File Integrity Monitoring API v2

User Guide
Version 2.0

July 26, 2019

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Preface

This user guide is intended for application developers who will use the Qualys FIM API.

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 File Integrity Monitoring API.

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 FIM 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 File Integrity Monitoring 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.

<baseurl>	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: https://gateway.qg1.apps.qualys.com
<module>	The API module. For the FIM API, the module is: “fim”.
<object>	The module specific object.
<object_id>	(Optional) The module specific object ID, if appropriate.
<operation>	The request operation, such as count.

Base URL to the Qualys API Server

The Qualys API documentation and sample code within it use the API server URL for Qualys US Platform 1: gateway.qg1.apps.qualys.com.

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

Account Login	API Server URL
Qualys US Platform 1	https://gateway.qg1.apps.qualys.com
Qualys US Platform 2	https://gateway.qg2.apps.qualys.com
Qualys US Platform 3	https://gateway.qg3.apps.qualys.com
Qualys EU Platform 1	https://gateway.qg1.apps.qualys.eu
Qualys EU Platform 2	https://gateway.qg2.apps.qualys.eu
Qualys India Platform 1	https://gateway.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://gateway.<customer_base_url>

Introduction to FIM 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 FIM 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 FIM 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 FIM API calls. The token expires in 4 hours. You must regenerate the token to continue using the FIM 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 i s required.

Want to learn more? Visit https://curl.haxx.se/

The following Curl options are used according to different situations:

Option	Description
-X GET/POST	The GET method or the POST method is used as per requirement.
-H 'authorization: Bearer <token>'	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 <token>` For information about Qualys authentication API, see Authentication.
-H 'content-type: application/json'	Denotes that content is in JSON format.
-d @request.json	Provide a request.json file for parameter input.
--data-urlencode	Used to encode spaces and special characters in the URL/Parameter values.

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/fim/v2/events/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Fetching more than ten thousand events

FIM APIs are designed to fetch less that ten thousand (9999 events) per page for optimum performance. You can use the searchAfter parameter in order to fetch more than ten thousand events.

First you need to use the sort parameter to sort events using a filter that has unique values such as ID, name, etc. Each event is returned with an identifier called sortValue. To fetch events beyond the current page size, in subsequent API requests, provide the sortValue of an event to the searchAfter parameter to fetch events after that specific event.

searchAfter is supported for the following APIs:

```
/fim/v2/events/search
/fim/v2/events/ignore/search
/fim/v2/incidents/{incidentId}/events/search
```

For example, suppose you have fifteen thousand FIM events in your account. The first API request will only return 9999 events. To get events beyond 9999, in a subsequent API request, provide the sortValue of the 9999th event in the searchAfter parameter. The second API request will now fetch the remaining events starting from the 10000th event.

For better performance, it is recommended to use smaller page sizes of 1000/2000 records.

Example

You need to sort a list before you can use searchAfter.

Step 1) Search events using the sort parameter:

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"sort":"[{\"dateTime\":\"desc\"},{\"id\":\"desc\"}]",
"pageSize":10
}
```

Response:


```
[
    {
        "sortValues": [
            1556199372947,
            "9df007e9-9532-3558-a3a8-0b14d943670d"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.947+0000",
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                     OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                             f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                   Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
```

```
            "userID": "S-1-5-21-122566442-3410611961-
                1220210811-500"
        },
        "newContent": null,
        "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
        "name": "setupapi.app.log",
        "action": "Attributes",
        "id": "9df007e9-9532-3558-a3a8-0b14d943670d",
        "asset": {
            "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
            "interfaces": [
                {
                    "hostname": "MALWARELAB-IOC",
                    "macAddress": "00:50:56:AA:6B:B8",
                    "address": "10.115.77.190",
                    "interfaceName": "Intel(R) PRO/1000 MT
                      Network Connection"
                }
            ],
            "lastCheckedIn": "2019-04-25T13:51:48.000Z",
            "created": "2018-11-01T04:58:21.000+0000",
            "hostId": "290890",
          "operatingSystem": "Microsoft Windows 7 Professional
              6.1.7601 Service Pack 1 Build 7601",
            "tags": [
                "7650412",
                "7655820",
                "7895614"
            ],
            "assetType": "HOST",
            "system": {
                "lastBoot": "2019-03-13T21:49:47.500Z"
            },
            "ec2": null,
            "lastLoggedOnUser": ".\\Administrator",
            "netbiosName": "MALWARELAB-IOC",
            "name": "MALWARELAB-IOC",
            "agentVersion": "3.0.0.101",
            "updated": "2019-04-25T13:51:48.729+0000"
        },
        "class": "Disk"
    }
},
{
    "sortValues": [
```

```
            1556199372947,
            "05a9bbea-d03c-3bc3-9421-5d3cbb8ac630"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.947+0000",
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                      OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                             f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                     Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
                "userID": "S-1-5-21-122566442-3410611961-
                    1220210811-500"
            },
            "newContent": null,
            "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
```

```
            "name": "setupapi.app.log",
            "action": "Attributes",
            "id": "05a9bbea-d03c-3bc3-9421-5d3cbb8ac630",
            "asset": {
                "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
                "interfaces": [
                    {
                        "hostname": "MALWARELAB-IOC",
                        "macAddress": "00:50:56:AA:6B:B8",
                        "address": "10.115.77.190",
                        "interfaceName": "Intel(R) PRO/1000 MT
                          Network Connection"
                    }
                ],
                "lastCheckedIn": "2019-04-25T13:51:48.000Z",
                "created": "2018-11-01T04:58:21.000+0000",
                "hostId": "290890",
              "operatingSystem": "Microsoft Windows 7 Professional
                 6.1.7601 Service Pack 1 Build 7601",
                "tags": [
                    "7650412",
                    "7655820",
                    "7895614"
                ],
                "assetType": "HOST",
                "system": {
                    "lastBoot": "2019-03-13T21:49:47.500Z"
                },
                "ec2": null,
                "lastLoggedOnUser": ".\\Administrator",
                "netbiosName": "MALWARELAB-IOC",
                "name": "MALWARELAB-IOC",
                "agentVersion": "3.0.0.101",
                "updated": "2019-04-25T13:51:48.729+0000"
            },
            "class": "Disk"
        }
    },
    {
        "sortValues": [
            1556199372946,
            "d47984c3-71d8-36b5-84d4-bb0ec34af828"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.946+0000",
```

