`	Whether the action has been manually cleared by an operator.

Example Response

```
[
  {
    "codeid": 4764,
    "did": 316,
    "ip": "10.0.18.224",
    "action": "quarantine",
    "label": "Quarantine device",
    "detail": "",
    "score": 0.3,
    "pbid": 442301,
    "model": "Antigena / Network / External Threat / Antigena Quarantine Example",
    "modeluuid": "d92d6f73-gc1b-cg96-d4g8-df8a79f2a3cd",
    "start": 1582038124000,
    "expires": 1582041724000,
    "blocked": true,
    "agemail": false,
    "active": true,
    "cleared": false
  },
...
]
```

Response is abbreviated.

`fulldevicedetails=true`

Response Field	Type	Example Value	Description
`actions`	array		An array of Antigena actions.
`actions.codeid`	numeric	`4895`	A unique id for the Antigena action.
`actions.did`	numeric	`101`	The “device id” of the device the action is applied against.
`actions.ip`	string	`192.168.72.4`	The IP that the action is applied against.
`actions.action`	string	`quarantine`	The type of action being performed.
`actions.label`	string	`Quarantine device`	The readable label for the action being performed.
`actions.detail`	string		Any additional detail about the action being performed.
`actions.score`	numeric	`0.3`	The model breach score of the model breach that triggered the Antigena action.
`actions.pbid`	numeric	`449859`	The model breach ‘policy breach id’ of the model breach that triggered the action.
`actions.model`	string	`Anomalous File::Masqueraded File Transfer`	The name of the model that triggered the Antigena action.
`actions.modeluuid`	string	`ee88d329-6cdd-8dd3-5baa-2e323g3fa833`	The unique identifier for the model that triggered the Antigena action.
`actions.start`	numeric	`1586937600000`	The start time of the action in epoch time.
`actions.expires`	numeric	`1584265931000`	The expiry time of the action in epoch time.
`actions.blocked`	boolean	`FALSE`	Whether the action blocked any matching connections.

Response Field	Type	Example Value	Description
actions.updated	string	1584265931000	When the action was last updated. For example, a user extending an action.
actions.agemail	boolean	FALSE	Whether the action was triggered by Antigena Email.
actions.cleared	boolean	FALSE	Whether the action has been manually cleared by an operator.
devices	array		An array of devices that correspond to the “did” values in the actions array.
devices.did	numeric	101	The “device id”, a unique identifier.
devices.quarantine	numeric	1586937600000	The time that quarantine began upon the device in epoch time.
devices.ip	string	192.168.72.4	The current IP associated with the device.
devices.ips	array		IPs associated with the device historically.
devices.ips.ip	string	192.168.72.4	A historic IP associated with the device.
devices.ips.timems	numeric	1584265931000	The time the IP was last seen associated with that device in epoch time.
devices.ips.time	string	2020-03-15 09:52:11	The time the IP was last seen associated with that device in readable format.
devices.ips.sid	numeric	12	The subnet id for the subnet the IP belongs to.
devices.sid	numeric	12	The subnet id for the subnet the device is currently located in.
devices.firstSeen	numeric	1528812000000	The first time the device was seen on the network.
devices.lastSeen	numeric	1584265931000	The last time the device was seen on the network.
devices.os	string	Linux 3.11 and newer	The device operating system if Darktrace is able to derive it.
devices.typename	string	desktop	The device type in system format.
devices.typelabel	string	Desktop	The device type in readable format.
devices.tags	array		An object describing tags applied to the device.
devices.tags.tid	numeric	50	The “tag id”. A unique value.
devices.tags.expiry	numeric	0	The expiry time for the tag when applied to a device.
devices.tags.thid	numeric	50	The “tag history” id. Increments if the tag is edited.
devices.tags.name	string	Multi-use	The tag label displayed in the user interface or in objects that reference the tag.
devices.tags.restricted	boolean	FALSE	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
devices.tags.data	object		An object containing information about the tag.
devices.tags.data.auto	boolean	FALSE	Whether the tag was auto-generated.
devices.tags.data.color	numeric	200	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.

Response Field	Type	Example Value	Description
`devices.tags.data.description`	string	`Device is a pool device.`	An optional description summarizing the purpose of the tag.
`devices.tags.isReferenced`	boolean	`TRUE`	A system field.
`devices.tags.data.visibility`	string	`Public`	Whether the tag is used by one or more model components.
`devices.macaddress`	string	`56:2d:4b:9c:18:42`	The current MAC address associated with the device.
`devices.vendor`	string		The vendor of the device network card as derived by Darktrace from the MAC address.
`devices.hostname`	string	`ws173`	The current device hostname.

Example Response

```
{
  "actions": [
    {
      "codeid": 4764,
      "did": 316,
      "ip": "10.0.18.224",
      "action": "quarantine",
      "label": "Quarantine device",
      "detail": "",
      "score": 0.3,
      "pbid": 442301,
      "model": "Antigena / Network / External Threat / Antigena Quarantine Example",
      "modeluuid": "d92d6f73-gc1b-cg96-d4g8-df8a79f2a3cd",
      "start": 1582038124000,
      "expires": 1582041724000,
      "blocked": true,
      "agemail": false,
      "active": true,
      "cleared": false
    },
    ...
  ],
  "devices": [
    {
      "did": 316,
      "ip": "10.0.18.224",
       "ips": [
          {
            "ip": "10.0.18.224",
            "timems": 1581508800000,
            "time": "2020-02-12 12:00:00",
            "sid": 23
          }
        ],
       "did": 316,
       "sid": 23,
       "hostname": "Sarah Development",
       "firstseen": 1528807092000,
       "lastseen": 1581510431000,
       "os": "Linux 3.11 and newer",
       "typename": "desktop",
       "typelabel": "Desktop"
       "tags": [
          {
              "tid": 9,
              "expiry": 0,
              "thid": 9,
              "name": "Antigena All",
              "restricted": false,
              "data": {
                "auto": false,
                "color": 200,
                "description": ""
              },
              "isReferenced": true
            },
        ...
      ]
```

Response is abbreviated.

Response Schema - `includeconnections=true`

Response Field	Type	Example Value	Description
`actions`	array		An array of Antigena actions.
`actions.codeid`	numeric	`4895`	A unique id for the Antigena action.

Response Field	Type	Example Value	Description
`actions.did`	numeric	239	The "device id" of the device the action is applied against.
`actions.ip`	string	10.12.14.2	The IP that the action is applied against.
`actions.action`	string	quarantine	The type of action being performed.
`actions.label`	string	Quarantine device	The readable label for the action being performed.
`actions.detail`	string		Any additional detail about the action being performed.
`actions.score`	numeric	0.3	The model breach score of the model breach that triggered the Antigena action.
`actions.pbid`	numeric	449859	The model breach 'policy breach id' of the model breach that triggered the action.
`actions.model`	string	Anomalous File::Masqueraded File Transfer	The name of the model that triggered the Antigena action.
`actions.modeluuid`	string	ee88d329-6cdd-8dd3-5baa-2e323g3fa833	The unique identifier for the model that triggered the Antigena action.
`actions.start`	numeric	1586190000000	The start time of the action in epoch time.
`actions.expires`	numeric	1586190000000	The expiry time of the action in epoch time.
`actions.blocked`	boolean	FALSE	Whether the action blocked any matching connections.
`actions.updated`	string	1586190000000	When the action was last updated. For example, a user extending an action.
`actions.agemail`	boolean	FALSE	Whether the action was triggered by Antigena Email.
`actions.active`	boolean	TRUE	Whether the action has been activated at some point.
`actions.cleared`	boolean	FALSE	Whether the action has been manually cleared by an operator.
`connections`	array		An array of connections blocked by one or more Antigena actions.
`connections.action`	string	quarantine	The type of action being performed that blocked the connection.
`connections.label`	string	Quarantine device	The readable label for the action being performed.
`connections.did`	numeric	239	The "device id" of the device the action is applied against.
`connections.direction`	string	outgoing	The direction of the blocked connection in relation to the actioned device.
`connections.ip`	string	10.0.18.224	Depending on connection direction, the IP that the actioned device is connecting to or is being connected to by.
`connections.port`	numeric	3128	Depending on connection direction, the port that the actioned device is connecting to or is being connected to on.
`connections.timems`	numeric	1584265931000	The time that the blocked connection was attempted in epoch time.

Response Field	Type	Example Value	Description
`connections.time`	string	`2020-03-15 09:52:11`	The time that the blocked connection was attempted in readable format.

Example Response

```
{
  "actions": [
    {
      "codeid": 4764,
      "did": 316,
      "ip": "10.0.18.224",
      "action": "quarantine",
      "label": "Quarantine device",
      "detail": "",
      "score": 0.3,
      "pbid": 442301,
      "model": "Antigena / Network / External Threat / Antigena Quarantine Example",
      "modeluuid": "d92d6f73-gc1b-cg96-d4g8-df8a79f2a3cd",
      "start": 1582038124000,
      "expires": 1582041724000,
      "blocked": true,
      "agemail": false,
      "active": true,
      "cleared": false
    },
    ...
  ],
  "connections": [
    {
      "action": "quarantine",
      "label": "Quarantine device",
      "did": 316,
      "direction": "outgoing",
      "ip": "10.0.18.224",
      "port": 443,
      "timems": 1582033860000,
      "time": "2020-02-18 13:51:00"
    },
    ...
  ]
}
```

Response is abbreviated.

/components

Components are segments of model logic that are evaluated; the `/components` endpoint returns a list of all component parts of defined models, identified by their `cid` . The `cid` is referenced in the data attribute for model breaches.

A component is a series of filters which an event or connection is assessed against as part of a larger model. The first part of the component describes the combinations of filters that must occur for the component to fire, where each filter is identified by a capital letter. The second part of the response describes the logic of each filter. Filters with an ID like “A” or “F” are referenced in the model logic, whereas filters with an ID like “d1” or “d4” are display filters - filters that are displayed in the UI when a breach occurs and have no impact on the component logic.

For certain `filtertypes` , the returned argument is a numeric value that corresponds to an enumerated type. See (/enums) for a full list.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` information about all model components:

```
https://<applianceIP>/components
```

2. `GET` the component with `cid: 8977` :

```
https://<applianceIP>/components/8977
```

Example Response

Request: /components/8977

```
{
  "cid": 8977,
  "chid": 15524,
  "mlid": 33,
  "threshold": 5242880,
  "interval": 3600,
  "logic": {
    "data": {
      "left": "A",
      "operator": "AND",
      "right": {
        "left": "B",
        "operator": "AND",
        "right": {
          "left": "C",
          "operator": "AND",
          "right": {
            "left": "D",
            "operator": "AND",
            "right": "E"
          }
        }
      }
    },
    "version": "v0.1"
  },
  "filters": [{
      "id": "A",
      "cfid": 59205,
      "cfhid": 99603,
      "filtertype": "Direction",
      "comparator": "is",
      "arguments": {
        "value": "out"
      }
    },
    {
      "id": "B",
      "cfid": 59206,
      "cfhid": 99604,
      "filtertype": "Tagged internal source",
      "comparator": "does not have tag",
      "arguments": {
        "value": 38
      }
    } {
      "id": "C",
      "cfid": 59207,
      "cfhid": 99605,
      "filtertype": "Internal source device type",
      "comparator": "is not",
      "arguments": {
        "value": "9"
      }
    },
    {
      "id": "D",
      "cfid": 59208,
      "cfhid": 99606,
      "filtertype": "Internal source device type",
      "comparator": "is not",
      "arguments": {
        "value": "13"
      }
    },
    {
      "id": "E",
      "cfid": 59209,
      "cfhid": 99607,
      "filtertype": "Connection hostname",
      "comparator": "matches regular expression",
      "arguments": {
        "value": "^(.+\\.)?dropbox.com$"
      }
    },
    {
      "id": "d1",
      "cfid": 59210,
      "cfhid": 99608,
      "filtertype": "Connection hostname",
      "comparator": "display",
      "arguments": {}
    }
```

/components Response Schema

Response Schema

Response Field	Type	Example Value	Description
`cid`	numeric	`4650`	The “component id”. A unique identifier.
`chid`	numeric	`6664`	The “component history id”. Increments when the component is edited.
`mlid`	numeric	`232`	The ‘metric logic id’ for the metric used in the component.
`threshold`	numeric	`1`	The number of times the component logic must be met within the interval timeframe.
`interval`	numeric	`7200`	The timeframe in seconds within which the threshold must be satisfied.
`logic`	object		An object describing the component logic.
`logic.data`	object		An object representing the logical relationship between component filters. Each filter is given an alphabetical reference and the contents of this object describe the relationship between those objects.
`logic.data.left`	object		Objects on the left will be compared with the object on the right using the specified operator.
`logic.data.operator`	string	`OR`	A logical operator to compare filters with.
`logic.data.right`	object		Objects on the left will be compared with the object on the right using the specified operator.
`logic.version`	string	`v0.1`	The version of the component logic.
`filters`	array		The filters that comprise the component.
`filters.id`	string	`A`	A filter that is used in the component logic. All filters are given alphabetical identifiers. Display filters - those that appear in the breach notification - can be identified by a lowercase ‘d’ and a numeral.
`filters.cfid`	numeric	`34019`	The ‘component filter id’. A unique identifier for the filter as part of a the component.
`filters.cfhid`	numeric	`46783`	The “component filter history id”. Increments when the filter is edited.
`filters.filtertype`	string	`Message`	The filtertype that is used in the filter. A full list of filtertypes can be found on the / filtertypes endpoint.
`filters.comparator`	string	`matches regular expression`	The comparator. A full list of comparators available for each filtertype can be found on the /filtertypes endpoint.
`filters.arguments`	object		An object containing the value to be compared. Display filters will have an empty object.
`filters.arguments.value`	string	`(Anomalous`	Compromise
`active`	boolean	`TRUE`	Whether the component is currently active as part of a model.

Example Response

Request: /components/8977

```
{
  "cid": 8977,
  "chid": 15524,
  "mlid": 33,
  "threshold": 5242880,
  "interval": 3600,
  "logic": {
    "data": {
      "left": "A",
      "operator": "AND",
      "right": {
        "left": "B",
        "operator": "AND",
        "right": {
          "left": "C",
          "operator": "AND",
          "right": {
            "left": "D",
            "operator": "AND",
            "right": "E"
          }
        }
      }
    },
    "version": "v0.1"
  },
  "filters": [
    {
      "id": "A",
      "cfid": 59205,
      "cfhid": 99603,
      "filtertype": "Direction",
      "comparator": "is",
      "arguments": {
        "value": "out"
      }
    },
    {
      "id": "B",
      "cfid": 59206,
      "cfhid": 99604,
      "filtertype": "Tagged internal source",
      "comparator": "does not have tag",
      "arguments": {
        "value": 38
      }
    } {
      "id": "C",
      "cfid": 59207,
      "cfhid": 99605,
      "filtertype": "Internal source device type",
      "comparator": "is not",
      "arguments": {
        "value": "9"
      }
    },
    {
      "id": "D",
      "cfid": 59208,
      "cfhid": 99606,
      "filtertype": "Internal source device type",
      "comparator": "is not",
      "arguments": {
        "value": "13"
      }
    },
    {
      "id": "E",
      "cfid": 59209,
      "cfhid": 99607,
      "filtertype": "Connection hostname",
      "comparator": "matches regular expression",
      "arguments": {
        "value": "^(.+\\.)?dropbox.com$"
      }
    },
    {
      "id": "d1",
      "cfid": 59210,
      "cfhid": 99608,
      "filtertype": "Connection hostname",
      "comparator": "display",
      "arguments": {}
```

/details

The `/details` endpoint returns a time-sorted list of connections and events for a device or entity (such as a SaaS credential). The request requires either a device (`did`), a model breach ID (`pbid`) or a message field value (`msg`). It is used to populate event log data for a device.

This endpoint can be used to gather detailed information about a specific device and its connections for investigation or monitoring purposes.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`applicationprotocol`	string	This filter can be used to filter the returned data by application protocol. See /enums for the list of application protocols.
`count`	numeric	Specifies the maximum number of items to return.
`ddid`	numeric	Identification number of a destination device modelled in the Darktrace system to restrict data to.
`deduplicate`	boolean	Display only one equivalent connection per hour.
`destinationport`	numeric	This filter can be used to filter the returned data by destination port.
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`eventtype`	string	Specifies an type of event to return details for. Possible values are connection, unusualconnection, newconnection, notice, devicehistory, modelbreach.
`externalhostname`	string	Specifies an external hostname to return details for.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`intext`	string	This filter can be used to filter the returned data to that which interacts with external sources and destinations, or is restricted to internal. Valid values or internal and external.
`msg`	string	Specifies the value of the message field in notice events to return details for. Typically used to specify user credential strings.
`odid`	numeric	Other Device ID - Identification number of a device modelled in the Darktrace system to restrict data to. Typically used with ddid and odid to specify device pairs regardless of source/ destination.
`pbid`	numeric	Only return the model breach with the specified ID.
`port`	numeric	This filter can be used to filter the returned data by source or destination port.
`protocol`	string	This filter can be used to filter the returned data by IP protocol. See /enums for the list of protocols.
`sourceport`	numeric	This filter can be used to filter the returned data by source port.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`uid`	string	Specifies a connection UID to return.

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- Time parameters must always be specified in pairs.
- If the `from` or `starttime` parameter is used in a request, the `count` parameter must not be used.
- The default `eventtype` is `connection` .
- SaaS devices do not return connection information.

Example Request

1. `GET` the first 100 unusual connections for device with `did=1` :

```
https://<applianceIP>/details?did=1&count=100&eventtype=unusualconnection
```

2. `GET` all connections from December 1st 2020 (12:00:00) to December 2nd 2020 (00:00:00) for device with `did=1` :

```
https://<applianceIP>/details?did=1&from=2020-12-01T12:00:00&to=2020-12-02
```

Example Response

Request: /details?did=1&count=100&eventtype=notice

```
{
    "time": "2020-04-06 16:50:50",
    "timems": 1586191850000,
    "action": "notice",
    "eventType": "notice",
    "nid": 8180165,
    "uid": "ZJW3xVFQtEykPRPy",
    "direction": "in",
    "mlid": 339,
    "type": "SSH::Heuristic_Login_Success",
    "msg": "10.12.14.2 logged in to 192.168.72.4 successfully via SSH.",
    "destinationPort": 22,
    "details": "",
    "sourceDevice": {
      "id": -6,
      "did": -6,
      "ip": "10.12.14.2",
      "sid": -6,
      "time": "1528807047000",
      "devicelabel": "Internal Traffic",
      "typename": "networkrange",
      "typelabel": "Network Range"
    },
    "destinationDevice": {
      "id": 532,
      "did": 532,
      "macaddress": "93:gb:28:g1:fc:g1",
      "ip": "192.168.72.4",
      "ips": [
        {
          "ip": "192.168.72.4",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 12
        }
      ],
      "sid": 12,
      "hostname": "workstation-local-82",
      "time": "1528807077000",
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    "source": "Internal Traffic",
    "destination": "workstation-local-82",
  }
  ...
```

Response is abbreviated.

/details Response Schema

Note: The /details endpoint response has a large number of variations. All major **eventtypes** are covered in this schema, but the response will differ by protocol, model or platform (e.g., SaaS or ICS notices). Whether a proxy has been detected will also affect all connection-type events.

Response Schema - `eventtype=connection`

Please note, the proxy fields included in this schema may appear in any connection-type event response.

Response Field	Type	Example Value	Description
`time`	string	`2020-04-15 08:00:00`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1586937600000`	The timestamp when the record was created in readable format.
`action`	string	`connection`	The action associated with the device that has generated this record.
`eventType`	string	`connection`	The event type.
`uid`	string	`VGBIDXXfTVFPww1d`	A unique identifier for the connection - can be entered into Advanced Search or the omnisearch bar to locate associated connections.
`status`	string	`ongoing`	Can contain “failed” for failed connections or “ongoing” for continued connections. Completed connections will not return this field.
`proxyPort`	numeric	`3128`	If a proxy was detected - the port used.
`sdid`	numeric	`29`	The device id of the source device. Will only appear if the source device has been observed by Darktrace.
`ddid`	numeric	`3765`	The device id of the destination device. Will only appear if the destination device has been observed by Darktrace.
`port`	numeric	`443`	In the majority of cases, the destination port connected to.
`sourcePort`	numeric	`22`	The port connected from on the source device.
`destinationPort`	numeric	`443`	The port connected to on the destination device.
`direction`	string	`out`	The direction of the connection.
`applicationprotocol`	string	`HTTPS`	The application protocol used in the connection as derived by Darktrace.
`protocol`	string	`TCP`	The network protocol used for the connection as derived by Darktrace.
`sourceDevice`	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
`destinationDevice`	object		An object describing the destination device. There are multiple formats this may take, please see the separate destinationDevice object schemas.

Response Field	Type	Example Value	Description
`proxyDevice`	object		If a proxy was detected - an object describing the proxy.
`proxyDevice.ip`	string	`10.0.18.224`	If a proxy was detected - the proxy IP.
`source`	string	`ws173`	The hostname or IP of the source device.
`destination`	string	`google.com`	The hostname or IP of the destination device.
`proxy`	string	`192.168.72.4`	If a proxy was detected - the proxy IP.

Example Response

```
{
  "time": "2020-04-20 09:44:35",
  "timems": 1587375875452,
  "action": "connection",
  "eventType": "connection",
  "uid": "VGBIDXXfTVFPww1d",
  "status": "failed",
  "sdid": 76,
  "ddid": 532,
  "port": 6514,
  "sourcePort": 55498,
  "destinationPort": 6514,
  "direction": "out",
  "applicationprotocol": "Unknown",
  "protocol": "TCP",
  "sourceDevice": {
    "id": 76,
    "did": 76,
    "macaddress": "2g:d8:a2:a8:54:c6",
    "ip": "10.12.14.2",
    "ips": [
      {
        "ip": "10.12.14.2",
        "timems": 1587135600000,
        "time": "2020-04-17 15:00:00",
        "sid": 15
      }
    ],
    "sid": 15,
    "time": "1528807103000",
    "os": "Linux 3.11 and newer",
    "devicelabel": "Pool Laptop 6",
    "typename": "desktop",
    "typelabel": "Desktop"
  },
  "destinationDevice": {
    "id": 532,
    "did": 532,
    "ip": "192.168.72.4",
    "sid": 12,
    "hostname": "workstation-local-82",
    "time": "1528807077000",
    "os": "Linux 3.11 and newer",
    "typename": "desktop",
    "typelabel": "Desktop"
  },
  "source": "10.12.14.2",
  "destination": "workstation-local-82",
}
```

Response Schema - `eventtype=newconnection`

Response Field	Type	Example Value	Description
`time`	string	`2020-03-15 09:52:11`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1584265931000`	The timestamp when the record was created in readable format.
`action`	string	`connection`	The action associated with the device that has generated this record.
`eventType`	string	`connection`	The event type.
`uid`	string	`ZJW3xVFQtEykPRPy`	A unique identifier for the connection - can be entered into Advanced Search or the omnisearch bar to locate associated connections.
`status`	string	`ongoing`	Can contain “failed” for failed connections or “ongoing” for continued connections. Completed connections will not return this field.
`sdid`	numeric	`446`	The device id of the source device. Will only appear if the source device has been observed by Darktrace.
`ddid`	numeric	`239`	The device id of the destination device. Will only appear if the destination device has been observed by Darktrace.
`port`	numeric	`80`	In the majority of cases, the destination port connected to.
`sourcePort`	numeric	`80`	The port connected from on the source device.
`destinationPort`	numeric	`80`	The port connected to on the destination device.
`info`	string	`A new connection internally on port 80`	A message describing the event.
`direction`	string	`out`	The direction of the connection.
`applicationprotocol`	string	`DHCP`	The application protocol used in the connection as derived by Darktrace.
`protocol`	string	`UDP`	The network protocol used for the connection as derived by Darktrace.
`sourceDevice`	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
`destinationDevice`	object		An object describing the destination device. There are multiple formats this may take, please see the separate destinationDevice object schemas.
`source`	string	`D7S45E001`	The hostname or IP of the source device.
`destination`	string	`sarah-desktop-12`	The hostname or IP of the destination device.

Example Response

```
[
  {
    "time": "2020-04-16 10:31:01",
    "timems": 1587033061581,
    "action": "connection",
    "eventType": "connection",
    "uid": "T6X3VCrEXAm4KJeZ",
    "sdid": 76,
    "ddid": 532,
    "port": 67,
    "sourcePort": 68,
    "destinationPort": 67,
    "info": "A new connection internally on port 67",
    "direction": "out",
    "applicationprotocol": "DHCP",
    "protocol": "UDP",
    "sourceDevice": {
      "id": 76,
      "did": 76,
      "macaddress": "2g:d8:a2:a8:54:c6",
      "ip": "10.12.14.2",
      "ips": [
        {
          "ip": "10.12.14.2",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 15
        }
      ],
      "sid": 15,
      "time": "1528807103000",
      "os": "Linux 3.11 and newer",
      "devicelabel": "Pool Laptop 6",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    "destinationDevice": {
      "id": 532,
      "did": 532,
      "ip": "192.168.72.4",
      "sid": 12,
      "hostname": "workstation-local-82",
      "time": "1528807077000",
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    "source": "10.12.14.2",
    "destination": "workstation-local-82",
  }
]
```

Response Schema - `eventtype=unusualconnection`

Response Field	Type	Example Value	Description
`time`	string	`2020-03-15 09:52:11`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1584265931000`	The timestamp when the record was created in readable format.
`action`	string	`connection`	The action associated with the device that has generated this record.
`eventType`	string	`connection`	The event type.

Response Field	Type	Example Value	Description
uid	string	VGBIDXXfTVFPww1d	A unique identifier for the connection - can be entered into Advanced Search or the omnisearch bar to locate associated connections.
status	string	ongoing	Can contain “failed” for failed connections or “ongoing” for continued connections. Completed connections will not return this field.
sdid	numeric	239	The device id of the source device. Will only appear if the source device has been observed by Darktrace.
ddid	numeric	772	The device id of the destination device. Will only appear if the destination device has been observed by Darktrace.
port	numeric	443	In the majority of cases, the destination port connected to.
sourcePort	numeric	444	The port connected from on the source device.
destinationPort	numeric	443	The port connected to on the destination device.
info	string	An unusual connection compared with similar devices internally on port 443	A message describing the event.
direction	string	out	The direction of the connection.
applicationprotocol	string	HTTPS	The application protocol used in the connection as derived by Darktrace.
protocol	string	TCP	The network protocol used for the connection as derived by Darktrace.
sourceDevice	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
destinationDevice	object		An object describing the destination device. There are multiple formats this may take, please see the separate destinationDevice object schemas.
source	string	workstation-local-82	The hostname or IP of the source device.
destination	string	ws83	The hostname or IP of the destination device.

Example Response

```
{
   "time": "2020-04-15 07:38:05",
   "timems": 1586936285538,
   "action": "connection",
   "eventType": "connection",
   "uid": "K18S2Iqiu7Wz1jaN",
   "sdid": 76,
   "ddid": 5487,
   "port": 22,
   "sourcePort": 49568,
   "destinationPort": 22,
   "info": "A recent increase in incoming data volume from 10.12.14.2 port 22",
   "direction": "out",
   "applicationprotocol": "SSH",
   "protocol": "TCP",
   "sourceDevice": {
     "id": 76,
     "did": 76,
     "macaddress": "2g:d8:a2:a8:54:c6",
     "ip": "10.12.14.2",
     "ips": [
       {
         "ip": "10.12.14.2",
         "timems": 1587135600000,
         "time": "2020-04-17 15:00:00",
         "sid": 15
       }
     ],
     "sid": 15,
     "time": "1528807103000",
     "os": "Linux 3.11 and newer",
     "devicelabel": "Pool Laptop 6",
     "typename": "desktop",
     "typelabel": "Desktop"
   }
```

Response Schema - `eventtype=notice`

Generic Notice

Response Field	Type	Example Value	Description
`time`	string	`2019-06-12 14:00:00`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1528812000000`	The timestamp when the record was created in readable format.
`action`	string	`notice`	The action associated with the device that has generated this record.
`eventType`	string	`notice`	The event type.
`nid`	numeric	`8180398`	A unique identifier for the notice.
`uid`	string	`VGBIDXXfTVFPww1d`	A unique identifier of the notice which can be used to locate the notice and related connections in Advanced Search.
`direction`	string	`out`	The direction of the connection that triggered the notice.
`mlid`	numeric	`339`	The metric id of the corresponding system metric (where applicable) for this notice.

Response Field	Type	Example Value	Description
type	string	SSH::Heuristic_Login_Success	The notice type. A list of notices derived during processing (without the “DT” prefix) can be found in the Advanced Search documentation.
msg	string	10.12.14.2 logged in to 10.0.18.224 successfully via SSH.	A human readable description of the notice.
destinationPort	numeric	22	The destination port used by the device.
details	string		Details may be an object or a string describing further information about the event.
sourceDevice	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
destinationDevice	object		An object describing the destination device. There are multiple formats this may take, please see the separate destinationDevice object schemas.
source	string	sarah-desktop-12	The hostname or IP of the source device.
destination	string	10.0.18.224	The hostname or IP of the destination device.

Example Response

```
{
    "time": "2020-04-06 16:50:50",
    "timems": 1586191850000,
    "action": "notice",
    "eventType": "notice",
    "nid": 8180165,
    "uid": "ZJW3xVFQtEykPRPy",
    "direction": "in",
    "mlid": 339,
    "type": "SSH::Heuristic_Login_Success",
    "msg": "10.12.14.2 logged in to 192.168.72.4 successfully via SSH.",
    "destinationPort": 22,
    "details": "",
    "sourceDevice": {
      "id": -6,
      "did": -6,
      "ip": "10.12.14.2",
      "sid": -6,
      "time": "1528807047000",
      "devicelabel": "Internal Traffic",
      "typename": "networkrange",
      "typelabel": "Network Range"
    },
    "destinationDevice": {
      "id": 532,
      "did": 532,
      "macaddress": "93:gb:28:g1:fc:g1",
      "ip": "192.168.72.4",
      "ips": [
        {
          "ip": "192.168.72.4",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 12
        }
      ],
      "sid": 12,
      "hostname": "workstation-local-82",
      "time": "1528807077000",
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    "source": "Internal Traffic",
    "destination": "workstation-local-82",
  }
```

Model Breach Notice

Response Field	Type	Example Value	Description
time	string	2020-03-15 09:52:11	The timestamp when the record was created in epoch time.
timems	numeric	1584265931000	The timestamp when the record was created in readable format.
action	string	notice	The action associated with the device that has generated this record.
nuid	string	MMOiOUDO0EwgWYBW	Notices generated outside of DPI - those with the “DT” prefix - will have a “notice unique identifier” instead of a “uid”. This can be entered into the omnisearch bar to locate the event.
eventType	string	notice	The event type.
nid	numeric	8125619	A unique identifier for the notice.

Response Field	Type	Example Value	Description
uid	string		Notices generated outside of DPI - those with the “DT” prefix - do not have a uid value.
direction	string	out	The direction of the connection that triggered the notice.
mlid	numeric	232	The metric id of the corresponding system metric (where applicable) for this notice.
type	string	DT::ModelBreach	The notice type. A list of notices derived during processing (without the “DT” prefix) can be found in the Advanced Search documentation.
msg	string	Anomalous File / Masqueraded File Transfer	A human readable description of the notice.
destinationPort	numeric	80	The destination port used by the device.
size	numeric	38	The model breach score (out of 100).
detail	object		Details may be an object or a string describing further information about the event. For model breaches, it will contain information about the model.
detail.pid	numeric	486	The “policy id” of the breached model.
detail.pbid	numeric	315602	The “policy breach id” of the breached model.
detail.tags	array	Test	An array describing tags applied to the model.
sourceDevice	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
destinationDevice	object		An object describing the destination device. There are multiple formats this may take, please see the separate destinationDevice object schemas.
source	string	ws83	The hostname or IP of the source device.
destination	string	workstation-local-82	The hostname or IP of the destination device.
antigena-email	boolean	FALSE	Whether the notice originated from Antigena Email.

Example Response

```
{
  "time": "2020-04-07 02:55:59",
  "timems": 1586228159000,
  "action": "notice",
  "nuid": "RLW8FVxUNkkA5Kfa",
  "eventType": "notice",
  "nid": 8186895,
  "uid": "",
  "direction": "out",
  "mlid": 232,
  "type": "DT::ModelBreach",
  "msg": "Anomalous Connection / Multiple Failed Connections to Rare Endpoint",
  "destinationPort": 80,
  "size": 41,
  "detail": {
    "pid": 486,
    "pbid": 315955,
    "tags": [
      "Admin",
      "Test"
    ]
  },
  "sourceDevice": {
    "id": 532,
    "did": 532,
    "macaddress": "93:gb:28:g1:fc:g1",
    "ip": "192.168.72.4",
    "ips": [
      {
        "ip": "192.168.72.4",
        "timems": 1587135600000,
        "time": "2020-04-17 15:00:00",
        "sid": 12
      }
    ],
    "sid": 12,
    "hostname": "workstation-local-82",
    "time": "1528807077000",
    "os": "Linux 3.11 and newer",
    "typename": "desktop",
    "typelabel": "Desktop"
  },
  "destinationDevice": {
    "longitude": -122.075,
    "latitude": 37.404,
    "city": "Mountain View",
    "country": "United States",
    "countrycode": "US",
    "asn": "AS15169 Google LLC",
    "region": "North America",
    "ip": "216.58.204.46",
    "hostname": "google.com",
    "hostnamepopularity": "100",
    "domain": "google.com",
    "domainpopularity": "100",
    "ippopularity": "10"
  },
  "source": "workstation-local-82",
  "destination": "google.com",
}
```

Similar Devices Notice

Response Field	Type	Example Value	Description
`time`	string	`2020-04-15 08:04:41`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1586937881000`	The timestamp when the record was created in readable format.

Response Field	Type	Example Value	Description
`action`	string	`notice`	The action associated with the device that has generated this record.
`nuid`	string	`IYA9RXjOCAGwwLYA`	Notices generated outside of DPI - those with the “DT” prefix - will have a “notice unique identifier” instead of a “uid”. This can be entered into the omnisearch bar to locate the event.
`eventType`	string	`notice`	The event type.
`nid`	numeric	`8105707`	A unique identifier for the notice.
`uid`	string		Notices generated outside of DPI - those with the “DT” prefix - do not have a uid value.
`mlid`	numeric	`212`	The metric id of the corresponding system metric (where applicable) for this notice.
`type`	string	`DT::DeviceClusterChange`	The notice type. A list of notices derived during processing (without the “DT” prefix) can be found in the Advanced Search documentation.
`similardevices`	string	`BGF5ACF39CCB47FFF244A96293E2AC7FBBFB61165AEF9F4911397CG894AA2F1381E3924367EFG2A6F8G527F3B57194E7`	A token which can be provided to the /similardevices endpoint to see the old and new list of devices.
`msg`	string	`4 different similar devices from a list of 30`	A human readable description of the notice.
`size`	numeric	`12`	A system field.
`details`	string		Details may be an object or a string describing further information about the event. For model breaches, it will contain information about the model.
`sourceDevice`	object		An object describing the source device. There are multiple formats this may take, please see the separate sourceDevice object schemas.
`source`	string	`sarah-desktop-12`	The hostname or IP of the source device.

Example Response

```
    {
      "time": "2020-04-06 13:39:10",
      "timems": 1586180350000,
      "action": "notice",
      "nuid": "IYA9RXjOCAGwwLYA",
      "eventType": "notice",
      "nid": 8177463,
      "uid": "",
      "mlid": 212,
      "type": "DT::DeviceClusterChange",
      "similardevices":
  "BGF5ACF39CCB47FFF244A96293E2AC7FBBFB61165AEF9F4911397CG894AA2F1381E3924367EFG2A6F8G527F3B57194E7",
      "msg": "6 different similar devices from a list of 30",
      "size": 17,
      "details": "",
      "sourceDevice": {
        "id": 532,
        "did": 532,
        "macaddress": "93:gb:28:g1:fc:g1",
        "ip": "192.168.72.4",
        "ips": [
          {
            "ip": "192.168.72.4",
            "timems": 1587135600000,
            "time": "2020-04-17 15:00:00",
            "sid": 12
          }
        ],
        "sid": 12,
        "hostname": "workstation-local-82",
        "time": "1528807077000",
        "os": "Linux 3.11 and newer",
        "typename": "desktop",
        "typelabel": "Desktop"
      },
      "source": "workstation-local-82"
    }
```

Response Schema - `sourceDevice` and `destinationDevice` objects

Internal `sourceDevice` and `destinationDevice` objects

Response Field	Type	Example Value	Description
`sourceDevice`	object		An object describing an internal source device for the connection.
`sourceDevice.id`	numeric	`76`	The “device id”, a unique identifier.
`sourceDevice.did`	numeric	`76`	The “device id”, a unique identifier.
`sourceDevice.macaddress`	string	`bc:ee:7b:9c:9f:1e`	The current MAC address associated with the device.
`sourceDevice.ip`	string	`10.12.14.2`	The current IP associated with the device.
`sourceDevice.ips`	array		IPs associated with the device historically.
`sourceDevice.ips.ip`	string	`10.12.14.2`	A historic IP associated with the device.
`sourceDevice.ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`sourceDevice.ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.

Response Field	Type	Example Value	Description
`sourceDevice.ips.sid`	numeric	`25`	The subnet id for the subnet the IP belongs to.
`sourceDevice.sid`	numeric	`25`	The subnet id for the subnet the device is currently located in.
`sourceDevice.hostname`	string	`workstation-local-82`	The current device hostname.
`sourceDevice.time`	string	`1564090000000`	The first time the device was seen on the network.
`sourceDevice.os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`sourceDevice.typename`	string	`desktop`	The device type in system format.
`sourceDevice.typelabel`	string	`Desktop`	The device type in readable format.

