Table of Contents

Preface ................................................................................................................................. 4
About Qualys ....................................................................................................................... 4
Contact Qualys Support ..................................................................................................... 4

Chapter 1 - Welcome ........................................................................................................ 5
Qualys API Framework ....................................................................................................... 5
Qualys API Gateway URL .................................................................................................. 6
Introduction to GAV/CSAM API Paradigm ....................................................................... 7
API Rate Limits .................................................................................................................. 9

Chapter 2 - Assets Host Data APIs .................................................................................. 11
Count of Assets ................................................................................................................. 11
Get Host details of specific asset ...................................................................................... 14
Get Host Details of All Assets .......................................................................................... 23

Appendix ......................................................................................................................... 35
Error Messages .................................................................................................................. 35
Supported Operators ......................................................................................................... 35
Preface

This user guide is intended for application developers who will use the Qualys Global AssetView (GAV)/CyberSecurity Asset Management (CSAM) API v2. It is recommended to use v2 APIs. For GAV, we are still supporting the v1 APIs. Refer API v1 User Guide to use v1 APIs.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.
Chapter 1 - Welcome

Welcome to GAV/CSAM API v2.

Get Started

Qualys API Framework - Learn the basics about making API requests. The base URL depends on the platform where your Qualys account is located.

Introduction to GAV/CSAM API Paradigm - Get tips on using the Curl command-line tool to make API requests. Every API request must authenticate using a JSON Web Token (JWT) obtained from the Qualys Authentication API.

Get API Notifications

Subscribe to our API Notifications RSS Feeds for announcements and latest news.

From our Community

Join our Community
API Notifications RSS Feeds

Qualys API Framework

The Qualys GAV/CSAM API uses the following framework.

Request URL

The URL for making API requests respects the following structure:

https://<baseurl>/<module>/<object>/<object_id>/<operation>

where the components are described below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baseurl&gt;</td>
<td>The Qualys API server URL that you should use for API requests depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: <a href="https://gateway.qg1.apps.qualys.com">https://gateway.qg1.apps.qualys.com</a></td>
</tr>
<tr>
<td>&lt;module&gt;</td>
<td>The API module. For the GAV/CSAM, the module is: “am”</td>
</tr>
<tr>
<td>&lt;object&gt;</td>
<td>The module specific object.</td>
</tr>
<tr>
<td>&lt;object_id&gt;</td>
<td>(Optional) The module specific object ID, if appropriate.</td>
</tr>
<tr>
<td>&lt;operation&gt;</td>
<td>The request operation, such as count.</td>
</tr>
</tbody>
</table>
Qualys API Gateway URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you’re on another platform, please replace this URL with the appropriate gateway URL for your account.
Introduction to GAV/CSAM API Paradigm

Authentication

You must authenticate to the Qualys Cloud Platform using Qualys account credentials (user name and password) and get the JSON Web Token (JWT) before you can start using the GAV/CSAM APIs. Use the Qualys Authentication API to get the JWT.

For example,

```
curl -X POST https://gateway.qg1.apps.qualys.com/auth -d
"username=value1&password=passwordValue&token=true" -H "Content-Type: application/x-www-form-urlencoded"
```

where gateway.qg1.apps.qualys.com is the base URL to the Qualys API server where your account is located.

- **username** and **password** are the credentials of the user account for which you want to fetch GAV/CSAM data
- **token** should be true
- **Content-Type** should be "application/x-www-form-urlencoded"

The Authentication API returns a JSON Web Token (JWT) which you can use for authentication during GAV/CSAM calls. **The token expires in 4 hours.** You must regenerate the token to continue using the GAV/CSAM API.

Using Curl

**Curl** is a multi-platform command-line tool used to transfer data using multiple protocols. This tool is supported on many systems, including Windows, Unix, Linux and Mac. In this document Curl is used in the examples to build Qualys API requests using the HTTP over SSL (https) protocol, which is required.

Want to learn more? Visit [https://curl.haxx.se/](https://curl.haxx.se/)

The following Curl options are used according to different situations:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-X &quot;POST&quot;</td>
<td>The POST method is required for all GAV/CSAM API requests.</td>
</tr>
<tr>
<td>-H &quot;Authorization: Bearer &lt;token&gt;&quot;</td>
<td>This option is used to provide a custom HTTP request header parameter for authentication. Provide the JSON Web Token (JWT) received from Qualys authentication API in the following format: Authorization: Bearer &lt;token&gt; For information about Qualys authentication API, see Authentication.</td>
</tr>
</tbody>
</table>

The sample below shows a typical Curl request using options mentioned above and how they interact with each other.

```
curl -X POST "https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/asset" -H
"Authorization: Bearer <token>"
```
Limit your results

Use the optional “fields” parameter for any API request to limit the amount of information returned in the results. Simply specify the fields you want to include or exclude in the output, and all other information will be filtered out (excluded). Multiple fields are comma separated.

Sample limit results

Use this request to get a list of all asset hosts with information for only the operatingSystem and hardware fields:

```
'https://gateway.qg1.apps.qualys.com/rest/2.0/search/am/asset?pageSize=100&includeFields=operatingSystem,hardware'
```

Note:

The response would still include all the fields, but other than the included fields, the value returned for all other fields would be null.

You can include the following fields to limit your results:

- address
- agent
- agentId
- assetName
- biosAssetTag
- biosDescription
- biosSerialNumber
- cloudProvider
- container
- cpuCount
- dnsName
- hardware
- hostId
- inventory
- isContainerHost
- lastBoot
- criticality
- businessInformation

- lastLocation
- lastLoggedOnUser
- netbiosName
- networkInterface
- openPort
- operatingSystem
- processor
- provider
- sensor
- service
- software
- tag
- timeZone
- totalMemory
- userAccount
- volume
- businessApps
- assignedLocation
API Rate Limits

The Qualys API enforces limits on the API calls a customer can make based on their subscription settings. The limits apply to the use of all Qualys APIs except “auth” API (JWT Token Generation API). Default API control settings are provided by the service. Note these settings may be customized per subscription by Qualys Support.