```
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                      OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                              f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                     Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
                "userID": "S-1-5-21-122566442-3410611961-
                     1220210811-500"
            },
            "newContent": null,
            "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
            "name": "setupapi.app.log",
            "action": "Attributes",
            "id": "d47984c3-71d8-36b5-84d4-bb0ec34af828",
            "asset": {
                "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
```

```
                "interfaces": [
                    {
                        "hostname": "MALWARELAB-IOC",
                        "macAddress": "00:50:56:AA:6B:B8",
                        "address": "10.115.77.190",
                        "interfaceName": "Intel(R) PRO/1000 MT
                          Network Connection"
                    }
                ],
                "lastCheckedIn": "2019-04-25T13:51:48.000Z",
                "created": "2018-11-01T04:58:21.000+0000",
                "hostId": "290890",
              "operatingSystem": "Microsoft Windows 7 Professional
                  6.1.7601 Service Pack 1 Build 7601",
                "tags": [
                    "7650412",
                    "7655820",
                    "7895614"
                ],
                "assetType": "HOST",
                "system": {
                    "lastBoot": "2019-03-13T21:49:47.500Z"
                },
                "ec2": null,
                "lastLoggedOnUser": ".\\Administrator",
                "netbiosName": "MALWARELAB-IOC",
                "name": "MALWARELAB-IOC",
                "agentVersion": "3.0.0.101",
                "updated": "2019-04-25T13:51:48.729+0000"
            },
            "class": "Disk"
        }
    },
    {
        "sortValues": [
            1556199372946,
            "0ac9f186-6787-339f-a768-929b39da6725"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.946+0000",
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
```

```
            OS_addTag",
        "rules": [
            {
                "severity": 4,
                "number": 6,
                "name": "Rule-6",
                "description": null,
                "id": "9287a14c-8036-4403-af88-
                  f98ae8f920fb",
                "type": "directory"
            }
        ],
        "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
        "type": "WINDOWS",
        "category": {
            "name": "PCI",
          "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
        }
    }
],
"type": "File",
"changedAttributes": null,
"platform": "WINDOWS",
"oldContent": null,
"actor": {
    "process": "NPFInstall.exe",
    "processID": 8632,
    "imagePath": "\\Device\\HarddiskVolume2\\Program
      Files\\Npcap\\NPFInstall.exe",
    "userName": "MALWARELAB-IOC\\Administrator",
    "userID": "S-1-5-21-122566442-3410611961-
        1220210811-500"
},
"newContent": null,
"customerId": "58b888be-a90f-e3be-838d-88877aee572b",
"name": "setupapi.app.log",
"action": "Attributes",
"id": "0ac9f186-6787-339f-a768-929b39da6725",
"asset": {
    "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
    "interfaces": [
        {
            "hostname": "MALWARELAB-IOC",
            "macAddress": "00:50:56:AA:6B:B8",
            "address": "10.115.77.190",
```

```
                        "interfaceName": "Intel(R) PRO/1000 MT
                         Network Connection"
                    }
                ],
                "lastCheckedIn": "2019-04-25T13:51:48.000Z",
                "created": "2018-11-01T04:58:21.000+0000",
                "hostId": "290890",
              "operatingSystem": "Microsoft Windows 7 Professional
                 6.1.7601 Service Pack 1 Build 7601",
                "tags": [
                    "7650412",
                    "7655820",
                    "7895614"
                ],
                "assetType": "HOST",
                "system": {
                    "lastBoot": "2019-03-13T21:49:47.500Z"
                },
                "ec2": null,
                "lastLoggedOnUser": ".\\Administrator",
                "netbiosName": "MALWARELAB-IOC",
                "name": "MALWARELAB-IOC",
                "agentVersion": "3.0.0.101",
                "updated": "2019-04-25T13:51:48.729+0000"
            },
            "class": "Disk"
        }
    },
...
]
```


Step 2) Take one of the sortValues from the above response and provide it as input for searchAfter. This will fetch events after that particular sortValue.

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"sort":"[{\"dateTime\":\"desc\"},{\"id\":\"desc\"}]",
"pageSize":10,
"searchAfter":[1556199372947,"05a9bbea-d03c-3bc3-9421-
5d3cbb8ac630"]}
```