Response Field	Type	Example Value	Description
`destinationDevice`	object		An object describing an internal destination device for the connection.
`destinationDevice.id`	numeric	`239`	The “device id”, a unique identifier.
`destinationDevice.did`	numeric	`239`	The “device id”, a unique identifier.
`destinationDevice.macaddress`	string	`6e:b7:31:d5:33:6c`	The current MAC address associated with the device.
`destinationDevice.ip`	string	`10.0.18.224`	The current IP associated with the device.
`destinationDevice.ips`	array		IPs associated with the device historically.
`destinationDevice.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`destinationDevice.ips.timems`	numeric	`1584265931000`	The time the IP was last seen associated with that device in epoch time.
`destinationDevice.ips.time`	string	`2020-03-15 09:52:11`	The time the IP was last seen associated with that device in readable format.
`destinationDevice.ips.sid`	numeric	`25`	The subnet id for the subnet the IP belongs to.
`destinationDevice.sid`	numeric	`25`	The subnet id for the subnet the device is currently located in.
`destinationDevice.hostname`	string	`workstation-local-82`	The current device hostname.
`destinationDevice.time`	string	`1564090000000`	The first time the device was seen on the network.
`destinationDevice.os`	string	`Windows 10`	The device operating system if Darktrace is able to derive it.
`destinationDevice.typename`	string	`desktop`	The device type in system format.
`destinationDevice.typelabel`	string	`Desktop`	The device type in readable format.

Example Object

```
"sourceDevice": {
  "id": 532,
  "did": 532,
  "macaddress": "93:gb:28:g1:fc:g1",
  "ip": "192.168.72.4",
  "ips": [
    {
      "ip": "192.168.72.4",
      "timems": 1587135600000,
      "time": "2020-04-17 15:00:00",
      "sid": 12
    }
  ],
  "sid": 12,
  "hostname": "workstation-local-82",
  "time": "1528807077000",
  "os": "Linux 3.11 and newer",
  "typename": "desktop",
  "typelabel": "Desktop"
}
```

External `sourceDevice` and `destinationDevice` objects

Response Field	Type	Example Value	Description
`sourceDevice`	object		An object describing an external source device for the connection.
`sourceDevice.hostname`	string	`customerportal.darktrace.com`	The hostname of the external source.
`sourceDevice.hostnamepopularity`	string	`10`	The popularity of that hostname within the network.
`sourceDevice.connectionhostnamepopularity`	string	`0`	The popularity of connections with the same profile to that hostname within the network.
`sourceDevice.domain`	string	`darktrace.com`	The domain of the hostname.
`sourceDevice.domainpopularity`	string	`10`	The popularity of the domain within the network.
`sourceDevice.connectiondomainpopularity`	string	`0`	The popularity of connections with the same profile to that domain within the network.
`sourceDevice.ippopularity`	string	`0`	The popularity of the IP within the network.
`sourceDevice.connectionippopularity`	string	`0`	The popularity of connections with the same profile to that IP within the network.

Response Field	Type	Example Value	Description
`destinationDevice`	object		An object describing an external destination device for the connection.
`destinationDevice.hostname`	string	`google.com`	The hostname of the external destination.
`destinationDevice.hostnamepopularity`	string	`10`	The popularity of that hostname within the network.

Response Field	Type	Example Value	Description
`destinationDevice.connectionhostnamepopularity`	string	`0`	The popularity of connections with the same profile to that hostname within the network.
`destinationDevice.domain`	string	`google.com`	The domain of the hostname.
`destinationDevice.domainpopularity`	string	`10`	The popularity of the domain within the network.
`destinationDevice.connectiondomainpopularity`	string	`0`	The popularity of connections with the same profile to that domain within the network.
`destinationDevice.ippopularity`	string	`0`	The popularity of the IP within the network.
`destinationDevice.connectionippopularity`	string	`0`	The popularity of connections with the same profile to that IP within the network.

External `sourceDevice` and `destinationDevice` objects with `fulldevicedetails=true`

Response Field	Type	Example Value	Description
`sourceDevice`	object		An object describing an external source device for the connection.
`sourceDevice.longitude`	numeric	`-97.822`	For the reported IP location, the longitude value to plot the corresponding IP on a map.
`sourceDevice.latitude`	numeric	`37.751`	For the reported IP location, the latitude value to plot the corresponding IP on a map.
`sourceDevice.country`	string	`United States`	The country that the corresponding IP is located in.
`sourceDevice.countrycode`	string	`US`	The system country code for the country that the corresponding IP is located in.
`sourceDevice.asn`	string	`AS13335 Cloudflare`	The ASN for the corresponding IP.
`sourceDevice.region`	string	`North America`	The geographical region the corresponding IP is located in.
`sourceDevice.ip`	string	`151.101.1.69`	The corresponding IP for the hostname.
`sourceDevice.hostname`	string	`stackoverflow.com`	The hostname of the external source.
`sourceDevice.hostnamepopularity`	string	`40`	The popularity of that hostname within the network.
`sourceDevice.connectionhostnamepopularity`	string	`20`	The popularity of connections with the same profile to that hostname within the network.
`sourceDevice.domain`	string	`stackoverflow.com`	The domain of the hostname.
`sourceDevice.domainpopularity`	string	`40`	The popularity of the domain within the network.
`sourceDevice.connectiondomainpopularity`	string	`20`	The popularity of connections with the same profile to that domain within the network.
`sourceDevice.ippopularity`	string	`40`	The popularity of the IP within the network.
`sourceDevice.connectionippopularity`	string	`20`	The popularity of connections with the same profile to that IP within the network.

Response Field	Type	Example Value	Description
`destinationDevice`	object		An object describing an external destination device for the connection.
`destinationDevice.longitude`	numeric	`-30`	For the reported IP location, the longitude value to plot the corresponding IP on a map.
`destinationDevice.latitude`	numeric	`35`	For the reported IP location, the latitude value to plot the corresponding IP on a map.
`destinationDevice.country`	string	`United States`	The country that the corresponding IP is located in.
`destinationDevice.countrycode`	string	`US`	The system country code for the country that the corresponding IP is located in.
`destinationDevice.asn`	string	`AS16509 Amazon.com Inc.`	The ASN for the corresponding IP.
`destinationDevice.region`	string	`North America`	The geographical region the corresponding IP is located in.
`destinationDevice.ip`	string	`104.20.203.23`	The corresponding IP for the hostname.
`destinationDevice.hostname`	string	`darktrace.com`	The hostname of the external destination.
`destinationDevice.hostnamepopularity`	string	`40`	The popularity of that hostname within the network.
`destinationDevice.connectionhostnamepopularity`	string	`20`	The popularity of connections with the same profile to that hostname within the network.
`destinationDevice.domain`	string	`darktrace.com`	The domain of the hostname.
`destinationDevice.domainpopularity`	string	`40`	The popularity of the domain within the network.
`destinationDevice.connectiondomainpopularity`	string	`20`	The popularity of connections with the same profile to that domain within the network.
`destinationDevice.ippopularity`	string	`40`	The popularity of the IP within the network.
`destinationDevice.connectionippopularity`	string	`20`	The popularity of connections with the same profile to that IP within the network.

Example Object

```
"destinationDevice": {
  "longitude": -122.075,
  "latitude": 37.404,
  "city": "Mountain View",
  "country": "United States",
  "countrycode": "US",
  "asn": "AS15169 Google LLC",
  "region": "North America",
  "ip": "216.58.204.46",
  "hostname": "google.com",
  "hostnamepopularity": "100",
  "domain": "google.com",
  "domainpopularity": "100",
  "ippopularity": "10"
}
```

Response Schema - `eventtype=modelbreach`

Response Field	Type	Example Value	Description
`time`	string	`2020-03-15 09:52:11`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1584265931000`	The timestamp when the record was created in readable format.
`pbid`	numeric	`315602`	The “policy breach ID” of the model breach.
`pid`	numeric	`486`	The “policy id” of the model that was breached.
`phid`	numeric	`3125`	The model “policy history” id. Increments when the model is modified.
`action`	string	`policybreach`	The action associated with the device that has generated this record.
`eventType`	string	`policybreach`	The event type.
`creationTime`	numeric	`1584265931000`	The timestamp that the record of the breach was created in epoch time.
`creationTimestamp`	string	`2020-03-15 09:52:11`	The timestamp that the record of the breach was created in readable format.
`name`	string	`Unusual Activity::Unusual DNS`	Name of the model that was breached.
`components`	array	`1090`	An array of ‘cid’ values which correspond to the components that are part of the model that breached.
`didRestrictions`	array		The device ids of devices on the blacklist for this model.
`didExclusions`	array		The device ids of devices on the whitelist for this model.
`throttle`	numeric	`3600`	For an individual device, this is the value in seconds for which this model will not fire again.
`sharedEndpoints`	boolean	`TRUE`	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
`interval`	numeric	`0`	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
`sequenced`	boolean	`FALSE`	A system field.
`active`	boolean	`TRUE`	Whether the model is active or not.
`retired`	boolean	`FALSE`	The model has since been deleted.
`instanceID`	numeric	`19000`	A system field.
`acknowledged`	boolean	`FALSE`	Whether the model breach has been acknowledged.
`state`	string	`New`	A system field.
`score`	numeric	`0.372238`	The model breach score, represented by a value between 0 and 1.

Response Field	Type	Example Value	Description
`commentCount`	numeric	`0`	The number of comments made against this breach.
`componentBreaches`	array	`1090`	Of the components associated with this model, the component ID(s) of those that were breached to trigger the alert.
`componentBreachTimes`	array	`1590000000000`	The time at which the component breach(es) occurred.
`devices`	array	`3877`	The device ids of the devices involved in this breach.
`deviceLabels`	array	`D7S45E001`	The corresponding device labels for devices involved in this breach.

Response Schema - `eventtype=devicehistory`

Response Field	Type	Example Value	Description
`time`	string	`2020-04-15 08:00:00`	The timestamp when the record was created in epoch time.
`timems`	numeric	`1586937600000`	The timestamp when the record was created in readable format.
`eventType`	string	`deviceHistory`	The event type.
`name`	string	`mac`	The type of change or the changed value.
`value`	string	`93:gb:28:g1:fc:g1`	The new or removed value, depending on the eventType.
`reason`	string	`DHCP`	The initiator of the change - it may be a model, an expiry, a user, a protocol etc.
`device`	object		An object describing the device in its current state.
`device.id`	numeric	`76`	The “device id”, a unique identifier.
`device.did`	numeric	`76`	The “device id”, a unique identifier.
`device.macaddress`	string	`93:gb:28:g1:fc:g1`	The current MAC address associated with the device.
`device.ip`	string	`10.15.3.39`	The current IP associated with the device.
`device.ips`	array		IPs associated with the device historically.
`device.ips.ip`	string	`10.15.3.39`	A historic IP associated with the device.
`device.ips.timems`	numeric	`1586937600000`	The time the IP was last seen associated with that device in epoch time.
`device.ips.time`	string	`2020-04-15 08:00:00`	The time the IP was last seen associated with that device in readable format.
`device.ips.sid`	numeric	`83`	The subnet id for the subnet the IP belongs to.
`device.sid`	numeric	`83`	The subnet id for the subnet the device is currently located in.
`device.hostname`	string	`sarah-desktop-12`	The current device hostname.
`device.time`	string	`1564090000000`	The first time the device was seen on the network.
`device.os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.

Response Field	Type	Example Value	Description
`device.typename`	string	`desktop`	The device type in system format.
`device.typelabel`	string	`Desktop`	The device type in readable format.

Example Response

```
{
  "time": "2020-04-10 00:43:43",
  "timems": 1586479423000,
  "eventType": "deviceHistory",
  "name": "removehostname",
  "value": "sarah-desktop-12",
  "reason": "Expired",
  "device": {
    "id": 76,
    "did": 76,
    "macaddress": "2g:d8:a2:a8:54:c6",
    "ip": "10.12.14.2",
    "ips": [
      {
        "ip": "10.12.14.2",
        "timems": 1587135600000,
        "time": "2020-04-17 15:00:00",
        "sid": 15
      }
    ],
    "sid": 15,
    "time": "1528807103000",
    "os": "Linux 3.11 and newer",
    "devicelabel": "Pool Laptop 6",
    "typename": "desktop",
    "typelabel": "Desktop"
  }
}
```

/deviceinfo

The `/deviceinfo` endpoint returns the data used in the “Connections Data” view for a specific device that can be accessed from the Threat Visualizer omnisearch. The data returned covers a 4 week period.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`datatype`	string	Return data for either connections (`co`), data size out (`sizeout`) or data size in (`sizein`).
`did`	numeric	Identification number of a device.
`externaldomain`	string	Restrict external data to a particular domain name
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`odid`	numeric	Identification number of a destination device modelled in the Darktrace system to restrict data to.
`showallgraphdata`	boolean	Return an entry for all time intervals in the graph data, including zero counts.
`similardevices`	numeric	Return data for the primary device and this number of similar devices.
`port`	numeric	Restricts returned connection data to the port specified.
`intervalhours`	numeric	The size in hours that the returned time series data is grouped by.

Notes

- The minimum time interval width is 1 hour. A value greater than 1 can be specified with `intervalhours` to create a larger interval for connection grouping.
- Setting `showallgraphdata` to false will remove empty time intervals with from the returned data - this can be helpful to reduce noise.
- To get external connectivity, use `odid=0` in the request parameters. This will add additional information to the response JSON about the external locations accessed.
- Only the top results across the four week interval will be returned - results below a certain threshold will be grouped into an ‘others’ category.
- Restricting the data to a domain or adding similar devices will change the structure of the returned JSON.
- `fulldevicedetails=true` will add a `devices` object with full details of the devices connected to and the device specified
- Specifying a number of similar devices to return will result in multiple objects in the `deviceinfo` array.

Example Request

1. `GET` the data transfer volume downloaded by the device with `did=1` on port 443 and return 3 devices with similar patterns of life:

```
/deviceinfo?did=1&showallgraphdata=true&port=443&datatype=sizein&similardevices=3
```

2. `GET` the number of connections from the device with `did=1` to the device with `did=100`, grouped into 12 hour windows:

```
https://<applianceIP>/deviceinfo?
did=1&odid=100&datatype=co&similardevices=0&intervalhours=12&fulldevicedetails=false
```

Example Response

Request: /deviceinfo?did=316&intervalhours=12&showallgraphdata=true&datatype=co&port=443&externaldomain=google.com

```
{
  "deviceInfo": [
    {
      "did": 316,
      "similarityScore": 100,
      "domain": "google.com",
      "graphData": [
        {
          "time": 1582243200000,
          "count": 0
        },
        ...
      ],
      "info": {
        "totalUsed": 302,
        "totalServed": 0,
        "totalDevicesAndPorts": 302,
        "devicesAndPorts": [],
        "externalDomains": [
          {
            "domain": "google.com",
            "size": 100
          }
        ],
        "portsUsed": [
          {
            "port": 443,
            "size": 100,
            "firstTime": 1584529392000
          }
        ],
        "portsServed": [],
        "devicesUsed": [
          {
            "did": 0,
            "size": 100,
            "firstTime": 1584529392000
          }
        ],
        "devicesServed": []
      }
    }
  ]
}
```

Response is abbreviated.

/deviceinfo Response Schema

Response Schema

`fulldevicedetails=false`

Response Field	Type	Example Value	Description
`deviceInfo`	array		An array of graphable connection information for the specified device.
`deviceInfo.did`	numeric	`225`	The “device id”, a unique identifier.
`deviceInfo.similarityScore`	numeric	`100`	A score describing how similar this device is in comparison to the original device. The original device will always return 100.
`deviceInfo.graphData`	array		An array of time series grouped connection data to be displayed graphically.
`deviceInfo.graphData.time`	numeric	`1580000000000`	Timestamp for the interval of grouped connection / data transfer data in epoch time.
`deviceInfo.graphData.count`	numeric	`355`	The volume of connections or data for that interval.
`deviceInfo.info`	object		Information about the connections.
`deviceInfo.info.totalUsed`	numeric	`374112`	The amount of data or connections where the device was the client.
`deviceInfo.info.totalServed`	numeric	`45`	The amount of data or connections where the device was the server.
`deviceInfo.info.totalDevicesAndPorts`	numeric	`374157`	The amount of data or connections.
`deviceInfo.info.devicesAndPorts`	array		An array of device/port pairs used in the connections or data transfers.
`deviceInfo.info.devicesAndPorts.deviceAndPort`	object		An object describing the device/port pairs and the direction of transfer.
`deviceInfo.info.devicesAndPorts.deviceAndPort.direction`	string	`out`	The direction of data flow.
`deviceInfo.info.devicesAndPorts.deviceAndPort.device`	numeric	`-6`	The “device id” of the device that connected to, or was connected to by, the original device.
`deviceInfo.info.devicesAndPorts.deviceAndPort.port`	numeric	`443`	The port used or served by the original device, depending on the connection direction.
`deviceInfo.info.devicesAndPorts.size`	numeric	`27`	What percentage of the total connections or data transfer used this port/device pair.
`deviceInfo.info.portsUsed`	array		An array of ports used by the device when making the connections returned in graph data.
`deviceInfo.info.portsUsed.port`	numeric	`443`	The port used.
`deviceInfo.info.portsUsed.size`	numeric	`44`	What percentage of the total outbound connections or data transfer used this port.
`deviceInfo.info.portsUsed.firstTime`	numeric	`1530000000000`	The first time this port was used by the device.

Response Field	Type	Example Value	Description
`deviceInfo.info.portsServed`	array		An array of ports served by the device when making the connections returned in graph data.
`deviceInfo.info.portsServed.port`	numeric	`22`	The port that was served by the device.
`deviceInfo.info.portsServed.size`	numeric	`53`	What percentage of the total inbound connections or data transfer used this port.
`deviceInfo.info.portsServed.firstTime`	numeric	`1530000000000`	The first time this port was served by the device in epoch time.
`deviceInfo.info.devicesUsed`	array		An array of devices connected to by the original device when making the connections returned in graph data.
`deviceInfo.info.devicesUsed.did`	numeric	`-6`	The “device id” of a device that was connected to by the original device.
`deviceInfo.info.devicesUsed.size`	numeric	`72`	The percentage of the total outbound connections or data transfer that used this device.
`deviceInfo.info.devicesUsed.firstTime`	numeric	`1530000000000`	The first time this device was connected to by the original device in epoch time.
`deviceInfo.info.devicesServed`	array		An array of devices that connected to the original device when making the connections returned in graph data.
`deviceInfo.info.devicesServed.did`	numeric	`354`	The “device id” of a device that connected to the original device.
`deviceInfo.info.devicesServed.size`	numeric	`53`	The percentage of the total inbound connections or data transfer that involved this device connecting to the original device.

Example Response

```
{
  "deviceInfo": [
    {
      "did": 316,
      "similarityScore": 100,
      "graphData": [
        {
          "time": 1582243200000,
          "count": 0
        },
        ...
      ],
      "info": {
        "totalUsed": 6284,
        "totalServed": 0,
        "totalDevicesAndPorts": 6284,
        "devicesAndPorts": [
          {
            "deviceAndPort": {
              "direction": "out",
              "device": 0,
              "port": 443
            },
            "size": 74
          },
          ...
        ],
        "portsUsed": [
          {
            "port": 443,
            "size": 100,
            "firstTime": 1576136929000
          }
        ],
        "portsServed": [],
        "devicesUsed": [
          {
            "did": 0,
            "size": 74,
            "firstTime": 1584529027000
          },
          ...
        ],
        "devicesServed": []
      }
    }
  ]
}
```

Response is abbreviated.

`fulldevicedetails=true`

Response Field	Type	Example Value	Description
`deviceInfo`	array		An array of graphable connection information for the specified device.
`deviceInfo.did`	numeric	`230`	The “device id”, a unique identifier.
`deviceInfo.similarityScore`	numeric	`100`	A score describing how similar this device is in comparison to the original device. The original device will always return 100.
`deviceInfo.graphData`	array		An array of time series grouped connection data to be displayed graphically.

Response Field	Type	Example Value	Description
deviceInfo.graphData.time	numeric	1580000000000	Timestamp for the interval of grouped connection / data transfer data in epoch time.
deviceInfo.graphData.count	numeric	355	The volume of connections or data for that interval.
deviceInfo.info	object		Information about the connections.
deviceInfo.info.totalUsed	numeric	374112	The amount of data or connections where the device was the client.
deviceInfo.info.totalServed	numeric	45	The amount of data or connections where the device was the server.
deviceInfo.info.totalDevicesAndPorts	numeric	374157	The amount of data or connections.
deviceInfo.info.devicesAndPorts	array		An array of device/port pairs used in the connections or data transfers.
deviceInfo.info.devicesAndPorts.deviceAndPort	object		An object describing the device/port pairs and the direction of transfer.
deviceInfo.info.devicesAndPorts.deviceAndPort.direction	string	out	The direction of data flow.
deviceInfo.info.devicesAndPorts.deviceAndPort.device	numeric	-6	The “device id” of the device that connected to, or was connected to by, the original device.
deviceInfo.info.devicesAndPorts.deviceAndPort.port	numeric	443	The port used or served by the original device, depending on the connection direction.
deviceInfo.info.devicesAndPorts.size	numeric	27	What percentage of the total connections or data transfer used this port/device pair.
deviceInfo.info.portsUsed	array		An array of ports used by the device when making the connections returned in graph data.
deviceInfo.info.portsUsed.port	numeric	443	The port used.
deviceInfo.info.portsUsed.size	numeric	44	What percentage of the total outbound connections or data transfer used this port.
deviceInfo.info.portsUsed.firstTime	numeric	1530000000000	The first time this port was used by the device.
deviceInfo.info.portsServed	array		An array of ports served by the device when making the connections returned in graph data.
deviceInfo.info.portsServed.port	numeric	22	What percentage of the total inbound connections or data transfer used this port.
deviceInfo.info.portsServed.size	numeric	53	The first time this port was served by the device in epoch time.
deviceInfo.info.devicesUsed	array		An array of devices connected to by the original device when making the connections returned in graph data.
deviceInfo.info.devicesUsed.did	numeric	-6	The “device id” of a device that was connected to by the original device.
deviceInfo.info.devicesUsed.size	numeric	72	The percentage of the total outbound connections or data transfer that used this device.
deviceInfo.info.devicesUsed.firstTime	numeric	1530000000000	The first time this device was connected to by the original device in epoch time.

Response Field	Type	Example Value	Description
`deviceInfo.info.devicesServed`	array		An array of devices that connected to the original device when making the connections returned in graph data.
`deviceInfo.info.devicesServed.did`	numeric	`354`	The “device id” of a device that connected to the original device.
`deviceInfo.info.devicesServed.size`	numeric	`53`	The percentage of the total inbound connections or data transfer that involved this device connecting to the original device.
`devices`	array		An array of information about the original device and any devices it interacted with as part of the connections.
`devices.did`	numeric	`57`	The “device id”, a unique identifier.
`devices.macaddress`	string	`93:gb:28:g1:fc:g1`	The current MAC address associated with the device.
`devices.vendor`	string	`Belkin International Inc.`	The vendor of the device network card as derived by Darktrace from the MAC address.
`devices.ip`	string	`10.15.3.39`	The current IP associated with the device.
`devices.ips`	array		IPs associated with the device historically.
`devices.ips.ip`	string	`10.15.3.39`	A historic IP associated with the device.
`devices.ips.timems`	numeric	`1584265931000`	The time the IP was last seen associated with that device in epoch time.
`devices.ips.time`	string	`2020-03-15 09:52:11`	The time the IP was last seen associated with that device in readable format.
`devices.ips.sid`	numeric	`17`	The subnet id for the subnet the IP belongs to.
`devices.sid`	numeric	`17`	The subnet id for the subnet the device is currently located in.
`devices.hostname`	string	`ws83`	The current device hostname.
`devices.firstSeen`	numeric	`1528810000000`	The first time the device was seen on the network.
`devices.lastSeen`	numeric	`1585140000000`	The last time the device was seen on the network.
`devices.os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`devices.devicelabel`	string	`Workstation 83`	An optional label applied to the device in Device Admin.
`devices.typename`	string	`laptop`	The device type in system format.
`devices.typelabel`	string	`Laptop`	The device type in readable format.
`devices.tags`	array		An object describing tags applied to the device.
`devices.tags.tid`	numeric	`180`	The “tag id”. A unique value.
`devices.tags.expiry`	numeric	`0`	The expiry time for the tag when applied to a device.
`devices.tags.thid`	numeric	`172`	The “tag history” id. Increments if the tag is edited.

Response Field	Type	Example Value	Description
`devices.tags.name`	string	`Finance`	The tag label displayed in the user interface or in objects that reference the tag.
`devices.tags.restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`devices.tags.data`	object		An object containing information about the tag.
`devices.tags.data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`devices.tags.data.color`	numeric	`200`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`devices.tags.data.description`	string	`Device is part of the Finance network.`	An optional description summarizing the purpose of the tag.
`devices.tags.data.visibility`	string		A system field.
`devices.tags.isReferenced`	boolean	`TRUE`	Whether the tag is used by one or more model components.

Example Response

```
{
  "deviceInfo": [
    {
      "did": 316,
      "similarityScore": 100,
      "graphData": [
        {
          "time": 1582243200000,
          "count": 0
        },
        ...
      ],
      "info": {
        "totalUsed": 125,
        "totalServed": 0,
        "totalDevicesAndPorts": 125,
        "devicesAndPorts": [
          {
            "deviceAndPort": {
              "direction": "out",
              "device": 18,
              "port": 443
            },
            "size": 100
          }
        ],
        "portsUsed": [
          {
            "port": 443,
            "size": 100,
            "firstTime": 1584529073000
          }
        ],
        "portsServed": [],
        "devicesUsed": [
          {
            "did": 2719,
            "size": 100,
            "firstTime": 1584529073000
          }
        ],
        "devicesServed": []
      }
    }
  ],
  "devices": [
    {
      "did": 2719,
      "ip": "192.168.120.39",
      "ips": [
        {
          "ip": "192.168.120.39",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 6
        }
      ],
      "sid": 6,
      "hostname": "sarah's iphone",
      "firstSeen": 1576581851000,
      "lastSeen": 1582131590000,
      "os": "Mac OS X",
      "typename": "mobile",
      "typelabel": "Mobile",
      "tags": [
        {
          "tid": 17,
          "expiry": 0,
          "thid": 17,
          "name": "iOS device",
          "restricted": false,
          "data": {
            "auto": false,
            "color": 181,
            "description": "",
            "visibility": "Public"
          },
          "isReferenced": true
        }
      ]
    },
    ...
    {
```

Response is abbreviated.

Response Schema - `externaldomain`

Response Field	Type	Example Value	Description
`deviceInfo`	array		An array of graphable connection information for the specified device.
`deviceInfo.did`	numeric	`57`	The “device id”, a unique identifier.
`deviceInfo.similarityScore`	numeric	`100`	A score describing how similar this device is in comparison to the original device. The original device will always return 100.
`deviceInfo.domain`	string	`google.com`	The external domain that connections or data transfer is limited to.
`deviceInfo.graphData`	array		An array of time series grouped connection data to be displayed graphically.
`deviceInfo.graphData.time`	numeric	`1580000000000`	Timestamp for the interval of grouped connection / data transfer data in epoch time.
`deviceInfo.graphData.count`	numeric	`1`	The volume of connections or data for that interval.
`deviceInfo.info`	object		Information about the connections.
`deviceInfo.info.totalUsed`	numeric	`3397`	The amount of data or connections where the device was the client.
`deviceInfo.info.totalServed`	numeric	`0`	The amount of data or connections where the device was the server.
`deviceInfo.info.totalDevicesAndPorts`	numeric	`3397`	The amount of data or connections.
`deviceInfo.info.devicesAndPorts`	array		An array of device/port pairs used in the connections or data transfers.
`deviceInfo.info.devicesAndPorts.deviceAndPort`	object		An object describing the device/port pairs and the direction of transfer.
`deviceInfo.info.devicesAndPorts.deviceAndPort.direction`	string	`out`	The direction of data flow.
`deviceInfo.info.devicesAndPorts.deviceAndPort.device`	numeric	`-6`	The “device id” of the device that connected to, or was connected to by, the original device.
`deviceInfo.info.devicesAndPorts.deviceAndPort.port`	numeric	`443`	The port used or served by the original device, depending on the connection direction.
`deviceInfo.info.devicesAndPorts.size`	numeric	`27`	What percentage of the total connections or data transfer used this port/device pair.
`deviceInfo.info.externalDomains`	array		An array of the external domains that were connected to.
`deviceInfo.info.externalDomains.domain`	string	`google.com`	An external domain that was accessed.
`deviceInfo.info.externalDomains.size`	numeric	`100`	What percentage of the total connections or data transfer involved this external domain.
`deviceInfo.info.portsUsed`	array		An array of ports used by the device when making the connections returned in graph data.

Response Field	Type	Example Value	Description
`deviceInfo.info.portsUsed.port`	numeric	`443`	The port used.
`deviceInfo.info.portsUsed.size`	numeric	`44`	What percentage of the total outbound connections or data transfer used this port.
`deviceInfo.info.portsUsed.firstTime`	numeric	`1530000000000`	The first time this port was used by the device.
`deviceInfo.info.portsServed`	array		An array of ports served by the device when making the connections returned in graph data.
`deviceInfo.info.portsServed.port`	numeric	`22`	The port that was served by the device.
`deviceInfo.info.portsServed.size`	numeric	`53`	What percentage of the total inbound connections or data transfer used this port.
`deviceInfo.info.portsServed.firstTime`	numeric	`1530000000000`	The first time this port was served by the device in epoch time.
`deviceInfo.info.devicesUsed`	array		An array of devices connected to by the original device when making the connections returned in graph data.
`deviceInfo.info.devicesUsed.did`	numeric	`-6`	The “device id” of a device that was connected to by the original device.
`deviceInfo.info.devicesUsed.size`	numeric	`72`	The percentage of the total outbound connections or data transfer that used this device.
`deviceInfo.info.devicesUsed.firstTime`	numeric	`1530000000000`	The first time this device was connected to by the original device in epoch time.
`deviceInfo.info.devicesServed`	array		An array of devices that connected to the original device when making the connections returned in graph data.
`deviceInfo.info.devicesServed.did`	numeric	`354`	The “device id” of a device that connected to the original device.
`deviceInfo.info.devicesServed.size`	numeric	`53`	The percentage of the total inbound connections or data transfer that involved this device connecting to the original device.

Example Response

```
{
  "deviceInfo": [
    {
      "did": 316,
      "similarityScore": 100,
      "domain": "google.com",
      "graphData": [
        {
          "time": 1582243200000,
          "count": 0
        },
        ...
      ],
      "info": {
        "totalUsed": 302,
        "totalServed": 0,
        "totalDevicesAndPorts": 302,
        "devicesAndPorts": [],
        "externalDomains": [
          {
            "domain": "google.com",
            "size": 100
          }
        ],
        "portsUsed": [
          {
            "port": 443,
            "size": 100,
            "firstTime": 1584529392000
          }
        ],
        "portsServed": [],
        "devicesUsed": [
          {
            "did": 0,
            "size": 100,
            "firstTime": 1584529392000
          }
        ],
        "devicesServed": []
      }
    }
  ]
}
```

Response is abbreviated.

Response Schema - `odid=0`

Response Field	Type	Example Value	Description
`deviceInfo`	array		An array of graphable connection information for the specified device.
`deviceInfo.did`	numeric	`230`	The “device id”, a unique identifier.
`deviceInfo.similarityScore`	numeric	`100`	A score describing how similar this device is in comparison to the original device. The original device will always return 100.
`deviceInfo.graphData`	array		An array of time series grouped connection data to be displayed graphically.
`deviceInfo.graphData.time`	numeric	`1582680000000`	Timestamp for the interval of grouped connection / data transfer data in epoch time.

Response Field	Type	Example Value	Description
`deviceInfo.graphData.count`	numeric	`72`	The volume of connections or data for that interval.
`deviceInfo.info`	object		Information about the connections.
`deviceInfo.info.totalUsed`	numeric	`321662`	The amount of data or connections where the device was the client.
`deviceInfo.info.totalServed`	numeric	`0`	The amount of data or connections where the device was the server.
`deviceInfo.info.totalDevicesAndPorts`	numeric	`321662`	The amount of data or connections.
`deviceInfo.info.devicesAndPorts`	array		An array of device/port pairs used in the connections or data transfers.
`deviceInfo.info.devicesAndPorts.deviceAndPort`	object		An object describing the device/port pairs and the direction of transfer.
`deviceInfo.info.devicesAndPorts.deviceAndPort.direction`	string	`out`	The direction of data flow.
`deviceInfo.info.devicesAndPorts.deviceAndPort.device`	numeric	`0`	The “device id” of the device that connected to, or was connected to by, the original device.
`deviceInfo.info.devicesAndPorts.deviceAndPort.port`	numeric	`443`	The port used or served by the original device, depending on the connection direction.
`deviceInfo.info.devicesAndPorts.size`	numeric	`19`	What percentage of the total connections or data transfer used this port/device pair.
`deviceInfo.info.externalASNs`	array		An array of external ASNs who served the external domains connected to by the device.
`deviceInfo.info.externalASNs.asn`	string	`AS15169 Google LLC`	An ASN.
`deviceInfo.info.externalASNs.size`	numeric	`53`	The percentage of connections that involved this ASN.
`deviceInfo.info.externalDomains`	array		An array of the external domains that were connected to.
`deviceInfo.info.externalDomains.domain`	string	`google.com`	An external domain that was accessed.
`deviceInfo.info.externalDomains.size`	numeric	`26`	What percentage of the total connections or data transfer involved this external domain.
`deviceInfo.info.portsUsed`	array		An array of ports used by the device when making the connections returned in graph data.
`deviceInfo.info.portsUsed.port`	numeric	`443`	The port used.
`deviceInfo.info.portsUsed.size`	numeric	`44`	What percentage of the total outbound connections or data transfer used this port.
`deviceInfo.info.portsUsed.firstTime`	numeric	`1530000000000`	The first time this port was used by the device.
`deviceInfo.info.portsServed`	array		An array of ports served by the device when making the connections returned in graph data.
`deviceInfo.info.portsServed.port`	numeric	`22`	The port that was served by the device.
`deviceInfo.info.portsServed.size`	numeric	`53`	What percentage of the total inbound connections or data transfer used this port.

Response Field	Type	Example Value	Description
`deviceInfo.info.portsServed.firstTime`	numeric	`1530000000000`	The first time this port was served by the device in epoch time.
`deviceInfo.info.devicesUsed`	array		An array of devices connected to by the original device when making the connections returned in graph data.
`deviceInfo.info.devicesUsed.did`	numeric	`-6`	The “device id” of a device that was connected to by the original device.
`deviceInfo.info.devicesUsed.size`	numeric	`72`	The percentage of the total outbound connections or data transfer that used this device.
`deviceInfo.info.devicesUsed.firstTime`	numeric	`1530000000000`	The first time this device was connected to by the original device in epoch time.
`deviceInfo.info.devicesServed`	array		An array of devices that connected to the original device when making the connections returned in graph data.
`deviceInfo.info.devicesServed.did`	numeric	`354`	The “device id” of a device that connected to the original device.
`deviceInfo.info.devicesServed.size`	numeric	`53`	The percentage of the total inbound connections or data transfer that involved this device connecting to the original device.

Example Response

```
{
  "deviceInfo": [
    {
      "did": 316,
      "similarityScore": 100,
      "graphData": [
        {
          "time": 1582243200000,
          "count": 0
        },
        ...
      ],
      "info": {
        "totalUsed": 21124,
        "totalServed": 0,
        "totalDevicesAndPorts": 21124,
        "devicesAndPorts": [
          {
            "deviceAndPort": {
              "direction": "out",
              "device": 0,
              "port": 443
            },
            "size": 22
          }
        ],
        "externalASNs": [
          {
            "asn": "AS15169 Google LLC.",
            "size": 8
          },
          ...
        ],
        "externalDomains": [
          {
            "domain": "google.com",
            "size": 21
          },
          ...
        ],
        "portsUsed": [
          {
            "port": 443,
            "size": 100,
            "firstTime": 1584529027000
          }
        ],
        "portsServed": [],
        "devicesUsed": [
          {
            "did": 0,
            "size": 22,
            "firstTime": 1584529027000
          }
        ],
        "devicesServed": []
      }
    }
  ]
}
```

Response is abbreviated.

/devices

The `/devices` endpoint returns a list of devices identified by Darktrace or details of a specific device given a time window. When a `did` is specified, the endpoint returns the information displayed in the UI pop-up when hovering over a device.

Changes to a device can be made with a POST request. The fields that can be changed are the device type (in enum format), the priority and the label.

`POST` requests to this endpoint can be made in JSON or parameter format. Fields which are not supported will be ignored when included in `POST` requests. Device objects can therefore be retrieved, modified and resubmitted to this endpoint to make changes.

For targeted searches, the `/devicesearch` endpoint is recommended.