The rate count and period are calculated dynamically each time an API call is received. The rate period represents a rolling window when API calls are counted.

API Controls Definition

**X-RateLimit-Remaining**: This indicates the total API calls remaining in current rate limit window.

**X-RateLimit-ToWait-Sec**: This time indicates the wait time for the rate limit to be reset. The customer has to wait for that time to execute next API calls.

**X-RateLimit-Window-Sec**: This value indicates the total time window assigned for the APIs to be executed.

**X-RateLimit-Limit**: This indicates the max number of API calls that can be executed in that particular rate limit window.

Sample Request

```
```

**Note**: Provide "-i" in the curl request as shown in the example returns the response headers which includes the rate limit related parameters.

After executing a curl request, check the following parameters in response headers to check the rate-limit status:

- X-RateLimit-Remaining: 0
- X-RateLimit-ToWait-Sec: 300
- X-RateLimit-Window-Sec: 3600
- X-RateLimit-Limit: 300

**Example**: A subscription for Standard API Service has the default API control settings. Consider that the API rate limit set for a customer is 300 API calls for a time window of 3600 seconds. If 300 API calls are received in a 5 minute period and none are blocked by any API limiting rules, then you need to wait 55 minutes before making the next call to the API. During the wait period API calls will be blocked by the rate limiting rule.
Sample HTTP Response Headers

Sample 1: Normal API call (API call not blocked)

Server: nginx/1.19.1
Date: Fri, 16 Apr 2021 12:29:52 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-RateLimit-Remaining: 4
X-RateLimit-Window-Sec: 100
X-RateLimit-Limit: 5
Vary: Accept-Encoding
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1 ; mode=block
Referrer-Policy: no-referrer

{"count":580,"responseCode":"SUCCESS","responseMessage":"Valid API Access"}

Sample 2: API Call Blocked - Rate Limit exceeded

Server: nginx/1.19.1
Date: Fri, 16 Apr 2021 12:28:53 GMT
Content-Length: 0
Connection: keep-alive
X-RateLimit-Remaining: 0
X-RateLimit-ToWait-Sec: 33
X-RateLimit-Window-Sec: 100
X-RateLimit-Limit: 5
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1 ; mode=block
Referrer-Policy: no-referrer
Chapter 2 - Assets Host Data APIs

Use these API functions to get host data from GAV/CSAM.

**Note**: The software.authorization and lifecycle related parameters are available only for CSAM subscription. Hence, you can use it in filter criteria and you can see it in the response if you’ve subscribed for CSAM.

**Permissions**
- User must have the GAV/CSAM module and the "App API Enabled" option enabled for that role.

**Count of Assets**

Get count of assets satisfying the specified filter criteria.

```
rest/2.0/count/am/asset
```

[POST]

**Input Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>Filter the events list by providing a filter in json and xml format. Make sure your filter criteria is provided in xml/json format in the request body. If you don’t provide filter parameter, it will show details of all the assets. For more information on supported operators, refer <a href="#">Supported Operators</a>.</td>
</tr>
</tbody>
</table>

**For example (json)**

```
{
   "filters": [
   {
      "field": "software.product",
      "operator": "CONTAINS",
      "value": "Python"
   }
   ]
}
```