Response:


```
[
    {
        "sortValues": [
            1556199372946,
            "d47984c3-71d8-36b5-84d4-bb0ec34af828"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.946+0000",
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                       OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                              f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                   Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
```

```
            "userID": "S-1-5-21-122566442-3410611961-
                 1220210811-500"
        },
        "newContent": null,
        "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
        "name": "setupapi.app.log",
        "action": "Attributes",
        "id": "d47984c3-71d8-36b5-84d4-bb0ec34af828",
        "asset": {
            "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
            "interfaces": [
                {
                    "hostname": "MALWARELAB-IOC",
                    "macAddress": "00:50:56:AA:6B:B8",
                    "address": "10.115.77.190",
                    "interfaceName": "Intel(R) PRO/1000 MT
                       Network Connection"
                }
            ],
            "lastCheckedIn": "2019-04-25T13:51:48.000Z",
            "created": "2018-11-01T04:58:21.000+0000",
            "hostId": "290890",
          "operatingSystem": "Microsoft Windows 7 Professional
            6.1.7601 Service Pack 1 Build 7601",
            "tags": [
                "7650412",
                "7655820",
                "7895614"
            ],
            "assetType": "HOST",
            "system": {
                "lastBoot": "2019-03-13T21:49:47.500Z"
            },
            "ec2": null,
            "lastLoggedOnUser": ".\\Administrator",
            "netbiosName": "MALWARELAB-IOC",
            "name": "MALWARELAB-IOC",
            "agentVersion": "3.0.0.101",
            "updated": "2019-04-25T13:51:48.729+0000"
        },
        "class": "Disk"
    }
},
{
    "sortValues": [
```

```
            1556199372946,
            "0ac9f186-6787-339f-a768-929b39da6725"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.946+0000",
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                       OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                              f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                   Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
                "userID": "S-1-5-21-122566442-3410611961-
                     1220210811-500"
            },
            "newContent": null,
            "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
```

```
            "name": "setupapi.app.log",
            "action": "Attributes",
            "id": "0ac9f186-6787-339f-a768-929b39da6725",
            "asset": {
                "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
                "interfaces": [
                    {
                        "hostname": "MALWARELAB-IOC",
                        "macAddress": "00:50:56:AA:6B:B8",
                        "address": "10.115.77.190",
                        "interfaceName": "Intel(R) PRO/1000 MT
                          Network Connection"
                    }
                ],
                "lastCheckedIn": "2019-04-25T13:51:48.000Z",
                "created": "2018-11-01T04:58:21.000+0000",
                "hostId": "290890",
              "operatingSystem": "Microsoft Windows 7 Professional
               6.1.7601 Service Pack 1 Build 7601",
                "tags": [
                    "7650412",
                    "7655820",
                    "7895614"
                ],
                "assetType": "HOST",
                "system": {
                    "lastBoot": "2019-03-13T21:49:47.500Z"
                },
                "ec2": null,
                "lastLoggedOnUser": ".\\Administrator",
                "netbiosName": "MALWARELAB-IOC",
                "name": "MALWARELAB-IOC",
                "agentVersion": "3.0.0.101",
                "updated": "2019-04-25T13:51:48.729+0000"
            },
            "class": "Disk"
        }
    },
    {
        "sortValues": [
            1556199372943,
            "eea0d64e-31ca-3269-91ed-cfb1112fbf17"
        ],
        "data": {
            "dateTime": "2019-04-25T13:36:12.943+0000",
```

```
            "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\inf\\setupapi.app.log",
            "severity": 4,
            "profiles": [
                {
                    "name": "Minimum Baseline for PCI for Windows
                       OS_addTag",
                    "rules": [
                        {
                            "severity": 4,
                            "number": 6,
                            "name": "Rule-6",
                            "description": null,
                            "id": "9287a14c-8036-4403-af88-
                              f98ae8f920fb",
                            "type": "directory"
                        }
                    ],
                    "id": "03dc1773-ae2a-4d5f-a5b3-e662e14afbd2",
                    "type": "WINDOWS",
                    "category": {
                        "name": "PCI",
                      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
                    }
                }
            ],
            "type": "File",
            "changedAttributes": null,
            "platform": "WINDOWS",
            "oldContent": null,
            "actor": {
                "process": "NPFInstall.exe",
                "processID": 8632,
                "imagePath": "\\Device\\HarddiskVolume2\\Program
                    Files\\Npcap\\NPFInstall.exe",
                "userName": "MALWARELAB-IOC\\Administrator",
                "userID": "S-1-5-21-122566442-3410611961-
                    1220210811-500"
            },
            "newContent": null,
            "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
            "name": "setupapi.app.log",
            "action": "Attributes",
            "id": "eea0d64e-31ca-3269-91ed-cfb1112fbf17",
            "asset": {
                "agentId": "f2a0a778-e5b6-4486-826d-a16762588a2a",
```

```
                "interfaces": [
                    {
                        "hostname": "MALWARELAB-IOC",
                        "macAddress": "00:50:56:AA:6B:B8",
                        "address": "10.115.77.190",
                        "interfaceName": "Intel(R) PRO/1000 MT
                          Network Connection"
                    }
                ],
                "lastCheckedIn": "2019-04-25T13:51:48.000Z",
                "created": "2018-11-01T04:58:21.000+0000",
                "hostId": "290890",
              "operatingSystem": "Microsoft Windows 7 Professional
                6.1.7601 Service Pack 1 Build 7601",
                "tags": [
                    "7650412",
                    "7655820",
                    "7895614"
                ],
                "assetType": "HOST",
                "system": {
                    "lastBoot": "2019-03-13T21:49:47.500Z"
                },
                "ec2": null,
                "lastLoggedOnUser": ".\\Administrator",
                "netbiosName": "MALWARELAB-IOC",
                "name": "MALWARELAB-IOC",
                "agentVersion": "3.0.0.101",
                "updated": "2019-04-25T13:51:48.729+0000"
            },
            "class": "Disk"
        }
    },
...
]
```

Chapter 2 - FIM Events API

Use these API functions to fetch FIM event data.

Fetch events

/fim/v2/events/search

[POST]

Get FIM events from the user account.

Input Parameters

filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] AND action: 'Create' Note: For dateTime filter start date should not be lower than 2017-01-01.
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
incidentContext (Boolean)	Search within incidents. Default is false.
incidentIds (String)	List of incident IDs to be included while searching for events in incidents.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"pageSize":100,
"filter":"profiles.name: Windows Profile - PCI(NJJ)"
}
```

Response:


```
[
  {
    "sortValues": [],
    "data": {
      "dateTime": "2018-04-25T17:33:29.806+0000",
      "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\System32\\config\\systemprofi
le\\ntuser.dat",
      "severity": 4,
      "profiles": [
        {
          "name": "Windows Profile - PCI(NJJ)",
          "rules": [
            {
              "severity": 4,
              "description": null,
              "id": "d6eb7f77-3726-47b3-90d8-3ecc8d8978e0",
              "type": "directory"
            }
          ],
          "id": "1c3b44f4-fd76-4c4d-8a4e-bebdad5fa124",
          "type": "WINDOWS",
          "category": null
        }
      ],
      "type": "File",
      "changedAttributes": [
        2,
        4,
        8,
        16
      ],
      "platform": "WINDOWS",
      "oldContent": null,
      "actor": {
        "process": "QualysAgent.exe",
        "processID": 11280,
        "imagePath": "\\Device\\HarddiskVolume2\\Program
```