Request Type(s)

`[GET]` `[POST]`

Parameters

Parameter	Type	Description
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`ip`	string	IP of the device modelled in the Darktrace system.
`iptime`	string	Returns the device which had the IP at a given time.
`mac`	string	Returns the device with this MAC address.
`seensince`	string	Relative offset for activity. Devices with activity in the specified time period are returned. The format is either a number representing a number of seconds before the current time, or a number with a modifier such as second, minute, hour day or week (Minimum=1 second).
`sid`	numeric	Identification number of a subnet modelled in the Darktrace system.
`count`	numeric	The number of devices to return. Only limits the number of devices within the current timeframe.
`includetags`	boolean	Whether to include tags applied to the device in the response.
`label`	string	An optional label to add to the device. Available for POST requests only.
`priority`	numeric	The device priority on a scale of -5 to 5 - priority affects the model breach score for the device and can be used to filter alert outputs. Available for POST requests only.
`type`	numeric	The device type in enum format (see /enums/sourcedevicetypes 130). Only device types which do not have `hidden=true` are available to set. Industrial device types are not available outside the IIS environment. Available for POST requests only.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- When specifying how many minutes/hours/days in the `seensince` parameter, do not use a plural for the unit. For example, `3min` = 3 mins, `5hour` = 5 hours, `6day` = 6 days, etc.
- Device objects may not have values for all of the attributes available. If a device does not have a MAC address, a label, credentials, or a hostname, they will not be included in the returned JSON.
- Devices with a priority of 0 will not have a priority attribute returned.
- This endpoint does not support searching for outside the `did` , `sid` , and `ip` parameters. To perform custom searches, the `/devicesearch` endpoint is recommended.

- The default timeframe is 7 days.
- When accessing the `/devices` endpoint from a browser, an additional parameter - `minscore` - is required. This parameter controls the devices that return by their device score (score of associated model breaches) and takes values from 0 to 1, where a score threshold of 70% would be `minscore=0.7` . To return all devices regardless of score, `minscore=0` should be added to the query. This parameter is not available when using the API programmatically with an authentication token - `minscore` is set to 0.

Example Request

1. `GET` a list of all the devices on the 10.0.0.0/24 subnet (`sid=25`) in the last 2 minutes:

```
https://<applianceIP>/devices?seensince=2min&sid=25
```

2. `GET` a device with IP 10.0.0.1:

```
https://<applianceIP>/devices?ip=10.0.0.1
```

3. `GET` a list of all the devices seen in the last hour:

```
https://<applianceIP>/devices?seensince=1hour
```

```
https://<applianceIP>/devices?seensince=3600
```

4. `POST` to update the label and change the device type to “Key Asset” for the device with `did=100` :

```
https://<applianceIP>/devices with body {"did":100,"label": "Finance File Server", "type":
10}
```

Example Response

Request: /devices?seensince=2hour&sid=23

```
[
  {
    "id": 316,
    "ip": "10.0.56.12",
    "ips": [
      {
        "ip": "10.0.56.12",
        "timems": 1581508800000,
        "time": "2020-02-12 12:00:00",
        "sid": 23
      }
    ],
    "did": 316,
    "sid": 23,
    "hostname": "Sarah Development",
    "time": 1528807092000,
    "endtime": 1581510431000,
    "os": "Linux 3.11 and newer",
    "typename": "desktop",
    "typelabel": "Desktop"
  }
]
```

/devices Response Schema

Note: Device objects may not have values for all of the attributes available. If a device does not have a MAC address, a label, credentials, or a hostname, they will not be included in the returned JSON.

Response Schema

Response Field	Type	Example Value	Description
`id`	numeric	`227`	The “device id”, a unique identifier.
`macaddress`	string	`56:2d:4b:9c:18:42`	The current MAC address associated with the device.
`vendor`	string	`Apple`	The vendor of the device network card as derived by Darktrace from the MAC address.
`ip`	string	`10.0.18.224`	The current IP associated with the device.
`ips`	array		IPs associated with the device historically.
`ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`ips.sid`	numeric	`10`	The subnet id for the subnet the IP belongs to.
`did`	numeric	`230`	The “device id”, a unique identifier.
`sid`	numeric	`10`	The subnet id for the subnet the device is currently located in.
`hostname`	string	`sarah-desktop-12`	The current device hostname.
`time`	numeric	`1528810000000`	The first time the device was seen on the network.
`endtime`	numeric	`1585310000000`	The last time the device was seen on the network.
`os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`devicelabel`	string	`Sarah Development`	An optional label applied to the device in the Device Admin page.
`typename`	string	`desktop`	The device type in system format.
`typelabel`	string	`Desktop`	The device type in readable format.

Example Response

```
{
  "id": 212,
  "macaddress": "6e:b7:31:d5:33:6c",
  "vendor": "Micro-Star INTL CO., LTD.",
  "ip": "10.12.14.2",
  "ips": [
    {
      "ip": "10.12.14.2",
      "timems": 1587132000000,
      "time": "2020-04-17 14:00:00",
      "sid": 12
    }
  ],
  "did": 212,
  "sid": 12,
  "hostname": "sarah-desktop-12",
  "time": 1528807083000,
  "endtime": 1587135192000,
  "os": "Linux 3.11 and newer",
  "typename": "desktop",
  "typelabel": "Desktop"
}
```

Response Schema - `includetags=true`

Response Field	Type	Example Value	Description
`id`	numeric	`227`	The “device id”, a unique identifier.
`macaddress`	string	`56:2d:4b:9c:18:42`	The current MAC address associated with the device.
`vendor`	string	`Apple`	The vendor of the device network card as derived by Darktrace from the MAC address.
`ip`	string	`10.0.18.224`	The current IP associated with the device.
`ips`	array		IPs associated with the device historically.
`ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`ips.sid`	numeric	`10`	The subnet id for the subnet the IP belongs to.
`did`	numeric	`227`	The “device id”, a unique identifier.
`sid`	numeric	`10`	The subnet id for the subnet the device is currently located in.
`hostname`	string	`sarah-desktop-12`	The current device hostname.
`time`	numeric	`1528810000000`	The first time the device was seen on the network.
`endtime`	numeric	`1585310000000`	The last time the device was seen on the network.
`tags`	array		An object describing tags applied to the device.
`tags.tid`	numeric	`22`	The “tag id”. A unique value.

Response Field	Type	Example Value	Description
`tags.expiry`	numeric	`0`	The expiry time for the tag when applied to a device.
`tags.thid`	numeric	`22`	The “tag history” id. Increments if the tag is edited.
`tags.name`	string	`Admin`	The tag label displayed in the user interface or in objects that reference the tag.
`tags.restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`tags.data`	object		An object containing information about the tag.
`tags.data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`tags.data.color`	numeric	`200`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`tags.data.description`	string	`Testing the use of tags.`	An optional description summarizing the purpose of the tag.
`tags.data.visibility`	string		A system field.
`tags.isReferenced`	boolean	`TRUE`	Whether the tag is used by one or more model components.
`os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`devicelabel`	string	`Sarah Development`	An optional label applied to the device in the Device Admin page.
`typename`	string	`desktop`	The device type in system format.
`typelabel`	string	`Desktop`	The device type in readable format.

Example Response

```
{
  "id": 212,
  "macaddress": "6e:b7:31:d5:33:6c",
  "vendor": "Micro-Star INTL CO., LTD.",
  "ip": "10.12.14.2",
  "ips": [
    {
      "ip": "10.12.14.2",
      "timems": 1587132000000,
      "time": "2020-04-17 14:00:00",
      "sid": 12
    }
  ],
  "did": 212,
  "sid": 12,
  "hostname": "sarah-desktop-12",
  "time": 1528807083000,
  "endtime": 1587135192000,
  "tags": [
    {
      "tid": 131,
      "expiry": 0,
      "thid": 62,
      "name": "Re-Activated Device",
      "restricted": false,
      "data": {
        "auto": false,
        "color": 142,
        "description": "A device that has been inactive for at least 4 weeks has re-appeared on
the network in the past 48 hours.",
        "visibility": "Public"
      },
      "isReferenced": true
    }
  ],
  "os": "Linux 3.11 and newer",
  "typename": "desktop",
  "typelabel": "Desktop"
}
```

/devicesearch

The `/devicesearch` endpoint provides a highly filterable search capacity to interrogate the list of devices Darktrace has seen on the network. It is more suited for inventory management and general queries than the `/devices` endpoint as it provides sorting and string searching capabilities.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`count`	numeric	The number of devices to return. If unspecified, defaults to 50.
`orderBy`	string	Orders the response by the specified filter, default value is `lastSeen`. Valid values are `priority`, `hostname`, `ip`, `macaddress`, `vendor`, `os`, `firstSeen`, `lastSeen`, `devicelabel` or `typelabel`.
`order`	string	Sets the sort order for returned devices as ascending or descending, can take `asc` or `desc`. Default is ascending.
`query`	string	An optional string search. Can query all fields or take a specific field filter from `label`, `tag`, `type`, `hostname`, `ip`, `mac`, `vendor` and `os`
`offset`	numeric	An offset for the results returned.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- The `query` parameter can take a string directly to search all key/value pairs (.e.g `query="value"`) or be limited to a certain data type (.e.g `query=label:"test"`). Wildcards (*) are supported and multiple queries can be space-separated (`query=tag:"*T*" label:"Test"`); the space must be percent-encoded when making the final request but not when producing the signature.
- The `priority` field will not be included in the response for a device if the value is 0.
- Returned data can be paginated by limiting the `count` value and making multiple requests, incrementing the `offset` value by the `count` value each time (e.g., `count=50`, multiple queries for `offset=0, offset=50, offset=100`).

Example Request

1. `GET` a list of devices with “sarah” anywhere in the device information (e.g., hostname, label, tags):

```
https://<applianceIP>/devicesearch?&query="sarah"
```

2. `GET` a list of devices tagged with “Security Device”, ordered by oldest `lastSeen` time:

```
https://<applianceIP>/devicesearch?query=tag:"Security Device"&orderBy=lastSeen&order=asc
```

If using cUrl, ensure the space is percent-encoded when making the final request

3. `GET` a list of 10 highest priority devices with any “Antigena” tag in the subnet 10.0.1.0/24, sorted by descending priority:

```
https://<applianceIP>/devicesearch?count=10&query=tag:"Antigena*"
ip:"10.0.1.*"&orderBy=priority&order=desc
```

If using cUrl, ensure the space is percent-encoded when making the final request

Example Response

Request: /devicesearch?query=“sarah”

```
{
  "totalCount": 2185,
  "devices": [
    {
      "id": 316,
      "ip": "10.0.56.12",
      "ips": [
        {
          "ip": "10.0.56.12",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 23
        }
      ],
      "did": 316,
      "sid": 23,
      "hostname": "Sarah Development",
      "firstseen": 1528807092000,
      "lastseen": 1581510431000,
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    {
      "id": 2719,
      "ip": "192.168.120.39",
      "ips": [
        {
          "ip": "192.168.120.39",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 6
        }
      ],
      "did": 2719,
      "sid": 6,
      "hostname": "sarah's iphone",
      "firstSeen": 1576581851000,
      "lastSeen": 1582131590000,
      "os": "Mac OS X",
      "typename": "mobile",
      "typelabel": "Mobile",
      "tags": [
        {
          "tid": 17,
          "expiry": 0,
          "thid": 17,
          "name": "iOS device",
          "restricted": false,
          "data": {
            "auto": false,
            "color": 181,
            "description": "",
            "visibility": "Public"
          },
          "isReferenced": true
        }
      ]
    }
  ]
}
```

/devicesearch Response Schema

Response Schema

Response Field	Type	Example Value	Description
`totalCount`	numeric	`2191`	The total number of devices that meet the query parameters.
`devices`	array		An array of devices that meet the query parameters.
`devices.did`	numeric	`227`	The “device id”, a unique identifier.
`devices.macaddress`	string	`56:2d:4b:9c:18:42`	The current MAC address associated with the device.
`devices.vendor`	string	`Apple`	The vendor of the device network card as derived by Darktrace from the MAC address.
`devices.ip`	string	`10.0.18.224`	The current IP associated with the device.
`devices.ips`	array		IPs associated with the device historically.
`devices.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`devices.ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`devices.ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`devices.ips.sid`	numeric	`10`	The subnet id for the subnet the IP belongs to.
`devices.sid`	numeric	`10`	The subnet id for the subnet the device is currently located in.
`devices.hostname`	string	`sarah-desktop-12`	The current device hostname.
`devices.firstSeen`	numeric	`1528810000000`	The first time the device was seen on the network.
`devices.lastSeen`	numeric	`1585310000000`	The last time the device was seen on the network.
`devices.os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`devices.devicelabel`	string	`Sarah Development`	An optional label applied to the device in the Device Admin page.
`devices.typename`	string	`desktop`	The device type in system format.
`devices.typelabel`	string	`Desktop`	The device type in readable format.
`devices.tags`	array		An object describing tags applied to the device.
`devices.tags.tid`	numeric	`73`	The “tag id”. A unique value.
`devices.tags.expiry`	numeric	`0`	The expiry time for the tag when applied to a device.
`devices.tags.thid`	numeric	`78`	The “tag history” id. Increments if the tag is edited.
`devices.tags.name`	string	`Test Tag`	The tag label displayed in the user interface or in objects that reference the tag.

Response Field	Type	Example Value	Description
`devices.tags.restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`devices.tags.data`	object		An object containing information about the tag.
`devices.tags.data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`devices.tags.data.color`	numeric	`134`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`devices.tags.data.description`	string	`Testing the use of tags.`	An optional description summarizing the purpose of the tag.
`devices.tags.data.visibility`	string	`Public`	A system field.
`devices.tags.isReferenced`	boolean	`FALSE`	Whether the tag is used by one or more model components.

Example Response

Request: /devicesearch?&query="sarah"

```
{
  "totalCount": 2185,
  "devices": [
    {
      "id": 316,
      "ip": "10.0.56.12",
      "ips": [
        {
          "ip": "10.0.56.12",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 23
        }
      ],
      "did": 316,
      "sid": 23,
      "hostname": "Sarah Development",
      "firstseen": 1528807092000,
      "lastseen": 1581510431000,
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    {
      "id": 2719,
      "ip": "192.168.120.39",
      "ips": [
        {
          "ip": "192.168.120.39",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 6
        }
      ],
      "did": 2719,
      "sid": 6,
      "hostname": "sarah's iphone",
      "firstSeen": 1576581851000,
      "lastSeen": 1582131590000,
      "os": "Mac OS X",
      "typename": "mobile",
      "typelabel": "Mobile",
      "tags": [
        {
          "tid": 17,
          "expiry": 0,
          "thid": 17,
          "name": "iOS device",
          "restricted": false,
          "data": {
            "auto": false,
            "color": 181,
            "description": "",
            "visibility": "Public"
          },
          "isReferenced": true
        }
      ]
    }
  ]
}
```

/endpointdetails

`/endpointdetails` returns location, IP address and (optionally) device connection information for external IPs and hostnames. It can be used to return intel about endpoints and the devices that have been seen accessing them.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`additionalinfo`	boolean	Return additional information about the endpoint.
`devices`	boolean	Return a list of devices which have recently connected to the endpoint.
`score`	boolean	Return rarity data for this endpoint.
`hostname`	string	Return data for this hostname.
`ip`	string	Return data for this ip address.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.
`score`	boolean	Return rarity data for this endpoint.

Notes

- The “popularity” score = 100 – (IP or domain) rarity score.
- For hostname queries, `additionalinfo=true` will add an `ips` object and a `locations` object with details of the IP addresses Darktrace has seen associated with the hostname and the physical locations of those IPs where derivable.
- Queries for IPs that are internal (or treated as such) will return `"name": "internal_ip",` in the response and different key/value fields.

Example Request

1. `GET` details for 8.8.8.8:

```
https://<applianceIP>/endpointdetails?ip=8.8.8.8
```

2. `GET` details for darktrace.com, including a list of devices that have connected to it:

```
https://<applianceIP>/endpointdetails?hostname=darktrace.com&devices=true
```

Example Response

Request: /endpointdetails?hostname=darktrace.com&devices=true

```
{
  "hostname": "darktrace.com",
  "firsttime": 1528807217000,
  "devices": [
    {
      "did": 316,
      "ip": "10.0.56.12",
      "ips": [
        {
          "ip": "10.0.56.12",
          "timems": 1581508800000,
          "time": "2020-02-12 12:00:00",
          "sid": 23
        }
      ],
      "sid": 23,
      "hostname": "Sarah Development",
      "firstSeen": 1528807078000,
      "lastSeen": 1581960902000,
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop"
    },
    ...
  ]
```

Response is abbreviated.

/endpointdetails Response Schema

Response Schema - `ip=[external IP]`

`devices=false`

Response Field	Type	Example Value	Description
`ip`	string	`8.8.8.8`	The IP being queried.
`firsttime`	numeric	`1528810000000`	The first time the queried IP was seen on the network in epoch time.
`country`	string	`United States`	The country that the IP is located in.
`asn`	string	`AS15169 Google LLC`	The ASN for the IP.
`city`	string		If available, the city the IP is located in.
`region`	string	`North America`	The geographical region the IP is located in.
`name`	string		If an internal IP, this field will return “internal_ip”
`longitude`	numeric	`-97.822`	For the reported IP location, the longitude value to plot the IP on a map.
`latitude`	numeric	`37.751`	For the reported IP location, the latitude value to plot the IP on a map.

Example Response

```
{
  "ip": "172.217.169.36",
  "firsttime": 1528807105000,
  "country": "United States",
  "asn": "AS15169 Google LLC",
  "city": "",
  "region": "North America",
  "name": "",
  "longitude": -97.822,
  "latitude": 37.751
}
```

`devices=true`

Response Field	Type	Example Value	Description
`ip`	string	`8.8.8.8`	The IP being queried.
`firsttime`	numeric	`1586937600000`	The first time the queried IP was seen on the network in epoch time.
`country`	string	`United States`	The country that the IP is located in.
`asn`	string	`AS15169 Google LLC`	The ASN for the IP.
`city`	string		If available, the city the IP is located in.
`region`	string	`North America`	The geographical region the IP is located in.

Response Field	Type	Example Value	Description
name	string		If an internal IP, this field will return “internal_ip”
longitude	numeric	-97.822	For the reported IP location, the longitude value to plot the IP on a map.
latitude	numeric	37.751	For the reported IP location, the latitude value to plot the IP on a map.
devices	array		An array of devices that have been seen connecting to the IP.
devices.did	numeric	228	The “device id”, a unique identifier.
devices.ip	string	10.12.14.2	The current IP associated with the device.
devices.ips	array		IPs associated with the device historically.
devices.ips.ip	string	10.12.14.2	A historic IP associated with the device.
devices.ips.timems	numeric	1586937600000	The time the IP was last seen associated with that device in epoch time.
devices.ips.time	string	2020-04-15 08:00:00	The time the IP was last seen associated with that device in readable format.
devices.ips.sid	numeric	14	The subnet id for the subnet the IP belongs to.
devices.sid	numeric	14	The subnet id for the subnet the device is currently located in.
devices.hostname	string	ws83	The current device hostname.
devices.firstSeen	numeric	1582720000000	The first time the device was seen on the network.
devices.lastSeen	numeric	1584990000000	The last time the device was seen on the network.
devices.os	string	Windows NT kernel	The device operating system if Darktrace is able to derive it.
devices.typename	string	desktop	The device type in system format.
devices.typelabel	string	Desktop	The device type in readable format.

Example Response

```
{
  "ip": "172.217.169.36",
  "firsttime": 1528807105000,
  "country": "United States",
  "asn": "AS15169 Google LLC",
  "city": "",
  "region": "North America",
  "name": "",
  "longitude": -97.822,
  "latitude": 37.751,
  "devices": [
    {
      "did": 3870,
      "macaddress": "56:2d:4b:9c:18:42",
      "vendor": "LCFC(HeFei) Electronics Technology co., ltd",
      "ip": "10.0.18.224",
      "ips": [
        {
          "ip": "10.0.18.224",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 17
        }
      ],
      "sid": 17,
      "firstSeen": 1564064256000,
      "lastSeen": 1587137042000,
      "os": "Windows NT kernel",
      "typename": "desktop",
      "typelabel": "Desktop"
    }
  ]
}
```

Response Schema - `hostname`

`devices=false`

Response Field	Type	Example Value	Description
`hostname`	string	`darktrace.com`	The hostname being queried.
`firsttime`	numeric	`1528810000000`	The first time the queried hostname was seen on the network in epoch time.

Example Response

```
{
  "hostname": "darktrace.com",
  "firsttime": 1528807217000
}
```

`devices=true`

Response Field	Type	Example Value	Description
`hostname`	string	`darktrace.com`	The IP being queried.

Response Field	Type	Example Value	Description
`firsttime`	numeric	`1528810000000`	The first time the queried IP was seen on the network in epoch time.
`devices`	array		An array of devices that have connected to this endpoint.
`devices.did`	numeric	`227`	The “device id”, a unique identifier.
`devices.ip`	string	`10.0.18.224`	The current IP associated with the device.
`devices.ips`	array		IPs associated with the device historically.
`devices.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`devices.ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`devices.ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`devices.ips.sid`	numeric	`10`	The subnet id for the subnet the IP belongs to.
`devices.sid`	numeric	`10`	The subnet id for the subnet the device is currently located in.
`devices.hostname`	string	`sarah-desktop-12`	The current device hostname.
`devices.firstSeen`	numeric	`1528810000000`	The first time the device was seen on the network.
`devices.lastSeen`	numeric	`1585310000000`	The last time the device was seen on the network.
`devices.os`	string	`Windows NT kernel`	The device operating system if Darktrace is able to derive it.
`devices.typename`	string	`desktop`	The device type in system format.
`devices.typelabel`	string	`Desktop`	The device type in readable format.

Example Response

```
{
  "hostname": "darktrace.com",
  "firsttime": 1528807217000,
  "devices": [
    {
      "did": 3870,
      "macaddress": "56:2d:4b:9c:18:42",
      "vendor": "LCFC(HeFei) Electronics Technology co., ltd",
      "ip": "10.0.18.224",
      "ips": [
        {
          "ip": "10.0.18.224",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 17
        }
      ],
      "sid": 17,
      "firstSeen": 1564064256000,
      "lastSeen": 1587137042000,
      "os": "Windows NT kernel",
      "typename": "desktop",
      "typelabel": "Desktop"
    }
  ]
}
```

Response Schema - `ip=[internal IP]`

`devices=false`

Response Field	Type	Example Value	Description
`subnetlabel`	string	`Finance`	The label assigned to the subnet in the Threat Visualizer that the IP is contained within.
`subnetid`	string	`18`	A unique “subnet id” for the subnet that the IP is contained within.
`subnetnetwork`	string	`10.0.18.0/24`	The IP address range that describes the subnet that the IP is contained within.
`country`	string		The country that the IP is located in.
`city`	string		If available, the city the IP is located in.
`region`	string		The geographical region the IP is located in.
`name`	string	`internal_ip`	If an internal IP, this field will return “internal_ip”
`longitude`	numeric	`-0.01`	The longitude value provided to Subnet Admin which is used to plot the subnet on a map.
`latitude`	numeric	`0.01`	The latitude value provided to Subnet Admin which is used to plot the subnet on a map.

Example Response

```
{
  "subnetlabel": "",
  "subnetid": "19",
  "subnetnetwork": "10.160.14.0/24",
  "country": "",
  "city": "",
  "region": "",
  "name": "internal_ip",
  "longitude": 0.0,
  "latitude": 0.0
}
```

`devices=true`

Response Field	Type	Example Value	Description
`subnetlabel`	string	`Finance`	The label assigned to the subnet in the Threat Visualizer that the IP is contained within.
`subnetid`	string	`18`	A unique “subnet id” for the subnet that the IP is contained within.
`subnetnetwork`	string	`10.0.18.0/24`	The IP address range that describes the subnet that the IP is contained within.
`country`	string		The country that the IP is located in.

Response Field	Type	Example Value	Description
city	string		If available, the city the IP is located in.
region	string		The geographical region the IP is located in.
name	string	internal_ip	If an internal IP, this field will return "internal_ip"
longitude	numeric	-0.01	The longitude value provided to Subnet Admin which is used to plot the subnet on a map.
latitude	numeric	0.01	The latitude value provided to Subnet Admin which is used to plot the subnet on a map.
devices	array		An array of devices that have connected to the IP.
devices.did	numeric	228	The "device id", a unique identifier.
devices.ip	string	10.12.14.2	The current IP associated with the device.
devices.ips	array		IPs associated with the device historically.
devices.ips.ip	string	10.12.14.2	A historic IP associated with the device.
devices.ips.timems	numeric	1586937600000	The time the IP was last seen associated with that device in epoch time.
devices.ips.time	string	2020-04-15 08:00:00	The time the IP was last seen associated with that device in readable format.
devices.ips.sid	numeric	14	The subnet id for the subnet the IP belongs to.
devices.sid	numeric	14	The subnet id for the subnet the device is currently located in.
devices.hostname	string	ws83	The current device hostname.
devices.firstSeen	numeric	1582720000000	The first time the device was seen on the network.
devices.lastSeen	numeric	1584990000000	The last time the device was seen on the network.
devices.os	string	Windows NT kernel	The device operating system if Darktrace is able to derive it.
devices.typename	string	desktop	The device type in system format.
devices.typelabel	string	Desktop	The device type in readable format.

Example Response

```
{
  "subnetlabel": "",
  "subnetid": "19",
  "subnetnetwork": "10.160.14.0/24",
  "country": "",
  "city": "",
  "region": "",
  "name": "internal_ip",
  "longitude": 0.0,
  "latitude": 0.0
  "devices": [
    {
      "did": 3870,
      "macaddress": "56:2d:4b:9c:18:42",
      "vendor": "LCFC(HeFei) Electronics Technology co., ltd",
      "ip": "10.0.18.224",
      "ips": [
        {
          "ip": "10.0.18.224",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 17
        }
      ],
      "sid": 17,
      "firstSeen": 1564064256000,
      "lastSeen": 1587137042000,
      "os": "Windows NT kernel",
      "typename": "desktop",
      "typelabel": "Desktop"
    }
  ]
}
```

/enums

The `/enums` endpoint returns the corresponding string values for numeric codes (enumerated types) used in many API responses.

The list of enums can be filtered using any of the following extensions:

- /applicationprotocols
- /countries
- /destinationdevicetypes
- /protocols
- /sourcedevicetypes

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- As `responsedata` only accepts keys from the top-level, we recommend using an extension in order to access enum type fields.

Example Request

1. `GET` a list of all enumerated types:

```
https://<applianceIP>/enums
```

2. `GET` a list of all enumerated country types:

```
https://<applianceIP>/enums/countries
```

Example Response

Request: /enums

```
[
  {
    "code": "0",
    "name": "None",
    "hidden": true
    "code": "1",
    "name": "Unknown"
  },
  {
    "code": "2",
    "name": "Laptop"
  },
  {
    "code": "3",
    "name": "Mobile"
  },
  ...
]
```

Response is abbreviated.

/enums Response Schema

Response Schema

Response Field	Type	Example Value	Description
`Country`	array		An array of countries and their corresponding system codes.
`Country.code`	string	`AD`	The country code.
`Country.name`	string	`Andorra`	The readable country name.
`Matching metrics`	array		An array of standard metrics used throughout the Threat Visualizer interface. The standard metrics available in your environment may differ from this list due to additional protocols seen or additional modules contributing data.
`Matching metrics.code`	string	`activeconnections`	The system name for the metric.
`Matching metrics.name`	string	`Active Connections`	The readable metric name.
`Proxied connection`	array		Boolean values for whether the connection was proxied.
`Proxied connection.code`	string	`TRUE`	The system code for the boolean.
`Proxied connection.name`	string	`TRUE`	The readable representation of the boolean.
`Trusted hostname`	array		Boolean values for whether the hostname is trusted.
`Trusted hostname.code`	string	`TRUE`	The system code for the boolean.
`Trusted hostname.name`	string	`TRUE`	The readable representation of the boolean.
`Day of the week`	array		An array of days of the week.
`Day of the week.code`	string	`Sunday`	The system name for the day.
`Day of the week.name`	string	`Sunday`	The readable day of the week.
`System message`	array		An array of system messages that may be fired as notices.
`System message.code`	string	`IP range excluded`	The system message code.
`System message.name`	string	`IP range excluded`	The system message text.
`Internal source device type`	array		An array of device types that an internal source device may be identified as.
`Internal source device type.code`	string	`2`	The system code for the device type.
`Internal source device type.name`	string	`Laptop`	The readable device type.
`Internal destination device type`	array		An array of device types that an internal destination device may be identified as.
`Internal destination device type.code`	string	`2`	The system code for the device type.
`Internal destination device type.name`	string	`Laptop`	The readable device type.
`Protocol`	array		An array of network protocols that may be identified within the network.
`Protocol.code`	string	`1`	The system code for the protocol.
`Protocol.name`	string	`ICMP`	The readable protocol name.

Response Field	Type	Example Value	Description
`Application protocol`	array		An array of application protocols that may be identified within the network.
`Application protocol.code`	string	`1053`	The system code for the protocol.
`Application protocol.name`	string	`BITTORRENT`	The readable protocol name.
`Malformed traffic type`	array		An array of types of malformed traffic which may be detected in the traffic fed to Darktrace, and their corresponding system codes.
`Malformed traffic type.code`	string	`bad_HTTP_reply`	The system code for the traffic type.
`Malformed traffic type.name`	string	`Bad HTTP reply`	The readable traffic type.
`Vendor`	array		An array of network card vendors and their corresponding system codes.
`Vendor.code`	string	`-16579579`	The system code for the vendor.
`Vendor.name`	string	`Cisco Systems, Inc`	The actual vendor name.

Example Response

```
{
  "Country": [
    {
    "code": "0",
    "name": "Unknown"
    }
    ...
  ]
  "Matching metrics": [
    {
    "code": "activeconnections",
    "name": "Active Connections"
    },
...
```

Response is abbreviated.

/filtertypes

`/filtertypes` returns all internal Darktrace filters used in the Model Editor, their filter type (for example, boolean or numeric) and the available comparators.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` a list of all filter types:

```
https://<applianceIP>/filtertypes
```

Example Response

Request: /filtertypes

```
[
  ...
  {
    "filtertype": "Data ratio",
    "valuetype": "numeric",
    "comparators": [
     "<",
     "<=",
     "=",
     "!=",
     ">=",
     ">"
    ]
   },
   {
    "filtertype": "Tagged internal destination",
    "valuetype": "id",
    "comparators": [
     "has tag",
     "does not have tag"
    ]
   },
   {
    "filtertype": "Tagged internal source",
    "valuetype": "id",
    "comparators": [
     "has tag",
     "does not have tag"
    ]
   },
   {
    "filtertype": "HTTP no referrer",
    "valuetype": "flag",
    "comparators": [
     "is"
    ]
   }
  ...
]
```

Response is abbreviated.

/filtertypes Response Schema

Response Schema

Response Field	Type	Example Value	Description
`filtertype`	string	`Destination IP`	The filter name.
`valuetype`	string	`ipv4`	The data type expected by the filter.
`graphable`	boolean	`TRUE`	Optional field. Will return as “true” if the filter can be used on a graph.
`comparators`	array	`matches`	The comparators available when creating model components or filtering using the filtertype.

Example Response

Request: /filtertypes

```
[
  {
      "filtertype": "Product",
      "valuetype": "string",
      "comparators": [
        "matches",
        "does not match",
        "contains",
        "does not contain",
        "matches regular expression",
        "does not match regular expression",
        "is longer than",
        "is shorter than"
      ]
    },
    {
      "filtertype": "Volume Size",
      "valuetype": "numeric",
      "comparators": [
        "<",
        "<=",
        "=",
        "!=",
        ">=",
        ">"
      ]
    },
    ...
```

Response is abbreviated.

/intelfeed

`/intelfeed` is the programmatic way to access Watched Domains, a list of domains, IPs and hostnames utilized by the Darktrace system, Darktrace Inoculation and STIXX/TAXII integration to create model breaches.

Watched domains are categorized by sources: if no source is specified in a request, the source string will be set to “default”. Multiple watched domains can be added and removed in one request.

`POST` requests to this endpoint must be made with parameters.

Request Type(s)

`[GET]` `[POST]`

Parameters

Parameter	Type	Description
`addentry`	string	Add an external domain, hostname or IP address. Available for POST requests.
`addlist`	string	Add a new line or comma separated list of external domains, hostnames and IP addresses. Available for POST requests.
`description`	string	Provide a description for added entries. The description must be under 256 characters. Available for POST requests
`expiry`	string	Set an expiration time for added items. Available for POST requests
`hostname`	boolean	Set to true to treat the added items as hostnames rather than domains. Available for POST requests.
`removeall`	boolean	Remove all external domains, hostnames and IP addresses.
`removeentry`	string	Remove an external domain, hostname or IP address.
`source`	string	Provide a source for added entries or restrict a retrieved list of entries to a particular source. A source is a textual label used to manage multiple lists of entities. Sources must be under 64 characters in length. The source of a watched endpoint entry can be used as a filter in models. A single entry can belong to any number of sources. Available for POST requests.
`sources`	boolean	Return the current set of sources rather than the list of watched endpoint/intelfeed entries.
`fulldetails`	boolean	Return full details about expiry time and description for each entry.
`iagn`	boolean	Enables automatic Antigena Network actions against the endpoint. Available for POST requests.

Notes

- The `removeall` and `addlist` parameters can be used together
- When supplying a description, do not use quotes around the string - this will result in a double-quoted string.
- Hostnames can be supplied using the `hostname=true` parameter. Hostnames will be treated as exact values and are indicated on the Watched Domains list with a `*`.
- The `removeall` parameter will remove **all** watched domain entries, regardless of source.

Example Request

1. `GET` the intelfeed list for the default source:

```
https://<applianceIP>/intelfeed
```

2. **GET** a list of sources for entries on the intelfeed list:

```
https://<applianceIP>/intelfeed?sources=true
```

3. **GET** the intel feed list for all entries under the 'CustomSet1' source:

```
https://<applianceIP>/intelfeed?source=CustomSet1
```

4. **POST** a new entry to the intel feed (example.com) with description 'Test' and source 'test'

```
https://<applianceIP>/intelfeed -d addentry=example-agn.com&description=test&source=test
```

5. **POST** a list of entries to the intel feed with the source "ThreatIntel" and the entry description "Test"

```
https://<applianceIP>/intelfeed -d
addlist=example1.com,example2.com,example3.com,example4.com&description=Test&source=Threat
Intel
```

Example Response

Request: /intelfeed?fulldetails=true

```
[
  {
    "name": "example.net",
    "description": "Test"
    "expiry": "2020-04-03 15:23:20"
  },
  ...
]
```

Response is abbreviated.

/intelfeed Response Schema

Response Schema

The response will be an array of domains.

Example Response

Request: /intelfeed

```
[
  "example1.com",
  "example2.com",
  "0.0.0.0"
]
```

Response Schema - `fulldetails=true`

Response Field	Type	Example Value	Description
`name`	string	`example1.com`	The domain, IP or hostname on the watch list.
`description`	string	`Example description.`	An optional description of why the entry has been added.
`expiry`	string	`2020-12-31T12:00:00`	An option expiry time at which the entry will be removed from the list.

Example Response

Request: /intelfeed&fulldetails=true

```
[
  {
    "name": "example1.com",
    "description": "Test"
  },
  {
    "name": "example2.com",
    "description": "Test"
  },
  {
    "name": "example3.com",
    "description": "Test"
  },
  {
    "name": "example4.com",
    "description": "Test"
  },
  {
    "name": "example5.com",
    "expiry": "2020-04-03 15:23:20"
  }
]
```

Response Schema - `sources=true`

The response will be an array of sources.

Example Response

Request: /intelfeed?sources=true

```
[
  "Default",
  "Test",
  "ThreatIntel"
]
```

/mbcomments

The `/mbcomments` endpoint returns all comments across model breaches, or for a specific model breach.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.
`count`	numeric	The number of comments to return. Only limits the number of comments within the specified timeframe.
`pbid`	numeric	Only return comments for the model breach with the specified ID.

Notes

- If not supplied, `count` will default to 100.

Example Request

1. `GET` all comments on model breaches on August 19th 2020:

```
https://<applianceIP>/mbcomments?starttime=1597795200000&endtime=1597881599000
```

2. `GET` all comments for a model breach with `pbid=123` :

```
https://<applianceIP>/mbcomments?pbid=123
```

Example Response

Request: /mbcomments

```
[
  {
    "time": 1597837975000,
    "pbid": 1432,
    "username": "lryan",
    "message": "Investigation completed",
    "pid": 17,
    "name": "Compliance::Messaging::Facebook Messenger"
  },
  {
    "time": 1586937600000,
    "pbid": 1329,
    "username": "ajohnston",
    "message": "Concerning behavior. Investigating possible compromise.",
    "pid": 52,
    "name": "Anomalous File::Masqueraded File Transfer"
  }
]
```

/mbcomments Response Schema

Response Schema

Response Field	Type	Example Value	Description
`time`	numeric	`1597837975000`	The comment text.
`pbid`	numeric	`1432`	The user who made the comment.
`username`	string	`lryan`	The time the comment was posted in epoch time.
`message`	string	`Investigation completed.`	The “policy breach ID” of the model breach commented on.
`pid`	numeric	`17`	The “policy id” of the model breach that was commented on.
`name`	string	`Compliance::Messaging::Facebook Messenger`	Name of the model that was breached.

Example Response

```
[
  {
    "time": 1597837975000,
    "pbid": 1432,
    "username": "lryan",
    "message": "Investigation completed",
    "pid": 17,
    "name": "Compliance::Messaging::Facebook Messenger"
  },
  {
    "time": 1586937600000,
    "pbid": 1329,
    "username": "ajohnston",
    "message": "Concerning behavior. Investigating possible compromise.",
    "pid": 52,
    "name": "Anomalous File::Masqueraded File Transfer"
  }
]
```

/metricdata

The `/metricdata` endpoint returns time series data for one or more metrics for a device. This information is shown in the Threat Visualizer when the ‘Open Graph’ button is clicked after searching for a device in the Omnisearch bar.