**For example (xml)**

```xml
<FilterRequest>
   <filters>
      <Criteria field="software.product" operator="CONTAINS">Python</Criteria>
   </filters>
</FilterRequest>
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assetLastUpdated (String)</td>
<td>Shows records updated on or after this date with the UTC format as yyyy-MM-ddTHH:mmZ e.g. 2019-03-01T11:30Z. This date gets updated whenever any activity happens on the asset. Few examples of such activity: - Vulnerability Management scan - Policy Compliance scan - Inventory collection - Security Configuration Assessment - CertView scan - AssetView or CloudView connector run - Secure Enterprise Mobility scan - Out-of-Band Configuration Assessment - Asset rename - Purge of VM, PC, OCA, CertView records - Agent manifest download - Asset Inventory asset identification updates</td>
</tr>
<tr>
<td>lastSeenAssetId (Integer)</td>
<td>Use to get the count of assets having asset id greater than the specified last seen assetid.</td>
</tr>
<tr>
<td>Authorization (String)</td>
<td>(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with &quot;Bearer&quot; and one space. For example - Bearer authToken</td>
</tr>
</tbody>
</table>
Sample - Get count of all assets with filter criteria

Request:

<JWTToken>' -H 'Content-Type: application/json' -i
'https://gateway.qgl.apps.qualys.com/rest/2.0/count/am/asset' <
filter.json

Here, filter.json file is the request in json format.

Sample Request body in json format (filter.json)

{
   "filters": [
      {
         "field": "software.authorization",
         "operator": "EQUALS",
         "value": "Authorized"
      }
   ]
}

Response:

{
   "count": 850,
   "responseCode": "SUCCESS",
   "responseMessage": "Valid API Access"
}
Get Host details of specific asset

Get details of specific asset by providing an asset id.

`rest/2.0/get/am/asset`

[GET]

### Input Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>excludeFields</td>
<td>Comma separated list of fields to be excluded from the asset object in the response. Default is None. You can choose from the list of fields specified in the section &quot;Limit your results&quot;. For example, to exclude openPort and software from the response: excludeFields=openPort,software</td>
</tr>
<tr>
<td>includeFields</td>
<td>Comma separated list of fields to be included in the asset object in the response. Default is All. You can choose from the list of fields specified in the section &quot;Limit your results&quot;. For example, to include only operatingSystem and hardware in the response: includeFields=operatingSystem,hardware</td>
</tr>
<tr>
<td>assetId</td>
<td>(Required) Use to specify theAssetId for which you want to retrieve the details.</td>
</tr>
<tr>
<td>softwareType</td>
<td>(Optional) Specify the software type to get the host details for specified software type. Available values for softwareType parameter are Application, Unknown, and Others.</td>
</tr>
<tr>
<td>Authorization</td>
<td>(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with &quot;Bearer&quot; and one space. For example - Bearer authToken</td>
</tr>
</tbody>
</table>

### Sample - Get host details of specified asset by assetid

**Request:**
```
```

**Response:**
```
{
    "responseMessage": "Valid API Access",
    "responseCode": "SUCCESS",
    "assetListData": {
        "asset": [
            {
                "assetId": 6920718,
                "assetUUID": "50d20290-c66a-42e7-8c0a-
```
ba6e92b6324c",
   "hostId": 1437386,
   "lastModifiedDate": "2021-04-06T10:02:33.000Z",
   "agentId": null,
   "createdDate": "2020-11-25T12:49:25.000Z",
   "sensorLastUpdatedDate": "2021-04-06T10:02:33.000Z",
   "assetType": "HOST",
   "address": "10.115.110.95",
   "dnsName": "localhost.localdomain",
   "assetName": "localhost.localdomain",
   "netbiosName": null,
   "timeZone": "IST",
   "biosDescription": null,
   "lastBoot": null,
   "totalMemory": 5806,
   "cpuCount": null,
   "lastLoggedOnUser": "root",
   "hwUUID": "422a2b16-4c8b-588a-a20c-c1851ad7e376",
   "biosSerialNumber": "VMware-42 2a 2b 16 4c 8b 58 8a-a2 0c cl 85 la d7 e3 76",
   "biosAssetTag": "No Asset Tag",
   "isContainerHost": false,
   "operatingSystem": {
      "osName": "The CentOS Project CentOS 7 (1810)",
      "fullName": "The CentOS Project CentOS 7 (1810)",
      "category": "Linux / Server",
      "category1": "Linux",
      "category2": "Server",
      "productName": "CentOS",
      "publisher": "The CentOS Project",
      "edition": null,
      "marketVersion": "7",
      "version": "1810",
      "update": null,
      "architecture": null,
      "lifecycle": {
         "gaDate": "2018-12-03T00:00:00.000Z",
         "eolDate": "2020-12-31T00:00:00.000Z",
         "eosDate": "2024-06-30T00:00:00.000Z",
         "stage": "EOL",
         "lifeCycleConfidence": "Exact",
         "eolSupportStage": "Full updates",
         "eosSupportStage": "Maintenance Updates"
      }
   }

"taxonomy": {  
  "id": null,  
  "name": "Linux / Server",  
  "category1": "Linux",  
  "category2": "Server" 
},  
"productFamily": null,  
"installDate": null 
},  
"hardware": {  
  "fullName": "VMware VMware Virtual Platform VMware Virtual Platform",  
  "category": "Virtualized / Virtual Machine",  
  "category1": "Virtualized",  
  "category2": "Virtual Machine",  
  "manufacturer": "VMware",  
  "productName": "VMware Virtual Platform",  
  "model": "VMware Virtual Platform",  
  "lifecycle": {  
    "introDate": null,  
    "gaDate": null,  
    "eosDate": null,  
    "obsoleteDate": null,  
    "stage": "Unknown",  
    "lifeCycleConfidence": " " 
  },  
  "taxonomy": {  
    "id": null,  
    "name": "Virtualized / Virtual Machine",  
    "category1": "Virtualized",  
    "category2": "Virtual Machine" 
  },  
  "productUrl": "https://www.linuxjournal.com/article/3458," ,  
  "productFamily": null 
},  
"userAccountListData": null,  
"openPortListData": {  
  "openPort": [  
  {  
    "port": 709,  
    "description": "",  
    "protocol": "UDP",  
    "detectedService": "portmap/rpcbind",  
  }  
  ]
}
Get Host details of specific asset

```json
{
  "firstFound": "2020-11-25T12:46:42.000Z",
  "lastUpdated": "2020-11-25T12:46:42.000Z"
}
{
  "port": 50000,
  "description": "",
  "protocol": "TCP",
  "detectedService": "IBM_DB2 Universal Database",
  "firstFound": "2020-11-25T12:46:42.000Z",
  "lastUpdated": "2020-11-25T12:46:42.000Z"
}
{
  "port": 6000,
  "description": "",
  "protocol": "TCP",
  "detectedService": "x11",
  "firstFound": "2020-11-25T12:46:42.000Z",
  "lastUpdated": "2020-11-25T12:46:42.000Z"
}
{
  "port": 22,
  "description": "",
  "protocol": "TCP",
  "detectedService": "ssh",
  "firstFound": "2020-11-25T12:46:41.000Z",
  "lastUpdated": "2020-11-25T12:46:41.000Z"
}
{
  "port": 3389,
  "description": "",
  "protocol": "TCP",
  "detectedService": null,
  "firstFound": "2020-11-25T12:46:42.000Z",
  "lastUpdated": "2020-11-25T12:46:42.000Z"
}
}```
Chapter 2 - Assets Host Data APIs