```
Files\\Qualys\\QualysAgent\\QualysAgent.exe",
        "userName": "NT AUTHORITY\\SYSTEM",
        "userID": "S-1-5-18"
      },
      "newContent": null,
      "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
      "name": "ntuser.dat",
      "action": "Attributes",
      "id": "af8b4ba2-d773-307a-834b-415e6b28d31f",
      "asset": {
        "agentId": "04b3dd30-e731-4d0d-a921-20b6b2d2997c",
        "interfaces": [
          {
            "hostname": "CAAUTOMATION-PC",
            "macAddress": "00:50:56:9F:FF:54",
            "address": "10.113.197.104",
            "interfaceName": "Intel(R) PRO/1000 MT Network
Connection"
          }
        ],
        "lastCheckedIn": "2018-04-26T05:52:19.000Z",
        "created": 1523941162000,
        "hostId": null,
        "operatingSystem": "Microsoft Windows 7 Professional
6.1.7601 Service Pack 1 Build 7601",
        "tags": [
          "7650412",
          "7655820",
          "7895614"
        ],
        "assetType": "HOST",
        "system": {
          "lastBoot": "2018-01-15T12:37:35.000Z"
        },
        "ec2": null,
        "lastLoggedOnUser": ".\\Administrator",
        "netbiosName": "CAAUTOMATION-PC",
        "name": "CAAUTOMATION-PC",
        "agentVersion": "2.0.6.1",
        "updated": 1524721941789
      },
      "class": "Disk"
    }
  }
]
```

Get event count

/fim/v2/events/count

[POST]

Get number of FIM events logged.

Input Parameters

filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] AND action: 'Content' Note: For dateTime filter start date should not be lower than 2017-01-01.
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]
interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d An interval lower than a second is not supported. Note: Value for each interval period should be 1. For example, you can specify an interval of 1y, 1M, 1w, and so on, but not 2y, 3M, etc.
incidentContext (Boolean)	Search within incidents. Default is false.
incidentIds (String)	List of incident IDs to be included while searching for events in incidents.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/count -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"groupBy":["profiles.rules.type","profiles.rules.severity","profil
es.rules.id"]
}
```

Response:


```
{
  "directory": {
    "1": {
      "290f7715-125b-4514-817b-7974444ac59d": 8548,
      "25e681d0-522b-4a2c-b0e6-86b25b47f77f": 7699,
      "611c3a90-1ad5-4b5b-ad88-9edd62182031": 7699,
      "3e447775-418a-424c-8279-5567a89cf811": 1455,
      "d82d238e-53a3-49b8-8e5b-a5e3244e4f07": 474,
      "ae25c204-a184-4c71-b7df-b1267692666a": 238,
      "9c10eaaf-8725-426b-8eb8-793364269b6c": 33,
      "61993871-66cb-4966-a3ab-9b3ec6066858": 1
    },
    "2": {
      "df74b8e2-704b-419e-818e-3c7f4e4a2838": 49274,
      "c9a0d542-2d00-4a34-8ffd-b07a4826739a": 49274,
      "9ca5cb5e-f638-4c9f-b007-fa2a37e1fc49": 37664,
      "828d233b-5958-4867-bb8f-8514afd0a697": 12976,
      "8bf9c8c6-03a7-44be-9f4b-fb52ca0b14a4": 1652,
      "9e923f5d-85b1-42eb-beba-2021e56609af": 698,
      "838a1bd0-910b-467a-88d0-ab5fa7ac9ba6": 28,
      "0a514a18-6ee0-47c1-98da-071a5c0b3dd6": 28,
      "df742229-0abd-4038-b39c-1e99b4c97273": 26,
      "69482025-4b82-4c68-8e36-16ddd4cfbe69": 14
    },
    "3": {
      "e8b4dc7b-3450-4cb2-a265-2d49534a7c62": 1760,
      "b7518092-541a-432e-81d6-8bdba04eead4": 1277,
      "94963cf2-e01d-44da-a320-9ce6b832670f": 942,
      "9bed868e-750c-4b5b-841a-5827d4d2186a": 395,
      "158a1aad-bd57-4a35-8fee-937181bce082": 364,
      "9d9ce724-a0ba-42f0-9305-1019d57b9024": 296,
      "c996ebc2-2915-4ef3-a518-bfbabac16e03": 239,
      "c9a0d542-2d00-4a34-8ffd-b07a4826739a": 49,
      "df742229-0abd-4038-b39c-1e99b4c97273": 26,
      "df74b8e2-704b-419e-818e-3c7f4e4a2838": 26
    },
    "4": {
      "29724aad-2279-4664-bf1e-a4e5cdf458f8": 8912801,
```

```
      "37118a46-f57f-4db4-8f90-b3ddd9d27796": 214872,
      "9287a14c-8036-4403-af88-f98ae8f920fb": 79785,
      "04aebb37-c9b1-4b19-a6e0-aefe1035bbeb": 63629,
      "e75ceb46-5d15-4562-9825-13a9378722b8": 55542,
      "67988adf-9af9-4623-8a92-097e46dadcec": 28026,
      "881e9489-2c12-4182-a790-4d40808ac2ad": 24935,
      "7af95303-9cf8-477b-980c-1dc52003ae28": 24387,
      "304501ca-f8a6-4190-a752-2fbf21c0613b": 22169,
      "939cd6a9-f651-4a2e-aa9d-395afab04592": 19797
    },
    "5": {
      "97e14351-ba9e-4af3-bca9-643c3d7c3410": 493263,
      "fecc66e3-bb79-460e-8b26-11dd82799e14": 136166,
      "3c167cbb-ef59-43ce-8a38-95ccc6a9d93e": 109226,
      "c9a0d542-2d00-4a34-8ffd-b07a4826739a": 49283,
      "df74b8e2-704b-419e-818e-3c7f4e4a2838": 49274,
      "9ca5cb5e-f638-4c9f-b007-fa2a37e1fc49": 37664,
      "1bdb2e8b-3de0-4ec5-9d7a-dc1926919612": 29212,
      "f7c18f88-f94e-4060-a7ef-7475f47af9a5": 19651,
      "637df747-9b6e-43e3-a4ac-d3c50277ba38": 17145,
      "f8d2340e-7efb-4cb9-8273-edeb4403f7c6": 16584
    }
  },
  "file": {
    "1": {
      "ae25c204-a184-4c71-b7df-b1267692666a": 14,
      "57fd59b2-c0ca-47bb-96b2-9cd0119e33bb": 14
    },
    "3": {
      "57fd59b2-c0ca-47bb-96b2-9cd0119e33bb": 2,
      "9ad7a143-b2e4-440f-be68-26042c0f8e3f": 2,
      "ae25c204-a184-4c71-b7df-b1267692666a": 2,
      "80bda0f3-a37b-40c3-af41-ed51eb70da7e": 1
    },
    "4": {
      "80bda0f3-a37b-40c3-af41-ed51eb70da7e": 145,
      "fe0b4a7e-cbb0-4589-9d2e-0867afbf1d4f": 144,
      "1a087a1d-001a-49a2-91c8-ac7127eced84": 3,
      "9ad7a143-b2e4-440f-be68-26042c0f8e3f": 1
    },
    "5": {
      "fe0b4a7e-cbb0-4589-9d2e-0867afbf1d4f": 144,
      "80bda0f3-a37b-40c3-af41-ed51eb70da7e": 144,
      "8be4e5fd-cf77-4ca6-a7a7-3ada1c15067a": 19,
      "57fd59b2-c0ca-47bb-96b2-9cd0119e33bb": 17,
```

```
        "ae25c204-a184-4c71-b7df-b1267692666a": 16,
        "f21d22c0-6954-4b71-ab6e-7c8d5b673d2f": 1,
        "d12c2959-c695-418f-8706-6a9a0eca7bc0": 1,
        "ec356ca7-9800-4e28-8491-4deb29be14ce": 1
      }
    }
  }
```

Fetch event details

/fim/v2/events/{eventId}

[GET]

Fetch details for an event.