To specify a `metric`, use the system name - the `name` field found on `/metrics` - rather than the label. For example, when using the metric “External Data Transfer” (`mlid=1`), the system name “externaldatatransfervolume” must be specified in the query.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`applicationprotocol`	string	This filter can be used to filter the returned data by application protocol. See /enums for the list of application protocols.
`breachtimes`	boolean	Return additional information for the model breach times for the device.
`ddid`	numeric	Identification number of a destination device modelled in the Darktrace system to restrict data to.
`destinationport`	numeric	This filter can be used to filter the returned data by destination port.
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`interval`	numeric	Time interval size to group data into in seconds. The maximum value for any interval is returned.
`metric`	string	Name of a metric. See `/metrics` for the full list of current metrics.
`odid`	numeric	Other Device ID - Identification number of a device modelled in the Darktrace system to restrict data to. Typically used with ddid to specify device pairs.
`port`	numeric	This filter can be used to filter the returned data by source or destination port.
`protocol`	string	This filter can be used to filter the returned data by IP protocol. See /enums for the list of protocols.)
`sourceport`	numeric	This filter can be used to filter the returned data by source port.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.

Notes

- Time parameters must always be specified in pairs.
- To specify multiple metrics to return time-series data for, replace the `metric` parameter with `metric1=`, `metric2=`, etc. Multiple metric objects will then be returned.
- The `interval` value allows data to be grouped into wider ‘bars’ for time-series graphs. The default interval is 1 minute (`interval=60`).
- `breachtimes=true` will return any model breaches that happened within the timeframe on the device or within the subnet specified. This parameter will alter the structure of the returned data.

Example Request

1. `GET` all connections for the device with `did=1` for 20th March 2020 at an interval of 1 hour:

```
https://<applianceIP>/metricdata?
did=1&metric=connections&from=2020-03-20T00:00:00&to=2020-03-20T23:59:59&interval=3600
```

2. `GET` the number of TCP connections from the device with `did=1` to the device with `did=18` between 9am and 10am for 20th March 2020 at an interval of 5 minutes:

```
https://<applianceIP>/metricdata?
metric=internalconnections&startTime=1584694800000&endTime=1584698400000&did=1&&ddid=18&pr
otocol=6&interval=300
```

Example Response

Request: /metricdata?metric=externalconnections&startTime=1582900189000&endTime=1582921789000&did=1&interval=60&breachtimes=true

```
[
  {
    "breachtimes": [
      {
        "pid": 341,
        "pbid": 292504,
        "score": 0.6043,
        "name": "Compromise::Sustained SSL or HTTP Increase",
        "time": 1582902068000
      },
      ...
    ]
  },
  {
    "metric": "externalconnections",
    "data": [
      {
        "time": "2020-02-28 14:29:00",
        "timems": 1582900140000,
        "size": 14,
        "in": 0,
        "out": 14
      },
      {
        "time": "2020-02-28 14:30:00",
        "timems": 1582900200000,
        "size": 18,
        "in": 0,
        "out": 18
      },
    ]
  }
]
```

Response is abbreviated.

/metricdata Response Schema

Response Schema

Response Field	Type	Example Value	Description
`metric`	string	`connections`	The metric data is returned for.
`data`	array		A list of time series data for the metric.
`data.time`	string	`24/03/2019 00:00`	A timestamp in readable format for the data. Time series data is grouped by intervals.
`data.timems`	numeric	`1550000000000`	A timestamp in epoch time for the data. Time series data is grouped by intervals.
`data.size`	numeric	`12`	The total size of the data (in and out).
`data.in`	numeric	`1`	The number of inbound events or the total amount of inbound data (metric-dependent) seen during the time interval.
`data.out`	numeric	`11`	The number of outbound events or the total amount of outbound data (metric-dependent) seen during the time interval.

Example Response

Request: /metricdata?metric=connections&did=1

```
[
  {
    "metric": "connections",
    "data": [
      {
        "time": "2020-02-28 14:29:00",
        "timems": 1582900140000,
        "size": 14,
        "in": 0,
        "out": 14
      },
      {
        "time": "2020-02-28 14:30:00",
        "timems": 1582900200000,
        "size": 18,
        "in": 0,
        "out": 18
      },
      ...
    ]
  }
]
```

Response is abbreviated.

Response Schema - `breachtimes=true`

Response Field	Type	Example Value	Description
`breachtimes`	array		An array of model breaches seen on the device or subnet during the time window provided.

Response Field	Type	Example Value	Description
`breachtimes.pid`	numeric	`341`	The “policy id” of the model that was breached.
`breachtimes.pbid`	numeric	`292504`	The “policy breach ID” of the model breach.
`breachtimes.score`	numeric	`0.6043`	The model breach score, represented by a value between 0 and 1.
`breachtimes.name`	string	`Compromise::Sustained SSL or HTTP Increase`	Name of the model that was breached.
`breachtimes.time`	numeric	`1583310000000`	The timestamp when the record was created in epoch time.
`metric`	string	`connections`	The metric data is returned for.
`data`	array		A list of time series data for the metric.
`data.time`	string	`2020-03-15 09:52:11`	A timestamp in readable format for the data. Time series data is grouped by intervals.
`data.timems`	numeric	`1584265931000`	A timestamp in epoch time for the data. Time series data is grouped by intervals.
`data.size`	numeric	`9`	The total size of the data (in and out).
`data.in`	numeric	`0`	The number of inbound events or the total amount of inbound data (metric-dependent) seen during the time interval.
`data.out`	numeric	`9`	The number of outbound events or the total amount of outbound data (metric-dependent) seen during the time interval.

Example Response

Request: /metricdata?metric=connections&breachtimes=true&did=1

```
[
  {
    "breachtimes": [
      {
        "pid": 341,
        "pbid": 292504,
        "score": 0.6043,
        "name": "Compromise::Sustained SSL or HTTP Increase",
        "time": 1582902068000
      },
      ...
    ]
  },
  {
    "metric": "connections",
    "data": [
      {
        "time": "2020-02-28 14:29:00",
        "timems": 1582900140000,
        "size": 14,
        "in": 0,
        "out": 14
      },
      {
        "time": "2020-02-28 14:30:00",
        "timems": 1582900200000,
        "size": 18,
        "in": 0,
        "out": 18
      },
    ]
  }
]
```

Response is abbreviated.

/metrics

This endpoint returns the list of metrics available for filtering other API calls and for use in model making.

See metrics for definitions of a subset of standard metrics available for model editing.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- Metrics with a `set` value of “C” are used for visual analysis and are not available for model making.

Example Request

1. `GET` a list of all metrics available for models:

```
https://<applianceIP>/metrics
```

2. `GET` information about the metric “Internal Data Transfer”:

```
https://<applianceIP>/metrics/4
```

Example Response

Request: /metrics/13

```
{
  "mlid": 13,
  "name": "multicasts",
  "label": "Multicasts",
  "units": "",
  "filtertypes": [
    "Feature model",
    "Process popularity",
    "Destination IP",
    "Protocol",
    "Source port",
    "Destination port",
    "Same port",
    "Application protocol",
    "Internal source device type",
    "Internal source",
    "New connection",
    "Unusual connectivity",
    "Unusual incoming data volume",
    "Unusual outgoing data volume",
    "Unusual number of connections",
    "Unusual sustained connectivity for group",
    "Unusual individual connection for group",
    "Unique ports",
    "Time since first connection",
    "Day of the week",
    "Hour of the day"
  ],
  "unitsinterval": 3600,
  "lengthscale": 9999960
}
```

/metrics Response Schema

Response Schema

Response Field	Type	Example Value	Description
`mlid`	numeric	`1`	The “metric logic” id - unique identifier.
`name`	string	`externalconnections`	The metric which data is returned for in system format.
`label`	string	`External Connections`	The metric which data is returned for in readable format.
`units`	string		The units the metric is measured in, if applicable.
`filtertypes`	array	`Direction`	An array of filters which can be used with this metric.
`unitsinterval`	numeric	`3600`	The default time interval for the metric.
`lengthscale`	numeric	`9999960`	A system field.

Example Response

```
[
  {
    "mlid": 4,
    "name": "internaldatatransfervolume",
    "label": "Internal Data Transfer",
    "set": "A",
    "units": "bytes",
    "filtertypes": [
      "Feature model",
      "DNS host lookup",
      "Process popularity",
       ...
    ],
    "unitsinterval": 3600,
    "lengthscale": 9999960
  },
  ...
]
```

Response is abbreviated.

/models

The `/models` endpoint returns a list of all models that currently exist on the Threat Visualizer, including custom models and de-activated models. The returned JSON does not contain full model logic - this can be sourced from the `/components` endpoint using the numerical values in the `data` array as `cid` 's.

This endpoint only supports filtering on the `uuid` parameter. To search for models by any other attribute, the full list must be returned and parsed.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`uuid`	string	All models have a uuid and a pid. The uuid (universally unique identifier) is a 128-bit hexadecimal number.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` a list of all models:

```
https://<applianceIP>/models
```

2. `GET` the model “Anomalous File / Anomalous Octet Stream”:

```
https://<applianceIP>/models?uuid=80010119-6d7f-0000-0305-5e0000000420
```

```
https://<applianceIP>/models/12
```

Example Response

```
{
  "name": "Compliance::File Storage::Dropbox",
  "pid": 130,
  "phid": 5198,
  "uuid": "80010119-6d7f-0000-0305-5e0000000268",
  "logic": {
      "data": [
        {
          "cid": 8977,
          "weight": 9
        },
        {
          "cid": 8978,
          "weight": 1
        },
        {
          "cid": 8976,
          "weight": 1
        }
      ],
      "targetScore": 10,
      "type": "weightedComponentList",
      "version": 1
    },
  "throttle": 86400,
  "sharedEndpoints": false,
  "actions": {
      "alert": true,
      "antigena": {},
      "breach": true,
      "model": true,
      "setPriority": false,
      "setTag": false,
      "setType": false
    },
  "tags": [
      "AP: Egress"
    ],
  "interval": 300,
  "sequenced": false,
  "active": true,
  "modified": "2019-02-19 04:34:12",
  "activeTimes": {
      "devices": {},
      "tags": {},
      "type": "exclusions",
      "version": 2
    },
  "priority": 0,
  "autoUpdatable": true,
  "autoUpdate": true,
  "autoSuppress": false,
  "description": "A device is using an external third party file storage platform.\\n\\nAction:
Investigate if the device has been downloading data from any internal systems prior to the upload
and whether the storage platform should be used for business purposes.",
  "behaviour": "decreasing",
  "created": {
      "by": "Unknown"
    },
  "edited": {
      "by": "System"
    },
  "history": [
      {
        "modified": "2019-02-19 04:34:12",
        "active": true,
        "message": "Adding components to give more details for easier triage",
        "by": "System",
        "phid": 5198
      },
      {
        "modified": "2018-08-16 14:15:27",
        "active": false,
        "message": "Updated to a meta model to enable more flexible alerting
        options",
        "by": "System",
        "phid": 4349
      },
    ],
  "message": "Adding components to give more details for easier triage",
  "version":18
}
```

/models Response Schema

Response Schema

Response Field	Type	Example Value	Description
name	string	Anomalous File::Anomalous Octet Stream	The name of the model.
pid	numeric	12	The “policy id” of the model.
phid	numeric	2842	The model “policy history” id. Increments when the model is modified.
uuid	string	80010119-6d7f-0000-0305-5e0000000420	A unique ID that is generated on creation of the model.
logic	object		A data structure that describes the conditions to bring about a breach.
logic.data	array	3621	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
logic.type	string	componentList	The type of model.
logic.version	numeric	1	A number representing the version of model logic.
throttle	numeric	3600	For an individual device, this is the value in seconds for which this model will not fire again.
sharedEndpoints	boolean	FALSE	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
actions	object		The action to perform as a result of matching this model firing.
actions.alert	boolean	TRUE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
actions.antigena	object		An object containing the antigena response to be applied as a result of the model breaching.
actions.breach	boolean	TRUE	If true, generates a model breach that will appear in the threat tray.
actions.model	boolean	TRUE	If true, creates an event in the device’s event log without creating an alert/ model breach in the threat tray.
actions.setPriority	boolean	FALSE	If no priority change action, a false boolean. If the priority is to be changed on breach, the numeric value it should become.
actions.setTag	boolean	FALSE	If no tag action, a false boolean. If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied.

Response Field	Type	Example Value	Description
actions.setType	boolean	FALSE	If no change device type action is applied to the model, a false boolean. If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied.
tags	array	AP: Tooling	DNS Server
interval	numeric	0	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
sequenced	boolean	FALSE	Whether the components are required to fire in the specified order for the model breach to occur.
active	boolean	TRUE	Whether the model is enabled or disabled.
modified	string	2020-03-15 09:52:11	The time in UTC at which the model was last modified.
activeTimes	object		An object describing device whitelisting or blacklisting configured for this model.
activeTimes.devices	object		The device ids for devices on the list.
activeTimes.tags	object		A system field.
activeTimes.type	string	exclusions	The type of list: “restrictions” indicates a blacklist, “exclusions” a whitelist.
activeTimes.version	numeric	2	A system field.
priority	numeric	2	The model’s priority affects the strength with which it breaches (0-5 scale).
autoUpdatable	boolean	FALSE	Whether the model is suitable for auto update.
autoUpdate	boolean	TRUE	Whether the model is enabled for auto update.
autoSuppress	boolean	TRUE	Whether the model will automatically be suppressed in the case of over-breaching.
description	string	A device has downloaded a rare data stream which is not specifying a specific data type. \n\nAction: Investigate the endpoint the data is being sent from and consider downloading a PCAP or reviewing the hash if you believe the endpoint to be untrustworthy.	The optional description of the model.
behaviour	string	decreasing	The score modulation function as set in the editor.
defeats	array		A system field.
created	object		An object describing the creation of the model.

Response Field	Type	Example Value	Description
`created.by`	string	`smartinez_admin`	Username that created the model.
`edited`	object		User ID that created the model.
`edited.by`	string	`ajohnston`	Username that last edited the model.
`edited.userID`	numeric	`24`	User ID that last edited the model.
`history`	array		An object describing the edit history of the model.
`history.modified`	string	`15/11/2019 11:42`	The last modified date in UTC.
`history.active`	boolean	`TRUE`	Whether the model was enabled or disabled at the time.
`history.message`	string	`Improved rarity filters`	The most recent commit message for the model.
`history.by`	string	`ajohnston`	The user who made the change.
`history.phid`	numeric	`2842`	The “policy history id” at that change.
`message`	string	`Improved rarity filters`	The commit message for the change.
`version`	numeric	`40`	The model version, increments on edit.

Example Response

Request: /models?uuid=80010119-6d7f-0000-0305-5e0000000420

```
{
  "name": "Anomalous File::Anomalous Octet Stream",
  "pid": 12,
  "phid": 2842,
  "uuid": "80010119-6d7f-0000-0305-5e0000000420",
  "logic": {
    "data": [
      3621
    ],
    "type": "componentList",
    "version": 1
  },
  "throttle": 3600,
  "sharedEndpoints": false,
  "actions": {
    "alert": true,
    "antigena": {},
    "breach": true,
    "model": true,
    "setPriority": false,
    "setTag": false,
    "setType": false
  },
  "tags": [
    "AP: Tooling",
    "DNS Server"
  ],
  "interval": 0,
  "sequenced": false,
  "active": true,
  "modified": "2019-11-15 11:42:20",
  "activeTimes": {
    "devices": {},
    "tags": {},
    "type": "exclusions",
    "version": 2
  },
  "priority": 2,
  "autoUpdatable": false,
  "autoUpdate": true,
  "autoSuppress": true,
  "description": "A device has downloaded a rare data stream which is not specifying a specific
data type.\\n\\nAction: Investigate the endpoint the data is being sent from and consider
downloading a PCAP or reviewing the hash if you believe the endpoint to be untrustworthy.",
  "behaviour": "decreasing",
  "defeats": [],
  "created": {
    "by": "System"
  },
  "edited": {
    "by": "Sarah",
    "userID": 24
  },
  "history": [
    {
      "modified": "2019-11-15 11:42:20",
      "active": true,
      "message": "Improved rarity filters, and merged exclusion filters",
      "by": "Sarah",
      "phid": 2842
    },
    ...
  ],
  "message": "Improved rarity filters, and merged exclusion filters",
  "version": 40
}
```

Response is abbreviated.

/modelbreaches

The `/modelbreaches` endpoint returns a time-sorted list of model breaches, filtered by the specified parameters. This endpoint is the most important for organizations who wish to integrate Darktrace programmatically into their SOC environment.

The following recommendations represent a good starting point when initially approaching the query parameters. These parameters may change over time in response to your business logic and concerns of each security team. Organizations with a defined playbook may start with a different set of parameters - the API call can always be refined at a later date.

- Busy network environments with many devices may produce a large volume of alerts over a short space of time. It is recommended, therefore, that queries are made at more frequent intervals and cover a shorter duration of time. A shorter query timeframe will always return a response faster.
- Organizations that want more data returned for use in their external system can use the `minimal=false` and `fulldevicedetails=true` parameters. Setting these parameters will return full model component and device information in the JSON response, allowing for more investigation to be carried within the SOC environment.
- Acknowledged breaches can be optionally returned by this endpoint - this can be useful for logging resolved events to an external server or reporting on historic acknowledgment. Depending on your organizational approach and workflow, you may prefer to export all breaches to an external system - including acknowledged breaches - and make the decision there on whether the breach needs to be investigated or discussed further. This will, however, produce a large number of alerts so should be reviewed on a regular basis.
- Like the Email Alerting and the Mobile App, alert score can be used as a threshold to return model breaches. Using `minscore` will only return breaches above the specified fractional amount (e.g., 0.8 is a breach score of 80%). This parameter can be used to mimic the “Minimum Breach Score” on the System Config page to match other alerting formats if desired.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`deviceattop`	boolean	Return the device JSON object as a value of the top-level object rather than within each matched component. Defaults to true in the Threat Visualizer UI and in JSON alert formats and false for the programmatic API. requests.
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`expandenums`	boolean	Expand numeric enumerated types to their descriptive string representation.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`historicmodelonly`	boolean	Return the JSON for the historic version of the model details only, rather than both the historic and current definition.
`includeacknowledged`	boolean	Include acknowledged breaches in the data.
`includebreachurl`	boolean	Return a URL for the model breach in the long form of the model breach data, this requires that the FQDN configuration parameter is set.
`minimal`	boolean	Reduce the amount of data returned for the API call. In the Threat Visualizer, this parameter defaults to false when any of the `starttime` , `from` , `pid` , `uuid` , `pbid` or `did` parameters are used. When accessed programmatically, always defaults to false.
`minscore`	fractional numeric	Return only breaches with a minimum score.

Parameter	Type	Description
`pbid`	numeric	Only return the model breach with the specified ID.
`pid`	numeric	Only return model breaches for the specified model.
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format
`uuid`	string	Only return model breaches for the specified model. All models have a uuid and a pid. The uuid (universally unique identifier) is a 128-bit hexadecimal number.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- A time window for the returned model breaches can be specified using `YYYY-MM-DD HH:MM:SS` format with the `to` / `from` parameters, or `starttime` / `endtime` using unix time. If no time period is specified, breaches are pulled from beginning of memory with a limit of one year per response. Time parameters must always be specified in pairs.
- Specifying `historicmodelonly` will return a single model object for the model entity at the time of breach.
- The `includebreachURL` parameter will only return a URL if `minimal=false` . This URL will be the second object returned and it will take the format `"breachUrl": "https://darktrace-dt-XXX-YY/#modelbreach/123"`
- `expandenums` toggles numeric values in certain nested lists to full strings - the numerical codes and associated strings for enums can be found at the `/enums` endpoint (/enums).
- By default, the `minimal` parameter is `false` when accessing model breaches programmatically. This returns reduced model logic details for the model that breached. The `/modelbreaches` endpoint in the Threat Visualizer has `minimal=true` by default for multiple breaches and `minimal=false` when filtering by a `pbid` . Setting `minimal` to `false` will allow more investigation in the external environment but will also produce more noise in the returned JSON.
- By default, the `deviceattop` parameter is `true` when accessing model breaches programmatically. This means device information is contained in a top level JSON object “ `device` ”, rather than contained within the `triggeredComponents` object. The `/modelbreaches` endpoint in the Threat Visualizer has `deviceattop=false` by default, so device information is nested within the `triggeredComponents` object when viewed with a browser.
- Alert priority is only returned when `minimal=false` and cannot be used as a filter for returned breaches.

Example Request

1. `GET` all model breaches - including acknowledged breaches - for the 7 day period from 3rd to 9th February 2020:

```
https://<applianceIP>/modelbreaches?
from=2020-02-03T00:00:00&to=2020-02-9T23:59:59&minimal=true&includeacknowledged=true
```

2. `GET` model breaches for the device with `did=1` since January 1st 2020 with a breach score above 60%:

```
https://<applianceIP>/modelbreaches?did=1&starttime=1577836800000&minscore=0.6
```

3. `GET` model breaches for the “Anomalous File / Anomalous Octet Stream” model:

```
https://<applianceIP>/modelbreaches?pid=12
```

```
https://<applianceIP>/modelbreaches?uuid=80010119-6d7f-0000-0305-5e0000000420
```

4. `GET` the information for model breach `pbid=123` with information about the model at the time of breach only:

```
https://<applianceIP>/modelbreaches?pbid=123&historicmodelonly=true
```

```
https://<applianceIP>/modelbreaches/123?historicmodelonly=true
```

Example Response

Request: /modelbreaches/123?historicmodelonly=true

```
{
  "creationTime": 1582213002000,
  "commentCount": 0,
  "pbid": 287232,
  "time": 1582212986000,
  "model": {
    "name": "Compromise::HTTP Beaconing to Rare Destination",
    "pid": 143,
    "phid": 123,
    "uuid": "1a814475-5fef-499b-a467-4e2e68352cbb",
    "logic": {
      "data": [
        265
      ],
      "type": "componentList",
      "version": 1
    },
    "throttle": 3600,
    "sharedEndpoints": false,
    "actions": {
      "alert": true,
      "antigena": {},
      "breach": true,
      "model": true,
      "setPriority": false,
      "setTag": false,
      "setType": false
    },
    "tags": [
      "AP: C2 Comms",
      "DNS Server"
    ],
    "interval": 0,
    "sequenced": false,
    "active": true,
    "modified": "2019-11-15 11:42:21",
    "activeTimes": {
      "devices": {},
      "tags": {},
      "type": "exclusions",
      "version": 2
    },
    "priority": 0,
    "autoUpdatable": true,
    "autoUpdate": true,
    "autoSuppress": true,
    "description": "A device is making regular HTTP connections to a rare external location.\\n\
\nAction: Review the domains / IPs involved to see if they have a legitimate purpose. Many types
of software exhibit this type of behaviour by checking for updates or sending out usage
statistics. Consider why this device is running software that is not common within the network.",
    "behaviour": "decreasing",
    "defeats": [],
    "created": {
      "by": "System"
    },
    "edited": {
      "by": "Sarah",
      "userID": 24
    },
    "version": 16
  },
  "triggeredComponents": [
    {
      "time": 1582212985000,
      "cbid": 305422,
      "cid": 265,
      "chid": 265,
      "size": 3,
      "threshold": 2,
      "interval": 14400,
      "logic": {
        "data": {
          "left": "A",
          "operator": "AND",
          "right": {
            "left": "B",
            "operator": "AND",
            "right": {
            ...
          }
        },
        "version": "v0.1"
      },
```

Response is abbreviated.

/modelbreaches Response Schema

Response Schema - No Parameters

Response Field	Type	Example Value	Description
creationTime	numeric	1528810000000	The timestamp that the record of the breach was created. This is distinct from the “time” field.
commentCount	numeric	2	The number of comments made against this breach.
pbid	numeric	123	The “policy breach ID” of the model breach.
time	numeric	1528810000000	The timestamp when the record was created in epoch time.
model	object		An object describing the model logic and history of the model that was breached.
model.then	object		An object describing the model logic at the time of breach. Requires `historicModelOnly=false` .
model.then.name	string	Anomalous Connection::1 GiB Outbound	Name of the model that was breached.
model.then.pid	numeric	1	The “policy id” of the model that was breached.
model.then.phid	numeric	1	The model “policy history” id. Increments when the model is modified.
model.then.uuid	string	80010119-6d7f-0000-0305-5e0000000215	A unique ID that is generated on creation of the model.
model.then.logic	object		A data structure that describes the conditions to bring about a breach.
model.then.logic.data	array	1	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
model.then.logic.type	string	componentList	The type of model.
model.then.logic.version	numeric	1	A number representing the version of model logic.
model.then.throttle	numeric	3600	For an individual device, this is the value in seconds for which this model will not fire again.

Response Field	Type	Example Value	Description
model.then.sharedEndpoints	boolean	FALSE	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
model.then.actions	object		The action to perform as a result of matching this model firing.
model.then.actions.alert	boolean	TRUE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
model.then.actions.antigena	object		An object containing the antigena response to be applied as a result of the model breaching.
model.then.actions.breach	boolean	TRUE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
model.then.actions.model	boolean	TRUE	If true, creates an event in the device's event log without creating an alert/ model breach in the threat tray.
model.then.actions.setPriority	boolean	FALSE	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.
model.then.actions.setTag	boolean	FALSE	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
model.then.actions.setType	boolean	FALSE	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
model.then.tags	array	AP: Egress	A list of tags that have been applied to this model in the Threat Visualizer model editor.
model.then.interval	numeric	0	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
model.then.sequenced	boolean	FALSE	Whether the components are required to fire in the specified order for the model breach to occur.

Response Field	Type	Example Value	Description
model.then.active	boolean	TRUE	Whether the model is enabled or disabled.
model.then.modified	string	43263.58333	Timestamp at which the model was last modified, in a readable format.
model.then.activeTimes	object		An object describing device whitelisting or blacklisting configured for this model.
model.then.activeTimes.devices	object		The device ids for devices on the list.
model.then.activeTimes.tags	object		A system field.
model.then.activeTimes.type	string	exclusions	The type of list: “restrictions” indicates a blacklist, “exclusions” a whitelist.
model.then.activeTimes.version	numeric	2	A system field.
model.then.priority	numeric	1	The model’s priority affects the strength with which it breaches (0-5 scale).
model.then.autoUpdatable	boolean	TRUE	Whether the model is suitable for auto update.
model.then.autoUpdate	boolean	TRUE	Whether the model is enabled for auto update.
model.then.autoSuppress	boolean	TRUE	Whether the model will automatically be suppressed in the case of over-breaching.
model.then.description	string	A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.	The optional description of the model.
model.then.behaviour	string	decreasing	The score modulation function as set in the model editor.
model.then.created	object		An object describing the creation of the model.
model.then.created.by	string	System	Username that created the model.
model.then.edited	object		An object describing the edit history of the model.
model.then.edited.by	string	smartinez_admin	Username that last edited the model.
model.then.version	numeric	16	The version of the model. Increments on each edit.
model.now	object		An object describing the model logic at the time of request. Requires `historicModelOnly=false` .
model.now.name	string	Anomalous Connection::1 GiB Outbound	Name of the model that was breached.

Response Field	Type	Example Value	Description
model.now.pid	numeric	1	The “policy id” of the model that was breached.
model.now.phid	numeric	3343	The model “policy history” id. Increments when the model is modified.
model.now.uuid	string	80010119-6d7f-0000-0305-5e0000000215	A unique ID that is generated on creation of the model.
model.now.logic	object		A data structure that describes the conditions to bring about a breach.
model.now.logic.data	array	1	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
model.now.logic.type	string	componentList	The type of model.
model.now.logic.version	numeric	1	A number representing the version of model logic.
model.now.throttle	numeric	3600	For an individual device, this is the value in seconds for which this model will not fire again.
model.now.sharedEndpoints	boolean	FALSE	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
model.now.actions	object		The action to perform as a result of matching this model firing.
model.now.actions.alert	boolean	FALSE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
model.now.actions.antigena	object		An object containing the antigena response to be applied as a result of the model breaching.
model.now.actions.breach	boolean	TRUE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
model.now.actions.model	boolean	TRUE	If true, creates an event in the device’s event log without creating an alert/ model breach in the threat tray.
model.now.actions.setPriority	boolean	FALSE	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.

Response Field	Type	Example Value	Description
model.now.actions.setTag	boolean	FALSE	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
model.now.actions.setType	boolean	FALSE	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
model.now.tags	array	AP: Egress	AP: Bruteforce
model.now.interval	numeric	0	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
model.now.sequenced	boolean	FALSE	Whether the components are required to fire in the specified order for the model breach to occur.
model.now.active	boolean	TRUE	Whether the model is enabled or disabled.
model.now.modified	string	43263.58333	Timestamp at which the model was last modified, in a readable format.
model.now.activeTimes	object		An object describing device whitelisting or blacklisting configured for this model.
model.now.activeTimes.devices	object		The device ids for devices on the list.
model.now.activeTimes.tags	object		A system field.
model.now.activeTimes.type	string	exclusions	The type of list: “restrictions” indicates a blacklist, “exclusions” a whitelist.
model.now.activeTimes.version	numeric	2	A system field.
model.now.priority	numeric	0	The model’s priority affects the strength with which it breaches (0-5 scale).
model.now.autoUpdatable	boolean	FALSE	Whether the model is suitable for auto update.
model.now.autoUpdate	boolean	TRUE	Whether the model is enabled for auto update.
model.now.autoSuppress	boolean	TRUE	Whether the model will automatically be suppressed in the case of over-breaching.

Response Field	Type	Example Value	Description
model.now.description	string	A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.	The optional description of the model.
model.now.behaviour	string	decreasing	The score modulation function as set in the model editor.
model.now.created	object		An object describing the creation of the model.
model.now.created.by	string	System	Username that created the model.
model.now.edited	object		An object describing the edit history of the model.
model.now.edited.by	string	smartinez_admin	Username that last edited the model.
model.now.edited.userID	numeric	24	Username that last edited the model.
model.now.message	string	updated display filters to simplify output	The commit message for the change.
model.now.version	numeric	24	The version of the model. Increments on each edit.
triggeredComponents	array		An array describing the model components that were triggered to create the model breach.
triggeredComponents.time	numeric	1528810000000	A timestamp in Epoch time at which the components were triggered.
triggeredComponents.cbid	numeric	1729	The “component breach id”. A unique identifier for the component breach.
triggeredComponents.cid	numeric	1	The “component id”. A unique identifier.
triggeredComponents.chid	numeric	1	The “component history id”. Increments when the component is edited.
triggeredComponents.size	numeric	1155203452	The ‘metric logic id’ for the metric used in the component.
triggeredComponents.threshold	numeric	1073741824	The number of times the component logic must be met within the interval timeframe.
triggeredComponents.interval	numeric	3600	The timeframe in seconds within which the threshold must be satisfied.

Response Field	Type	Example Value	Description
triggeredComponents.logic.data	object		An object representing the logical relationship between component filters. Each filter is given an alphabetical reference and the contents of this object describe the relationship between those objects.
triggeredComponents.logic.data.left	string	A	Objects on the left will be compared with the object on the right using the specified operator.
triggeredComponents.logic.data.operator	string	AND	A logical operator to compare filters with.
triggeredComponents.logic.data.right	object	D	Objects on the left will be compared with the object on the right using the specified operator.
triggeredComponents.logic.version	string	v0.1	The version of the component logic.
triggeredComponents.metric	object		An object describing the metric used in the component that triggered the Model Breach.
triggeredComponents.metric.mlid	numeric	33	The “metric logic” id - unique identifier.
triggeredComponents.metric.name	string	externalclientdatatransfervolume	The metric which data is returned for in system format.
triggeredComponents.metric.label	string	External Data Volume as a Client	The metric which data is returned for in readable format.
triggeredComponents.triggeredFilters	array		The filters that comprise the component that were triggered to produce the model breach.
triggeredComponents.triggeredFilters.cfid	numeric	1	The ‘component filter id’. A unique identifier for the filter as part of a the component.
triggeredComponents.triggeredFilters.id	string	A	A filter that is used in the component logic. All filters are given alphabetical identifiers. Display filters - those that appear in the breach notification - can be identified by a lowercase ‘d’ and a numeral.
triggeredComponents.triggeredFilters.filterType	string	Direction	The filtertype that is used in the filter. A full list of filtertypes can be found on the /filtertypes endpoint.
triggeredComponents.triggeredFilters.arguments	object		Whether the component is currently active as part of a model.
triggeredComponents.triggeredFilters.arguments.value	numeric	out	The value the filtertype should be compared against (using the specified comparator) to create the filter.

Response Field	Type	Example Value	Description
triggeredComponents.triggeredFilters.comparatorType	string	is	The comparator. A full list of comparators available for each filtertype can be found on the /filtertypes endpoint.
triggeredComponents.triggeredFilters.trigger	object		An object contaning the value to be compared. Display filters will have an empty object.
triggeredComponents.triggeredFilters.trigger.value	string	out	The actual value that triggered the filter.
score	numeric	0.443	The model breach score, represented by a value between 0 and 1.
device	object		An object describing a device seen by Darktrace.
device.did	numeric	96	The “device id”, a unique identifier.
device.ip	string	10.0.18.224	The current IP associated with the device.
device.ips	array		IPs associated with the device historically.
device.ips.ip	string	10.0.18.224	A historic IP associated with the device.
device.ips.timems	numeric	1.52881E+12	The time the IP was last seen associated with that device in epoch time.
device.ips.time	string	43263.58333	The time the IP was last seen associated with that device in readable format.
device.ips.sid	numeric	34	The subnet id for the subnet the IP belongs to.
device.sid	numeric	34	The subnet id for the subnet the device is currently located in.
device.hostname	string	fs182	The current device hostname.
device.firstSeen	numeric	1528810000000	The first time the device was seen on the network.
device.lastSeen	numeric	1528810000000	The last time the device was seen on the network.
device.typename	string	server	The device type in system format.
device.typelabel	string	Server	The device type in readable format.

Example Response

Request: /modelbreaches/123

```
{
  "creationTime": 1582213002000,
  "commentCount": 0,
  "pbid": 123,
  "time": 1582212986000,
  "model": {
    "then":{
      "name": "Compromise::HTTP Beaconing to Rare Destination",
      "pid": 143,
      "phid": 123,
      "uuid": "1a814475-5fef-499b-a467-4e2e68352cbb",
      "logic": {
        "data": [
          265
        ],
        "type": "componentList",
        "version": 1
      },
      "throttle": 3600,
      "sharedEndpoints": false,
      "actions": {
        "alert": true,
        "antigena": {},
        "breach": true,
        "model": true,
        "setPriority": false,
        "setTag": false,
        "setType": false
      },
      "tags": [
        "AP: C2 Comms",
        "DNS Server"
      ],
      "interval": 0,
      "sequenced": false,
      "active": true,
      "modified": "2019-11-15 11:42:21",
      "activeTimes": {
        "devices": {},
        "tags": {},
        "type": "exclusions",
        "version": 2
      },
      "priority": 0,
      "autoUpdatable": true,
      "autoUpdate": true,
      "autoSuppress": true,
      "description": "A device is making regular HTTP connections to a rare external location.\\n\
\nAction: Review the domains / IPs involved to see if they have a legitimate purpose. Many types
of software exhibit this type of behaviour by checking for updates or sending out usage
statistics. Consider why this device is running software that is not common within the network.",
      "behaviour": "decreasing",
      "defeats": [],
      "created": {
        "by": "System"
      },
      "edited": {
        "by": "Sarah",
        "userID": 24
      },
      "version": 16
    }
  },
    "now": {
      "name": "Compromise::HTTP Beaconing to Rare Destination",
      "pid": 143,
      "phid": 123,
      "uuid": "1a814475-5fef-499b-a467-4e2e68352cbb",
      "logic": {
        "data": [
          265
        ],
        "type": "componentList",
        "version": 1
      },
      "throttle": 3600,
      "sharedEndpoints": false,
      "actions": {
        "alert": true,
        "antigena": {},
        "breach": true,
        "model": true,
        "setPriority": false,
```

Response Schema - `deviceattop=false`

Response Field	Type	Example Value	Description
`creationTime`	numeric	`1528810000000`	The timestamp that the record of the breach was created. This is distinct from the “time” field.
`breachUrl`	string	`https://appliance-fqdn/#modelbreaches/123`	A link to the specific model breach in the Darktrace Threat Visualizer - the configuration option FQDN must be set for this field to appear.
`commentCount`	numeric	`2`	The number of comments made against this breach.
`pbid`	numeric	`123`	The “policy breach ID” of the model breach.
`time`	numeric	`1528810000000`	The timestamp when the record was created in epoch time.
`model`	object		An object describing the model logic and history of the model that was breached.
`model.then`	object		An object describing the model logic at the time of breach. Requires `historicModelOnly=false` .
`model.then.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.then.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.then.phid`	numeric	`1`	The model “policy history” id. Increments when the model is modified.
`model.then.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.then.logic`	object		A data structure that describes the conditions to bring about a breach.
`model.then.logic.data`	array	`1`	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
`model.then.logic.type`	string	`componentList`	The type of model.
`model.then.logic.version`	numeric	`1`	A number representing the version of model logic.
`model.then.throttle`	numeric	`3600`	For an individual device, this is the value in seconds for which this model will not fire again.
`model.then.sharedEndpoints`	boolean	`FALSE`	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
`model.then.actions`	object		The action to perform as a result of matching this model firing.
`model.then.actions.alert`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
`model.then.actions.antigena`	object		An object containing the antigena response to be applied as a result of the model breaching.

Response Field	Type	Example Value	Description
model.then.actions.breach	boolean	TRUE	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
model.then.actions.model	boolean	TRUE	If true, creates an event in the device's event log without creating an alert/ model breach in the threat tray.
model.then.actions.setPriority	boolean	FALSE	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.
model.then.actions.setTag	boolean	FALSE	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
model.then.actions.setType	boolean	FALSE	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
model.then.tags	array	AP: Egress	A list of tags that have been applied to this model in the Threat Visualizer model editor.
model.then.interval	numeric	0	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
model.then.sequenced	boolean	FALSE	Whether the components are required to fire in the specified order for the model breach to occur.
model.then.active	boolean	TRUE	Whether the model is enabled or disabled.
model.then.modified	string	2018-06-12 14:00:00	Timestamp at which the model was last modified, in a readable format.
model.then.activeTimes	object		An object describing device whitelisting or blacklisting configured for this model.
model.then.activeTimes.devices	object		The device ids for devices on the list.
model.then.activeTimes.tags	object		A system field.
model.then.activeTimes.type	string	exclusions	The type of list: "restrictions" indicates a blacklist, "exclusions" a whitelist.
model.then.activeTimes.version	numeric	2	A system field.
model.then.priority	numeric	1	The model's priority affects the strength with which it breaches (0-5 scale).
model.then.autoUpdatable	boolean	TRUE	Whether the model is suitable for auto update.
model.then.autoUpdate	boolean	TRUE	Whether the model is enabled for auto update.
model.then.autoSuppress	boolean	TRUE	Whether the model will automatically be suppressed in the case of over-breaching.