Get Host details of specific asset

```json
{
  "port": 111,
  "description": "",
  "protocol": "UDP",
  "detectedService": "rpc_udp",
  "firstFound": "2020-11-25T12:46:42.000Z",
  "lastUpdated": "2020-11-25T12:46:42.000Z"
},
{
  "port": 111,
  "description": "",
  "protocol": "TCP",
  "detectedService": "rpc",
  "firstFound": "2020-11-25T12:46:41.000Z",
  "lastUpdated": "2020-11-25T12:46:41.000Z"
}
}

"volumelistData": {
  "volume": [
    {
      "name": "tmpfs",
      "free": 2737078272,
      "size": 3043934208
    },
    {
      "name": "/dev/mapper/centos-home",
      "free": 18629619712,
      "size": 18700304384
    },
    {
      "name": "devtmpfs",
      "free": 3026444288,
      "size": 3026444288
    },
    {
      "name": "/dev/mapper/centos-root",
      "free": 19672580096,
      "size": 38304645120
    },
    {
      "name": "/dev/sda1",
      "free": 2737078272,
      "size": 3043934208
    }
  ]
}
```
"free": 876040192,
"size": 1063256064
]
],
"networkInterfaceListData": {
"networkInterface": [
{
"hostname": "localhost.localdomain",
"addressIpV4": "192.168.122.1",
"addressIpV6": null,
"macAddress": "52:54:00:77:e1:71",
"interfaceName": "virbr0",
"dnsAddress": null,
"gatewayAddress": "",
"manufacturer": null,
"macVendorIntroDate": null,
"addresses": null
},
{
"hostname": "localhost.localdomain",
"addressIpV4": "192.168.122.1",
"addressIpV6": null,
"macAddress": "52:54:00:77:e1:71",
"interfaceName": "virbr0",
"dnsAddress": null,
"gatewayAddress": "",
"manufacturer": null,
"macVendorIntroDate": null,
"addresses": null
}
],
"softwareListData": {
"software": [
{
"id": -5698725809391962787,
"fullName": "Python 2.7.5 64-Bit",
"softwareType": "Application",
"isIgnored": false,
"ignoredReason": null,
"category": "Application Development /
Programming Languages",
"category1": "Application Development",
"category2": "Programming Languages"}]}
"productName": "Python",
"component": null,
"publisher": "Python",
"edition": null,
"marketVersion": "2",
"version": "2.7",
"update": "2.7.5",
"architecture": "64-Bit",
"installDate": "2020-03-27T16:11:47.000Z",
"installPath": null,
"lastUpdated": "2020-11-25T12:46:46.000Z",
"lastUseDate": null,
"language": null,
"formerlyKnownAs": null,
"isPackage": false,
"isPackageComponent": false,
"packageName": null,
"lifecycle": {
  "gaDate": "2010-07-03T00:00:00.000Z",
  "eolDate": "2020-01-01T00:00:00.000Z",
  "eosDate": "2020-01-01T00:00:00.000Z",
  "stage": "EOL/EOS",
  "lifeCycleConfidence": "Exact",
  "eolSupportStage": "End-of-life",
  "eosSupportStage": "End-of-life"
},
"supportStageDesc": "Python's policy is to drop support major versions once they reach their end of life",
"license": {
  "category": "Open Source",
  "subcategory": "Python License (Python-2.0)"
},
"authorization": "Authorized"}
"isIgnored": false,
"ignoredReason": null,
"category": "Networking / Access Software",
"category1": "Networking",
"category2": "Access Software",
"productName": "OpenSSH",
"component": "Server",
"publisher": "OpenBSD",
"edition": null,
"marketVersion": "7",
"version": "7.4",
"update": "7.4p1",
"architecture": null,
"installDate": "2020-03-05T14:23:53.000Z",
"installPath": null,
"lastUpdated": "2020-11-25T12:46:53.000Z",
"lastUseDate": null,
"language": null,
"formerlyKnownAs": "OpenBSD Secure Shell",
"isPackage": true,
"isPackageComponent": false,
"packageName": null,
"productUrl": "https://en.wikipedia.org/wiki/OpenSSH,",
"lifecycle": {
    "gaDate": "2016-12-19T00:00:00.000Z",
    "eolDate": null,
    "eosDate": null,
    "stage": "EOL",
    "lifeCycleConfidence": "Calculated",
    "eolSupportStage": "",
    "eosSupportStage": ""
},
"supportStageDesc": null,
"license": {
    "category": "Open Source",
    "subcategory": "BSD 2-Clause License (FreeBSD/Simplified)"
},
"authorization": "Authorized"}
Get host details of specific asset

```
{  
  "provider": null,  
  "cloudProvider": null,  
  "agent": null,  
  "sensor": {  
    "activatedForModules": [  
      "VM"  
    ],  
    "pendingActivationForModules": [],  
    "lastVMScan": 1606306572000,  
    "lastComplianceScan": 0,  
    "lastFullScan": 1606306572000  
  },  
  "container": null,  
  "inventory": {  
    "source": "IP",  
    "created": 1606308565000,  
    "lastUpdated": 1617703353000  
  },  
  "activity": null,  
  "tagList": {  
    "tag": [  
      {  
        "tagId": 14151022,  
        "tagName": "static split",  
        "foregroundColor": 0,  
        "backgroundColor": -65536,  
        "businessImpact": null,  
        "criticalityScore": 2  
      }  
    ]  
  },  
  "serviceList": null,  
  "lastLocation": null,  
  "criticality": {  
    "score": 2,  
    "isDefault": true,  
    "lastUpdated": "2021-06-30T09:43:27.000Z"  
  },  
  "processor": null  
}
```
Get Host Details of All Assets

Get details of all assets that satisfy the filter criteria to include or exclude specified fields. If you don’t provide filter parameter, it will show details of all the assets.

`rest/2.0/search/am/asset`

[POST]

### Input Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>excludeFields</td>
<td>Comma separated list of fields to be excluded from the asset object in the response. Default is None. You can choose from the list of fields specified in the section “Limit your results”. For example, to exclude openPort and software from the response: excludeFields=openPort,software</td>
</tr>
<tr>
<td>includeFields</td>
<td>Comma separated list of fields to be included in the asset object in the response. Default is All. You can choose from the list of fields specified in the section “Limit your results”. For example, to include only operatingSystem and hardware in the response: includeFields=operatingSystem,hardware</td>
</tr>
<tr>
<td>assetLastUpdated</td>
<td>Shows records updated on or after this date with the UTC format as yyyy-MM-ddTHH:mmZ e.g. 2019-03-01T11:30Z. This date gets updated whenever any activity happens on the asset. Few examples of such activity: - Vulnerability Management scan - Policy Compliance scan - Inventory collection - Security Configuration Assessment - CertView scan - AssetView or CloudView connector run - Secure Enterprise Mobility scan - Out-of-Band Configuration Assessment - Asset rename - Purge of VM, PC, OCA, CertView records - Agent manifest download - Asset Inventory asset identification updates</td>
</tr>
<tr>
<td>lastSeenAssetId</td>
<td>Use to get the count of assets having asset id greater than the specified last seen assetid.</td>
</tr>
<tr>
<td>pageSize</td>
<td>The number of records per page to be included in the response. If pageSize is not specified in the request, 100 records will be fetched by default. The maximum value supported for pageSize is 300.</td>
</tr>
</tbody>
</table>
**filter (String)**  
Filter the events list by providing a filter in json and xml format. Make sure your filter criteria is provided in xml/json format in the request body. If you don’t provide filter parameter, it will show details of all the assets. For more information on supported operators, refer **Supported Operators**.