Input Parameters

eventId (String)	(Required) ID of the event you want to fetch the details for.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X GET
https://gateway.qg1.apps.qualys.com/fim/v2/events/af8b4ba2-d773-
307a-834b-415e6b28d31f -H 'authorization: Bearer <token>' -H
'content-type: application/json'
```

Response:

```
{
  "dateTime": "2018-04-25T17:33:29.806+0000",
  "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\System32\\config\\systemprofi
le\\ntuser.dat",
  "severity": 4,
  "profiles": [
    {
      "name": "Windows Profile - PCI(NJJ)",
      "rules": [
        {
          "severity": 4,
          "description": null,
          "id": "d6eb7f77-3726-47b3-90d8-3ecc8d8978e0",
```

```
          "type": "directory"
        }
      ],
      "id": "1c3b44f4-fd76-4c4d-8a4e-bebdad5fa124",
      "type": "WINDOWS",
      "category": null
    }
  ],
  "type": "File",
  "changedAttributes": [
    2,
    4,
    8,
    16
  ],
  "platform": "WINDOWS",
  "oldContent": null,
  "actor": {
    "process": "QualysAgent.exe",
    "processID": 11280,
    "imagePath": "\\Device\\HarddiskVolume2\\Program
Files\\Qualys\\QualysAgent\\QualysAgent.exe",
    "userName": "NT AUTHORITY\\SYSTEM",
    "userID": "S-1-5-18"
  },
  "newContent": null,
  "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
  "name": "ntuser.dat",
  "action": "Attributes",
  "attributes": {
    "old": null,
    "new": [
      "Archive"
    ]
  },
  "id": "af8b4ba2-d773-307a-834b-415e6b28d31f",
  "asset": {
    "agentId": "04b3dd30-e731-4d0d-a921-20b6b2d2997c",
    "interfaces": [
      {
        "hostname": "CAAUTOMATION-PC",
        "macAddress": "00:50:56:9F:FF:54",
        "address": "10.113.197.104",
        "interfaceName": "Intel(R) PRO/1000 MT Network Connection"
      }
    ],
```

```
    "lastCheckedIn": "2018-04-26T05:52:19.000Z",
    "created": 1523941162000,
    "hostId": null,
    "operatingSystem": "Microsoft Windows 7 Professional 6.1.7601
Service Pack 1 Build 7601",
    "tags": [
      "7650412",
      "7655820",
      "7895614"
    ],
    "assetType": "HOST",
    "system": {
      "lastBoot": "2018-01-15T12:37:35.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
    "netbiosName": "CAAUTOMATION-PC",
    "name": "CAAUTOMATION-PC",
    "agentVersion": "2.0.6.1",
    "updated": 1524721941789
  },
  "class": "Disk"
}
```

Chapter 3 - Ignored FIM Events API

Use these API functions to fetch FIM event data for ignored events.

Fetch ignored events

/fim/v2/events/ignore/search

[POST]

Get FIM events that are ignored.

Input Parameters

filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] Note: For dateTime filter start date should not be lower than 2017-01-01.
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/ignore/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"pageSize":1,
```

```
"filter":"dateTime:['2018-06-25T18:30:00.000Z'..'2019-02-
20T18:29:59.999Z']"
}
```

Response:


```
[
  {
    "sortValues": [],
    "data": {
      "dateTime": "2018-07-12T15:19:33.704+0000",
      "fullPath":
"\\Device\\HarddiskVolume2\\FIM\\MobaXterm_installer.msi",
      "severity": 5,
      "profiles": [
        {
          "name": "Bug_Test_1",
          "rules": [
            {
              "severity": 2,
              "description": "",
              "id": "df74b8e2-704b-419e-818e-3c7f4e4a2838",
              "type": "directory"
            }
          ],
          "id": "a0f61a71-fc03-4d9e-a234-fb39afa35d66",
          "type": "WINDOWS",
          "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
          }
        },
        {
          "name": "Bug_Test_Profile",
          "rules": [
            {
              "severity": 5,
              "description": "",
              "id": "c9a0d542-2d00-4a34-8ffd-b07a4826739a",
              "type": "directory"
            }
          ],
          "id": "f214c35a-441e-450a-b817-2f162add6854",
          "type": "WINDOWS",
          "category": {
            "name": "PCI",
```

```
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
          }
        }
      ],
      "type": "File",
      "changedAttributes": null,
      "platform": "WINDOWS",
      "oldContent": null,
      "actor": {
        "process": "Explorer.EXE",
        "processID": 312,
        "imagePath":
"\\Device\\HarddiskVolume2\\Windows\\Explorer.EXE",
        "userName": "CAAUTOMATION-PC\\Administrator",
        "userID": "S-1-5-21-3436480518-4193688097-2835352598-500"
      },
      "newContent": null,
      "ignoreDate": "2018-07-24",
      "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
      "name": "MobaXterm_installer.msi",
      "action": "Delete",
      "id": "c6d7929c-85cb-3791-b6ed-2bcd9a7682cb",
      "asset": {
        "agentId": "fe94430f-f12c-4c6d-a9c2-a660049d69e5",
        "interfaces": [
          {
            "hostname": "CAAUTOMATION-PC",
            "macAddress": "00:50:56:9F:FF:54",
            "address": "10.113.197.104",
            "interfaceName": "Intel(R) PRO/1000 MT Network
Connection"
          }
        ],
        "lastCheckedIn": "2018-07-12T15:07:23.000Z",
        "created": 1531195694000,
        "hostId": null,
        "operatingSystem": "Microsoft Windows 7 Professional
6.1.7601 Service Pack 1 Build 7601",
        "tags": [
          "8072536",
          "7895614",
          "7655820",
          "7650412"
        ],
        "assetType": "HOST",
        "system": {
```

```
            "lastBoot": "2018-06-14T16:29:03.000Z"
          },
          "ec2": null,
          "lastLoggedOnUser": ".\\Administrator",
          "netbiosName": "CAAUTOMATION-PC",
          "name": "IOC-104",
          "agentVersion": "2.0.6.1",
          "updated": 1531408044017
        },
        "class": "Disk"
      }
    }
  ]
```


Get ignored events count

/fim/v2/events/ignore/count

[POST]

Get number of ignored events logged.