Response Field	Type	Example Value	Description
`model.then.description`	string	`A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.`	The optional description of the model.
`model.then.behaviour`	string	`decreasing`	The score modulation function as set in the model editor.
`model.then.defeats`	array		A system field.
`model.then.created`	object		An object describing the creation of the model.
`model.then.created.by`	string	`System`	Username that created the model.
`model.then.edited`	object		An object describing the edit history of the model.
`model.then.edited.by`	string	`smartinez_admin`	Username that last edited the model.
`model.then.version`	numeric	`16`	The version of the model. Increments on each edit.
`model.now`	object		An object describing the model logic at the time of request. Requires `historicModelOnly=false` .
`model.now.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.now.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.now.phid`	numeric	`3343`	The model “policy history” id. Increments when the model is modified.
`model.now.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.now.logic`	object		A data structure that describes the conditions to bring about a breach.
`model.now.logic.data`	array	`1`	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
`model.now.logic.type`	string	`componentList`	The type of model.
`model.now.logic.version`	numeric	`1`	A number representing the version of model logic.
`model.now.throttle`	numeric	`3600`	For an individual device, this is the value in seconds for which this model will not fire again.
`model.now.sharedEndpoints`	boolean	`FALSE`	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
`model.now.actions`	object		The action to perform as a result of matching this model firing.

Response Field	Type	Example Value	Description
`model.now.actions.alert`	boolean	`FALSE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
`model.now.actions.antigena`	object		An object containing the antigena response to be applied as a result of the model breaching.
`model.now.actions.breach`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
`model.now.actions.model`	boolean	`TRUE`	If true, creates an event in the device's event log without creating an alert/ model breach in the threat tray.
`model.now.actions.setPriority`	boolean	`FALSE`	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.
`model.now.actions.setTag`	boolean	`FALSE`	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
`model.now.actions.setType`	boolean	`FALSE`	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
`model.now.tags`	array	`AP: Egress`	AP: Bruteforce
`model.now.interval`	numeric	`0`	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
`model.now.sequenced`	boolean	`FALSE`	Whether the components are required to fire in the specified order for the model breach to occur.
`model.now.active`	boolean	`TRUE`	Whether the model is enabled or disabled.
`model.now.modified`	string	`2018-06-12 14:00:00`	Timestamp at which the model was last modified, in a readable format.
`model.now.activeTimes`	object		An object describing device whitelisting or blacklisting configured for this model.
`model.now.activeTimes.devices`	object		The device ids for devices on the list.
`model.now.activeTimes.tags`	object		A system field.
`model.now.activeTimes.type`	string	`exclusions`	The type of list: "restrictions" indicates a blacklist, "exclusions" a whitelist.
`model.now.activeTimes.version`	numeric	`2`	A system field.
`model.now.priority`	numeric	`0`	The model's priority affects the strength with which it breaches (0-5 scale).
`model.now.autoUpdatable`	boolean	`FALSE`	Whether the model is suitable for auto update.
`model.now.autoUpdate`	boolean	`TRUE`	Whether the model is enabled for auto update.
`model.now.autoSuppress`	boolean	`TRUE`	Whether the model will automatically be suppressed in the case of over-breaching.

Response Field	Type	Example Value	Description
`model.now.description`	string	`A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.`	The optional description of the model.
`model.now.behaviour`	string	`decreasing`	The score modulation function as set in the model editor.
`model.now.defeats`	array		A system field.
`model.now.created`	object		An object describing the creation of the model.
`model.now.created.by`	string	`System`	Username that created the model.
`model.now.edited`	object		An object describing the edit history of the model.
`model.now.edited.by`	string	`smartinez_admin`	Username that last edited the model.
`model.now.edited.userID`	numeric	`24`	Username that last edited the model.
`model.now.message`	string	`updated display filters to simplify output`	The commit message for the change.
`model.now.version`	numeric	`24`	The version of the model. Increments on each edit.
`triggeredComponents`	array		An array describing the model components that were triggered to create the model breach.
`triggeredComponents.time`	numeric	`1528810000000`	A timestamp in Epoch time at which the components were triggered.
`triggeredComponents.cbid`	numeric	`1729`	The “component breach id”. A unique identifier for the component breach.
`triggeredComponents.cid`	numeric	`1`	The “component id”. A unique identifier.
`triggeredComponents.chid`	numeric	`1`	The “component history id”. Increments when the component is edited.
`triggeredComponents.size`	numeric	`1155203452`	The ‘metric logic id’ for the metric used in the component.
`triggeredComponents.threshold`	numeric	`1073741824`	The number of times the component logic must be met within the interval timeframe.
`triggeredComponents.interval`	numeric	`3600`	The timeframe in seconds within which the threshold must be satisfied.
`triggeredComponents.logic`	object		An object describing the component logic.
`triggeredComponents.logic.data`	object		An object representing the logical relationship between component filters. Each filter is given an alphabetical reference and the contents of this object describe the relationship between those objects.

Response Field	Type	Example Value	Description
`triggeredComponents.logic.data.left`	string	`A`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.data.operator`	string	`AND`	A logical operator to compare filters with.
`triggeredComponents.logic.data.right`	object	`D`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.version`	string	`v0.1`	The version of the component logic.
`triggeredComponents.metric`	object		An object describing the metric used in the component that triggered the Model Breach.
`triggeredComponents.metric.mlid`	numeric	`33`	The “metric logic” id - unique identifier.
`triggeredComponents.metric.name`	string	`externalclientdatatransfervolume`	The metric which data is returned for in system format.
`triggeredComponents.metric.label`	string	`External Data Volume as a Client`	The metric which data is returned for in readable format.
`triggeredComponents.device`	object		An object describing a device seen by Darktrace.
`triggeredComponents.device.did`	numeric	`96`	The “device id”, a unique identifier.
`triggeredComponents.device.ip`	string	`10.0.18.224`	The current IP associated with the device.
`triggeredComponents.device.ips`	array		IPs associated with the device historically.
`triggeredComponents.device.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`triggeredComponents.device.ips.timems`	numeric	`1528812000000`	The time the IP was last seen associated with that device in epoch time.
`triggeredComponents.device.ips.time`	string	`2018-06-12 14:00:00`	The time the IP was last seen associated with that device in readable format.
`triggeredComponents.device.ips.sid`	numeric	`34`	The subnet id for the subnet the IP belongs to.
`triggeredComponents.device.sid`	numeric	`34`	The subnet id for the subnet the device is currently located in.
`triggeredComponents.device.hostname`	string	`fs182`	The current device hostname.
`triggeredComponents.device.firstSeen`	numeric	`1528810000000`	The first time the device was seen on the network.
`triggeredComponents.device.lastSeen`	numeric	`1528810000000`	The last time the device was seen on the network.
`triggeredComponents.device.typename`	string	`server`	The device type in system format.
`triggeredComponents.device.typelabel`	string	`Server`	The device type in readable format.
`triggeredComponents.triggeredFilters`	array		The filters that comprise the component that were triggered to produce the model breach.
`triggeredComponents.triggeredFilters.cfid`	numeric	`1`	The ‘component filter id’. A unique identifier for the filter as part of a the component.
`triggeredComponents.triggeredFilters.id`	string	`A`	A filter that is used in the component logic. All filters are given alphabetical identifiers. Display filters - those that appear in the breach notification - can be identified by a lowercase ‘d’ and a numeral.

Response Field	Type	Example Value	Description
`triggeredComponents.triggeredFilters.filterType`	string	`Direction`	The filtertype that is used in the filter. A full list of filtertypes can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.arguments`	object		Whether the component is currently active as part of a model.
`triggeredComponents.triggeredFilters.arguments.value`	string	`out`	The value the filtertype should be compared against (using the specified comparator) to create the filter.
`triggeredComponents.triggeredFilters.comparatorType`	string	`is`	The comparator. A full list of comparators available for each filtertype can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.trigger`	object		An object contaning the value to be compared. Display filters will have an empty object.
`triggeredComponents.triggeredFilters.trigger.value`	string	`out`	The actual value that triggered the filter.
`score`	numeric	`0.443`	The model breach score, represented by a value between 0 and 1.

Example Response

Request: /modelbreaches/123?deviceattop=false

```
{
  "creationTime": 1582213002000,
  "commentCount": 0,
  "pbid": 123,
  "time": 1582212986000,
  "model": {
    "then":{
      ... (same as above)
    }
  },
    "now": {
      ... (same as above)
    }
  },
  "triggeredComponents": [
    {
      "time": 1582212985000,
      "cbid": 305422,
      "cid": 265,
      "chid": 265,
      "size": 3,
      "threshold": 2,
      "interval": 14400,
      "logic": {
        "data": {
          "left": "A",
          "operator": "AND",
          "right": {
            "left": "B",
            "operator": "AND",
            "right": {
            ...
          }
        },
        "version": "v0.1"
      },
      "metric": {
        "mlid": 1,
        "name": "externalconnections",
        "label": "External Connections"
      },
      "device": {
        "did": 316,
        "ip": "10.0.56.12",
        "ips": [
          {
            "ip": "10.0.56.12",
            "timems": 1581508800000,
            "time": "2020-02-12 12:00:00",
            "sid": 23
          }
        ],
        "sid": 23,
        "hostname": "Sarah Development",
        "firstSeen": 1581591070000,
        "lastSeen": 1582645442000,
        "typename": "desktop",
        "typelabel": "Desktop"
      },
      "triggeredFilters": [
        {
          "cfid": 2087,
          "id": "A",
          "filterType": "Rare external endpoint",
          "arguments": {
            "value": 90
          },
          "comparatorType": ">",
          "trigger": {
            "value": "94"
          }
        },
        ...
      ]
    }
  ],
  "score": 0.325
}
```

Response is abbreviated.

Response Schema - `historicmodelonly=true`

Response Field	Type	Example Value	Description
`creationTime`	numeric	`1530000000000`	The timestamp that the record of the breach was created. This is distinct from the "time" field.
`breachUrl`	string	`https://appliance-fqdn/#modelbreaches/123`	A link to the specific model breach in the Darktrace Threat Visualizer - the configuration option FQDN must be set for this field to appear.
`commentCount`	numeric	`2`	The number of comments made against this breach.
`pbid`	numeric	`123`	The "policy breach ID" of the model breach.
`time`	numeric	`1530000000000`	The timestamp when the record was created in epoch time.
`model`	object		An object describing the model logic at the time of request. Requires `historicModelOnly=true` .
`model.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.pid`	numeric	`1`	The "policy id" of the model that was breached.
`model.phid`	numeric	`1`	The model "policy history" id. Increments when the model is modified.
`model.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.logic`	object		A data structure that describes the conditions to bring about a breach.
`model.logic.data`	array	`1`	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
`model.logic.type`	string	`componentList`	The type of model.
`model.logic.version`	numeric	`1`	A number representing the version of model logic.
`model.throttle`	numeric	`3600`	For an individual device, this is the value in seconds for which this model will not fire again.
`model.sharedEndpoints`	boolean	`FALSE`	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
`model.actions`	object		The action to perform as a result of matching this model firing.
`model.actions.alert`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.

Response Field	Type	Example Value	Description
`model.actions.antigena`	object		An object containing the antigena response to be applied as a result of the model breaching.
`model.actions.breach`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
`model.actions.model`	boolean	`TRUE`	If true, creates an event in the device's event log without creating an alert/ model breach in the threat tray.
`model.actions.setPriority`	boolean	`FALSE`	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.
`model.actions.setTag`	boolean	`FALSE`	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
`model.actions.setType`	boolean	`FALSE`	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
`model.tags`	array	`AP: Egress`	A list of tags that have been applied to this model in the Threat Visualizer model editor.
`model.interval`	numeric	`0`	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
`model.sequenced`	boolean	`FALSE`	Whether the components are required to fire in the specified order for the model breach to occur.
`model.active`	boolean	`TRUE`	Whether the model is enabled or disabled.
`model.modified`	string	`2018-06-12 14:00:00`	Timestamp at which the model was last modified, in a readable format.
`model.activeTimes`	object		An object describing device whitelisting or blacklisting configured for this model.
`model.activeTimes.devices`	object		The device ids for devices on the list.
`model.activeTimes.tags`	object		A system field.
`model.activeTimes.type`	string	`exclusions`	The type of list: "restrictions" indicates a blacklist, "exclusions" a whitelist.
`model.activeTimes.version`	numeric	`2`	A system field.
`model.priority`	numeric	`1`	The model's priority affects the strength with which it breaches (0-5 scale).
`model.autoUpdatable`	boolean	`TRUE`	Whether the model is suitable for auto update.
`model.autoUpdate`	boolean	`TRUE`	Whether the model is enabled for auto update.
`model.autoSuppress`	boolean	`TRUE`	Whether the model will automatically be suppressed in the case of over-breaching.

Response Field	Type	Example Value	Description
`model.description`	string	`A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.`	The optional description of the model.
`model.behaviour`	string	`decreasing`	The score modulation function as set in the model editor.
`model.defeats`	array		A system field.
`model.created`	object		An object describing the creation of the model.
`model.created.by`	string	`System`	Username that created the model.
`model.edited`	object		An object describing the edit history of the model.
`model.edited.by`	string	`smartinez_admin`	Username that last edited the model.
`model.version`	numeric	`16`	The version of the model. Increments on each edit.
`triggeredComponents`	array		An array describing the model components that were triggered to create the model breach.
`triggeredComponents.time`	numeric	`1530000000000`	A timestamp in Epoch time at which the components were triggered.
`triggeredComponents.cbid`	numeric	`1729`	The “component breach id”. A unique identifier for the component breach.
`triggeredComponents.cid`	numeric	`1`	The “component id”. A unique identifier.
`triggeredComponents.chid`	numeric	`1`	The “component history id”. Increments when the component is edited.
`triggeredComponents.size`	numeric	`1155203452`	The ‘metric logic id’ for the metric used in the component.
`triggeredComponents.threshold`	numeric	`1073741824`	The number of times the component logic must be met within the interval timeframe.
`triggeredComponents.interval`	numeric	`3600`	The timeframe in seconds within which the threshold must be satisfied.
`triggeredComponents.logic`	object		An object describing the component logic.
`triggeredComponents.logic.data`	object		An object representing the logical relationship between component filters. Each filter is given an alphabetical reference and the contents of this object describe the relationship between those objects.
`triggeredComponents.logic.data.left`	string	`A`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.data.operator`	string	`AND`	A logical operator to compare filters with.

Response Field	Type	Example Value	Description
`triggeredComponents.logic.data.right`	object	`D`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.version`	string	`v0.1`	The version of the component logic.
`triggeredComponents.metric`	object		An object describing the metric used in the component that triggered the Model Breach.
`triggeredComponents.metric.mlid`	numeric	`33`	The "metric logic" id - unique identifier.
`triggeredComponents.metric.name`	string	`externalclientdatatransfervolume`	The metric which data is returned for in system format.
`triggeredComponents.metric.label`	string	`External Data Volume as a Client`	The metric which data is returned for in readable format.
`triggeredComponents.triggeredFilters`	array		The filters that comprise the component that were triggered to produce the model breach.
`triggeredComponents.triggeredFilters.cfid`	numeric	`1`	The 'component filter id'. A unique identifier for the filter as part of a the component.
`triggeredComponents.triggeredFilters.id`	string	`A`	A filter that is used in the component logic. All filters are given alphabetical identifiers. Display filters - those that appear in the breach notification - can be identified by a lowercase 'd' and a numeral.
`triggeredComponents.triggeredFilters.filterType`	string	`Direction`	The filtertype that is used in the filter. A full list of filtertypes can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.arguments`	object		Whether the component is currently active as part of a model.
`triggeredComponents.triggeredFilters.arguments.value`	string	`out`	The value the filtertype should be compared against (using the specified comparator) to create the filter.
`triggeredComponents.triggeredFilters.comparatorType`	string	`is`	The comparator. A full list of comparators available for each filtertype can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.trigger`	object		An object containing the value to be compared. Display filters will have an empty object.
`triggeredComponents.triggeredFilters.trigger.value`	string	`out`	The actual value that triggered the filter.
`score`	numeric	`0.443`	The model breach score, represented by a value between 0 and 1.
`device`	object		An object describing a device seen by Darktrace.
`device.did`	numeric	`96`	The "device id", a unique identifier.
`device.ip`	string	`10.0.18.224`	The current IP associated with the device.
`device.ips`	array		IPs associated with the device historically.
`device.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`device.ips.timems`	numeric	`1528812000000`	The time the IP was last seen associated with that device in epoch time.
`device.ips.time`	string	`2018-06-12 14:00:00`	The time the IP was last seen associated with that device in readable format.

Response Field	Type	Example Value	Description
`device.ips.sid`	numeric	`34`	The subnet id for the subnet the IP belongs to.
`device.sid`	numeric	`34`	The subnet id for the subnet the device is currently located in.
`device.hostname`	string	`fs182`	The current device hostname.
`device.firstSeen`	numeric	`1530000000000`	The first time the device was seen on the network.
`device.lastSeen`	numeric	`1530000000000`	The last time the device was seen on the network.
`device.typename`	string	`server`	The device type in system format.
`device.typelabel`	string	`Server`	The device type in readable format.

Example Response

Request:/modelbreaches/123?historicmodelonly=true

```
Where `deviceattop=true`

{
  "creationTime": 1582213002000,
  "commentCount": 0,
  "pbid": 123,
  "time": 1582212986000,
  "model": {
    "name": "Compromise::HTTP Beaconing to Rare Destination",
    "pid": 143,
    "phid": 123,
    "uuid": "1a814475-5fef-499b-a467-4e2e68352cbb",
    "logic": {
      "data": [
        265
      ],
      "type": "componentList",
      "version": 1
    },
    "throttle": 3600,
    "sharedEndpoints": false,
    "actions": {
      "alert": true,
      "antigena": {},
      "breach": true,
      "model": true,
      "setPriority": false,
      "setTag": false,
      "setType": false
    },
    "tags": [
      "AP: C2 Comms",
      "DNS Server"
    ],
    "interval": 0,
    "sequenced": false,
    "active": true,
    "modified": "2019-11-15 11:42:21",
    "activeTimes": {
      "devices": {},
      "tags": {},
      "type": "exclusions",
      "version": 2
    },
    "priority": 0,
    "autoUpdatable": true,
    "autoUpdate": true,
    "autoSuppress": true,
    "description": "A device is making regular HTTP connections to a rare external location.\\n\
\nAction: Review the domains / IPs involved to see if they have a legitimate purpose. Many types
of software exhibit this type of behaviour by checking for updates or sending out usage
statistics. Consider why this device is running software that is not common within the network.",
    "behaviour": "decreasing",
    "defeats": [],
    "created": {
      "by": "System"
    },
    "edited": {
      "by": "Sarah",
      "userID": 24
    },
    "version": 16
  },
  "triggeredComponents": [
    {
      "time": 1582212985000,
      "cbid": 305422,
      "cid": 265,
      "chid": 265,
      "size": 3,
      "threshold": 2,
      "interval": 14400,
      "logic": {
        "data": {
          "left": "A",
          "operator": "AND",
          "right": {
            "left": "B",
            "operator": "AND",
            "right": {
            ...
          }
        },
```

Response is abbreviated.

Response Schema - `historicmodelonly=true&deviceattop=false`

Response Field	Type	Example Value	Description
`creationTime`	numeric	`1530000000000`	The timestamp that the record of the breach was created. This is distinct from the “time” field.
`breachUrl`	string	`https://appliance-fqdn/#modelbreaches/123`	A link to the specific model breach in the Darktrace Threat Visualizer - the configuration option FQDN must be set for this field to appear.
`commentCount`	numeric	`2`	The number of comments made against this breach.
`pbid`	numeric	`123`	The “policy breach ID” of the model breach.
`time`	numeric	`1530000000000`	The timestamp when the record was created in epoch time.
`model`	object		An object describing the model logic at the time of request. Requires `historicModelOnly=true` .
`model.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.phid`	numeric	`1`	The model “policy history” id. Increments when the model is modified.
`model.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.logic`	object		A data structure that describes the conditions to bring about a breach.
`model.logic.data`	array	`1`	If the model is a checklist type this will be a list of component ID numbers. If this model is a weighted type this will be a list of component ID, weight object pairs.
`model.logic.type`	string	`componentList`	The type of model.
`model.logic.version`	numeric	`1`	A number representing the version of model logic.
`model.throttle`	numeric	`3600`	For an individual device, this is the value in seconds for which this model will not fire again.
`model.sharedEndpoints`	boolean	`FALSE`	For models that contain multiple components that reference an endpoint, this value indicates whether all endpoints should be identical for the model to fire.
`model.actions`	object		The action to perform as a result of matching this model firing.
`model.actions.alert`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.

Response Field	Type	Example Value	Description
`model.actions.antigena`	object		An object containing the antigena response to be applied as a result of the model breaching.
`model.actions.breach`	boolean	`TRUE`	If true, an alert turned on will be pushed out to external systems if conditions for such alerting are met.
`model.actions.model`	boolean	`TRUE`	If true, creates an event in the device's event log without creating an alert/ model breach in the threat tray.
`model.actions.setPriority`	boolean	`FALSE`	If the priority is to be changed on breach, the numeric value it should become. If no priority change action, a false boolean.
`model.actions.setTag`	boolean	`FALSE`	If a tag is to be applied on model breach, a single number or array of the system ID for the tag(s) to be applied. If no tag action, a false boolean.
`model.actions.setType`	boolean	`FALSE`	If a change device type action is to be applied on model breach, the numeric system ID for the label to be applied. If no change device type action is applied to the model, a false boolean.
`model.tags`	array	`AP: Egress`	A list of tags that have been applied to this model in the Threat Visualizer model editor.
`model.interval`	numeric	`0`	Where a model contains multiple components, this interval represents the time window in seconds in which all the components should fire for this model to be breached.
`model.sequenced`	boolean	`FALSE`	Whether the components are required to fire in the specified order for the model breach to occur.
`model.active`	boolean	`TRUE`	Whether the model is enabled or disabled.
`model.modified`	string	`2018-06-12 14:00:00`	Timestamp at which the model was last modified, in a readable format.
`model.activeTimes`	object		An object describing device whitelisting or blacklisting configured for this model.
`model.activeTimes.devices`	object		The device ids for devices on the list.
`model.activeTimes.tags`	object		A system field.
`model.activeTimes.type`	string	`exclusions`	The type of list: "restrictions" indicates a blacklist, "exclusions" a whitelist.
`model.activeTimes.version`	numeric	`2`	A system field.
`model.priority`	numeric	`1`	The model's priority affects the strength with which it breaches (0-5 scale).
`model.autoUpdatable`	boolean	`TRUE`	Whether the model is suitable for auto update.
`model.autoUpdate`	boolean	`TRUE`	Whether the model is enabled for auto update.
`model.autoSuppress`	boolean	`TRUE`	Whether the model will automatically be suppressed in the case of over-breaching.

Response Field	Type	Example Value	Description
`model.description`	string	`A device is moving large volumes of data (1GiB+) out of the network within a short period of time. \n\nAction: Investigate if the external data transfer is a legitimate business activity or a loss of corporate data.`	The optional description of the model.
`model.behaviour`	string	`decreasing`	The score modulation function as set in the model editor.
`model.defeats`	array		A system field.
`model.created`	object		An object describing the creation of the model.
`model.created.by`	string	`System`	Username that created the model.
`model.edited`	object		An object describing the edit history of the model.
`model.edited.by`	string	`smartinez_admin`	Username that last edited the model.
`model.version`	numeric	`16`	The version of the model. Increments on each edit.
`triggeredComponents`	array		An array describing the model components that were triggered to create the model breach.
`triggeredComponents.time`	numeric	`1530000000000`	A timestamp in Epoch time at which the components were triggered.
`triggeredComponents.cbid`	numeric	`1729`	The “component breach id”. A unique identifier for the component breach.
`triggeredComponents.cid`	numeric	`1`	The “component id”. A unique identifier.
`triggeredComponents.chid`	numeric	`1`	The “component history id”. Increments when the component is edited.
`triggeredComponents.size`	numeric	`1155203452`	The ‘metric logic id’ for the metric used in the component.
`triggeredComponents.threshold`	numeric	`1073741824`	The number of times the component logic must be met within the interval timeframe.
`triggeredComponents.interval`	numeric	`3600`	The timeframe in seconds within which the threshold must be satisfied.
`triggeredComponents.logic`	object		An object describing the component logic.
`triggeredComponents.logic.data`	object		An object representing the logical relationship between component filters. Each filter is given an alphabetical reference and the contents of this object describe the relationship between those objects.
`triggeredComponents.logic.data.left`	string	`A`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.data.operator`	string	`AND`	A logical operator to compare filters with.

Response Field	Type	Example Value	Description
`triggeredComponents.logic.data.right`	object	`D`	Objects on the left will be compared with the object on the right using the specified operator.
`triggeredComponents.logic.version`	string	`v0.1`	The version of the component logic.
`triggeredComponents.metric`	object		An object describing the metric used in the component that triggered the Model Breach.
`triggeredComponents.metric.mlid`	numeric	`33`	The “metric logic” id - unique identifier.
`triggeredComponents.metric.name`	string	`externalclientdatatransfervolume`	The metric which data is returned for in system format.
`triggeredComponents.metric.label`	string	`External Data Volume as a Client`	The metric which data is returned for in readable format.
`triggeredComponents.device`	object		An object describing a device seen by Darktrace.
`triggeredComponents.device.did`	numeric	`96`	The “device id”, a unique identifier.
`triggeredComponents.device.ip`	string	`10.0.18.224`	The current IP associated with the device.
`triggeredComponents.device.ips`	array		IPs associated with the device historically.
`triggeredComponents.device.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`triggeredComponents.device.ips.timems`	numeric	`1528812000000`	The time the IP was last seen associated with that device in epoch time.
`triggeredComponents.device.ips.time`	string	`2018-06-12 14:00:00`	The time the IP was last seen associated with that device in readable format.
`triggeredComponents.device.ips.sid`	numeric	`34`	The subnet id for the subnet the IP belongs to.
`triggeredComponents.device.sid`	numeric	`34`	The subnet id for the subnet the device is currently located in.
`triggeredComponents.device.hostname`	string	`fs182`	The current device hostname.
`triggeredComponents.device.firstSeen`	numeric	`1528810000000`	The first time the device was seen on the network.
`triggeredComponents.device.lastSeen`	numeric	`1528810000000`	The last time the device was seen on the network.
`triggeredComponents.device.typename`	string	`server`	The device type in system format.
`triggeredComponents.device.typelabel`	string	`Server`	The device type in readable format.
`triggeredComponents.triggeredFilters`	array		The filters that comprise the component that were triggered to produce the model breach.
`triggeredComponents.triggeredFilters.cfid`	numeric	`1`	The ‘component filter id’. A unique identifier for the filter as part of a the component.
`triggeredComponents.triggeredFilters.id`	string	`A`	A filter that is used in the component logic. All filters are given alphabetical identifiers. Display filters - those that appear in the breach notification - can be identified by a lowercase ‘d’ and a numeral.
`triggeredComponents.triggeredFilters.filterType`	string	`Direction`	The filtertype that is used in the filter. A full list of filtertypes can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.arguments`	object		Whether the component is currently active as part of a model.

Response Field	Type	Example Value	Description
`triggeredComponents.triggeredFilters.arguments.value`	string	`out`	The value the filtertype should be compared against (using the specified comparator) to create the filter.
`triggeredComponents.triggeredFilters.comparatorType`	string	`is`	The comparator. A full list of comparators available for each filtertype can be found on the /filtertypes endpoint.
`triggeredComponents.triggeredFilters.trigger`	object		An object containing the value to be compared. Display filters will have an empty object.
`triggeredComponents.triggeredFilters.trigger.value`	string	`out`	The actual value that triggered the filter.
`score`	numeric	`0.443`	The model breach score, represented by a value between 0 and 1.

Example Response

Request: /modelbreaches/123?historicmodelonly=true&deviceattop=false

```
{
  "creationTime": 1582213002000,
  "commentCount": 0,
  "pbid": 123,
  "time": 1582212986000,
  "model": {
    "name": "Compromise::HTTP Beaconing to Rare Destination",
    "pid": 143,
    "phid": 123,
    "uuid": "1a814475-5fef-499b-a467-4e2e68352cbb",
    "logic": {
      "data": [
        265
      ],
      "type": "componentList",
      "version": 1
    },
    "throttle": 3600,
    "sharedEndpoints": false,
    "actions": {
      "alert": true,
      "antigena": {},
      "breach": true,
      "model": true,
      "setPriority": false,
      "setTag": false,
      "setType": false
    },
    "tags": [
      "AP: C2 Comms",
      "DNS Server"
    ],
    "interval": 0,
    "sequenced": false,
    "active": true,
    "modified": "2019-11-15 11:42:21",
    "activeTimes": {
      "devices": {},
      "tags": {},
      "type": "exclusions",
      "version": 2
    },
    "priority": 0,
    "autoUpdatable": true,
    "autoUpdate": true,
    "autoSuppress": true,
    "description": "A device is making regular HTTP connections to a rare external location.\\n\
\nAction: Review the domains / IPs involved to see if they have a legitimate purpose. Many types
of software exhibit this type of behaviour by checking for updates or sending out usage
statistics. Consider why this device is running software that is not common within the network.",
    "behaviour": "decreasing",
    "defeats": [],
    "created": {
      "by": "System"
    },
    "edited": {
      "by": "Sarah",
      "userID": 24
    },
    "version": 16
  },
  "triggeredComponents": [
    {
      "time": 1582212985000,
      "cbid": 305422,
      "cid": 265,
      "chid": 265,
      "size": 3,
      "threshold": 2,
      "interval": 14400,
      "logic": {
        "data": {
          "left": "A",
          "operator": "AND",
          "right": {
            "left": "B",
            "operator": "AND",
            "right": {
            ...
          }
        },
        "version": "v0.1"
      },
```

Response is abbreviated.

`minimal=true`

Response Field	Type	Example Value	Description
`commentCount`	numeric	`2`	The number of comments made against this breach.
`pbid`	numeric	`123`	The “policy breach ID” of the model breach.
`time`	numeric	`1528812554000`	The timestamp when the record was created in epoch time.
`model`	object		An object describing the model logic and history of the model that was breached.
`model.then`	object		An object describing the model logic at the time of breach. Requires `historicModelOnly=false` .
`model.then.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.then.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.then.phid`	numeric	`1`	The model “policy history” id. Increments when the model is modified.
`model.then.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.now`	object		An object describing the model logic at the time of request. Requires `historicModelOnly=false` .
`model.now.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.now.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.now.phid`	numeric	`3343`	The model “policy history” id. Increments when the model is modified.
`model.now.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`triggeredComponents`	array		A data structure that describes the conditions to bring about a breach. Empty when `minimal` is used.
`score`	numeric	`0.443`	The model breach score, represented by a value between 0 and 1.
`device`	object		An object describing a device seen by Darktrace.
`device.did`	numeric	`96`	The “device id”, a unique identifier.
`device.ip`	string	`10.0.18.224`	The current IP associated with the device.
`device.ips`	array		IPs associated with the device historically.
`device.ips.ip`	string	`10.0.18.224`	A historic IP associated with the device.
`device.ips.timems`	numeric	`1528812000000`	The time the IP was last seen associated with that device in epoch time.

Response Field	Type	Example Value	Description
`device.ips.time`	string	`6/12/18 14:00`	The time the IP was last seen associated with that device in readable format.
`device.ips.sid`	numeric	`34`	The subnet id for the subnet the IP belongs to.
`device.sid`	numeric	`34`	The subnet id for the subnet the device is currently located in.
`device.hostname`	string	`fs182`	The current device hostname.
`device.typename`	string	`server`	The device type in system format.
`device.typelabel`	string	`Server`	The device type in readable format.

Example Response

```
{
  "commentCount": 2,
  "pbid": 123,
  "time": 1528812554000,
  "model": {
    "then": {
      "name": "Anomalous Connection::1 GiB Outbound",
      "pid": 1,
      "phid": 1,
      "uuid": "80010119-6d7f-0000-0305-5e0000000215"
    },
    "now": {
      "name": "Anomalous Connection::1 GiB Outbound",
      "pid": 1,
      "phid": 3343,
      "uuid": "80010119-6d7f-0000-0305-5e0000000215"
    }
  },
  "triggeredComponents": [
    {}
  ],
  "score": 0.443,
  "device": {
    "did": 96,
    "ip": "10.0.18.224",
    "ips": [
      {
        "ip": "10.0.18.224",
        "timems": 1528812000000,
        "time": "2018-06-12 14:00:00",
        "sid": 34
      }
    ],
    "sid": 34,
    "hostname": "fs182",
    "typename": "server",
    "typelabel": "Server"
  }
```

Response Schema - `minimal=true&deviceattop=false`

Response Field	Type	Example Value	Description
`commentCount`	numeric	`2`	The number of comments made against this breach.
`pbid`	numeric	`123`	The “policy breach ID” of the model breach.
`time`	numeric	`1528812554000`	The timestamp when the record was created in epoch time.

Response Field	Type	Example Value	Description
`model`	object		An object describing the model logic and history of the model that was breached.
`model.then`	object		An object describing the model logic at the time of breach. Requires `historicModelOnly=false` .
`model.then.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.then.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.then.phid`	numeric	`1`	The model “policy history” id. Increments when the model is modified.
`model.then.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`model.now`	object		An object describing the model logic at the time of request. Requires `historicModelOnly=false` .
`model.now.name`	string	`Anomalous Connection::1 GiB Outbound`	Name of the model that was breached.
`model.now.pid`	numeric	`1`	The “policy id” of the model that was breached.
`model.now.phid`	numeric	`3343`	The model “policy history” id. Increments when the model is modified.
`model.now.uuid`	string	`80010119-6d7f-0000-0305-5e0000000215`	A unique ID that is generated on creation of the model.
`triggeredComponents`	array		A data structure that describes the conditions to bring about a breach.
`triggeredComponents.device`	object	`0.443`	An object describing a device that triggered the breach.
`triggeredComponents.device.did`	numeric		The “device id”, a unique identifier.
`triggeredComponents.device.ip`	string	`96`	The current IP associated with the device.
`triggeredComponents.device.ips`	array	`10.0.18.224`	IPs associated with the device historically.
`triggeredComponents.device.ips.ip`	string		A historic IP associated with the device.
`triggeredComponents.device.ips.timems`	numeric	`10.0.18.224`	The time the IP was last seen associated with that device in epoch time.
`triggeredComponents.device.ips.time`	string	`1528812000000`	The time the IP was last seen associated with that device in readable format.
`triggeredComponents.device.ips.sid`	numeric	`6/12/18 14:00`	The subnet id for the subnet the IP belongs to.
`triggeredComponents.device.sid`	numeric	`34`	The subnet id for the subnet the device is currently located in.
`triggeredComponents.device.hostname`	string	`34`	The current device hostname.
`triggeredComponents.device.typename`	string	`fs182`	The device type in system format.
`triggeredComponents.device.typelabel`	string	`server`	The device type in readable format.
`score`	numeric	`Server`	The model breach score, represented by a value between 0 and 1.

Example Response

```
{
  "commentCount": 2,
  "pbid": 123,
  "time": 1528812554000,
  "model": {
    "then": {
      "name": "Anomalous Connection::1 GiB Outbound",
      "pid": 1,
      "phid": 1,
      "uuid": "80010119-6d7f-0000-0305-5e0000000215"
    },
    "now": {
      "name": "Anomalous Connection::1 GiB Outbound",
      "pid": 1,
      "phid": 3343,
      "uuid": "80010119-6d7f-0000-0305-5e0000000215"
    }
  },
  "triggeredComponents": [
    {
      "device": {
        "did": 96,
        "ip": "10.0.18.224",
        "ips": [
          {
            "ip": "10.0.18.224",
            "timems": 1528812000000,
            "time": "2018-06-12 14:00:00",
            "sid": 34
          }
        ],
        "sid": 34,
        "hostname": "fs182",
        "typename": "server",
        "typelabel": "Server"
      }
    }
  ],
  "score": 0.443
}
```

minimal=true&historicmodelonly=true

Response Field	Type	Example Value	Description
commentCount	numeric	2	The number of comments made against this breach.
pbid	numeric	123	The “policy breach ID” of the model breach.
time	numeric	1528812554000	The timestamp when the record was created in epoch time.
model	object		An object describing the model logic and history of the model that was breached.
model.name	string	Anomalous Connection::1 GiB Outbound	Name of the model that was breached.
model.pid	numeric	1	The “policy id” of the model that was breached.
model.phid	numeric	1	The model “policy history” id. Increments when the model is modified.