**For example (json)** -
```json
{
    "filters": [
        {
            "field": "software.product",
            "operator": "CONTAINS",
            "value": "Python"
        }
    ]
}
```

**For example (xml)** -
```xml
<FilterRequest>
    <filters>
        <Criteria field="software.product" operator="CONTAINS">Python</Criteria>
    </filters>
</FilterRequest>
```

**softwareType (String)**  
(Optional) Specify the software type to get the host details for specified software type. Available values for softwareType parameter are Application, Unknown, and Others.

**Authorization (String)**  
(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken
Sample - Get details of all asset

Request (without filter):
```bash
```

Request (with filter - xml):
```bash
```

Here, *filter.xml* file is the request in xml format.

Request (with filter - json):
```bash
```

Here, *filter.json* file is the request in json format.

Sample Request body in xml format (filter.xml)
```xml
<FilterRequest>
  <filters>
    <Criteria field="operatingSystem.category1" operator="EQUALS">Mac</Criteria>
  </filters>
</FilterRequest>
```

Sample Request body in json format (filter.json)
```json
{
  "filters": [
    {
      "field": "operatingSystem.category1",
      "operator": "EQUALS",
      "value": "Mac"
    }
  ]
}
```

Response:
```json
{
  "responseMessage": "Valid API Access",
```
"count": 1,
"responseCode": "SUCCESS",
"lastSeenAssetId": 6920718,
"hasMore": 1,
"assetListData": {
    "asset": [
        {
            "assetId": 6920718,
            "assetUUID": "50d20290-c66a-42e7-8c0a-ba6e92b6324c",
            "hostId": 1437386,
            "lastModifiedDate": "2021-04-06T10:02:33.000Z",
            "agentId": null,
            "createdDate": "2020-11-25T12:49:25.000Z",
            "sensorLastUpdatedDate": "2021-04-06T10:02:33.000Z",
            "assetType": "HOST",
            "address": "10.115.110.95",
            "dnsName": "localhost.localdomain",
            "assetName": "localhost.localdomain",
            "netbiosName": null,
            "timeZone": "IST",
            "biosDescription": null,
            "lastBoot": null,
            "totalMemory": 5806,
            "cpuCount": null,
            "lastLoggedOnUser": "root",
            "hwUUID": "422a2b16-4c8b-588a-a20c-c1851ad7e376",
            "biosSerialNumber": "VMware-42 2a 2b 16 4c 8b 58 8a-a2 0c c1 85 1a d7 e3 76",
            "biosAssetTag": "No Asset Tag",
            "isContainerHost": false,
            "operatingSystem": {
                "osName": "The CentOS Project CentOS 7 (1810)",
                "fullName": "The CentOS Project CentOS 7 (1810)",
                "category": "Linux / Server",
                "category1": "Linux",
                "category2": "Server",
                "productName": "CentOS",
                "publisher": "The CentOS Project",
                "edition": null,
                "marketVersion": "7",
                "version": "1810",
                "update": null,
                "architecture": null,
            }
        }
    ]
}
"lifecycle": {
  "gaDate": "2018-12-03T00:00:00.000Z",
  "eolDate": "2020-12-31T00:00:00.000Z",
  "eosDate": "2024-06-30T00:00:00.000Z",
  "stage": "EOL",
  "lifeCycleConfidence": "Exact",
  "eolSupportStage": "Full updates",
  "eosSupportStage": "Maintenance Updates"
},
"taxonomy": {
  "id": null,
  "name": "Linux / Server",
  "category1": "Linux",
  "category2": "Server"
},
"productFamily": null,
"installDate": null
},
"hardware": {
  "fullName": "VMware VMware Virtual Platform VMware Virtual Platform",
  "category": "Virtualized / Virtual Machine",
  "category1": "Virtualized",
  "category2": "Virtual Machine",
  "manufacturer": "VMware",
  "productName": "VMware VMware Virtual Platform",
  "model": "VMware VMware Virtual Platform",
  "lifecycle": {
    "introDate": null,
    "gaDate": null,
    "eosDate": null,
    "obsoletedate": null,
    "stage": "Unknown",
    "lifeCycleConfidence": " "
  },
  "taxonomy": {
    "id": null,
    "name": "Virtualized / Virtual Machine",
    "category1": "Virtualized",
    "category2": "Virtual Machine"
  },
  "productUrl": "https://www.linuxjournal.com/article/3458,",
  "productFamily": null
"userAccountListData": null,
"openPortListData": {
  "openPort": [
  {
    "port": 709,
    "description": ",",
    "protocol": "UDP",
    "detectedService": "portmap/rpcbind",
    "firstFound": "2020-11-25T12:46:42.000Z",
    "lastUpdated": "2020-11-25T12:46:42.000Z"
  },
  {
    "port": 50000,
    "description": ",",
    "protocol": "TCP",
    "detectedService": "IBM_DB2_Universal_Database",
    "firstFound": "2020-11-25T12:46:42.000Z",
    "lastUpdated": "2020-11-25T12:46:42.000Z"
  },
  {
    "port": 6000,
    "description": ",",
    "protocol": "TCP",
    "detectedService": "x11",
    "firstFound": "2020-11-25T12:46:42.000Z",
    "lastUpdated": "2020-11-25T12:46:42.000Z"
  },
  {
    "port": 22,
    "description": ",",
    "protocol": "TCP",
    "detectedService": "ssh",
    "firstFound": "2020-11-25T12:46:41.000Z",
    "lastUpdated": "2020-11-25T12:46:41.000Z"
  }
  ]
},

"port": 3389,
"description": "",
"protocol": "TCP",
"detectedService": null,
"firstFound": "2020-11-25T12:46:42.000Z",
"lastUpdated": "2020-11-25T12:46:42.000Z",

"port": 111,
"description": "",
"protocol": "UDP",
"detectedService": "rpc_udp",
"firstFound": "2020-11-25T12:46:42.000Z",
"lastUpdated": "2020-11-25T12:46:42.000Z",