Input Parameters

filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] AND action: 'Content' Note: For dateTime filter start date should not be lower than 2017-01-01.
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]

interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d An interval lower than a second is not supported. Note: Value for each interval period should be 1. For example, you can specify an interval of 1y, 1M, 1w, and so on, but not 2y, 3M, etc.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/events/ignore/count -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"filter":"dateTime:['2018-06-25T18:30:00.000Z'..'2019-06-
20T18:29:59.999Z']"
}
```

Response:

```
{
  "count":234
}
```

Fetch ignored event details

/fim/v2/events/ignore/{ignoredEventId}

[GET]

Fetch details for an ignored event.

Input Parameters

eventId (String)	(Required) ID of the ignored event you want to fetch the details for.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X GET
https://gateway.qg1.apps.qualys.com/fim/v2/events/ignore/f214c35a-
441e-450a-b817-2f162add6854 -H 'authorization: Bearer <token>' -H
'content-type: application/json'
```

Response:


```
{
  "dateTime": "2018-06-19T07:09:07.116+0000",
  "fullPath": "\\Device\\HarddiskVolume2\\FIM\\ProdCerts",
  "severity": 3,
  "profiles": [
    {
      "name": "Bug_Test_Profile",
      "rules": [
        {
          "severity": 3,
          "description": "",
          "id": "c9a0d542-2d00-4a34-8ffd-b07a4826739a",
          "type": "directory"
        }
      ],
      "id": "f214c35a-441e-450a-b817-2f162add6854",
      "type": "WINDOWS",
      "category": {
        "name": "PCI",
        "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
      }
    }
```

```
  ],
  "type": "Directory",
  "changedAttributes": null,
  "platform": "WINDOWS",
  "oldContent": null,
  "actor": {
    "process": "Explorer.EXE",
    "processID": 312,
    "imagePath":
"\\Device\\HarddiskVolume2\\Windows\\Explorer.EXE",
    "userName": "CAAUTOMATION-PC\\Administrator",
    "userID": "S-1-5-21-3436480518-4193688097-2835352598-500"
  },
  "newContent": null,
  "ignoreDate": "2018-06-19",
  "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
  "name": "ProdCerts",
  "action": "Delete",
  "id": "5ca3af2b-991d-3154-acce-6ebbad2a6cc1",
  "asset": {
    "agentId": "b1362e7f-a29c-4226-a9a2-f91747f7e009",
    "interfaces": [
      {
        "hostname": "CAAUTOMATION-PC",
        "macAddress": "00:50:56:9F:FF:54",
        "address": "10.113.197.104",
        "interfaceName": "Intel(R) PRO/1000 MT Network Connection"
      }
    ],
    "lastCheckedIn": "2018-06-19T07:02:08.000Z",
    "created": 1529071987000,
    "hostId": null,
    "operatingSystem": "Microsoft Windows 7 Professional 6.1.7601
Service Pack 1 Build 7601",
    "tags": [
      "7895614",
      "7655820",
      "7650412",
      "8072536"
    ],
    "assetType": "HOST",
    "system": {
      "lastBoot": "2018-06-14T16:29:03.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
```

```
    "netbiosName": "CAAUTOMATION-PC",
    "name": "CAAUTOMATION-PC",
    "agentVersion": "2.0.6.1",
    "updated": 1529391745750
  },
  "class": "Disk"
}
```

Chapter 4 - FIM Incidents API

Use these API functions to fetch FIM incident data.

Fetch incidents

/fim/v2/incidents/search

[POST]

Get FIM incidents for an user account.

Input Parameters

filter (String)	Filter the incidents list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - action: 'Content'
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
attributes (String)	Search based on certain attributes (provide comma separated list).
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/incidents/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
 "filter":"status:OPEN",
 "pageSize":10,
 "pageNumber":2
}
```

Response:

```
[
  {
    "approvalStatus": null,
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554705662981
    },
    "filterToDate": "2019-04-08T04:40:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime : ['2019-04-04T10:10:00' .. '2019-04-08T10:10:00']
and action:Create",
      "actor.processID=0"
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
    "filterFromDate": "2019-04-04T04:40:00.000+0000",
    "createdBy": {
      "date": 1554705662981
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "new Incident-pod01_rule_15",
    "comment": null,
    "dispositionCategory": null,
    "id": "2fce3272-41ed-43a1-8224-0cacb3b72b1a",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554708253311
```

```
    },
    "filterToDate": "2019-04-08T12:10:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime : ['2019-04-08T17:40:00' .. '2019-04-08T17:40:00']
and action:Create",
      "actor.processID=0"
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
    "filterFromDate": "2019-04-08T12:10:00.000+0000",
    "createdBy": {
      "date": 1554708253311
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "new Incident-pod01_rule_14",
    "comment": null,
    "dispositionCategory": null,
    "id": "37013195-4c12-46d4-9eb6-0663050582f1",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554727110924
    },
    "filterToDate": "2019-04-08T05:50:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime: ['2019-04-08T01:01:00.000Z'..'2019-04-
08T05:50:00.000Z'] and action:Create and
actor.process:\"svchost.exe\""
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
```

```
    "filterFromDate": "2019-04-08T01:01:00.000+0000",
    "createdBy": {
      "date": 1554727110924
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Incident-aa85ac30-ce17-4370-ba1d-7471d8a0fa35-
pod01_rule_29",
    "comment": null,
    "dispositionCategory": null,
    "id": "85eb37a0-0b64-45de-95b9-668eaa58eca8",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554727339894
    },
    "filterToDate": "2019-04-08T09:30:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime: ['2019-04-08T09:30:00.000Z'..'2019-04-
08T09:30:00.000Z'] and action:Create and
actor.process:\"svchost.exe\""
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
    "filterFromDate": "2019-04-08T09:30:00.000+0000",
    "createdBy": {
      "date": 1554727339894
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Incident-edda32e6-f8cc-4961-a4ea-90c4e9d967d7-
pod01_rule_26",
    "comment": null,
    "dispositionCategory": null,
    "id": "cde0ae52-e49c-4c62-8264-3400f7f1b591",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
```