Response Field	Type	Example Value	Description
model.uuid	string	80010119-6d7f-0000-0305-5e0000000215	A unique ID that is generated on creation of the model.
triggeredComponents	array		A data structure that describes the conditions to bring about a breach.
score	numeric	0.443	The model breach score, represented by a value between 0 and 1.
device	object		An object describing a device seen by Darktrace.
device.did	numeric	96	The “device id”, a unique identifier.
device.ip	string	10.0.18.224	The current IP associated with the device.
device.ips	array		IPs associated with the device historically.
device.ips.ip	string	10.0.18.224	A historic IP associated with the device.
device.ips.timems	numeric	1528812000000	The time the IP was last seen associated with that device in epoch time.
device.ips.time	string	6/12/18 14:00	The time the IP was last seen associated with that device in readable format.
device.ips.sid	numeric	34	The subnet id for the subnet the IP belongs to.
device.sid	numeric	34	The subnet id for the subnet the device is currently located in.
device.hostname	string	fs182	The current device hostname.
device.typename	string	server	The device type in system format.
device.typelabel	string	Server	The device type in readable format.

Example Response

```
{
  "commentCount": 2,
  "pbid": 123,
  "time": 1528812554000,
  "model": {
    "name": "Anomalous Connection::1 GiB Outbound",
    "pid": 1,
    "phid": 1,
    "uuid": "80010119-6d7f-0000-0305-5e0000000215"
  },
  "triggeredComponents": [
    {
      "device": {
        "did": 96,
        "ip": "10.0.18.224",
        "ips": [
          {
            "ip": "10.0.18.224",
            "timems": 1528812000000,
            "time": "2018-06-12 14:00:00",
            "sid": 34
          }
        ],
        "sid": 34,
        "hostname": "fs182",
        "typename": "server",
        "typelabel": "Server"
      }
    }
  ],
  "score": 0.443
}
```

/modelbreaches/[pbid]/comments

The `/comments` extension of the `/modelbreaches` endpoint returns current comments on a model breach and allows for new comments to be posted, given a `pbid` value. The `pbid` must be specified as part of the extension in the format: `/modelbreaches/[pbid]/comments` .

`POST` requests to this endpoint must be made in JSON format.

Request Type(s)

`[GET]` `[POST]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object. Available for GET requests only.

Example Request

1. `GET` all comments for a model breach with `pbid=123` :

```
https://<applianceIP>/modelbreaches/123/comments
```

2. `POST` a comment to a model breach with `pbid=123` :

```
https://<applianceIP>/modelbreaches/123/comments with body {"message": "Test Comment"}
```

Example Response

Request: /modelbreaches/123/comments

```
[
  {
    "message": "Test Comment",
    "username": "Sarah",
    "time": 1582120499000,
    "pid": 12
  },
  {
    "message": "Test Comment 2",
    "username": "Chris",
    "time": 1582120616000,
    "pid": 12
  }
]
```

/modelbreaches/[pbid]/comments Response Schema

Response Schema

Response Field	Type	Example Value	Description
`message`	string	`Assigned to Aidan Johnston for investigation.`	The comment text.
`username`	string	`ecarr`	The user who made the comment.
`time`	numeric	`1580000000000`	The time the comment was posted in epoch time.
`pid`	numeric	`806`	The policy id of the model that was breached.

Example Response

```
[
  {
    "message": "Test Comment",
    "username": "ecarr",
    "time": 1582120499000,
    "pid": 12
  },
  {
    "message": "Assigned to Aidan Johnston for investigation",
    "username": "cchester_admin",
    "time": 1582120616000,
    "pid": 12
  }
]
```

/modelbreaches/[pbid]/acknowledge and /unacknowledge

The `/acknowledge` and `/unacknowledge` extensions of the `/modelbreaches` endpoint allow for breaches to be acknowledged or unacknowledged programmatically, given a `pbid` value. This can be very useful when integrating Darktrace with other SOC or ticket-management tools.

The `pbid` must be specified as part of the extension in the format: `/modelbreaches/[pbid]/acknowledge` or `/modelbreaches/[pbid]/unacknowledge`.

Request Type(s)

`[POST]`

Parameters

Parameter	Type	Description
`acknowledge`	boolean	Acknowledge the model breach. Only available for the `/acknowledge` endpoint

Parameter	Type	Description
`unacknowledge`	boolean	Unacknowledge the model breach. Only available for the `/unacknowledge` endpoint

Example Request

1. `POST` to acknowledge a model breach with `pbid=123`:

```
https://<applianceIP>/modelbreaches/123/acknowledge with body acknowledge=true
```

2. `POST` to unacknowledge a model breach with `pbid=123`:

```
https://<applianceIP>/modelbreaches/123/unacknowledge with body unacknowledge=true
```

/network

The `/network` endpoint returns data about connectivity between two or more devices - it can take a device or subnet option - and can be used for investigative and monitoring purposes.

The default metric used is “Data Transfer Volume”, but any metric may be specified to monitor connectivity, behavior and protocol usage. See /metrics for details of how to review all metrics available, and metrics for definitions of a subset of available metrics.

The statistics object returns the information found on the right-hand side of the Threat Visualizer when a subnet is focused upon.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`applicationprotocol`	string	This filter can be used to filter the returned data by application protocol. See /enums for the list of application protocols.
`destinationport`	numeric	This filter can be used to filter the returned data by destination port.
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`endtime`	numeric	End time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`from`	string	Start time of data to return in YYYY-MM-DD HH:MM:SS format.
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`intext`	string	This filter can be used to filter the returned data to that which interacts with external sources and destinations, or is restricted to internal. Valid values are internal and external.
`ip`	string	Return data for this IP address.
`metric`	string	Name of a metric. See the `/metrics` endpoint for the full list of current metrics.
`port`	numeric	This filter can be used to filter the returned data by source or destination port.
`protocol`	string	This filter can be used to filter the returned data by IP protocol. See /enums for the list of protocols.
`sourceport`	numeric	This filter can be used to filter the returned data by source port
`starttime`	numeric	Start time of data to return in millisecond format, relative to midnight January 1st 1970 UTC.
`to`	string	End time of data to return in YYYY-MM-DD HH:MM:SS format.
`viewsubnet`	numeric	Takes an `sid` value to focus on a specific subnet.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- Time parameters must always be specified in pairs.
- The devices object contains any internal source/destination devices, the connection direction will not be specified. The connections object will specify source/target device pairs and directions.

- The default query for devices uses `intext=internal` , filtering the returned connections by internal only. Specifying `intext=external` will add an `externaldevices` object containing any external source/ destination devices the device has interacted with. The default query for subnets will return both internal and external.
- The default timeframe is one hour.
- Please note, this endpoint does not support SaaS metrics.

Example Request

1. `GET` the data transfer volume for the device with id 1 on December 10th 2019:

```
https://<applianceIP>/network?
did=1&metric=datatransfervolume&from=2019-12-10T12:00:00&to=2019-12-10
```

Example Response

Request: /network?did=212&metric=datatransfervolume&fulldevicedetails=false

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "Single device",
          "in": false,
          "out": false
        },
        {
          "View": "All devices",
          "in": false,
          "out": false
        },
        {
          "View": "Breach devices",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "Normal",
          "in": 51430,
          "out": 25305
        },
        {
          "Connections": "New",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Unusual",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Remote Ports": [
        {
          "rport": 53,
          "in": 51430,
          "out": 24990
        }
        ...
      ]
    },
    {
      "Local Ports": [
        {
          "lport": 58335,
          "in": 51430,
          "out": 24990
        }
        ...
      ]
    },
    {
      "devices": [
        {
          "device": "192.168.72.4",
          "ip": "192.168.72.4",
          "in": 43078,
          "out": 16660
        }
        ...
      ]
    },
    {
      "Subnets": []
    },
    {
      "intext": [
        {
          "intext": "Internal",
```

/network Response Schema

Note: The `statistics` object will always contain statistics about data transfer, regardless of the metric specified in the request.

Response Schema - `did`

`fulldevicedetails=false`

Response Field	Type	Example Value	Description
`statistics`	array		An array of statistics about the connections made by the device or subnet. Regardless of the metric specified, these statistics will always relate to data transfer volumes.
`statistics.Views`	array		An array of system fields
`statistics.Views.View`	string	`Single device`	A system field
`statistics.Views.in`	boolean	`FALSE`	A system field
`statistics.Views.out`	boolean	`FALSE`	A system field
`statistics.Connection Status`	array		An array of statuses that the connections may be classified as
`statistics.Connection Status.Connections`	string	`Normal`	A connection status. May be Normal, Unusual, New or Breached.
`statistics.Connection Status.in`	numeric	`95567`	The total inbound data transfer for the device during the timeframe in bytes
`statistics.Connection Status.out`	numeric	`36964662`	The total outbound data transfer for the device during the timeframe in bytes
`statistics.Remote Ports`	array		An array of remote ports (ports on other devices) that the device has sent data to or received data from
`statistics.Remote Ports.rport`	numeric	`51728`	A remote port interacted with by the specified device
`statistics.Remote Ports.in`	numeric	`41813`	The amount of data received from the remote port
`statistics.Remote Ports.out`	numeric	`36939077`	The amount of data sent to the remote port
`statistics.Local Ports`	array		An array of local ports (ports on the specified device) that the device has sent data from or received data to
`statistics.Local Ports.lport`	numeric	`22`	A local port on the specified device
`statistics.Local Ports.in`	numeric	`41813`	The amount of data received by that local port
`statistics.Local Ports.out`	numeric	`36939225`	The amount of data sent from that local port
`statistics.devices`	array		An array of other devices that the device has sent data to or received data from
`statistics.devices.device`	string	`10.0.18.224`	The hostname or IP of the other device
`statistics.devices.ip`	string	`10.0.18.224`	The IP of the other device
`statistics.devices.in`	numeric	`41813`	The amount of data received from that device

Response Field	Type	Example Value	Description
`statistics.devices.out`	numeric	`36939225`	The amount of data sent to that device
`statistics.Subnets`	array		When a subnet is specified, an array of subnets that devices in the specified subnet have interacted with.
`statistics.intext`	array		An array of information about the type of connection and data transferred
`statistics.intext.intext`	string	`Internal`	The connection type filter - either external or internal
`statistics.intext.in`	numeric	`95567`	The total inbound data transfer for the device during the timeframe in bytes
`statistics.intext.out`	numeric	`36964662`	The total outbound data transfer for the device during the timeframe in bytes
`statistics.protocols`	array		An array of network protocols identified in the connections
`statistics.protocols.protocol`	string	`TCP`	A network protocol
`statistics.protocols.in`	numeric	`41813`	The volume of inbound data transferred using that protocol
`statistics.protocols.out`	numeric	`36939225`	The volume of outbound data transferred using that protocol
`statistics.applicationprotocols`	array		An array of application protocols used in the connections
`statistics.applicationprotocols.applicationprotocol`	string	`SSH`	An application protocol
`statistics.applicationprotocols.in`	numeric	`41813`	The volume of inbound data transferred using that protocol
`statistics.applicationprotocols.out`	numeric	`36939225`	The volume of outbound data transferred using that protocol
`subnets`	array		An array of subnets that have been interacted with by the device
`devices`	array		When a single device is specified, information about that specific device and any others it has communicated with.
`devices.did`	numeric	`174`	The “device id” of the specified device.
`devices.size`	numeric	`37060229`	Depending on the metric specified, the amount of data transferred in the connections involving that device or the number of matching connections.
`devices.timems`	numeric	`1586270000000`	The time the IP was last seen associated with that device in epoch time
`devices.ips`	array	`10.15.3.39`	IPs associated with the device historically
`devices.sid`	numeric	`82`	The subnet id for the subnet the device is currently located in
`devices.ip`	string	`10.15.3.39`	The current IP associated with the device
`devices.network`	string	`10.15.3.0/24`	The IP address range that describes the subnet the IP is contained within
`metric`	object		An object describing the metric queried upon
`metric.mlid`	numeric	`17`	The “metric logic” id - unique identifier.

Response Field	Type	Example Value	Description
`metric.name`	string	`datatransfervolume`	The metric which data is returned for in system format
`metric.label`	string	`Data Transfer`	The metric which data is returned for in readable format
`metric.units`	string	`bytes`	The units the metric is measured in, if applicable.
`metric.filtertypes`	array	`Unusual ASN for domain`	An array of filters which can be used with this metric
`metric.unitsinterval`	numeric	`3600`	The default time interval for the metric
`metric.lengthscale`	numeric	`599997600`	A system field
`connections`	array		An array of connection objects associated with the device and metric over the time period
`connections.source`	object		An object describing the source of a connection
`connections.source.id`	numeric	`-6`	The device id for the source of the connection
`connections.source.ip`	string	`10.15.3.39`	The IP of the source device
`connections.source.type`	string	`subnet`	The type of device, host or entity originating the connection.
`connections.target`	object		An object describing the source of a target
`connections.target.id`	numeric	`174`	The device id for the target of the connection
`connections.target.ip`	string	`10.15.3.39`	The IP of the target device
`connections.target.type`	string	`device`	The type of device, host or entity targeted by the connection.
`connections.timems`	numeric	`1586270000000`	A timestamp for the connection in epoch time
`connections.size`	numeric	`36000000`	The time frame covered by the initial request in seconds x 10000

Example Response

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "Single device",
          "in": false,
          "out": false
        },
        {
          "View": "All devices",
          "in": false,
          "out": false
        },
        {
          "View": "Breach devices",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "Normal",
          "in": 51430,
          "out": 25305
        },
        {
          "Connections": "New",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Unusual",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Remote Ports": [
        {
          "rport": 53,
          "in": 51430,
          "out": 24990
        }
        ...
      ]
    },
    {
      "Local Ports": [
        {
          "lport": 58335,
          "in": 51430,
          "out": 24990
        }
        ...
      ]
    },
    {
      "devices": [
        {
          "device": "192.168.72.4",
          "ip": "192.168.72.4",
          "in": 43078,
          "out": 16660
        }
        ...
      ]
    },
    {
      "Subnets": []
    },
    {
      "intext": [
        {
          "intext": "Internal",
```

Response is abbreviated.

`fulldevicedetails=true`

Response Field	Type	Example Value	Description
`statistics`	array		An array of statistics about the connections made by the device or subnet. Regardless of the metric specified, these statistics will always relate to data transfer volumes.
`statistics.Views`	array		An array of system fields.
`statistics.Views.View`	string	`Single device`	A system field.
`statistics.Views.in`	boolean	`FALSE`	A system field.
`statistics.Views.out`	boolean	`FALSE`	A system field.
`statistics.Connection Status`	array		An array of statuses that the connections may be classified as.
`statistics.Connection Status.Connections`	string	`Normal`	A connection status. May be Normal, Unusual, New or Breached.
`statistics.Connection Status.in`	numeric	`95747`	The total inbound data transfer for the device during the timeframe in bytes.
`statistics.Connection Status.out`	numeric	`38059962`	The total outbound data transfer for the device during the timeframe in bytes.
`statistics.Remote Ports`	array		An array of remote ports (ports on other devices) that the device has sent data to or received data from.
`statistics.Remote Ports.rport`	numeric	`51728`	A remote port interacted with by the specified device.
`statistics.Remote Ports.in`	numeric	`42137`	The amount of data received from the remote port.
`statistics.Remote Ports.out`	numeric	`38034377`	The amount of data sent to the remote port.
`statistics.Local Ports`	array		An array of local ports (ports on the specified device) that the device has sent data from or received data to.
`statistics.Local Ports.lport`	numeric	`22`	A local port on the specified device.
`statistics.Local Ports.in`	numeric	`42137`	The amount of data received by that local port.
`statistics.Local Ports.out`	numeric	`38034525`	The amount of data sent from that local port.
`statistics.devices`	array		An array of other devices that the device has sent data to or received data from.
`statistics.devices.device`	string	`10.0.18.224`	The hostname or IP of the other device.
`statistics.devices.ip`	string	`10.0.18.224`	The IP of the other device.
`statistics.devices.in`	numeric	`42137`	The amount of data received from that device.
`statistics.devices.out`	numeric	`38034525`	The amount of data sent to that device.
`statistics.Subnets`	array		When a subnet is specified, an array of subnets that devices in the specified subnet have interacted with.

Response Field	Type	Example Value	Description
statistics.intext	array		An array of information about the type of connection and data transferred.
statistics.intext.intext	string	Internal	The connection type filter - either external or internal.
statistics.intext.in	numeric	95747	The total inbound data transfer for the device during the timeframe in bytes.
statistics.intext.out	numeric	38059962	The total outbound data transfer for the device during the timeframe in bytes.
statistics.protocols	array		An array of network protocols identified in the connections.
statistics.protocols.protocol	string	TCP	A network protocol.
statistics.protocols.in	numeric	42137	The volume of inbound data transferred using that protocol.
statistics.protocols.out	numeric	38034525	The volume of outbound data transferred using that protocol.
statistics.applicationprotocols	array		An array of application protocols used in the connections.
statistics.applicationprotocols.applicationprotocol	string	SSH	An application protocol.
statistics.applicationprotocols.in	numeric	42137	The volume of inbound data transferred using that protocol.
statistics.applicationprotocols.out	numeric	38034525	The volume of outbound data transferred using that protocol.
subnets	array		An array of subnets that have been interacted with by the device.
devices	array		When a single device is specified, information about that specific device and any others it has communicated with.
devices.did	numeric	532	The “device id” of the specified device.
devices.macaddress	string	6e:b7:31:d5:33:6c	The current MAC address associated with the device.
devices.vendor	string	ASUSTek COMPUTER INC.	The vendor of the device network card as derived by Darktrace from the MAC address.
devices.ip	string	10.12.14.2	The current IP associated with the device.
devices.ips	array		IPs associated with the device historically.
devices.ips.ip	string	10.12.14.2	The current IP associated with the device.
devices.ips.timems	numeric	1586937881000	The time the IP was last seen associated with that device in epoch time.
devices.ips.time	string	2020-04-15 08:04:41	The time the IP was last seen associated with that device in readable format.
devices.ips.sid	numeric	39	The subnet id for the subnet the IP belongs to.
devices.sid	numeric	39	The subnet id for the subnet the device is currently located in.
devices.hostname	string	sarah-desktop-12	The current device hostname.
devices.firstSeen	numeric	1530000000000	The first time the device was seen on the network.

Response Field	Type	Example Value	Description
devices.lastSeen	numeric	1590000000000	The last time the device was seen on the network.
devices.os	string	Linux 3.11 and newer	The device operating system if Darktrace is able to derive it.
devices.typename	string	desktop	The device type in system format.
devices.typelabel	string	Desktop	The device type in readable format.
devices.tags	array		An object describing tags applied to the device.
devices.tags.tid	numeric	73	The “tag id”. A unique value.
devices.tags.expiry	numeric	0	The expiry time for the tag when applied to a device.
devices.tags.thid	numeric	78	The “tag history” id. Increments if the tag is edited.
devices.tags.name	string	Test Tag	The tag label displayed in the user interface or in objects that reference the tag.
devices.tags.restricted	boolean	FALSE	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
devices.tags.data	object		An object containing information about the tag.
devices.tags.data.auto	boolean	FALSE	Whether the tag was auto-generated.
devices.tags.data.color	numeric	134	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
devices.tags.data.description	string	Testing the use of tags.	An optional description summarizing the purpose of the tag.
devices.tags.data.visibility	string	Public	A system field.
devices.tags.isReferenced	boolean	FALSE	Whether the tag is used by one or more model components.
devices.size	numeric	38155709	Depending on the metric specified, the amount of data transferred in the connections involving that device or the number of matching connections.
devices.timems	numeric	1590000000000	A timestamp at which the data was gathered in epoch time.
devices.network	string	10.12.14.0/24	The IP address range that describes the subnet the IP is contained within
metric	object		An object describing the metric queried upon.
metric.mlid	numeric	17	The “metric logic” id - unique identifier.
metric.name	string	datatransfervolume	The metric which data is returned for in system format.
metric.label	string	Data Transfer	The metric which data is returned for in readable format.
metric.units	string	bytes	The units the metric is measured in, if applicable.
metric.filtertypes	array	Direction	An array of filters which can be used with this metric.
metric.unitsinterval	numeric	3600	The default time interval for the metric.

Response Field	Type	Example Value	Description
`metric.lengthscale`	numeric	`599997600`	A system field.
`connections`	array		An array of connection objects associated with the device and metric over the time period.
`connections.source`	object		An object describing the source of a connection.
`connections.source.id`	numeric	`-6`	The device id for the source of the connection.
`connections.source.ip`	string	`10.15.3.39`	The IP of the source device.
`connections.source.type`	string	`subnet`	The type of device, host or entity originating the connection.
`connections.target`	object		An object describing the source of a target.
`connections.target.id`	numeric	`532`	The device id for the target of the connection.
`connections.target.ip`	string	`10.12.14.2`	The IP of the target device.
`connections.target.type`	string	`device`	The type of device, host or entity targeted by the connection.
`connections.timems`	numeric	`1590000000000`	A timestamp for the connection in epoch time.
`connections.size`	numeric	`36000000`	The time frame covered by the initial request in seconds x 10000.

Example Response

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "Single device",
          "in": false,
          "out": false
        },
        {
          "View": "All devices",
          "in": false,
          "out": false
        },
        {
          "View": "Breach devices",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "Normal",
          "in": 51574,
          "out": 25305
        },
        {
          "Connections": "New",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Unusual",
          "in": 0,
          "out": 0
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Remote Ports": [
        {
          "rport": 53,
          "in": 51574,
          "out": 24990
        }
        ...
      ]
    },
    {
      "Local Ports": [
        {
          "lport": 58335,
          "in": 51574,
          "out": 24990
        }
        ...
      ]
    },
    {
      "devices": [
        {
          "device": "192.168.72.4",
          "ip": "192.168.72.4",
          "in": 43078,
          "out": 16660
        }
        ...
      ]
    },
    {
      "Subnets": []
    },
    {
      "intext": [
        {
          "intext": "Internal",
```

Response is abbreviated.

Response Schema - `did` and `intext=external`

`fulldevicedetails=false`

Response Field	Type	Example Value	Description
`statistics`	array		An array of statistics about the connections made by the device or subnet. Regardless of the metric specified, these statistics will always relate to data transfer volumes.
`statistics.Views`	array		An array of system fields.
`statistics.Views.View`	string	`Single device`	A system field.
`statistics.Views.in`	boolean	`FALSE`	A system field.
`statistics.Views.out`	boolean	`FALSE`	A system field.
`statistics.Connection Status`	array		An array of statuses that the connections may be classified as.
`statistics.Connection Status.Connections`	string	`Normal`	A connection status. May be Normal, Unusual, New or Breached.
`statistics.Connection Status.in`	numeric	`20573`	The total inbound data transfer for the device during the timeframe in bytes.
`statistics.Connection Status.out`	numeric	`4793`	The total outbound data transfer for the device during the timeframe in bytes.
`statistics.Remote Ports`	array		An array of remote ports (ports on other devices) that the device has sent data to or received data from.
`statistics.Remote Ports.rport`	numeric	`443`	A remote port interacted with by the specified device.
`statistics.Remote Ports.in`	numeric	`20573`	The amount of data received from the remote port.
`statistics.Remote Ports.out`	numeric	`4793`	The amount of data sent to the remote port.
`statistics.Local Ports`	array		An array of local ports (ports on the specified device) that the device has sent data from or received data to.
`statistics.Local Ports.lport`	numeric	`51416`	A local port on the specified device.
`statistics.Local Ports.in`	numeric	`7955`	The amount of data received by that local port.
`statistics.Local Ports.out`	numeric	`1733`	The amount of data sent from that local port.
`statistics.devices`	array		An array of other devices that the device has sent data to or received data from.
`statistics.devices.device`	string	`google.com`	The hostname or IP of the other device.
`statistics.devices.ip`	string	`google.com`	The IP of the other device. For external locations, this may be a hostname.
`statistics.devices.in`	numeric	`15023`	The amount of data received from that device.
`statistics.devices.out`	numeric	`3467`	The amount of data sent to that device.

Response Field	Type	Example Value	Description
statistics.intext	array		An array of information about the type of connection and data transferred.
statistics.intext.intext	string	External	The connection type filter - either external or internal.
statistics.intext.in	numeric	20573	The total inbound data transfer for the device during the timeframe in bytes.
statistics.intext.out	numeric	4793	The total outbound data transfer for the device during the timeframe in bytes.
statistics.protocols	array		An array of network protocols identified in the connections.
statistics.protocols.protocol	string	TCP	A network protocol.
statistics.protocols.in	numeric	20573	The volume of inbound data transferred using that protocol.
statistics.protocols.out	numeric	4793	The volume of outbound data transferred using that protocol.
statistics.applicationprotocols	array		An array of application protocols used in the connections.
statistics.applicationprotocols.applicationprotocol	string	HTTPS	An application protocol.
statistics.applicationprotocols.in	numeric	20573	The volume of inbound data transferred using that protocol.
statistics.applicationprotocols.out	numeric	4793	The volume of outbound data transferred using that protocol.
subnets	array		An array of subnets that have been interacted with by the device.
devices	array		When a single device is specified, information about that specific device and any others it has communicated with.
devices.did	numeric	83	The “device id” of the specified device.
devices.size	numeric	18490	Depending on the metric specified, the amount of data transferred in the connections involving that device or the number of matching connections.
devices.timems	numeric	1586937881000	A timestamp at which the data was gathered in epoch time.
devices.ips	array	10.15.3.39	IPs associated with the device historically.
devices.sid	numeric	77	The subnet id for the subnet the device is currently located in.
devices.ip	string	10.15.3.39	The current IP associated with the device.
devices.network	string	10.15.3.0/24	The IP address range that describes the subnet the IP is contained within
externaldevices	array		An array of external devices that the specified device has interacted with.
externaldevices.id	numeric	0	Where applicable, an id for the external device. This can be cross-referenced with the connections object.
externaldevices.size	numeric	18490	Depending on the metric specified, the amount of data transferred in the connections involving that external location or the number of matching connections.

Response Field	Type	Example Value	Description
externaldevices.timems	numeric	1586937881000	A timestamp at which the data was gathered in epoch time.
externaldevices.hostname	string	google.com	A hostname associated with the external device.
externaldevices.name	string	104.20.203.23	A hostname or IP associated with the external device.
externaldevices.hostnames	array		An array of hostnames that have been historically associated with the external location.
externaldevices.hostnames.hostname	string	google.com	A hostname associated with the external device.
externaldevices.hostnames.count	numeric	3	The number of connections to that hostname during the specified timeframe.
externaldevices.ip	string	172.217.169.36	The IP associated with the hostname.
externaldevices.longitude	numeric	172.217.169.36	For the reported IP location, the longitude value to plot the IP on a map.
externaldevices.latitude	numeric	37.751	For the reported IP location, the latitude value to plot the IP on a map.
externaldevices.country	string	United States	The country that the IP is located in.
externaldevices.countrycode	string	US	The system country code for the country that the IP is located in.
externaldevices.asn	string	AS15169 Google LLC	The ASN for the IP.
externaldevices.region	string	North America	The geographical region the IP is located in.
metric	object		An object describing the metric queried upon.
metric.mlid	numeric	17	The “metric logic” id - unique identifier.
metric.name	string	datatransfervolume	The metric which data is returned for in system format.
metric.label	string	Data Transfer	The metric which data is returned for in readable format.
metric.units	string	bytes	The units the metric is measured in, if applicable.
metric.filtertypes	array	Feature model	An array of filters which can be used with this metric.
metric.unitsinterval	numeric	3600	The default time interval for the metric.
metric.lengthscale	numeric	599997600	A system field.
connections	array		An array of connection objects associated with the device and metric over the time period.
connections.source	object		An object describing the source of a connection.
connections.source.id	numeric	2899945802	The device id for the source of the connection.
connections.source.ip	string	10.15.3.39	The IP of the source device. For external locations, this field may not appear.
connections.source.type	string	externaldevice	The type of device, host or entity originating the connection.

Response Field	Type	Example Value	Description
`connections.target`	object		An object describing the source of a target.
`connections.target.id`	numeric	`83`	The device id for the target of the connection.
`connections.target.ip`	string	`192.168.72.4`	The IP of the target device. For external locations, this field may not appear.
`connections.target.type`	string	`device`	The type of device, host or entity targeted by the connection.
`connections.timems`	numeric	`1586937881000`	A timestamp for the connection in epoch time.
`connections.size`	numeric	`36000000`	The time frame covered by the initial request in seconds x 10000.

Example Response

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "Single device",
          "in": false,
          "out": false
        },
        {
          "View": "All devices",
          "in": false,
          "out": false
        },
        {
          "View": "Breach devices",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "New",
          "in": false,
          "out": false
        },
        {
          "Connections": "Unusual",
          "in": false,
          "out": false
        },
        {
          "Connections": "Normal",
          "in": false,
          "out": false
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "applicationprotocols": [
        {
          "applicationprotocol": "HTTPS",
          "in": 13500,
          "out": 4794
        }
      ]
    }
  ],
  "subnets": [],
  "devices": [
    {
      "did": 212,
      "size": 76735,
      "timems": 1587138366410,
      "ips": [
        "10.15.3.39"
      ],
      "sid": 12,
      "ip": "10.15.3.39",
      "network": "10.15.3.0/24"
    }
  ],
  "externaldevices": [
    {
      "id": 3627731978,
      "size": 15004,
      "timems": 1587142558420,
      "hostname": "google.com",
      "name": "google.com",
      "hostnames": [
        {
          "hostname": "google.com",
          "count": 6
        }
      ],
      "longitude": -122.075,
```

Response is abbreviated.

`fulldevicedetails=true`

Response Field	Type	Example Value	Description
`statistics`	array		An array of statistics about the connections made by the device or subnet. Regardless of the metric specified, these statistics will always relate to data transfer volumes.
`statistics.Views`	array		An array of system fields.
`statistics.Views.View`	string	`Single device`	A system field.
`statistics.Views.in`	boolean	`FALSE`	A system field.
`statistics.Views.out`	boolean	`FALSE`	A system field.
`statistics.Connection Status`	array		An array of statuses that the connections may be classified as.
`statistics.Connection Status.Connections`	string	`Normal`	A connection status. May be Normal, Unusual, New or Breached.
`statistics.Connection Status.in`	numeric	`20573`	The total inbound data transfer for the device during the timeframe in bytes.
`statistics.Connection Status.out`	numeric	`4793`	The total outbound data transfer for the device during the timeframe in bytes.
`statistics.Remote Ports`	array		An array of remote ports (ports on other devices) that the device has sent data to or received data from.
`statistics.Remote Ports.rport`	numeric	`443`	A remote port interacted with by the specified device.
`statistics.Remote Ports.in`	numeric	`20573`	The amount of data received from the remote port.
`statistics.Remote Ports.out`	numeric	`4793`	The amount of data sent to the remote port.
`statistics.Local Ports`	array		An array of local ports (ports on the specified device) that the device has sent data from or received data to.
`statistics.Local Ports.lport`	numeric	`51416`	A local port on the specified device.
`statistics.Local Ports.in`	numeric	`7955`	The amount of data received by that local port.
`statistics.Local Ports.out`	numeric	`1733`	The amount of data sent from that local port.
`statistics.devices`	array		An array of other devices that the device has sent data to or received data from.
`statistics.devices.device`	string	`google.com`	The hostname or IP of the other device.
`statistics.devices.ip`	string	`google.com`	The IP of the other device. For external locations, this may be a hostname.
`statistics.devices.in`	numeric	`15023`	The amount of data received from that device.
`statistics.devices.out`	numeric	`3467`	The amount of data sent to that device.
`statistics.intext`	array		An array of information about the type of connection and data transferred.

Response Field	Type	Example Value	Description
`statistics.intext.intext`	string	`External`	The connection type filter - either external or internal.
`statistics.intext.in`	numeric	`20573`	The total inbound data transfer for the device during the timeframe in bytes.
`statistics.intext.out`	numeric	`4793`	The total outbound data transfer for the device during the timeframe in bytes.
`statistics.protocols`	array		An array of network protocols identified in the connections.
`statistics.protocols.protocol`	string	`TCP`	A network protocol.
`statistics.protocols.in`	numeric	`20573`	The volume of inbound data transferred using that protocol.
`statistics.protocols.out`	numeric	`4793`	The volume of outbound data transferred using that protocol.
`statistics.applicationprotocols`	array		An array of application protocols used in the connections.
`statistics.applicationprotocols.applicationprotocol`	string	`HTTPS`	An application protocol.
`statistics.applicationprotocols.in`	numeric	`20573`	The volume of inbound data transferred using that protocol.
`statistics.applicationprotocols.out`	numeric	`4793`	The volume of outbound data transferred using that protocol.
`subnets`	array		An array of subnets that have been interacted with by the device.
`devices`	array		When a single device is specified, information about that specific device and any others it has communicated with.
`devices.did`	numeric	`3877`	The “device id” of the specified device.
`devices.macaddress`	string	`93:gb:28:g1:fc:g1`	The current MAC address associated with the device.
`devices.vendor`	string	`ASUSTek COMPUTER INC.`	The vendor of the device network card as derived by Darktrace from the MAC address.
`devices.ip`	string	`10.15.3.39`	The current IP associated with the device.
`devices.ips`	array		IPs associated with the device historically.
`devices.ips.ip`	string	`10.15.3.39`	The current IP associated with the device.
`devices.ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`devices.ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`devices.ips.sid`	numeric	`82`	The subnet id for the subnet the IP belongs to.
`devices.sid`	numeric	`82`	The subnet id for the subnet the device is currently located in.
`devices.hostname`	string	`ws83`	The current device hostname.
`devices.firstSeen`	numeric	`1528812000000`	The first time the device was seen on the network.
`devices.lastSeen`	numeric	`1586937881000`	The last time the device was seen on the network.

Response Field	Type	Example Value	Description
`devices.os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`devices.typename`	string	`desktop`	The device type in system format.
`devices.typelabel`	string	`Desktop`	The device type in readable format.
`devices.tags`	array		An object describing tags applied to the device.
`devices.tags.tid`	numeric	`73`	The “tag id”. A unique value.
`devices.tags.expiry`	numeric	`0`	The expiry time for the tag when applied to a device.
`devices.tags.thid`	numeric	`78`	The “tag history” id. Increments if the tag is edited.
`devices.tags.name`	string	`Test Tag`	The tag label displayed in the user interface or in objects that reference the tag.
`devices.tags.restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`devices.tags.data`	object		An object containing information about the tag.
`devices.tags.data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`devices.tags.data.color`	numeric	`134`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`devices.tags.data.description`	string	`Testing the use of tags.`	An optional description summarizing the purpose of the tag.
`devices.tags.data.visibility`	string	`Public`	A system field.
`devices.tags.isReferenced`	boolean	`FALSE`	Whether the tag is used by one or more model components.
`devices.size`	numeric	`18490`	Depending on the meric specified, the amount of data transferred in the connections involving that device or the number of matching connections.
`devices.timems`	numeric	`1586937881000`	A timestamp at which the data was gathered in epoch time.
`devices.network`	string	`10.140.15.0/24`	The IP address range that describes the subnet the IP is contained within
`externaldevices`	array		An array of external devices that the specified device has interacted with.
`externaldevices.id`	numeric	`0`	Where applicable, an id for the external device. This can be corss-referenced with the connections object.
`externaldevices.hostname`	string	`google.com`	Depending on the meric specified, the amount of data transferred in the connections involving that external location or the number of matching connections.
`externaldevices.name`	string	`google.com`	A timestamp at which the data was gathered in epoch time.
`externaldevices.hostnames`	array		A hostname associated with the external device.
`externaldevices.hostnames.hostname`	string	`google.com`	A hostname or IP associated with the external device.

Response Field	Type	Example Value	Description
`externaldevices.hostnames.count`	numeric	`3`	An array of hostnames that have been historically associated with the external location.
`externaldevices.ip`	string	`172.217.169.36`	A hostname or IP associated with the external device.
`externaldevices.size`	numeric	`18490`	The number of connections to that hostname during the specified timeframe.
`externaldevices.timems`	numeric	`1586937881000`	The IP associated with the hostname.
`externaldevices.longitude`	numeric	`-97.822`	For the reported IP location, the longitude value to plot the IP on a map.
`externaldevices.latitude`	numeric	`37.751`	For the reported IP location, the latitude value to plot the IP on a map.
`externaldevices.country`	string	`United States`	The country that the IP is located in.
`externaldevices.countrycode`	string	`US`	The system country code for the country that the IP is located in.
`externaldevices.asn`	string	`AS15169 Google LLC`	The ASN for the IP.
`externaldevices.region`	string	`North America`	The geographical region the IP is located in.
`metric`	object		An object describing the metric queried upon.
`metric.mlid`	numeric	`17`	The “metric logic” id - unique identifier.
`metric.name`	string	`datatransfervolume`	The metric which data is returned for in system format.
`metric.label`	string	`Data Transfer`	The metric which data is returned for in readable format.
`metric.units`	string	`bytes`	The units the metric is measured in, if applicable.
`metric.filtertypes`	array	`Direction`	An array of filters which can be used with this metric.
`metric.unitsinterval`	numeric	`3600`	The default time interval for the metric.
`metric.lengthscale`	numeric	`599997600`	A system field.
`connections`	array		An array of connection objects associated with the device and metric over the time period.
`connections.source`	object		An object describing the source of a connection.
`connections.source.ip`	string	`172.217.169.36`	The device id for the source of the connection.
`connections.source.id`	numeric	`2899945802`	The IP of the source device. For external locations, this field may not appear.
`connections.source.type`	string	`externaldevice`	The type of device, host or entity originating the connection.
`connections.target`	object		An object describing the source of a target.
`connections.target.id`	numeric	`938`	The device id for the target of the connection.
`connections.target.ip`	string	`10.15.3.39`	The IP of the target device. For external locations, this field may not appear.

Response Field	Type	Example Value	Description
`connections.target.type`	string	`device`	The type of device, host or entity targeted by the connection.
`connections.timems`	numeric	`1586937881000`	A timestamp for the connection in epoch time.
`connections.size`	numeric	`36000000`	The time frame covered by the initial request in seconds x 10000.