"port": 111,
"description": "",
"protocol": "TCP",
"detectedService": "rpc",
"firstFound": "2020-11-25T12:46:42.000Z",
"lastUpdated": "2020-11-25T12:46:42.000Z",

"port": 111,
"description": "",
"protocol": "TCP",
"detectedService": "rpc",
"firstFound": "2020-11-25T12:46:42.000Z",
"lastUpdated": "2020-11-25T12:46:42.000Z",

"volumeListData": {
    "volume": [
        {
            "name": "tmpfs",
            "free": 2737078272,
            "size": 3043934208
        },
        {
            "name": "/dev/mapper/centos-home",
            "free": 18629619712,
            "size": 18700304384
        },
        {
            "name": "devtmpfs",
            "free": 3026444288,
            "size": 3043934208
        }
    ]
}
}
"size": 3026444288,
},
{
  "name": "/dev/mapper/centos-root",
  "free": 19672580096,
  "size": 38304645120
},
{
  "name": "/dev/sda1",
  "free": 876040192,
  "size": 1063256064
}
]}

"networkInterfaceListData": {
  "networkInterface": [
    {
      "hostname": "localhost.localdomain",
      "addressIpV4": "192.168.122.1",
      "addressIpV6": null,
      "macAddress": "52:54:00:77:e1:71",
      "interfaceName": "virbr0",
      "dnsAddress": null,
      "gatewayAddress": 
      "manufacturer": null,
      "macVendorIntroDate": null,
      "addresses": null
    },
    {
      "hostname": "localhost.localdomain",
      "addressIpV4": "10.115.110.95",
      "addressIpV6": "fe80:0:0:0:250:56ff:feaa:e2da",
      "macAddress": "00:50:56:aa:e2:da",
      "interfaceName": "ens192",
      "dnsAddress": null,
      "gatewayAddress": 
      "manufacturer": "VMware",
      "macVendorIntroDate": 946944000000,
      "addresses": null
    }
  ]
},

"softwareListData": {
  "software": [
"id": -5698725809391962787,
"fullName": "Python 2.7.5 64-Bit",
"softwareType": "Application",
"isIgnored": false,
"ignoredReason": null,
"category": "Application Development / Programming Languages",
"category1": "Application Development",
"category2": "Programming Languages",
"productName": "Python",
"component": null,
"publisher": "Python",
"edition": null,
"marketVersion": "2",
"version": "2.7",
"update": "2.7.5",
"architecture": "64-Bit",
"installDate": "2020-03-27T16:11:47.000Z",
"installPath": null,
"lastUpdated": "2020-11-25T12:46:46.000Z",
"lastUseDate": null,
"language": null,
"formerlyKnownAs": null,
"isPackage": false,
"isPackageComponent": false,
"packageName": null,
"lifecycle": {
  "gaDate": "2010-07-03T00:00:00.000Z",
  "eolDate": "2020-01-01T00:00:00.000Z",
  "eosDate": "2020-01-01T00:00:00.000Z",
  "stage": "EOL/EOS",
  "lifeCycleConfidence": "Exact",
  "eolSupportStage": "End-of-life",
  "eosSupportStage": "End-of-life"
},
"supportStageDesc": "Python's policy is to drop support major versions once they reach their end of life",
"license": {
  "category": "Open Source",
  "subcategory": "Python License"
(Python-2.0)"

},
"authorization": "Authorized"
},

{
"id": 9136542396418607016,
"fullName": "OpenBSD OpenSSH Server 7.4p1",
"softwareType": "Application",
"isIgnored": false,
"ignoredReason": null,
"category": "Networking / Access Software",
"category1": "Networking",
"category2": "Access Software",
"productName": "OpenSSH",
"component": "Server",
"publisher": "OpenBSD",
"edition": null,
"marketVersion": "7",
"version": "7.4",
"update": "7.4p1",
"architecture": null,
"installDate": "2020-03-05T14:23:53.000Z",
"installPath": null,
"lastUpdated": "2020-11-25T12:46:53.000Z",
"lastUseDate": null,
"language": null,
"formerlyKnownAs": "OpenBSD Secure Shell",
"isPackage": true,
"isPackageComponent": false,
"packageName": null,
"productUrl": "https://en.wikipedia.org/wiki/OpenSSH,,",
"lifecycle": {
"gaDate": "2016-12-19T00:00:00.000Z",
"eolDate": null,
"eosDate": null,
"stage": "EOL",
"lifecycleConfidence": "Calculated",
"eolSupportStage": "",
"eosSupportStage": ""
}
}
"supportStageDesc": null,
"license": {
  "category": "Open Source",
  "subcategory": "BSD 2-Clause License
(FreeBSD/Simplified)"
},
"authorization": "Authorized"
}]
"provider": null,
"cloudProvider": null,
"agent": null,
"sensor": {
  "activatedForModules": [
    "VM"
  ],
  "pendingActivationForModules": [],
  "lastVMScan": 1606306572000,
  "lastComplianceScan": 0,
  "lastFullScan": 1606306572000
},
"container": null,
"inventory": {
  "source": "IP",
  "created": 1606308565000,
  "lastUpdated": 1617703353000
},
"activity": null,
"tagList": {
  "tag": [
    {
      "tagId": 14151022,
      "tagName": "static split",
      "foregroundColor": 0,
      "backgroundColor": -65536,
      "businessImpact": null,
      "criticalityScore": 3
    }
  ]
},
"serviceList": null,
"lastLocation": null,
"criticality": {
  "score": 2,
  "isDefault": true,
"lastUpdated": "2021-06-30T09:43:27.000Z"
],
"processor": null
]
}
]
Appendix

This appendix describes the types of error messages returned from GAV/CSAM API requests, list of operators with supported attributes.