```
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554784098839
    },
    "filterToDate": "2019-04-09T17:30:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime: ['2019-04-09T01:00:00.000Z'..'2019-04-
09T17:30:00.000Z'] and actor.process:\"svchost.exe\""
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
    "filterFromDate": "2019-04-09T01:00:00.000+0000",
    "createdBy": {
      "date": 1554784098839
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Incident-a170f7bf-e74d-41bc-bb76-0ddbed938794-
pod01_rule_21",
    "comment": null,
    "dispositionCategory": null,
    "id": "1f995877-6123-4308-ae71-7086a597972e",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": true,
    "lastUpdatedBy": {
      "date": 1537879192143
    },
    "filterToDate": "2018-04-10T05:33:34.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": "COMPLETED",
    "filters": [
      "dateTime : ['2018-04-01T05:33:34' .. '2018-04-10T05:33:34']
and action : Security"
    ],
    "type": "DEFAULT",
```

```
    "reviewers": [],
    "deleted": false,
    "filterFromDate": "2018-04-01T05:33:34.000+0000",
    "createdBy": {
      "date": 1537879192143
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Auto_Incident_${timestampseconds}",
    "comme100  7157    0  7091  100    66   4282     39  0:00:01
0:00:01 --:--:--  4321atus": null,
    "comment": null,
    "dispositionCategory": null,
    "id": "6fcdd288-1c91-46c4-b119-7f9d19fa79c8",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": true,
    "lastUpdatedBy": {
      "date": 1548756063438,
      "user": {
        "name": "FIM Tester",
        "id": "70ad9ad4-8728-d7df-8092-980c303de8e0"
      }
    },
    "filterToDate": "2018-02-04T16:31:00.000+0000",
    "approvalDate": null,
    "assignDate": "2018-10-17T11:05:52.562+0000",
    "changeType": "MANUAL",
    "approvalType": "MANUAL",
    "markupStatus": "COMPLETED",
    "filters": [
      "dateTime : ['2018-01-01T16:30:00' .. '2018-02-04T16:31:00']
and action:Create"
    ],
    "type": "DEFAULT",
    "reviewers": [
      "quays_ap10"
    ],
    "deleted": false,
    "filterFromDate": "2018-01-01T16:30:00.000+0000",
    "createdBy": {
      "date": 1539774352558,
      "user": {
        "name": "FIM Tester",
        "id": "70ad9ad4-8728-d7df-8092-980c303de8e0"
```

```
      }
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Auto_Incident_1539774352",
    "comment": null,
    "dispositionCategory": null,
    "id": "bfba6647-2849-403e-bf91-95d8ff492c79",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": false,
    "lastUpdatedBy": {
      "date": 1554713282992
    },
    "filterToDate": "2019-04-08T12:10:00.000+0000",
    "approvalDate": null,
    "assignDate": null,
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": null,
    "filters": [
      "dateTime : ['2019-04-08T17:40:00' .. '2019-04-08T17:40:00']
and action:Create",
      "actor.processID=0"
    ],
    "type": "DEFAULT",
    "reviewers": null,
    "deleted": false,
    "filterFromDate": "2019-04-08T12:10:00.000+0000",
    "createdBy": {
      "date": 1554713282992
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "Incident-d353f6bc-11d8-480e-a26a-3fb3a4324689-
pod01_rule_14",
    "comment": null,
    "dispositionCategory": null,
    "id": "7556fce9-a928-43b4-9724-1849f0650db1",
    "status": "OPEN"
  },
  {
    "approvalStatus": null,
    "marked": true,
    "lastUpdatedBy": {
      "date": 1557127498543,
```

```
      "user": {
        "name": "FIM Tester",
        "id": "70ad9ad4-8728-d7df-8092-980c303de8e0"
      }
    },
    "filterToDate": "2019-05-06T18:29:59.999+0000",
    "approvalDate": null,
    "assignDate": "2019-05-06T07:24:58.544+0000",
    "changeType": null,
    "approvalType": "MANUAL",
    "markupStatus": "COMPLETED",
    "filters": [
      "dateTime: ['2019-04-05T18:30:00.000Z'..'2019-05-
06T18:29:59.999Z'] and action:Create and severity:2"
    ],
    "type": "DEFAULT",
    "reviewers": [
      "quays_ft"
    ],
    "deleted": false,
    "filterFromDate": "2019-04-05T18:30:00.000+0000",
    "createdBy": {
      "date": 1557127498543,
      "user": {
        "name": "FIM Tester",
        "id": "70ad9ad4-8728-d7df-8092-980c303de8e0"
      }
    },
    "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
    "name": "create_sev2",
    "comment": null,
    "dispositionCategory": null,
    "id": "7682e33c-f8bb-4129-88fb-1528ad0f87b7",
    "status": "OPEN"
  }
]
```

Fetch events for an incident

/fim/v2/incidents/{incidentId}/events/search

[POST]

Get events logged under an incident.

Input Parameters

incidentId (String)	(Required) ID of the incident you want to fetch the events for.
filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query. For example - action: 'Content'
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
attributes (String)	Search based on certain attributes (provide comma separated list).
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/incidents/{incidentId}/
events/search -H 'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"sort":"[{\"name\":\"desc\"}]",
"pageNumber":2,
"attributes":"name"
}
```