Example Response

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "Single device",
          "in": false,
          "out": false
        },
        {
          "View": "All devices",
          "in": false,
          "out": false
        },
        {
          "View": "Breach devices",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "New",
          "in": false,
          "out": false
        },
        {
          "Connections": "Unusual",
          "in": false,
          "out": false
        },
        {
          "Connections": "Normal",
          "in": false,
          "out": false
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "applicationprotocols": [
        {
          "applicationprotocol": "HTTPS",
          "in": 13500,
          "out": 4794
        }
      ]
    }
  ],
  "subnets": [],
  "devices": [
    {
      "did": 212,
      "macaddress": "2g:d8:a2:a8:54:c6",
      "vendor": "ASUSTek COMPUTER INC.",
      "ip": "10.15.3.39",
      "ips": [
        {
          "ip": "10.15.3.39",
          "timems": 1587135600000,
          "time": "2020-04-17 15:00:00",
          "sid": 12
        }
      ],
      "sid": 12,
      "hostname": "ws83",
      "firstSeen": 1528807077000,
      "lastSeen": 1587136632000,
      "os": "Linux 3.11 and newer",
      "typename": "desktop",
      "typelabel": "Desktop",
      "tags": [
        {
          "tid": 73,
          "expiry": 0,
          "thid": 78,
          "name": "Admin",
```

Response is abbreviated.

Response Schema = `viewsubnet`

Response Field	Type	Example Value	Description
`statistics`	array		An array of statistics about the connections made by the device or subnet. Regardless of the metric specified, these statistics will always relate to data transfer volumes.
`statistics.Views`	array		An array of system fields.
`statistics.Views.View`	string	`All subnets`	A system field.
`statistics.Views.in`	boolean	`FALSE`	A system field.
`statistics.Views.out`	boolean	`FALSE`	A system field.
`statistics.Connection Status`	array		An array of statuses that the connections may be classified as.
`statistics.Connection Status.Connections`	string	`Normal`	A connection status. May be Normal, Unusual, New or Breached.
`statistics.Connection Status.in`	numeric	`1273420401`	The total inbound data transfer for the subnet during the timeframe in bytes.
`statistics.Connection Status.out`	numeric	`1273420401`	The total outbound data transfer for the subnet during the timeframe in bytes.
`statistics.devices`	array		An array of devices within the subnet that have made connections which transferred data.
`statistics.devices.device`	string	`sarah-desktop-12`	The hostname or IP of the device.
`statistics.devices.ip`	string	`10.12.14.2`	The IP of the device.
`statistics.devices.in`	numeric	`14857836`	The amount of data received from by device.
`statistics.devices.out`	numeric	`574830077`	The amount of data sent from that device.
`statistics.Subnets`	array		When a subnet is specified, an array of subnets that devices in the specified subnet have interacted with.
`statistics.Subnets.subnet`	string	`10.0.18.0/24`	The network range describing the subnet.
`statistics.Subnets.in`	numeric	`2024715`	The amount of data received from this subnet.
`statistics.Subnets.out`	numeric	`4329923`	The amount of data sent to this subnet.
`statistics.intext`	array		An array of information about the type of connections and data transferred.
`statistics.intext.intext`	string	`Internal`	The connection type filter - either external or internal.
`statistics.intext.in`	numeric	`972652917`	The total inbound data transfer for the device during the timeframe in bytes.
`statistics.intext.out`	numeric	`972652917`	The total outbound data transfer for the device during the timeframe in bytes.
`statistics.protocols`	array		An array of network protocols identified in the connections.
`statistics.protocols.protocol`	string	`TCP`	A network protocol.

Response Field	Type	Example Value	Description
`statistics.protocols.in`	numeric	`1259912584`	The volume of inbound data transferred using that protocol.
`statistics.protocols.out`	numeric	`1259912584`	The volume of outbound data transferred using that protocol.
`statistics.applicationprotocols`	array		An array of application protocols used in the connections.
`statistics.applicationprotocols.applicationprotocol`	string	`SSH`	An application protocol.
`statistics.applicationprotocols.in`	numeric	`967854515`	The volume of inbound data transferred using that protocol.
`statistics.applicationprotocols.out`	numeric	`967854515`	The volume of outbound data transferred using that protocol.
`subnets`	array		An array of subnets that have interacted with the subnet.
`subnets.sid`	numeric	`-6`	The subnet id for the other subnet.
`subnets.size`	numeric	`966432307`	The amount of data transferred to or from that subnet.
`subnets.timems`	numeric	`1586937881000`	A timestamp at which the data was gathered in epoch time.
`subnets.network`	string		The network range describing the subnet.
`subnets.label`	string	`Internal Traffic`	The subnet label applied in Subnet Admin (if applicable).
`devices`	array		When a subnet is specified, information about the devices within that subnet and any devices they have communicated with.
`devices.did`	numeric	`54`	The “device id” of the device.
`devices.size`	numeric	`153541`	Depending on the metric specified, the amount of data transferred in the connections involving that device or the number of matching connections.
`devices.timems`	numeric	`1586937881000`	A timestamp at which the data was gathered in epoch time.
`devices.ips`	array	`10.12.14.2`	IPs associated with the device historically.
`devices.sid`	numeric	`82`	The subnet id for the subnet the device is currently located in.
`devices.ip`	string	`10.12.14.2`	The current IP associated with the device.
`devices.network`	string	`10.12.14.0/24`	The IP address range that describes the subnet the IP is contained within
`metric`	object		An object describing the metric queried upon.
`metric.mlid`	numeric	`17`	The “metric logic” id - unique identifier.
`metric.name`	string	`datatransfervolume`	The metric which data is returned for in system format.
`metric.label`	string	`Data Transfer`	The metric which data is returned for in readable format.
`metric.units`	string	`bytes`	The units the metric is measured in, if applicable.

Response Field	Type	Example Value	Description
`metric.filtertypes`	array	`Direction`	An array of filters which can be used with this metric.
`metric.unitsinterval`	numeric	`3600`	The default time interval for the metric.
`metric.lengthscale`	numeric	`599997600`	A system field.
`connections`	array		An array of connection objects associated with the subnet and metric over the time period.
`connections.source`	object		An object describing the source of a connection.
`connections.source.id`	numeric	`-6`	The device id or subnet id of the source of the connection, where applicable.
`connections.source.ip`	string	`10.12.14.2`	The IP of the source device.
`connections.source.type`	string	`subnet`	The type of device, host or entity originating the connection.
`connections.target`	object		An object describing the source of a target.
`connections.target.id`	numeric	`-6`	The device id or subnet id of the destination for the connection, where applicable.
`connections.target.ip`	string	`10.0.18.224`	The IP of the target device.
`connections.target.type`	string	`subnet`	The type of device, host or entity targeted by the connection.
`connections.timems`	numeric	`1586937600000`	A timestamp for the connection in epoch time.
`connections.score`	numeric	`18`	Where a connection is deemed unusual, the percentage unusualness of the connection.
`connections.size`	numeric	`36000000`	The time frame covered by the initial request in seconds x 10000.

Example Response

```
{
  "statistics": [
    {
      "Views": [
        {
          "View": "All subnets",
          "in": false,
          "out": false
        },
        {
          "View": "This subnet",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "Connection Status": [
        {
          "Connections": "Normal",
          "in": 4262370976,
          "out": 4262370976
        },
        {
          "Connections": "Unusual",
          "in": 61505,
          "out": 61505
        },
        {
          "Connections": "New",
          "in": 31284,
          "out": 31284
        },
        {
          "Connections": "Breached",
          "in": false,
          "out": false
        }
      ]
    },
    {
      "devices": [
        {
          "device": "workstation-local-82",
          "ip": "10.0.18.224",
          "in": 4372649,
          "out": 3039203929
        },
    ...
      ]
    },
    {
      "Subnets": [
        {
          "subnet": "10.0.18.0/24",
          "in": 37399591,
          "out": 132264717
        }
        ...
      ]
    },
    {
      "intext": [
        {
          "intext": "Internal",
          "in": 3983454402,
          "out": 3983454402
        },
        {
          "intext": "External",
          "in": 278978079,
          "out": 278978079
        }
      ]
    },
    {
      "protocols": [
        {
          "protocol": "TCP",
          "in": 4248515456,
          "out": 4248515456
        }
        ...
```

Response is abbreviated.

/similardevices

This endpoint returns a list of similar devices when given the `did` of a specific device on the network. This information is shown in the Threat Visualizer when the ‘View Similar Devices’ button is clicked after searching for a device in the Omnisearch bar.

The similarity between the specified device and the returned devices is indicated by the `score` . The returned data will be ordered by similarity score, with the most similar device first.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`count`	numeric	Specifies the maximum number of items to return.
`fulldevicedetails`	boolean	Returns the full device detail objects for all devices referenced by data in an API response. Use of this parameter will alter the JSON structure of the API response for certain calls.
`token`	string	Takes a token value returned by a system notice about a change in similar devices for a specified device. Will return the old and new list of devices.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` a list of three most similar devices to the device with `did=123` :

```
https://<applianceIP>/similardevices?did=123&count=3
```

Example Response

Request: /similardevices?did=123&count=3

```
[
  {
    "did": 34,
    "score": 100,
    "ip": "10.91.44.12",
    "ips": [
      {
        "ip": "10.91.44.12",
        "timems": 1581933600000,
        "time": "2020-02-17 10:00:00",
        "sid": 7
      }
    ],
    "sid": 7,
    "firstSeen": 1550492002000,
    "lastSeen": 1581935040000,
    "os": "Linux 2.2.x-3.x",
    "typename": "desktop",
    "typelabel": "Desktop"
  },
  {
    "did": 72,
    "score": 99,
     ...
  },
  {
    "did": 78,
    "score": 72,
     ...
  }
]
```

Response is abbreviated.

/similardevices Response Schema

Response Schema - `fulldevicedetails=false`

Response Field	Type	Example Value	Description
`did`	numeric	`112`	The “device id”, a unique identifier.
`score`	numeric	`99`	A score describing how similar this device is in comparison to the original device.
`ip`	string	`10.15.3.39`	The current IP associated with the device.
`ips`	array		IPs associated with the device historically.
`ips.ip`	string	`10.15.3.39`	A historic IP associated with the device.
`ips.timems`	numeric	`1586937881000`	The time the IP was last seen associated with that device in epoch time.
`ips.time`	string	`2020-04-15 08:04:41`	The time the IP was last seen associated with that device in readable format.
`ips.sid`	numeric	`29`	The subnet id for the subnet the IP belongs to.
`sid`	numeric	`29`	The subnet id for the subnet the device is currently located in.
`hostname`	string	`workstation-local-82`	The current device hostname.
`firstSeen`	numeric	`2018-06-12 14:00:00`	The first time the device was seen on the network.
`lastSeen`	numeric	`2020-03-15 09:52:11`	The last time the device was seen on the network.
`os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`typename`	string	`desktop`	The device type in system format.
`typelabel`	string	`Desktop`	The device type in readable format.

Example Response

Request: /similardevices?did=123&count=3&fulldevicedetails=false

```
[
  {
    "did": 34,
    "score": 100,
    "ip": "10.91.44.12",
    "ips": [
      {
        "ip": "10.91.44.12",
        "timems": 1581933600000,
        "time": "2020-02-17 10:00:00",
        "sid": 7
      }
    ],
    "sid": 7,
    "firstSeen": 1550492002000,
    "lastSeen": 1581935040000,
    "os": "Linux 2.2.x-3.x",
    "typename": "desktop",
    "typelabel": "Desktop"
  },
  {
    "did": 72,
    "score": 99,
     ...
  },
  {
    "did": 78,
    "score": 72,
     ...
  }
]
```

Response is abbreviated.

Response Schema - `fulldevicedetails=true`

Response Field	Type	Example Value	Description
`did`	numeric	`17`	The “device id”, a unique identifier.
`score`	numeric	`99`	A score describing how similar this device is in comparison to the original device.
`ip`	string	`10.15.3.39`	The current IP associated with the device.
`ips`	array		IPs associated with the device historically.
`ips.ip`	string	`10.15.3.39`	A historic IP associated with the device.
`ips.timems`	numeric	`1586937600000`	The time the IP was last seen associated with that device in epoch time.
`ips.time`	string	`2020-04-15 08:00:00`	The time the IP was last seen associated with that device in readable format.
`ips.sid`	numeric	`10`	The subnet id for the subnet the IP belongs to.
`sid`	numeric	`10`	The subnet id for the subnet the device is currently located in.
`hostname`	string	`ws83`	The current device hostname.
`firstSeen`	numeric	`2020-04-15 08:00:00`	The first time the device was seen on the network.
`lastSeen`	numeric	`2020-03-15 09:52:11`	The last time the device was seen on the network.

Response Field	Type	Example Value	Description
`os`	string	`Linux 3.11 and newer`	The device operating system if Darktrace is able to derive it.
`typename`	string	`desktop`	The device type in system format.
`typelabel`	string	`Desktop`	The device type in readable format.
`tags`	array		An object describing tags applied to the device.
`tags.tid`	numeric	`73`	The “tag id”. A unique value.
`tags.expiry`	numeric	`0`	The expiry time for the tag when applied to a device.
`tags.thid`	numeric	`78`	The “tag history” id. Increments if the tag is edited.
`tags.name`	string	`Multi-use`	The tag label displayed in the user interface or in objects that reference the tag.
`tags.restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`tags.data`	object		An object containing information about the tag.
`tags.data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`tags.data.color`	numeric	`134`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`tags.data.description`	string	`Device is a pool device.`	An optional description summarizing the purpose of the tag.
`tags.isReferenced`	boolean	`FALSE`	Whether the tag is used by one or more model components.

Example Response

```
[
  {
    "did": 34,
    "score": 100,
    "ip": "10.91.44.12",
   "ips": [
      {
        "ip": "10.91.44.12",
        "timems": 1581933600000,
        "time": "2020-02-17 10:00:00",
        "sid": 7
      }
    ],
    "sid": 7,
    "firstSeen": 1550492002000,
    "lastSeen": 1581935040000,
    "os": "Linux 2.2.x-3.x",
    "typename": "desktop",
    "typelabel": "Desktop",
    "tags": [
      {
        "tid": 50,
        "expiry": 0,
        "thid": 50,
        "name": "Test",
        "restricted": false,
        "data": {
          "auto": false,
          "color": 200,
          "description": "Test Tag"
        },
        "isReferenced": true
      }
    ]
  },
  {
    "did": 72,
    "score": 99,
     ...
  },
  {
    "did": 78,
    "score": 72,
     ...
  }
]
```

Response is abbreviated.

/subnets

The `/subnets` endpoint allows subnets processed by Darktrace to be retrieved and edited programmatically. This can be useful when automating changes to large number of subnets or managing the quality of traffic across the network.

`POST` requests to this endpoint must be made with parameters. The `/editsubnet` endpoint for modifying subnets has now been deprecated.

Request Type(s)

`[GET]` `[POST]`

Parameters

Parameter	Type	Description
`seensince`	string	Relative offset for activity. Subnets with activity in the specified time period are returned. The format is either a number representing a number of seconds before the current time, or a number with a modifier such as day or week (Minimum=1 second, Maximum=6 months).
`sid`	numeric	Identification number of a subnet modeled in the Darktrace system.
`label`	string	An optional label to identify the subnet by. Available for POST requests only.
`network`	string	The IP address range that describes the subnet. Available for POST requests only.
`longitude`	numeric	For the actual location of the subnet as rendered on the Threat Visualizer, the longitude value. Available for POST requests only.
`latitude`	numeric	For the actual location of the subnet as rendered on the Threat Visualizer, the latitude value. Available for POST requests only.
`dhcp`	boolean	Whether DHCP is enabled for the subnet. Available for POST requests only.
`uniqueUsernames`	boolean	Whether the subnet is tracking by credential. Available for POST requests only.
`uniqueHostnames`	boolean	Whether the subnet is tracking by hostname. Available for POST requests only.
`excluded`	boolean	Whether traffic in this subnet should not be processed at all. Available for POST requests only.
`modelExcluded`	boolean	Whether devices within this subnet should be fully modeled. If true, the devices will be added to the `Internal Traffic` subnet. Available for POST requests only.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- When specifying how many minutes/hours/days in the `seensince` parameter, 3min = 3mins, 5hour = 5hours, 6day = 6days, etc.
- This API call does not support searching for subnets by anything other than the sid. If the user needs to search for subnets by label, network, etc. they will need to download the full list first and then parse on the returned data
- When making a POST request to update the subnet location, both `longitude` and `latitude` must be specified.
- When supplying a label, do not use quotes around the string - this will result in a double-quoted string.
- If changing the latitude or longitude via the API, whole values must still be passed with a decimal point. For example, `10.0` .

Example Request

1. `GET` information about the subnet with `sid=25` :

```
https://<applianceIP>/subnets?sid=25
```

2. `GET` a list of all the subnets seen in the last hour:

```
https://<applianceIP>/subnets?seensince=1hour
```

```
https://<applianceIP>/subnets?seensince=3600
```

3. `POST` a label change for the subnet with `sid=25` :

```
https://<applianceIP>/subnets -d sid=25&label=GuestWifi
```

4. `POST` to enable Tracking by Hostname and DHCP for a subnet with `sid=25` :

```
https://<applianceIP>/subnets -d {"sid":
25,"uniqueUsernames":false,"uniqueHostnames":true,"dhcp":true}
```

Example Response

Request: /subnets?sid=82

```
[
  {
    "sid": 82,
    "auto": false,
    "dhcp": true,
    "firstSeen": 1585930090000,
    "label": "Test Subnet",
    "lastSeen": 1585930212000,
    "latitude": 12.0,
    "longitude": 0.0,
    "network": "10.12.32.0/24",
    "shid": 144,
    "uniqueHostnames": false,
    "uniqueUsernames": false,
    "confidence": 2,
    "dhcpQuality": 0,
    "kerberosQuality": 0,
    "recentTrafficPercent": 100,
    "clientDevices": 61,
    "mostRecentTraffic": 1585930942000
  }
]
```

/subnets Response Schema

Response Schema

Response Field	Type	Example Value	Description
`sid`	numeric	`12`	A unique “subnet id”.
`auto`	boolean	`FALSE`	The subnet was created automatically from processed traffic and was not created by modifying a network range on the Subnet Admin page.
`dhcp`	boolean	`TRUE`	Whether DHCP is enabled for the subnet.
`firstSeen`	numeric	`1528812000000`	The first time the subnet was seen on the network in epoch time.
`label`	string	`Finance`	The label assigned to the subnet in the Threat Visualizer.
`lastSeen`	numeric	`1584265931000`	The last time the subnet was seen on the network in epoch time.
`latitude`	numeric	`0.01`	For the actual location of the subnet as rendered on the Threat Visualizer, the latitude value.
`longitude`	numeric	`-0.01`	For the actual location of the subnet as rendered on the Threat Visualizer, the longitude value.
`network`	string	`10.12.14.0/24`	The IP address range that describes the subnet.
`shid`	numeric	`104`	The “subnet history id”. Increments on edit.
`uniqueHostnames`	boolean	`TRUE`	Whether the subnet is tracking by hostname.
`uniqueUsernames`	boolean	`FALSE`	Whether the subnet is tracking by credential.
`confidence`	numeric	`-1`	A system field.
`lastDHCP`	numeric	`1584265931000`	The timestamp of the last DHCP seen for the subnet in epoch time.
`dhcpQuality`	numeric	`7`	The DHCP quality - out of 100.
`kerberosQuality`	numeric	`0`	The Kerberos quality - out of 100.
`recentTrafficPercent`	numeric	`100`	What percentage of processed traffic involved connections within this subnet. Inter-subnet traffic is included in the percentage for both subnets, so the total values may be greater than 100%.
`clientDevices`	numeric	`89`	The number of client devices within the subnet.
`mostRecentTraffic`	numeric	`1584265931000`	The most recent traffic seen for the subnet.

Example Response

```
{
  "sid": 25,
  "auto": true,
  "dhcp": true,
  "firstSeen": 1446663991000,
  "label": "Wireless",
  "lastSeen": 1553469389000,
  "latitude": 40.712,
  "longitude": -74.006,
  "network": "10.0.0.0/24",
  "shid": 881,
  "uniqueHostnames": false,
  "uniqueUsernames": false
}
```

/status

Detailed system health information from the Status page can be accessed programmatically with the `/status` API endpoint. This endpoint is ideal for monitoring in a NOC environment.

The `format=json` parameter is only required when accessing the endpoint in a browser; an authenticated API request will return JSON as standard.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`includechildren`	boolean	Determine whether information about probes is returned or not. True by default.
`fast`	boolean	When true, JSON will be returned faster but subnet connectivity information will not be included (if not cached).
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- The `fast=true` parameter will return any currently available data and will not query for subnet connectivity. However, as `/status` data is cached for a short period, a request with `fast=true` may sometimes return subnet connectivity information if a request has recently been made.
- The `responsedata` can be utilized to return only information about probes, subnets or to retrieve a specific desired field only.

Example Request

1. `GET` all status page information in JSON format:

```
https://<applianceIP>/status
```

Example Response

Request: /status?includechildren=false&fast=false

```
{
  "excessTraffic": false,
  "time": "2020-02-17 10:33",
  "installed": "2018-06-12",
  "version": "4.0.5 (bc90b2)",
  "modelsUpdated": "2020-02-14 14:03:09",
  "modelPackageVersion": "4.0-824~20200214103346~g7328d9",
  "bundleVersion": "40021",
  "bundleDate": "2020-02-14 12:38:02",
  "bundleInstalledDate": "2020-02-14 14:03:47",
  ...
  "internalIPRangeList": [],
  "internalIPRanges": 5,
  "dnsServers": 6,
  "internalDomains": 0,
  "internalAndExternalDomainList": [
    "darktrace.com",
  ],
  "internalAndExternalDomains": 2,
  "proxyServers": 2,
  "proxyServerIPs": [],
  "subnets": 9,
  "subnetData": [
    {
      "mostRecentTraffic": "2020-02-17",
      "sid": 1,
      "network": "10.0.12.0/24",
      "devices": 95,
      "clientDevices": 93,
      "mostRecentTraffic": "2020-02-17 10:00:00",
      "mostRecentDHCP": "2020-02-16 09:00:00",
      "dhcpQuality": 36,
      "kerberosQuality": 1
    },
    {
      ...
    }
  ]
}
```

Response is abbreviated.

/status Response Schema

Note: `/status` data is cached for a short period. Therefore, a request with `fast=true` may sometimes return subnet connectivity information if a request has recently been made.

The naming scheme and numbering of network interfaces returned will depend on your environment and the type of probes connected.

Response Schema - `includechildren=true`

Response Field	Type	Example Value	Description
`excessTraffic`	boolean	`FALSE`	Whether the appliance is receiving more traffic than it can reasonably process.
`time`	string	`2020-04-15 08:04:41`	The current server time in UTC.
`installed`	string	`2018-06-12 14:00:00`	The installation date of the appliance.
`mobileAppConfigured`	boolean	`TRUE`	Whether the Darktrace Mobile App is configured.
`version`	string	`4.0.7 (e592f9)`	The Threat Visualizer software version currently installed.
`ipAddress`	string	`10.12.14.2`	Where detectable, the IP address of the management interface.
`modelsUpdated`	string	`2020-04-15 08:04:41`	The last time default models were updated.
`modelPackageVersion`	string	`4.0-127720200318104843gcaafe1`	The model bundle information.
`bundleVersion`	string	`3407`	The Threat Visualizer software bundle number.
`bundleVariant`	string	`rc`	The type of bundle. Early adopter customers may receive release candidates as well as stable builds.
`bundleDate`	string	`2020-04-15 08:00:00`	The time that the Threat Visualizer software bundle was downloaded.
`bundleInstalledDate`	string	`2020-04-15 08:04:41`	The time that the Threat Visualizer software bundle was installed.
`hostname`	string	`darktrace-1234`	The appliance hostname.
`inoculation`	boolean	`FALSE`	Whether the appliance is subscribed to Darktrace inoculation.
`applianceOSCode`	string	`x`	A system field.
`saasConnectorLicense`	string		The expiry date for the current SaaS connector license.
`antigenaNetworkEnabled`	boolean	`TRUE`	Whether Antigena Network is enabled in the appliance console.
`antigenaNetworkConfirmationMode`	boolean	`TRUE`	Whether Antigena Network is in human confirmation mode.
`antigenaNetworkLicense`	string	`2020-08-15 00:00:00`	The expiry date for the current SaaS connector license.
`diskSpaceUsed_`	numeric	`87`	The percentage diskspace in use.
`type`	string	`master`	The type of appliance.

Response Field	Type	Example Value	Description
`diskUtilization`	numeric	`4`	This percentage value indicates the average disk I/O.
`load`	numeric	`73`	This percentage value indicates how in-demand resources are in the appliance processing.
`cpu`	numeric	`89`	This percentage value indicates the average amount of CPU usage (not idle).
`memoryUsed`	numeric	`97`	The percentage of memory in use.
`darkflowQueue`	numeric	`0`	The current queue from bandwidth ingestion to processing in seconds.
`networkInterfacesState_eth0`	string	`up`	Whether the network interface is up or down.
`networkInterfacesAddress_eth0`	string	`10.12.14.2`	The IP addresses if resolvable of the interface.
`networkInterfacesState_eth1`	string	`up`	Whether the network interface is up or down.
`networkInterfacesState_eth2`	string	`up`	Whether the network interface is up or down.
`networkInterfacesState_eth3`	string	`up`	Whether the network interface is up or down.
`networkInterfacesReceived_eth0`	numeric	`14578153880`	The number of bytes received by the interface
`networkInterfacesReceived_eth1`	numeric	`60700000000000`	The number of bytes received by the interface
`networkInterfacesReceived_eth2`	numeric	`858000000000`	The number of bytes received by the interface
`networkInterfacesReceived_eth3`	numeric	`29300000000000`	The number of bytes received by the interface
`networkInterfacesTransmitted_eth0`	numeric	`18834195843`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth1`	numeric	`0`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth2`	numeric	`0`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth3`	numeric	`0`	The number of bytes sent by the interface
`bandwidthCurrent`	numeric	`1905251164`	Ingested bandwidth over the last 10 minutes. Some bandwidth may not be processed due to system settings.
`bandwidthCurrentString`	string	`1.91 Gbps`	Ingested bandwidth over the last 10 minutes in a readable format. Some bandwidth may not be processed due to system settings.
`bandwidthAverage`	numeric	`923431000`	Average bandwidth over the last 2 weeks. Some bandwidth may not be processed due to system settings.
`bandwidthAverageString`	string	`923.43 Mbps`	Average bandwidth over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
`bandwidth7DayPeak`	numeric	`2095631949`	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days. Some bandwidth may not be processed due to system settings.

Response Field	Type	Example Value	Description
`bandwidth7DayPeakString`	string	`2.10 Gbps`	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days in a readable format. Some bandwidth may not be processed due to system settings.
`bandwidth2WeekPeak`	numeric	`2095631949`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks. Some bandwidth may not be processed due to system settings.
`bandwidth2WeekPeakString`	string	`2.10 Gbps`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
`processedBandwidthCurrent`	numeric	`1444151574`	Processed bandwidth over the last 10 minutes.
`processedBandwidthCurrentString`	string	`1.44 Gbps`	Processed bandwidth over the last 10 minutes in a readable format.
`processedBandwidthAverage`	numeric	`729322086`	Average bandwidth over the last 2 weeks.
`processedBandwidthAverageString`	string	`729.32 Mbps`	Average bandwidth over the last 2 weeks in a readable format.
`processedBandwidth7DayPeak`	numeric	`1841125885`	The highest bandwidth observed in any ten-minute interval over the last 7 days.
`processedBandwidth7DayPeakString`	string	`1.84 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 7 days in a readable format.
`processedBandwidth2WeekPeak`	numeric	`1906977109`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks.
`processedBandwidth2WeekPeakString`	string	`1.91 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format.
`probes`	object		An object describing any probes, whether physical or virtualized.
`probes.Probe1`	object		An object describing a specific probe.
`probes.Probe1.id`	numeric	`4`	The probe ID.
`probes.Probe1.version`	string	`4.0.6 (a2c4bf)`	The probe software version currently installed.
`probes.Probe1.hostname`	string	`TestProbe1`	The probe hostname. Some probes will return a label field rather than a hostname field, depending on their configuration.
`probes.Probe1.time`	string	`2020-04-15 08:00:00`	The current server time in UTC on the probe.
`probes.Probe1.applianceOSCode`	string	`x`	A system field.
`probes.Probe1.type`	string	`vSensor`	The type of probe.
`probes.Probe1.load`	numeric	`14`	This percentage value indicates how in-demand resources are in the probe processing.
`probes.Probe1.cpu`	numeric	`0`	This percentage value indicates the average amount of CPU usage (not idle) on the probe.
`probes.Probe1.memoryUsed`	numeric	`16`	The percentage of memory in use on the probe.

Response Field	Type	Example Value	Description
probes.Probe1.networkInterfacesState_eth0	string	up	Whether the network interface is up or down on the probe.
probes.Probe1.networkInterfacesAddress_eth0	string	10.0.18.224	The IP addresses if resolvable of the probe network interface.
probes.Probe1.networkInterfacesReceived_eth0	numeric	559588000000	The number of bytes received by the interface on the probe.
probes.Probe1.networkInterfacesTransmitted_eth0	numeric	39866733296	The number of bytes sent by the interface on the probe.
probes.Probe1.bandwidthCurrent	numeric	1720840	Bandwidth ingested by the probe over the last 10 minutes. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidthCurrentString	string	1.72 Mbps	Bandwidth ingested by the probe over the last 10 minutes in a readable format. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidthAverage	numeric	0	Average bandwidth ingested by the probe over the last 2 weeks. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidthAverageString	string	0 kbps	Average bandwidth ingested by the probe over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidth7DayPeak	numeric	0	The highest bandwidth ingested by the probe observed in any ten-minute interval over the last 7 days. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidth7DayPeakString	string	0 kbps	The highest bandwidth ingested by the probe observed in any ten-minute interval over the last 7 days in a readable format. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidth2WeekPeak	numeric	0	The highest bandwidth ingested by the probe observed in any ten-minute interval over the last 2 weeks. Some bandwidth may not be processed due to system settings.
probes.Probe1.bandwidth2WeekPeakString	string	0 kbps	The highest bandwidth ingested by the probe observed in any ten-minute interval over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
probes.Probe1.processedBandwidthCurrent	numeric	1720840	Bandwidth processed by the probe over the last 10 minutes.
probes.Probe1.processedBandwidthCurrentString	string	1.72 Mbps	Bandwidth processed by the probe over the last 10 minutes in a readable format.
probes.Probe1.processedBandwidthAverage	numeric	1041910	Average bandwidth processed by the probe over the last 2 weeks.
probes.Probe1.processedBandwidthAverageString	string	1.04 Mbps	Average bandwidth processed by the probe over the last 2 weeks in a readable format.
probes.Probe1.processedBandwidth7DayPeak	numeric	32829661	The highest bandwidth processed by the probe observed in any ten-minute interval over the last 7 days.

Response Field	Type	Example Value	Description
`probes.Probe1.processedBandwidth7DayPeakString`	string	`32.83 Mbps`	The highest bandwidth processed by the probe observed in any ten-minute interval over the last 7 days in a readable format.
`probes.Probe1.processedBandwidth2WeekPeak`	numeric	`32829661`	The highest bandwidth processed by the probe observed in any ten-minute interval over the last 2 weeks.
`probes.Probe1.processedBandwidth2WeekPeakString`	string	`32.83 Mbps`	The highest bandwidth processed by the probe observed in any ten-minute interval over the last 2 weeks in a readable format.
`probes.Probe1.connectionsPerMinuteCurrent`	numeric	`331`	Current number of connections processed by the probe in the last minute - includes ongoing (unfinished) connections and completed connections.
`probes.Probe1.connectionsPerMinuteAverage`	numeric	`326`	Average number of connections processed by the probe per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`probes.Probe1.connectionsPerMinute7DayPeak`	numeric	`752`	Highest number of connections processed by the probe per minute in the last 7 days - includes ongoing (unfinished) connections and completed connections.
`probes.Probe1.connectionsPerMinute2WeekPeak`	numeric	`752`	Highest number of connections processed by the probe per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinuteCurrent`	numeric	`31039`	Current number of connections processed in the last minute - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinuteAverage`	numeric	`13305`	Average number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute7DayPeak`	numeric	`36861`	Highest number of connections processed per minute in the last 7 days - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute2WeekPeak`	numeric	`39164`	Highest number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`operatingSystems`	numeric	`16`	The number of operating systems (as derived by Darktrace) seen over the last 4 weeks.
`newDevices4Weeks`	numeric	`792`	The number of new devices seen over the last 4 weeks.
`newDevices7Days`	numeric	`141`	The number of new devices seen over the last 7 days.
`newDevices24Hours`	numeric	`34`	The number of new devices seen over the last 24 hours.
`newDevicesHour`	numeric	`0`	The number of new devices seen over the last hour.

Response Field	Type	Example Value	Description
`activeDevices4Weeks`	numeric	`6035`	The number of active devices seen over the last 4 weeks. Active devices may also include unmodelled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges if activity is seen.
`activeDevices7Days`	numeric	`4019`	The number of active devices seen over the last 7 days. Active devices may also include unmodelled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`activeDevices24Hours`	numeric	`2313`	The number of active devices seen over the last 24 hours. Active devices may also include unmodelled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`activeDevicesHour`	numeric	`769`	The number of active devices seen over the last hour. Active devices may also include unmodelled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`deviceHostnames`	numeric	`728`	The number of device hostnames seen in the last 4 weeks.
`deviceMACAddresses`	numeric	`728`	The number of device MAC Addresses seen in the last 4 weeks.
`deviceRecentIPChange`	numeric	`13`	The nunber of devices that have changed IP in the last 7 days.
`models`	numeric	`593`	The number of active/enabled models on the system.
`modelsBreached`	numeric	`67509`	This figure represents the number of lifetime model breaches, unless the appliance is explicitly configured to expire model breaches.
`modelsSuppressed`	numeric	`382864`	This figure represents the number of lifetime model breaches that have been suppressed, unless the appliance is explicitly configured to expire model breaches.
`devicesModeled`	numeric	`4019`	The number of devices currently modeled. Unmodelled devices are not included in this value but may be included in the “Active Devices” tally, resulting in a slight deviation between the values.
`recentUnidirectionalConnections`	numeric	`0`	The percentage number of connections identified as unidirectional over the last 30 minutes. If data is not available, and average over the last 6 hours.
`mostRecentDHCPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent DHCP traffic across all subnets in UTC.
`mostRecentDNSTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent DNS traffic across all subnets in UTC.
`mostRecentDCE_RPCTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent DCE_RPC traffic across all subnets in UTC.
`mostRecentDTLSTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent HTTP traffic across all subnets in UTC.

Response Field	Type	Example Value	Description
`mostRecentHTTPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent HTTPS traffic across all subnets in UTC.
`mostRecentHTTPSTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent Kerberos traffic across all subnets in UTC.
`mostRecentIMAPTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent LDAP traffic across all subnets in UTC.
`mostRecentKERBEROSTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent NTP traffic across all subnets in UTC.
`mostRecentLDAPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent SMB traffic across all subnets in UTC.
`mostRecentNTLMTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent SMTP traffic across all subnets in UTC.
`mostRecentNTPTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent SNMP traffic across all subnets in UTC.
`mostRecentRADIUSTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent SSDP traffic across all subnets in UTC.
`mostRecentSIPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent SSH traffic across all subnets in UTC.
`mostRecentSMBTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent SSL traffic across all subnets in UTC.
`mostRecentSMB1Traffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent STUN traffic across all subnets in UTC.
`internalIPRangeList`	array	`10.0.0.0/8`	An array of IP address ranges modeled as internal IP ranges by Darktrace.
`internalIPRanges`	numeric	`5`	The number of internal IP ranges.
`dnsServers`	numeric	`14`	The number of devices identified as DNS server.
`internalDomains`	numeric	`0`	The number of internal domains.
`internalAndExternalDomainList`	array	`darktrace.com`	example.com
`internalAndExternalDomains`	numeric	`2`	The number of internally and externally resolvable domains.
`proxyServers`	numeric	`1`	The number of proxy servers detected by Darktrace.
`proxyServerIPs`	array	`192.168.72.4:443`	The IPs of servers identified as proxy servers.
`subnets`	numeric	`93`	The number of subnets currently active on the network and seen receiving/sending traffic within the last 7 days.
`subnetData`	array		An array of statistics about the quality and volume of data associated with the subnet.
`subnetData.sid`	numeric	`25`	The “subnet id”, a unique identifier.
`subnetData.network`	string	`10.0.18.0/24`	The IP address range that describes the subnet.
`subnetData.devices`	numeric	`254`	The number of devices associated with an IP address that places them within the subnet, where activity has been seen in the last 7 days.
`subnetData.clientDevices`	numeric	`252`	The number of client devices within the subnet.

Response Field	Type	Example Value	Description
`subnetData.mostRecentTraffic`	string	`2020-04-15 08:04:41`	The most recent traffic seen for the subnet.
`subnetData.mostRecentDHCP`	string	`Never`	The timestamp of the last DHCP seen for the subnet in epoch time.
`subnetData.dhcpQuality`	numeric	`90`	The DHCP quality - out of 100.
`subnetData.kerberosQuality`	numeric	`25`	The Kerberos quality - out of 100.

Example Response

