

Standart Özellikler / Sorgulama ve Dışa Aktarma

- [POST - Query API](#)
- [GET - Export API](#)

POST - Query API

Genel Bakış

Sorgu API'si, filtreleme ve sıralama yetenekleriyle nesneleri aramak için kullanılan API'dir. Bu, TheHive 4 tarafından tanıtılan ve yeni veri modeli için optimize edilmiş bir API'dir.

TheHive, önceden tanımlanmış arama Sorguları listesiyle birlikte gelir:

- `listOrganisation`
- `listUser`
- `listAlert`
- `listCase`

Sorgu API isteğinin gövdesi aşağıdaki alanlara sahip bir nesne olmalıdır:

`query` required: farklı türlerde işlemlerden oluşan bir dizi:

- Seçim: gerekli
 - nesnelerin listesi
 - tanımlayıcıya göre nesne
- Filtreleme: isteğe bağlı
- Sıralama: isteğe bağlı
- Sayfalandırma: isteğe bağlı

`excludeFields` isteğe bağlı: alan adlarından oluşan bir dizi.

Örnekler

- Basit Liste:

```
{
  "query": [
    {
      "_name": "listOrganisation"
    }
  ]
}
```

- Filtreli liste:

```
{
  "query": [
    {
      "_name": "listOrganisation"
    },
    {
      "_name": "filter",
      "_eq": {
        "_field": "name",
        "_value": "admin"
      }
    }
  ]
}
```

- Sayfalandırılmalı liste:

Admin adı verilen organizasyonları listeler, yükselen `_updatedAt` değerine göre sıralanır, ilk 15 öğeyi görüntülemek için sayfalandırılır.

```
{
  "query": [
    {
      "_name": "listOrganisation"
    },
    {
      "_name": "filter",
      "_eq": {
        "_field": "name",
        "_value": "admin"
      }
    },
    {
      "_name": "sort",
      "_fields": [
        {
          "_updatedAt": "asc"
        }
      ]
    }
  ],
}
```

```
{
  "_name": "page",
  "from": 0,
  "to": 15
}
]
```

- Zincirleme sorgular:

Kimliği ~1234 olan vaka için gözlemlenebilirleri listeleyin

```
{
  "query": [
    {
      "_name": "getCase",
      "idOrName": "~1234"
    },
    {
      "_name": "observables"
    },
    {
      "_name": "page",
      "from": 0,
      "to": 15
    }
  ]
}
```

- Alanları hariç tutun:

```
{
  "query": [
    {
      "_name": "listCase"
    }
  ],
  "excludeFields": ["description", "summary"]
}
```

Filtreler

Mevcut filtreler:

- `_and`: `{ "_and": [...other filters] }`
- `_or`: `{ "_or": [...other filters] }`
- `_not`: `{ "_not": { other filter } }`
- `_any`: `{ "_any": null }` herhangi bir varlıkla eşleşir
- `_lt`: `{ "_lt": { "_field": "<field>", "_value": <value> } }` daha az
- `_gt`: `{ "_gt": { "_field": "<field>", "_value": <value> } }` daha büyük
- `_lte`: `{ "_lte": { "_field": "<field>", "_value": <value> } }` eşit veya daha az
- `_gte`: `{ "_gte": { "_field": "<field>", "_value": <value> } }` daha büyük veya eşit
- `_ne`: `{ "_ne": { "_field": "<field>", "_value": <value> } }` eşit değil
- `_eq`: `{ "_eq": { "_field": "<field>", "_value": <value> } }` eşit
- `_is`: `{ "_is": { "_field": "<field>", "_value": <value> } }` aynı şekilde `_eq`
- `_startsWith`: `{ "_startsWith": { "_field": "<field>", "_value": "<value>" } }` dizesi ile başlar
- `_endsWith`: `{ "_endsWith": { "_field": "<field>", "_value": "<value>" } }` dizesi ile biter
- `_id`: `{ "_id": "~123" }` kimliğe göre filtrele
- `_between`: `{ "_between": { "_field": "<field>", "_from": <from>, "_to": <to> } }` aralık filtresi, from kapsayıcıdır, to özeldir, her ikisi de zorunludur
- `_in`: `{ "_in": { "_field": "<field>", "_values": [<value1>, ...] } }` alan bu değerlerden biridir
- `_contains`: `{ "_contains": "<field>" }` bir nesne bu alanı içeriyorsa
- `_like`: `{ "_like": { "_field": "<field>", "_value": "<value>" } }` alan (veya dizin türüne bağlı olarak bir sözcük) alt dizeyi içerir
- `_match`: `{ "_match": { "_field": "<field>", "_value": "<value>" } }` alan şu kelimeyi içerir