Response:

```
[
  {
    "sortValues": [
      "x86_microsoft-windows-t..icesframework-
```

```
msctf_31bf3856ad364e35_6.1.7601.23915_none_78558f3c6624167c"
    ],
    "data": {
      "name": "x86_microsoft-windows-t..icesframework-
msctf_31bf3856ad364e35_6.1.7601.23915_none_78558f3c6624167c",
      "id": "8b340728-411a-37d1-a028-0aae41362f1e"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69"
    ],
    "data": {
      "name": "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69",
      "id": "6f5878be-3abe-32b7-a943-d9b6c982190f"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69"
    ],
    "data": {
      "name": "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69",
      "id": "c9f2dea8-a14c-34e8-b2dc-a20d282bee73"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69"
    ],
    "data": {
      "name": "x86_microsoft-windows-t..-collaboration-
core_31bf3856ad364e35_6.1.7601.23892_none_bd47535b6dcd4b69",
      "id": "87d0d9b7-0518-3974-86c3-f48712323147"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-
shdocvw_31bf3856ad364e35_6.1.7601.23896_none_e9b14bab8385266b"
    ],
```

```
    "data": {
      "name": "x86_microsoft-windows-
shdocvw_31bf3856ad364e35_6.1.7601.23896_none_e9b14bab8385266b",
      "id": "3e68b55b-eff3-35ab-9c7f-95ad3be33c34"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-
shdocvw_31bf3856ad364e35_6.1.7601.23896_none_e9b14bab8385266b"
    ],
    "data": {
      "name": "x86_microsoft-windows-
shdocvw_31bf3856ad364e35_6.1.7601.23896_none_e9b14bab8385266b",
      "id": "e5bd74f2-03b9-301d-ba96-34b3d8a6bd7c"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e"
    ],
    "data": {
      "name": "x86_microsoft-windows-
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e",
      "id": "ea9e8bc7-1895-34fc-b2a7-f6c42be0ed0a"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e"
    ],
    "data": {
      "name": "x86_microsoft-windows-
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e",
      "id": "a5d68c5e-5f9e-3cc5-976f-8331e4404a73"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-
```

```
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e"
    ],
    "data": {
      "name": "x86_microsoft-windows-
shdocvw.resources_31bf3856ad364e35_6.1.7601.23896_en-
us_c9ff1fadd1da973e",
      "id": "452af9e5-c926-39a5-8a7d-e6b25a43a828"
    }
  },
  {
    "sortValues": [
      "x86_microsoft-windows-security-
credssp_31bf3856ad364e35_6.1.7601.23915_none_c64a109218ef01b4"
    ],
    "data": {
      "name": "x86_microsoft-windows-security-
credssp_31bf3856ad364e35_6.1.7601.23915_none_c64a109218ef01b4",
      "id": "249e4bdf-aad5-3ddd-bbbf-03f45eecd137"
    }
  }
]
```

Get event count for an incident

/fim/v2/incidents/{incidentId}/events/count

[POST]

Get number of events logged for an incident.

Input Parameters

incidentId (String)	(Required) ID of the incident you want to fetch the events for.
filter (String)	Filter the incidents list by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query. For example - action: 'Content'
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]
interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d An interval lower than a second is not supported. Note: Value for each interval period should be 1. For example, you can specify an interval of 1y, 1M, 1w, and so on, but not 2y, 3M, etc.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/incidents/{incidentId}/
events/count -H 'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"groupBy":["action","dateTime"],
"limit":2
}
```

Response:

```
{
  "Delete": {
    "2019-01-01T00:00:00.000Z": 1551
  },
  "Attributes": {
    "2019-01-01T00:00:00.000Z": 1159
  }
}
```

Get incident count

/fim/v2/incidents/count

[POST]

Get number of incidents in an user account.

Input Parameters

filter (String)	Filter the incidents list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - action: 'Content'
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]
interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d An interval lower than a second is not supported. Note: Value for each interval period should be 1. For example, you can specify an interval of 1y, 1M, 1w, and so on, but not 2y, 3M, etc.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -X POST
https://gateway.qg1.apps.qualys.com/fim/v2/incidents/count -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
"filter":"status:OPEN",
"groupBy":["approvalType","name","id"]
}
```

Response:


```
{
  "MANUAL": {
    "Incident-3a899bb5-493e-40b8-a348-408dee7b2314-pod01_rule_15":
{
      "af72cee0-3dd7-4173-b6ff-c0dfd1ad0465": 1,
      "70da4a11-35df-40a2-b20d-9878389d63d9": 1,
      "435d4e5b-753e-455f-bc64-7ebbdab38cad": 1
    },
    "Incident-4b5c6f12-a3dc-48d3-b9f5-be01d35449e7-pod01_rule_16":
{
      "689ea586-5c41-462e-b9f9-41635fa71889": 1,
      "b9760652-e642-43e3-a1bc-27441bd590c8": 1,
      "56660ef6-a0ed-447e-8738-4d2b26f44026": 1
    },
    "Incident-d353f6bc-11d8-480e-a26a-3fb3a4324689-pod01_rule_14":
{
      "d31f45da-f3b2-4a91-a84a-36992966c6ec": 1,
      "7556fce9-a928-43b4-9724-1849f0650db1": 1,
      "45630e02-bbee-44a8-9b89-966b95ef62a3": 1
    },
    "Incident-aa85ac30-ce17-4370-ba1d-7471d8a0fa35-pod01_rule_29":
{
      "e24ec4e4-87e1-49dd-b3ed-91959673da32": 1,
      "85eb37a0-0b64-45de-95b9-668eaa58eca8": 1
    },
    "Incident-47a9fce9-2b4c-4d2a-ab84-9853a41225d7-pod01_rule_27":
{
      "7f41087e-2d1d-4514-806f-d51fd78e312c": 1,
      "e913313d-eda2-4c4d-9550-32cae546f4b7": 1
    },
    "Incident-f534db2b-d4fa-43cb-a550-c2cce44e02f4-pod01_rule_25":
```

```
{
      "3907d4bd-3755-4191-89c3-d6f4e31fcd6e": 1,
      "f29cb285-e2a0-434e-9240-63b00bd420df": 1
    },
   "Incident-70060303-29a1-47b7-bd7a-17409cf1049b-pod01_rule_33":
{
      "b8b89269-f82d-4e08-bed5-607540930baa": 1,
      "ae70ad1b-f841-4ad9-9a92-49a481dd0383": 1
    },
   "Incident-84e3c230-5ce9-49bd-9a19-7ab9a63f5f48-pod01_rule_28":
{
      "50f8cfb8-383d-4605-85a8-e85968e6f8ef": 1,
      "3e020d72-c903-4076-bd43-f0a85b3275bf": 1
    },
   "Incident-a170f7bf-e74d-41bc-bb76-0ddbed938794-pod01_rule_21":
{
      "1f995877-6123-4308-ae71-7086a597972e": 1,
      "d20a61d4-9ec0-43ca-b6c1-c7ca93933ed3": 1
    },
   "Incident-f050635e-f1ce-4059-beed-f144b66de3c2-pod01_rule_24":
{
      "0678d417-af29-4ca9-9dc5-6cefacb459c9": 1,
      "65e51413-4802-415c-b8a5-469f7cd5f151": 1
    }
  }
}
```