Error Messages

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>The request could not be understood by the server due to malformed syntax. This error also occurs if you provide wrong (or unsupported) operator in the request.</td>
</tr>
<tr>
<td>403 Forbidden</td>
<td>This response code is returned for the following scenarios:</td>
</tr>
<tr>
<td></td>
<td>- If the Asset Inventory License is in &quot;Pending Activation&quot;.</td>
</tr>
<tr>
<td></td>
<td>- If &quot;App API Enabled&quot; option is not checked.</td>
</tr>
<tr>
<td></td>
<td>- If &quot;App API Enabled&quot; option is checked, but the license expiration date (for Trial/Full customers) has elapsed.</td>
</tr>
<tr>
<td></td>
<td>- If the customer’s license subscription cannot be validated.</td>
</tr>
<tr>
<td>404 Not found</td>
<td>The server has not found anything matching the Request</td>
</tr>
<tr>
<td>416 Requested Range Not Satisfiable</td>
<td>Please provide a Page Size value less than the max page size limit set.</td>
</tr>
<tr>
<td>500 Failure</td>
<td>The server encountered an unexpected condition which prevented it from fulfilling the request</td>
</tr>
</tbody>
</table>

Supported Operators

This section of the appendix lists supported operators for tokens.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NUMERIC_OPERATORS</td>
<td>EQUALS, IN, NOT_EQUALS, GREATER, LESSER, GREATER_THAN_EQUAL, and LESS_THAN_EQUAL</td>
</tr>
<tr>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
<td>EQUALS, IN, GREATER, LESSER, GREATER_THAN_EQUAL, LESS_THAN_EQUAL</td>
</tr>
<tr>
<td>STRING_OPERATORS</td>
<td>CONTAINS, IN, EQUALS, and NOT_EQUALS</td>
</tr>
<tr>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
<td>CONTAINS, IN, and EQUALS</td>
</tr>
</tbody>
</table>
### Supported Operators

<table>
<thead>
<tr>
<th>Operator</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE_OPERATORS</td>
<td>EQUALS, NOT_EQUALS, GREATER, LESSER, GREATER_THAN_EQUAL, and LESS_THAN_EQUAL</td>
</tr>
<tr>
<td>BOOLEAN_OPERATORS</td>
<td>EQUALS</td>
</tr>
<tr>
<td>ENUM_OPERATORS</td>
<td>EQUALS, NOT_EQUALS, and IN</td>
</tr>
<tr>
<td>UUID_OPERATORS</td>
<td>EQUALS and IN</td>
</tr>
<tr>
<td>IP_OPERATORS</td>
<td>EQUALS and IN</td>
</tr>
</tbody>
</table>

Following table lists different attributes with supported operators:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>asset.assetID</td>
<td>NUMERIC_OPERATORS</td>
</tr>
<tr>
<td>asset.name</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.created</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>asset.lastUpdated</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>asset.type</td>
<td>ENUM_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLoggedOnUser</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.totalMemory</td>
<td>NUMERIC_OPERATORS</td>
</tr>
<tr>
<td>asset.timezone</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.trackingMethod</td>
<td>ENUM_OPERATORS</td>
</tr>
<tr>
<td>asset.lastBoot</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>asset.netbiosName</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.hostID</td>
<td>NUMERIC_OPERATORS</td>
</tr>
<tr>
<td>asset.isContainerHost</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td>asset.biosAssetTag</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.biosDescription</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.biosHardwareUUID</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.biosSerialNumber</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.agentID</td>
<td>UUID_OPERATORS</td>
</tr>
<tr>
<td>asset.criticalityScore</td>
<td>NUMERIC_OPERATORS</td>
</tr>
<tr>
<td>accounts.username</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>provider</td>
<td>ENUM_OPERATORS</td>
</tr>
<tr>
<td>isDockerHost</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td><strong>Inventory Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>inventory.source</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>inventory.created</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>inventory.lastUpdated</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td><strong>Processor Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>processors</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>processors.speed</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td><strong>Container Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>container.noOfContainers</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>container.noOfImages</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>container.version</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td><strong>Interface Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>interfaces.hostname</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>interfaces.interfaceName</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>interfaces.macAddress</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>interfaces.manufacturer</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>interfaces.address</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>interfaces.dnsAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>interfaces.gatewayAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td><strong>Open Ports Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>openPorts.description</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>openPorts.detectedService</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>openPorts.protocol</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>openPorts.port</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>openPorts.firstFound</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>openPorts.lastUpdated</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td><strong>Services Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>services.description</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>services.name</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>services.status</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td><strong>Sensors Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>sensors.lastComplianceScan</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>sensors.lastFullScan</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>sensors.lastVmScan</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td><strong>Tag Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>tags.name</td>
<td>EQUALS, IN, CONTAINS</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>tags.businessImpact</td>
<td>EQUALS, IN, CONTAINS</td>
</tr>
<tr>
<td><strong>Volume Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>volumes.free</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>volumes.size</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>volumes.name</td>
<td>STRING_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td><strong>Agent Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>agent.version</td>
<td>NUMERIC_AND_NOT_EQUAL_OPERATORS</td>
</tr>
<tr>
<td>agent.connectedFrom</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>agent.errorStatus</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td>agent.lastActivity</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>agent.lastCheckedIn</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td><strong>Hardware Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>hardware</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.category</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.category1</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.category2</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.manufacturer</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.model</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.product</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.lifecycle.stage</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>hardware.lifecycle.eos</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>hardware.lifecycle.ga</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>hardware.lifecycle.intro</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>hardware.lifecycle.obs</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td><strong>Software Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>software.architecture</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.category</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.category1</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.category2</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.component</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.edition</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.marketVersion</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.name</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.product</td>
<td>STRING_OPERATORS</td>
</tr>
</tbody>
</table>
## Supported Operators

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>software.publisher</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.supportStage</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.version</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.update</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.isPackage</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td>software.isPackageComponent</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td>software.license.category</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.license.subcategory</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.lifecycle.stage</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>software.installDate</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.lastUseDate</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.lastUpdated</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.lifecycle.eol</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.lifecycle.eos</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.lifecycle.ga</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>software.authorization</td>
<td>EQUALS, NOT_EQUALS, and IN</td>
</tr>
</tbody>
</table>