```
{
  "excessTraffic": false,
  "time": "2020-04-17 16:39",
  "installed": "2018-06-12",
  "mobileAppConfigured": false,
  "version": "4.0.7 (e6e864)",
  "ipAddress": "10.0.18.224",
  "modelsUpdated": "2020-04-16 13:08:34",
  "modelPackageVersion": "4.0-1957~20200416110325~gffb630",
  "bundleVersion": "3421",
  "bundleVariant": "rc",
  "bundleDate": "2020-04-16 12:11:16",
  "bundleInstalledDate": "2020-04-16 13:08:32",
  "hostname": "dt-1234-01",
  "inoculation": true,
  "applianceOSCode": "x",
  "saasConnectorLicense": "2029-06-01 00:00:00",
  "antigenaNetworkEnabled": true,
  "antigenaNetworkConfirmationMode": false,
  "antigenaNetworkLicense": "",
  "diskSpaceUsed_var": 19,
  "type": "master",
  "diskUtilization": 1,
  "load": 21,
  "cpu": 16,
  "memoryUsed": 71,
  "darkflowQueue": 0,
  "digSuccessPercent": 0,
  "digQueue": 0,
  "networkInterfacesState_eth0": "up",
  "networkInterfacesAddress_eth0": "10.0.18.224",
  "networkInterfacesState_eth1": "up",
  "networkInterfacesReceived_eth0": 13946533696,
  "networkInterfacesReceived_eth1": 0,
  "networkInterfacesTransmitted_eth0": 6503033975,
  "networkInterfacesTransmitted_eth1": 0,
  "bandwidthCurrent": 61267847,
  "bandwidthCurrentString": "61.27 Mbps",
  "bandwidthAverage": 5826000,
  "bandwidthAverageString": "5.83 Mbps",
  "bandwidth7DayPeak": 349212676,
  "bandwidth7DayPeakString": "349.21 Mbps",
  "bandwidth2WeekPeak": 349212676,
  "bandwidth2WeekPeakString": "349.21 Mbps",
  "processedBandwidthCurrent": 36345045,
  "processedBandwidthCurrentString": "36.35 Mbps",
  "processedBandwidthAverage": 2958126,
  "processedBandwidthAverageString": "2.96 Mbps",
  "processedBandwidth7DayPeak": 304240636,
  "processedBandwidth7DayPeakString": "304.24 Mbps",
  "processedBandwidth2WeekPeak": 304240636,
  "processedBandwidth2WeekPeakString": "304.24 Mbps",
  "probes": {
       ...
    },
  "connectionsPerMinuteCurrent": 563,
  "connectionsPerMinuteAverage": 517,
  "connectionsPerMinute7DayPeak": 800,
  "connectionsPerMinute2WeekPeak": 984,
  "operatingSystems": 13,
  "newDevices4Weeks": 47,
  "newDevices7Days": 5,
  "newDevices24Hours": 1,
  "newDevicesHour": 0,
  "activeDevices4Weeks": 1105,
  "activeDevices7Days": 179,
  "activeDevices24Hours": 128,
  "activeDevicesHour": 31,
  "deviceHostnames": 40,
  "deviceMACAddresses": 75,
  "deviceRecentIPChange": 0,
  "models": 687,
  "modelsBreached": 177504,
  "modelsSuppressed": 143174,
  "devicesModeled": 1105,
  "recentUnidirectionalConnections": 0,
  "mostRecentDHCPTraffic": "2020-04-17 14:41:00",
  "mostRecentDNSTraffic": "2020-04-17 16:37:00",
    ...
  "internalIPRangeList": [
    "10.0.0.0/8",
    "172.16.0.0/12",
    "192.168.0.0/16",
```

Response is abbreviated.

Response Schema - `includechildren=false`

Response Field	Type	Example Value	Description
`excessTraffic`	boolean	`FALSE`	Whether the appliance is receiving more traffic than it can reasonably process.
`time`	string	`2020-03-15 09:52:11`	The current server time in UTC.
`installed`	string	`2018-06-12 14:00:00`	The installation date of the appliance.
`mobileAppConfigured`	boolean	`TRUE`	Whether the Darktrace Mobile App is configured.
`version`	string	`4.0.7 (e592f9)`	The Threat Visualizer software version currently installed.
`ipAddress`	string	`192.168.72.4`	Where detectable, the IP address of the management interface.
`modelsUpdated`	string	`2020-04-15 08:00:00`	The last time default models were updated.
`modelPackageVersion`	string	4.0-1277$_{20200318104843}$^{gcaafe1}	The model bundle information.
`bundleVersion`	string	`3407`	The Threat Visualizer software bundle number.
`bundleVariant`	string	`rc`	The type of bundle. Early adopter customers may receive release candidates as well as stable builds.
`bundleDate`	string	`2020-04-15 08:00:00`	The time that the Threat Visualizer software bundle was downloaded.
`bundleInstalledDate`	string	`2020-04-15 08:04:41`	The time that the Threat Visualizer software bundle was installed.
`hostname`	string	`darktrace-1234`	The appliance hostname.
`inoculation`	boolean	`FALSE`	Whether the appliance is subscribed to Darktrace inoculation.
`applianceOSCode`	string	`x`	A system field.
`saasConnectorLicense`	string		The expiry date for the current SaaS connector license.
`antigenaNetworkEnabled`	boolean	`TRUE`	Whether Antigena Network is enabled in the appliance console.
`antigenaNetworkConfirmationMode`	boolean	`TRUE`	Whether Antigena Network is in human confirmation mode.
`antigenaNetworkLicense`	string	`2020-09-15 08:00:00`	The expiry date for the current SaaS connector license.
`diskSpaceUsed_`	numeric	`88`	The percentage diskspace in use.
`type`	string	`master`	The type of appliance.
`diskUtilization`	numeric	`3`	This percentage value indicates the average disk I/O.
`load`	numeric	`73`	This percentage value indicates how in-demand resources are in the appliance processing.

Response Field	Type	Example Value	Description
`cpu`	numeric	`53`	This percentage value indicates the average amount of CPU usage (not idle).
`memoryUsed`	numeric	`96`	The percentage of memory in use.
`darkflowQueue`	numeric	`0`	The current queue from bandwidth ingestion to processing in seconds.
`networkInterfacesState_eth0`	string	`up`	Whether the network interface is up or down.
`networkInterfacesAddress_eth0`	string	`10.140.32.3`	The IP addresses if resolvable of the interface.
`networkInterfacesState_eth1`	string	`up`	Whether the network interface is up or down.
`networkInterfacesState_eth2`	string	`up`	Whether the network interface is up or down.
`networkInterfacesState_eth3`	string	`up`	Whether the network interface is up or down.
`networkInterfacesReceived_eth0`	numeric	`15071836933`	The number of bytes received by the interface
`networkInterfacesReceived_eth1`	numeric	`66900000000000`	The number of bytes received by the interface
`networkInterfacesReceived_eth2`	numeric	`916000000000`	The number of bytes received by the interface
`networkInterfacesReceived_eth3`	numeric	`32100000000000`	The number of bytes received by the interface
`networkInterfacesTransmitted_eth0`	numeric	`20605014804`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth1`	numeric	`0`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth2`	numeric	`0`	The number of bytes sent by the interface
`networkInterfacesTransmitted_eth3`	numeric	`0`	The number of bytes sent by the interface
`bandwidthCurrent`	numeric	`1807190579`	Ingested bandwidth over the last 10 minutes. Some bandwidth may not be processed due to system settings.
`bandwidthCurrentString`	string	`1.81 Gbps`	Ingested bandwidth over the last 10 minutes in a readable format. Some bandwidth may not be processed due to system settings.
`bandwidthAverage`	numeric	`924906000`	Average bandwidth over the last 2 weeks. Some bandwidth may not be processed due to system settings.
`bandwidthAverageString`	string	`924.91 Mbps`	Average bandwidth over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
`bandwidth7DayPeak`	numeric	`2095631949`	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days. Some bandwidth may not be processed due to system settings.
`bandwidth7DayPeakString`	string	`2.10 Gbps`	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days in a readable format. Some bandwidth may not be processed due to system settings.

Response Field	Type	Example Value	Description
`bandwidth2WeekPeak`	numeric	`2095631949`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks. Some bandwidth may not be processed due to system settings.
`bandwidth2WeekPeakString`	string	`2.10 Gbps`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
`processedBandwidthCurrent`	numeric	`1223844891`	Processed bandwidth over the last 10 minutes.
`processedBandwidthCurrentString`	string	`1.22 Gbps`	Processed bandwidth over the last 10 minutes in a readable format.
`processedBandwidthAverage`	numeric	`730082694`	Average bandwidth over the last 2 weeks.
`processedBandwidthAverageString`	string	`730.08 Mbps`	Average bandwidth over the last 2 weeks in a readable format.
`processedBandwidth7DayPeak`	numeric	`1841125885`	The highest bandwidth observed in any ten-minute interval over the last 7 days.
`processedBandwidth7DayPeakString`	string	`1.84 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 7 days in a readable format.
`processedBandwidth2WeekPeak`	numeric	`1901374248`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks.
`processedBandwidth2WeekPeakString`	string	`1.90 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format.
`connectionsPerMinuteCurrent`	numeric	`22045`	Current number of connections processed in the last minute - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinuteAverage`	numeric	`13521`	Average number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute7DayPeak`	numeric	`36861`	Highest number of connections processed per minute in the last 7 days - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute2WeekPeak`	numeric	`39164`	Highest number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`operatingSystems`	numeric	`16`	The number of operating systems (as derived by Darktrace) seen over the last 4 weeks.
`newDevices4Weeks`	numeric	`826`	The number of new devices seen over the last 4 weeks.
`newDevices7Days`	numeric	`176`	The number of new devices seen over the last 7 days.
`newDevices24Hours`	numeric	`69`	The number of new devices seen over the last 24 hours.
`newDevicesHour`	numeric	`1`	The number of new devices seen over the last hour.

Response Field	Type	Example Value	Description
`activeDevices4Weeks`	numeric	`6095`	The number of active devices seen over the last 4 weeks. Active devices may also include unmodeled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges if activity is seen.
`activeDevices7Days`	numeric	`4035`	The number of active devices seen over the last 7 days. Active devices may also include unmodeled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`activeDevices24Hours`	numeric	`2217`	The number of active devices seen over the last 24 hours. Active devices may also include unmodeled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`activeDevicesHour`	numeric	`471`	The number of active devices seen over the last hour. Active devices may also include unmodeled devices such as broadcast traffic, internal and external multicast traffic and any excluded ip ranges.
`deviceHostnames`	numeric	`714`	The number of device hostnames seen in the last 4 weeks.
`deviceMACAddresses`	numeric	`705`	The number of device MAC Addresses seen in the last 4 weeks.
`deviceRecentIPChange`	numeric	`13`	The number of devices that have changed IP in the last 7 days.
`models`	numeric	`593`	The number of active/enabled models on the system.
`modelsBreached`	numeric	`67658`	This figure represents the number of lifetime model breaches, unless the appliance is explicitly configured to expire model breaches.
`modelsSuppressed`	numeric	`382918`	This figure represents the number of lifetime model breaches that have been suppressed, unless the appliance is explicitly configured to expire model breaches.
`devicesModeled`	numeric	`4035`	The number of devices currently modeled. Unmodeled devices are not included in this value but may be included in the “Active Devices” tally, resulting in a slight deviation between the values.
`recentUnidirectionalConnections`	numeric	`0`	The percentage number of connections identified as unidirectional over the last 30 minutes. If data is not available, and average over the last 6 hours.
`mostRecentDHCPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent DHCP traffic across all subnets in UTC.
`mostRecentDNSTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent DNS traffic across all subnets in UTC.
`mostRecentDCE_RPCTraffic`	string	`2020-04-15 08:00:00`	The timestamp of the most recent DCE_RPC traffic across all subnets in UTC.
`mostRecentHTTPTraffic`	string	`2020-04-15 08:04:41`	The timestamp of the most recent HTTP traffic across all subnets in UTC.

Response Field	Type	Example Value	Description
mostRecentHTTPSTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent HTTPS traffic across all subnets in UTC.
mostRecentKERBEROSTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent Kerberos traffic across all subnets in UTC.
mostRecentLDAPTraffic	string	2020-03-15 09:52:11	The timestamp of the most recent LDAP traffic across all subnets in UTC.
mostRecentNTPTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent NTP traffic across all subnets in UTC.
mostRecentSMBTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent SMB traffic across all subnets in UTC.
mostRecentSMTPTraffic	string	2020-03-15 09:52:11	The timestamp of the most recent SMTP traffic across all subnets in UTC.
mostRecentSNMPTraffic	string	2020-03-15 09:52:11	The timestamp of the most recent SNMP traffic across all subnets in UTC.
mostRecentSSDPTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent SSDP traffic across all subnets in UTC.
mostRecentSSHTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent SSH traffic across all subnets in UTC.
mostRecentSSLTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent SSL traffic across all subnets in UTC.
mostRecentSTUNTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent STUN traffic across all subnets in UTC.
internalIPRangeList	string	10.0.0.0/8	An array of IP address ranges modeled as internal IP ranges by Darktrace.
internalIPRanges	string	5	The number of internal IP ranges.
dnsServers	string	14	The number of devices identified as DNS server.
internalDomains	string	0	The number of internal domains.
internalAndExternalDomainList	string	darktrace.com	example.com
internalAndExternalDomains	string	2	The number of internally and externally resolvable domains.
proxyServers	string	4	The number of proxy servers detected by Darktrace.
proxyServerIPs	string	192.168.72.4:443	The IPs of servers identified as proxy servers.
subnets	array	93	The number of subnets currently active on the network and seen receiving/sending traffic within the last 7 days.
subnetData	numeric		An array of statistics about the quality and volume of data associated with the subnet.
subnetData.sid	numeric	25	The “subnet id”, a unique identifier.
subnetData.network	numeric	10.0.18.0/24	The IP address range that describes the subnet.
subnetData.devices	array	254	The number of devices associated with an IP address that places them within the subnet, where activity has been seen in the last 7 days.
subnetData.clientDevices	numeric	252	The number of client devices within the subnet.

Response Field	Type	Example Value	Description
`subnetData.mostRecentTraffic`	numeric	`2020-04-15 08:04:41`	The most recent traffic seen for the subnet.
`subnetData.mostRecentDHCP`	array	`Never`	The timestamp of the last DHCP seen for the subnet in epoch time.
`subnetData.dhcpQuality`	numeric	`72`	The DHCP quality - out of 100.
`subnetData.kerberosQuality`	array	`25`	The Kerberos quality - out of 100.

Example Response

```
{
  "excessTraffic": false,
  "time": "2020-04-17 16:39",
  "installed": "2018-06-12",
  "mobileAppConfigured": false,
  "version": "4.0.7 (e6e864)",
  "ipAddress": "10.0.18.224",
  "modelsUpdated": "2020-04-16 13:08:34",
  "modelPackageVersion": "4.0-1957~20200416110325~gffb630",
  "bundleVersion": "3421",
  "bundleVariant": "rc",
  "bundleDate": "2020-04-16 12:11:16",
  "bundleInstalledDate": "2020-04-16 13:08:32",
  "hostname": "dt-1234-01",
  "inoculation": true,
  "applianceOSCode": "x",
  "saasConnectorLicense": "2029-06-01 00:00:00",
  "antigenaNetworkEnabled": true,
  "antigenaNetworkConfirmationMode": false,
  "antigenaNetworkLicense": "",
  "diskSpaceUsed_var": 19,
  "type": "master",
  "diskUtilization": 1,
  "load": 21,
  "cpu": 16,
  "memoryUsed": 71,
  "darkflowQueue": 0,
  "digSuccessPercent": 0,
  "digQueue": 0,
  "networkInterfacesState_eth0": "up",
  "networkInterfacesAddress_eth0": "10.0.18.224",
  "networkInterfacesState_eth1": "up",
  "networkInterfacesReceived_eth0": 13946533696,
  "networkInterfacesReceived_eth1": 0,
  "networkInterfacesTransmitted_eth0": 6503033975,
  "networkInterfacesTransmitted_eth1": 0,
  "bandwidthCurrent": 61267847,
  "bandwidthCurrentString": "61.27 Mbps",
  "bandwidthAverage": 5826000,
  "bandwidthAverageString": "5.83 Mbps",
  "bandwidth7DayPeak": 349212676,
  "bandwidth7DayPeakString": "349.21 Mbps",
  "bandwidth2WeekPeak": 349212676,
  "bandwidth2WeekPeakString": "349.21 Mbps",
  "processedBandwidthCurrent": 36345045,
  "processedBandwidthCurrentString": "36.35 Mbps",
  "processedBandwidthAverage": 2958126,
  "processedBandwidthAverageString": "2.96 Mbps",
  "processedBandwidth7DayPeak": 304240636,
  "processedBandwidth7DayPeakString": "304.24 Mbps",
  "processedBandwidth2WeekPeak": 304240636,
  "processedBandwidth2WeekPeakString": "304.24 Mbps",
  "connectionsPerMinuteCurrent": 563,
  "connectionsPerMinuteAverage": 517,
  "connectionsPerMinute7DayPeak": 800,
  "connectionsPerMinute2WeekPeak": 984,
  "operatingSystems": 13,
  "newDevices4Weeks": 47,
  "newDevices7Days": 5,
  "newDevices24Hours": 1,
  "newDevicesHour": 0,
  "activeDevices4Weeks": 1105,
  "activeDevices7Days": 179,
  "activeDevices24Hours": 128,
  "activeDevicesHour": 31,
  "deviceHostnames": 40,
  "deviceMACAddresses": 75,
  "deviceRecentIPChange": 0,
  "models": 687,
  "modelsBreached": 177504,
  "modelsSuppressed": 143174,
  "devicesModeled": 1105,
  "recentUnidirectionalConnections": 0,
  "mostRecentDHCPTraffic": "2020-04-17 14:41:00",
  "mostRecentDNSTraffic": "2020-04-17 16:37:00",
    ...
  "internalIPRangeList": [
    "10.0.0.0/8",
    "172.16.0.0/12",
    "192.168.0.0/16",
    "212.250.153.66/32",
    "122.222.222.0/24"
  ],
```

Response is abbreviated.

Response Schema - `fast=true&includechildren=false`

Response Field	Type	Example Value	Description
`excessTraffic`	boolean	`FALSE`	Whether the appliance is receiving more traffic than it can reasonably process.
`time`	string	`2020-04-15 08:04:41`	The current server time in UTC.
`installed`	string	`2018-06-12 14:00:00`	The installation date of the appliance.
`mobileAppConfigured`	boolean	`TRUE`	Whether the Darktrace Mobile App is configured.
`version`	string	`4.0.7 (e592f9)`	The Threat Visualizer software version currently installed.
`ipAddress`	string	`10.12.14.2`	Where detectable, the IP address of the management interface.
`modelsUpdated`	string	`2020-04-15 08:04:41`	The last time default models were updated.
`modelPackageVersion`	string	4.0-1277$_{20200318104843}$gcaafe1	The model bundle information.
`bundleVersion`	string	`3407`	The Threat Visualizer software bundle number.
`bundleVariant`	string	`rc`	The type of bundle. Early adopter customers may receive release candidates as well as stable builds.
`bundleDate`	string	`2020-04-15 08:00:00`	The time that the Threat Visualizer software bundle was downloaded.
`bundleInstalledDate`	string	`2020-04-15 08:04:41`	The time that the Threat Visualizer software bundle was installed.
`hostname`	string	`darktrace-1234`	The appliance hostname.
`inoculation`	boolean	`FALSE`	Whether the appliance is subscribed to Darktrace inoculation.
`applianceOSCode`	string	`x`	A system field.
`saasConnectorLicense`	string		The expiry date for the current SaaS connector license.
`antigenaNetworkEnabled`	boolean	`TRUE`	Whether Antigena Network is enabled in the appliance console.
`antigenaNetworkConfirmationMode`	boolean	`TRUE`	Whether Antigena Network is in human confirmation mode.
`antigenaNetworkLicense`	string	`2020-08-15 00:00:00`	The expiry date for the current SaaS connector license.
`diskSpaceUsed_`	numeric	`88`	The percentage diskspace in use.
`type`	string	`master`	The type of appliance.
`diskUtilization`	numeric	`3`	This percentage value indicates the average disk I/O.
`load`	numeric	`73`	This percentage value indicates how in-demand resources are in the appliance processing.

Response Field	Type	Example Value	Description
cpu	numeric	53	This percentage value indicates the average amount of CPU usage (not idle).
memoryUsed	numeric	96	The percentage of memory in use.
darkflowQueue	numeric	0	The current queue from bandwidth ingestion to processing in seconds.
networkInterfacesState_eth0	string	up	Whether the network interface is up or down.
networkInterfacesAddress_eth0	string	10.12.14.2	The IP addresses if resolvable of the interface.
networkInterfacesState_eth1	string	up	Whether the network interface is up or down.
networkInterfacesState_eth2	string	up	Whether the network interface is up or down.
networkInterfacesState_eth3	string	up	Whether the network interface is up or down.
networkInterfacesReceived_eth0	numeric	15071582939	The number of bytes received by the interface
networkInterfacesReceived_eth1	numeric	66936200000000	The number of bytes received by the interface
networkInterfacesReceived_eth2	numeric	915604000000	The number of bytes received by the interface
networkInterfacesReceived_eth3	numeric	32084600000000	The number of bytes received by the interface
networkInterfacesTransmitted_eth0	numeric	20596130558	The number of bytes sent by the interface
networkInterfacesTransmitted_eth1	numeric	0	The number of bytes sent by the interface
networkInterfacesTransmitted_eth2	numeric	0	The number of bytes sent by the interface
networkInterfacesTransmitted_eth3	numeric	0	The number of bytes sent by the interface
bandwidthCurrent	numeric	1807190579	Ingested bandwidth over the last 10 minutes. Some bandwidth may not be processed due to system settings.
bandwidthCurrentString	string	1.81 Gbps	Ingested bandwidth over the last 10 minutes in a readable format. Some bandwidth may not be processed due to system settings.
bandwidthAverage	numeric	924906000	Average bandwidth over the last 2 weeks. Some bandwidth may not be processed due to system settings.
bandwidthAverageString	string	924.91 Mbps	Average bandwidth over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
bandwidth7DayPeak	numeric	2095631949	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days. Some bandwidth may not be processed due to system settings.
bandwidth7DayPeakString	string	2.10 Gbps	The highest ingested bandwidth observed in any ten-minute interval over the last 7 days in a readable format. Some bandwidth may not be processed due to system settings.

Response Field	Type	Example Value	Description
`bandwidth2WeekPeak`	numeric	`2095631949`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks. Some bandwidth may not be processed due to system settings.
`bandwidth2WeekPeakString`	string	`2.10 Gbps`	The highest ingested bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format. Some bandwidth may not be processed due to system settings.
`processedBandwidthCurrent`	numeric	`1223844891`	Processed bandwidth over the last 10 minutes.
`processedBandwidthCurrentString`	string	`1.22 Gbps`	Processed bandwidth over the last 10 minutes in a readable format.
`processedBandwidthAverage`	numeric	`730082694`	Average bandwidth over the last 2 weeks.
`processedBandwidthAverageString`	string	`730.08 Mbps`	Average bandwidth over the last 2 weeks in a readable format.
`processedBandwidth7DayPeak`	numeric	`1841125885`	The highest bandwidth observed in any ten-minute interval over the last 7 days.
`processedBandwidth7DayPeakString`	string	`1.84 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 7 days in a readable format.
`processedBandwidth2WeekPeak`	numeric	`1901374248`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks.
`processedBandwidth2WeekPeakString`	string	`1.90 Gbps`	The highest bandwidth observed in any ten-minute interval over the last 2 weeks in a readable format.
`connectionsPerMinuteCurrent`	numeric	`22045`	Current number of connections processed in the last minute - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinuteAverage`	numeric	`13521`	Average number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute7DayPeak`	numeric	`36861`	Highest number of connections processed per minute in the last 7 days - includes ongoing (unfinished) connections and completed connections.
`connectionsPerMinute2WeekPeak`	numeric	`39164`	Highest number of connections processed per minute in the last 2 weeks - includes ongoing (unfinished) connections and completed connections.
`operatingSystems`	numeric	`16`	The number of operating systems (as derived by Darktrace) seen over the last 4 weeks.
`models`	numeric	`593`	The number of active/enabled models on the system.
`modelsBreached`	numeric	`67658`	This figure represents the number of lifetime model breaches, unless the appliance is explicitly configured to expire model breaches.

Response Field	Type	Example Value	Description
modelsSuppressed	numeric	382918	This figure represents the number of lifetime model breaches that have been suppressed, unless the appliance is explicitly configured to expire model breaches.
mostRecentDHCPTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent DHCP traffic across all subnets in UTC.
mostRecentDNSTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent DNS traffic across all subnets in UTC.
mostRecentDCE_RPCTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent DCE_RPC traffic across all subnets in UTC.
mostRecentHTTPTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent HTTP traffic across all subnets in UTC.
mostRecentHTTPSTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent HTTPS traffic across all subnets in UTC.
mostRecentKERBEROSTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent Kerberos traffic across all subnets in UTC.
mostRecentLDAPTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent LDAP traffic across all subnets in UTC.
mostRecentNTPTraffic	string	2020-03-15 09:52:11	The timestamp of the most recent NTP traffic across all subnets in UTC.
mostRecentSMBTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent SMB traffic across all subnets in UTC.
mostRecentSMTPTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent SMTP traffic across all subnets in UTC.
mostRecentSNMPTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent SNMP traffic across all subnets in UTC.
mostRecentSSHTraffic	string	2020-04-15 08:04:41	The timestamp of the most recent SSH traffic across all subnets in UTC.
mostRecentSSLTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent SSL traffic across all subnets in UTC.
mostRecentSTUNTraffic	string	2020-04-15 08:00:00	The timestamp of the most recent STUN traffic across all subnets in UTC.
internalIPRangeList	array	10.0.0.0/8	An array of IP address ranges modeled as internal IP ranges by Darktrace.
internalIPRanges	numeric	5	The number of internal IP ranges.
dnsServers	numeric	14	The number of devices identified as DNS server.
internalDomains	numeric	0	The number of internal domains.
internalAndExternalDomainList	array	darktrace.com	example.com
internalAndExternalDomains	numeric	2	The number of internally and externally resolvable domains.
proxyServers	numeric	4	The number of proxy servers detected by Darktrace.
proxyServerIPs	array	192.168.72.4:443	The IPs of servers identified as proxy servers.

Example Response

```
{
  "excessTraffic": false,
  "time": "2020-04-17 16:38",
  "installed": "2018-06-12",
  "mobileAppConfigured": false,
  "version": "4.0.7 (e6e864)",
  "ipAddress": "10.0.18.224",
  "modelsUpdated": "2020-04-16 13:08:34",
  "modelPackageVersion": "4.0-1957~20200416110325~gffb630",
  "bundleVersion": "3421",
  "bundleVariant": "rc",
  "bundleDate": "2020-04-16 12:11:16",
  "bundleInstalledDate": "2020-04-16 13:08:32",
  "hostname": "dt-1234-01",
  "inoculation": true,
  "applianceOSCode": "x",
  "saasConnectorLicense": "2029-06-01 00:00:00",
  "antigenaNetworkEnabled": true,
  "antigenaNetworkConfirmationMode": false,
  "antigenaNetworkLicense": "",
  "diskSpaceUsed_var": 19,
  "type": "master",
  "diskUtilization": 1,
  "load": 21,
  "cpu": 16,
  "memoryUsed": 71,
  "darkflowQueue": 0,
  "digSuccessPercent": 0,
  "digQueue": 0,
  "networkInterfacesState_eth0": "up",
  "networkInterfacesAddress_eth0": "10.0.18.224",
  "networkInterfacesState_eth1": "up",
  "networkInterfacesReceived_eth0": 13946434737,
  "networkInterfacesReceived_eth1": 0,
  "networkInterfacesTransmitted_eth0": 6502916079,
  "networkInterfacesTransmitted_eth1": 0,
  "bandwidthCurrent": 61267847,
  "bandwidthCurrentString": "61.27 Mbps",
  "bandwidthAverage": 5826000,
  "bandwidthAverageString": "5.83 Mbps",
  "bandwidth7DayPeak": 349212676,
  "bandwidth7DayPeakString": "349.21 Mbps",
  "bandwidth2WeekPeak": 349212676,
  "bandwidth2WeekPeakString": "349.21 Mbps",
  "processedBandwidthCurrent": 36345045,
 ...
  "processedBandwidth2WeekPeakString": "304.24 Mbps",
  "connectionsPerMinuteCurrent": 563,
  "connectionsPerMinuteAverage": 517,
  "connectionsPerMinute7DayPeak": 800,
  "connectionsPerMinute2WeekPeak": 984,
  "operatingSystems": 13,
  "models": 687,
  "modelsBreached": 177504,
  "modelsSuppressed": 143174,
  "mostRecentDHCPTraffic": "2020-04-17 14:41:00",
  "mostRecentDNSTraffic": "2020-04-17 16:37:00",
 ...
  "internalIPRangeList": [
    "10.0.0.0/8",
    "172.16.0.0/12",
    "192.168.0.0/16",
    "212.250.153.66/32",
    "122.222.222.0/24"
  ],
  "internalIPRanges": 5,
  "dnsServers": 4,
  "internalDomains": 0,
  "internalAndExternalDomainList": [
    "darktrace.com",
    "example.com"
  ],
  "internalAndExternalDomains": 2,
  "proxyServers": 1,
  "proxyServerIPs": [
    "192.168.72.4:443"
  ]
}
```

Response is abbreviated.

/summarystatistics

`/summarystatistics` returns simple statistics on device counts, processed bandwidth and the number of active Antigena actions. It can be used for simple NOC monitoring of the appliance device counts and processed bandwidth.

Request Type(s)

`[GET]`

Parameters

Parameter	Type	Description
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` the system information displayed on the homepage:

```
https://<applianceIP>/summarystatistics
```

Example Response

```
{
  "usercredentialcount": 304,
  "subnets": 8,
  "patterns": 122785,
  "bandwidth": [
    {
      "timems": 1577704800000,
      "time": "2020-01-02 11:20:00",
      "kb": 6433512
    },
    {
    ...
    },
  ],
  "antigenaDevices": 2,
  "antigenaActions": 2,
  "devicecount": {
    "unknown": 5,
    "laptop": 15,
    "mobile": 9,
    "desktop": 78,
    "server": 16,
    "dnsserver": 1,
    "saasprovider": 940,
    "totalClient": 102,
    "totalServer": 17,
    "totalOther": 5,
    "total": 1063
  }
}
```

Response is abbreviated.

/summarystatistics Response Schema

Response Schema

Response Field	Type	Example Value	Description
`usercredentialcount`	numeric	`448`	The number of active credentials seen by the Darktrace system.
`subnets`	numeric	`8`	The number of active subnets seen by the Darktrace system.
`patterns`	numeric	`96378`	The number of active connections seen by the Darktrace system.
`bandwidth`	array		Bandwidth of traffic ingested by Darktrace over the last seven days in the form of time-series data.
`bandwidth.timems`	numeric	`1584265931000`	Timestamp for the interval of grouped bandwidth data in epoch time.
`bandwidth.time`	string	`2020-03-15 09:52:11`	Timestamp for the interval of grouped bandwidth data in human readable time.
`bandwidth.kb`	numeric	`109426603`	The bandwidth volume ingested during the time interval.
`devicecount`	object		An object describing the number of devices seen in the last month.
`devicecount.unknown`	numeric	`6`	The number of active devices seen by the Darktrace system that cannot be categorized.
`devicecount.laptop`	numeric	`14`	The number of active devices categorized as laptops seen by the Darktrace system.
`devicecount.mobile`	numeric	`8`	The number of active devices categorized as mobile phones seen by the Darktrace system.
`devicecount.desktop`	numeric	`84`	The number of active devices categorized as desktops seen by the Darktrace system.
`devicecount.server`	numeric	`19`	The number of active devices categorized as servers seen by the Darktrace system.
`devicecount.dnsserver`	numeric	`1`	The number of active devices categorized as DNS servers seen by the Darktrace system.
`devicecount.saasprovider`	numeric	`73`	The number of active devices created from users of SaaS services seen by the Darktrace system.
`devicecount.totalClient`	numeric	`106`	The total number of active client devices seen by the Darktrace system.
`devicecount.totalServer`	numeric	`20`	The total number of active server devices seen by the Darktrace system.
`devicecount.totalOther`	numeric	`6`	The total number of active devices performing other operations seen by the Darktrace system.
`devicecount.total`	numeric	`204`	Total number of active devices seen by the Darktrace system.

Example Response

```
{
  "usercredentialcount": 304,
  "subnets": 8,
  "patterns": 122785,
  "bandwidth": [
    {
      "timems": 1577704800000,
      "time": "2020-01-02 11:20:00",
      "kb": 6433512
    },
    {
    ...
    },
  ],
  "antigenaDevices": 2,
  "antigenaActions": 2,
  "devicecount": {
    "unknown": 5,
    "laptop": 15,
    "mobile": 9,
    "desktop": 78,
    "server": 16,
    "dnsserver": 1,
    "saasprovider": 940,
    "totalClient": 102,
    "totalServer": 17,
    "totalOther": 5,
    "total": 1063
  }
}
```

Response is abbreviated.

/tags

The `/tags` endpoint allows tags to be controlled programmatically - tags can be reviewed, created or deleted via the API. Tags which are restricted or referenced by model components cannot be deleted.

Tags applied to a device can be controlled by the `/tags/entities` extension.

`POST` requests to this endpoint must be made in JSON format.

Request Type(s)

`[GET]` `[POST]` `[DELETE]`

Parameters

Parameter	Type	Description
`tag`	string	The name of an existing tag
`name`	string	A name for the created tag. POST requests in JSON format only.
`color`	numeric	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface. POST requests in JSON format only.
`description`	string	An optional description for the tag. POST requests in JSON format only.
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Notes

- `/tags` returns the details for all current tags. An individual tag can be references either by using the `tag` parameter and its name, or using the `tid` as an extension.
- The minimum requirements for a `POST` to create a new tag are the `name` parameter and an empty `data` object. `description` and `color` are optional but highly recommended.

Example Request

1. `GET` all details for 'Active Threat' tag:

```
https://<applianceIP>/tags/5
```

```
https://<applianceIP>/tags?tag=active threat
```

If using cUrl, ensure the space is percent-encoded when making the final request

2. `POST` to create a new tag called "Suspicious Behavior":

```
https://<applianceIP>/tags with body {"name":"Suspicious Behavior","data":
{"description":"Device is behaving suspiciously","color":100}}
```

3. `DELETE` the tag "Temporary Tag" which has `tid=89` :

```
https://<applianceIP>/tags/89
```

Example Response

Request: /tags/24

```
{
  "tid": 24,
  "expiry": 0,
  "thid": 24,
  "name": "DNS Server",
  "restricted": false,
  "data": {
    "auto": false,
    "color": 112,
    "description": "Devices receiving and making DNS queries",
    "visibility": "Public"
  },
  "isReferenced": true
}
```

/tags/entities

`/tags/entities` can be used to list the devices for a tag, list the tags for a device, add a tag to a device or remove a tag from a device. It requires either a `did` or a `tag` parameter to be specified.

Request Type(s)

`[GET]` `[POST]` `[DELETE]`

Parameters

Parameter	Type	Description
`did`	numeric	Identification number of a device modelled in the Darktrace system.
`duration`	numeric	How long the tag should be set for the device. The tag will be removed once this duration has expired.
`tag`	string	The name of an existing tag
`responsedata`	string	When given the name of a top-level field or object, restricts the returned JSON to only that field or object.

Example Request

1. `GET` the current tags for the device with `did=1` :

```
https://<applianceIP>/tags/entities?did=1
```

2. `DELETE` the ‘Guest’ tag from device with `did=1` :

```
https://<applianceIP>/tags/entities?tag=Guest&did=1
```

3. `POST` the ‘Active Threat’ tag for one hour on a device with `did=1` :

```
https://<applianceIP>/tags/entities    -d tag=Active Threat&did=1&duration=3600
```

If using cUrl, ensure the space is percent-encoded when making the final request

Example Response

Request: /tags/entities?did=1

```
[
  {
    "tid": 22,
    "expiry": 0,
    "thid": 22,
    "name": "Admin",
    "restricted": false,
    "data": {
      "auto": false,
      "color": 200,
      "description": "",
      "visibility": ""
    },
    "isReferenced": true
  },
  {
    "tid": 131,
    "expiry": 0,
    "thid": 62,
    "name": "Re-Activated Device",
    "restricted": false,
    "data": {
      "auto": false,
      "color": 142,
      "description": "A device that has been inactive for at least 4 weeks has re-appeared on the network in the past 48 hours.",
      "visibility": "Public"
    },
    "isReferenced": true
  }
]
```

/tags and /tags/entities Response Schema

Note: The following schema applies to responses from both `/tags` and `/tags/entities` .

Response Schema

Response Field	Type	Example Value	Description
`tid`	numeric	`5`	The “tag id”. A unique value.
`expiry`	numeric	`0`	The default expiry time for the tag when applied to a device.
`thid`	numeric	`5`	The “tag history” id. Increments if the tag is edited.
`name`	string	`Active Threat`	The tag label displayed in the user interface or in objects that reference the tag.
`restricted`	boolean	`FALSE`	Indicates a read-only tag - these tags can only be modified or applied by Darktrace.
`data`	object		An object containing information about the tag.
`data.auto`	boolean	`FALSE`	Whether the tag was auto-generated.
`data.color`	numeric	`200`	The hue value (in HSL) used to color the tag in the Threat Visualizer user interface.
`data.description`	string	`A tag indicating the device is behaving anomalously and potentially compromised.`	An optional description summarizing the purpose of the tag.
`isReferenced`	boolean	`TRUE`	Whether the tag is used by one or more model components.

Example Response

Request: /tags/24

```
{
  "tid": 24,
  "expiry": 0,
  "thid": 24,
  "name": "DNS Server",
  "restricted": false,
  "data": {
    "auto": false,
    "color": 112,
    "description": "Devices receiving and making DNS queries",
    "visibility": "Public"
  },
  "isReferenced": true
},
```

US:+1 415 229 9100 UK:+44 (0) 1223 394 100 LATAM:+55 11 4949 7696 APAC:+65 6804 5010 info@darktrace.com darktrace.com