Sıralama

Kullanım: `{ "_name": "sort", "fields": [{ "<field>": "<direction>" }, ...] }`

Yön(`direction`), `asc` veya `desc` olabilir.

Sayfalama ve Ek Veriler

Basit sayfalama: `{ "_name": "page", "from": 0, "to": 30 }`

Nesne ile ek veri iste: `{ "_name": "page", "from": 0, "to": 30, "extraData": ["shareCount", "contributors"] }`

Nesnenin `extraData` alanı, seçilen alanları içeren bir JSON nesnesini içerecektir. Kullanılabilir ek veriler, istenen varlığa bağlıdır.

AUTHORIZATIONS: (Api Key) OR (Basic) OR (Session)

QUERY PARAMETERS

query required	string
options required	string

Yanıtlar

✓ 200

RESPONSE HEADERS

X-Total	integer <int64> Total size of the results when <code>page > extraData</code> contains <code>"total"</code>
---------	--

RESPONSE SCHEMA: application/json

any

✓ 400 BadRequest

RESPONSE SCHEMA: application/json

type required	string
message required	string

✓ 401 AuthenticationError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 403 AuthorizationError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 404 NotFoundError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 500 GenericError

RESPONSE SCHEMA: application/json

type required	string
message required	string

GET - Export API

Uyarı: Bu kararlı olmayan bir rota. Gelecekteki sürümlerde değişiklikler olabilir.

Bir sorgunun sonuçlarını belirtilen formatta indirilebilir bir dosya olarak dışa aktarır.

Sorgu `query` parametresi, Sorgu belgesinde açıklanan formata uygunlaştırılmış bir stringleştirilmiş JSON değeridir.

Seçenekler `query` parametresi, aşağıdaki formattan birine sahip olabilir:

- CSV dışa aktarımı için:
 - `format`: (string) "csv" değerine sahip olmalıdır.
 - `fileName`: (optional, string) uzantısız dosya adı
 - Aşağıdaki iki alandan en az biri sağlanmalıdır:
 - `model`: (optional, string) Kabul edilen değerler şunlardır `"Case"`, `"Alert"`, `"User"`, `"Organisation"`, `"Procedure"` ve `"Task"`
 - `fields`: (optional, array of strings) Dışa aktarılan verilere eklenecek ekstra alanlar
 - `delimiter`: (optional, character)
 - `quoteChar`: (optional, character)
 - `escapeChar`: (optional, character)
- JSON dışa aktarımı için:
 - `format`: (string) "json" değerine sahip olmalıdır
 - `fileName`: (optional, string) Dosya adı, uzantısı olmadan

AUTHORIZATIONS: ([Api Key](#)) OR ([Basic](#)) OR ([Session](#))

QUERY PARAMETERS

<code>query</code> <code>required</code>	string
<code>options</code> <code>required</code>	string

Yanıtlar

✓ 200

RESPONSE HEADERS

Content-Type required	string the content-type of the file
X-Total	string the total number of elements
Content-Disposition required	string will be of kind attachment with the filename
Transfer-Encoding required	string

RESPONSE SCHEMA: application/octet-stream

string <binary>

✓ 400 BadRequest

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 401 AuthenticationError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 403 AuthorizationError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 404 NotFoundError

RESPONSE SCHEMA: application/json

type required	string
message required	string

▼ 500 GenericError

RESPONSE SCHEMA: application/json

type required	string
message required	string