## Operating System Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>operatingSystem</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.category</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.category1</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.category2</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.architecture</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.component</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.edition</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.marketVersion</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.name</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.publisher</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.version</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.update</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.lifecycle.stage</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.installDate</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.lifecycle.eol</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.lifecycle.eos</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>operatingSystem.lifecycle.ga</td>
<td>DATE_OPERATORS</td>
</tr>
</tbody>
</table>
## Supported Operators

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AWS Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>aws.ec2.availabilityZone</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.instanceType</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.publicDNS</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.privateDNS</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.accountId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.imageId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.instanceId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.instanceState</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.region.code</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.subnetId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.vpcId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.hostname</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.privateIpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.publicIpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>aws.tags.key</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.tags.value</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.spotInstance</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.launchDate</td>
<td>DATE_OPERATORS</td>
</tr>
<tr>
<td>aws.ec2.hasAgent</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td><strong>Azure Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>azure.vm.imageOffer</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.imagePublisher</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.imageVersion</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.name</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.size</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.vmid</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.resourceGroupName</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.state</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.subnet</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.subscriptionId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.location</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.platform</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.macAddress</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>Attribute</td>
<td>Operator</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>azure.tags.value</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.tags.name</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.privatelpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.publicIpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>azure.vm.hasAgent</td>
<td>BOOLEAN_OPERATORS</td>
</tr>
<tr>
<td><strong>GCP Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>gcpcompute.hostname</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.instanceId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.machineType</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.network</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.projectId</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.projectNumber</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.macAddress</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.state</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.zone</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.privatelpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td>gcpcompute.publicIpAddress</td>
<td>IP_OPERATORS</td>
</tr>
<tr>
<td><strong>Geo IP Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>asset.lastLocation</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLocation.city</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLocation.country</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLocation.continent</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLocation.postal</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.lastLocation.state</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td><strong>Business Information Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>asset.org.company</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.org.department</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.ownedBy</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.managedBy</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.supportedBy</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.supportGroup</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.environment</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.operationalStatus</td>
<td>STRING_OPERATORS</td>
</tr>
<tr>
<td>asset.assignedLocation.name</td>
<td>STRING_OPERATORS</td>
</tr>
</tbody>
</table>
Supported Operators

**Note:** Following tokens are available only for CSAM License Subscriber:

- `hardware.lifecycle.stage`
- `hardware.lifecycle.eos`
- `hardware.lifecycle.ga`
- `hardware.lifecycle.intro`
- `hardware.lifecycle.obs`
- `software.authorization`
- `software.license.category`
- `software.license.subcategory`
- `software.lifecycle.eol`
- `software.lifecycle.eos`
- `software.lifecycle.ga`
- `software.lifecycle.stage`
- `software.isPackage`
- `software.isPackageComponent`
- `operatingSystem.lifecycle.eol`
- `operatingSystem.lifecycle.eos`
- `operatingSystem.lifecycle.ga`
- `operatingSystem.lifecycle.stage`

Following are some example to understand the different supported operators by comparing QQL(Ui) tokens:

**Example 1 - hardware.category1:Computers**

**Request Body in XML:**

```xml
<FilterRequest>
  <filters>
    <Criteria field="hardware.category1" operator="CONTAINS">
      <value>Computers</value>
    </Criteria>
  </filters>
</FilterRequest>
```

**OR Request Body in Json:**

```json
asset.assignedLocation.city STRING_OPERATORS
asset.assignedLocation.state STRING_OPERATORS
asset.assignedLocation.country STRING_OPERATORS
businessApp.name STRING_OPERATORS
businessApp.id STRING_OPERATORS
businessApp.businessCriticality STRING_OPERATORS
businessApp.ownedBy STRING_OPERATORS
businessApp.supportGroup STRING_OPERATORS
businessApp.operationalStatus STRING_OPERATORS
businessApp.environment STRING_OPERATORS
businessApp.managedBy STRING_OPERATORS
businessApp.supportedBy STRING_OPERATORS
```
Appendix

Supported Operators

```json
{
    "filters": [
        {
            "field": "hardware.category1",
            "operator": "CONTAINS",
            "value": "Computers"
        }
    ]
}
```

**Example 2 - `hardware.manufacturer:`Apple` OR `hardware.manufacturer:`HPE`**

*Request Body in XML:*

```xml
<FilterRequest>
    <filters>
        <Criteria field="hardware.manufacturer" operator="IN">
            <value>Apple,HPE</value>
        </Criteria>
    </filters>
</FilterRequest>
```

**Example 3 - `software:(product:Python and update:2.7.5)`**

*Request Body in XML:*

```xml
<FilterRequest>
    <filters>
        <Criteria field="software.product" operator="CONTAINS">
            <value>Python</value>
        </Criteria>
        <Criteria field="software.update" operator="CONTAINS">
            <value>2.7.5</value>
        </Criteria>
    </filters>
</FilterRequest>
```

**Example 4 - `operatingSystem.category1:`Mac` and `hardware.category:Notebook`**

*Request Body in XML:*

```xml
<FilterRequest>
    <filters>
        <Criteria field="operatingSystem.category1" operator="EQUALS">
            <value>Mac</value>
        </Criteria>
    </filters>
</FilterRequest>
```
<Criteria field="hardware.category" operator="EQUALS">
  <value>Notebook</value>
</Criteria>
</filters>
</FilterRequest>

Example 5 - operatingSystem.category1:`Mac` or hardware.category:Notebook

Request Body in XML:

<FilterRequest>
  <filters>
    <Criteria field="operatingSystem.category1" operator="EQUALS">
      <value>Mac</value>
    </Criteria>
    <Criteria field="hardware.category" operator="EQUALS">
      <value>Notebook</value>
    </Criteria>
  </filters>
  <operation>OR</operation>
</FilterRequest>

Example 6 - operatingSystem.category1:`Mac` and hardware.category:Notebook

Request Body in XML:

<FilterRequest>
  <filters>
    <Criteria field="operatingSystem.category1" operator="EQUALS">
      <value>Mac</value>
    </Criteria>
    <Criteria field="hardware.category" operator="EQUALS">
      <value>Notebook</value>
    </Criteria>
  </filters>
  <operation>AND</operation>
</FilterRequest>