



File Integrity Monitoring API v2 and v3

User Guide

Version 3.9

January 18, 2024

Copyright 2023-2024 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



Table of Contents

Preface.....	5
About Qualys	5
Contact Qualys Support	5
Welcome	6
Qualys API Framework	6
Qualys API URL	6
Qualys API Postman Collection	7
Introduction to FIM API Paradigm	8
FIM Events API.....	24
Fetch events	24
Get event count	38
Fetch event details	43
Ignored FIM Events API.....	52
Fetch ignored events	52
Get ignored events count	65
Fetch ignored event details	68
FIM Incidents API.....	79
Fetch incident count	80
Fetch incidents	83
Get event count for an incident	85
Fetch events for an incident	88
Create manual incident	95
Approve incidents	97
FIM Alerting API.....	100
Alerting Action API	100
Fetch all Alert Actions	100
Fetch Alert Actions for an Action ID	102
Alerting Rules API	104
Fetch Alert Rules	104
Fetch details for Alert Rule	106
Enable Alert Rule	108
Disable Alert Rule	109
Delete a Alert Rule	110
Alerting Activities API	111
Fetch the generated alerts for FIM	111

Count Number of Alerts Generated for FIM	113
FIM Correlation API.....	114
Fetch all Correlation Rules	115
Fetch Correlation Rule Details for a particular Rule ID	117
Fetch the count of Correlation Rules	119
Create Correlation Rules	121
Update Correlation Rule	124
Activate Correlation Rule	127
Deactivate Correlation Rule	128
Delete Correlation Rule	129
FIM Profile APIs.....	130
Search a Profile	131
Activate a Profile	133
Assign an Asset to a Profile	134
Assign Tags to a Profile	135
Export the Profile in XML Format	136
Export the Profile in JSON Format	140
Import a Profile from XML File Inputs	145
Import a Profile from JSON File Inputs	150
List the Profile Categories	155
Deactivate a Profile	157
Import Profile from CSV	158
Export Profile into CSV	160
Bulk Delete Profiles	161
FIM Assets API.....	162
Search Assets	163
Count the Assets	165

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/.

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.

[Ali g li ol!>i g g ohns](#)

[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.

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

Qualys API 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.

Qualys API Postman Collection

Interact with Qualys APIs using Postman. Instead of creating calls manually to send over the command line, you can use the Qualys Postman Collection to get started with Qualys APIs quickly.

[Click here to view the steps involved](#)

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://<qualys_base_url>/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 is 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://<qualys_base_url>/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 than 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  
/fim/v3/incidents/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://<qualys_base_url>/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-3bc3-9421-5d3ccb8ac630",
"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",
            "type": "Network"
        }
    ]
}
```

```

        "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://<qualys_base_url>/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-
5d3ccb8ac630"]}
```

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": "NPFIInstall.exe",
    "processID": 8632,
    "imagePath": "\Device\HarddiskVolume2\Program
Files\Npcap\NPFIInstall.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": [
        {
            "name": "Intel(R) Dual Band Wireless-AC 7265
PCIe Network Adapter"
        }
    ]
}
```

```
        "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"
}
},
...
]
```

FIM Events API

Use these API functions to fetch FIM event data.

[Fetch events](#)

[Get event count](#)

[Fetch event details](#)

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' You can filter events based on the time they are generated on the asset (dateTIme) or based on the time they are processed at Qualys (processedTime). Note: For the dateTIme filter start date should not be lower than 2017-01-01. The processedTime filter can be used only for events generated post FIM release 2.0.2.
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 1

Request:

```
curl -X POST https://<qualys_base_url>/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\\systemprofile\\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  
            ],  
            "lastModified": "2018-04-25T17:33:29.806+0000",  
            "version": 1  
        }  
    }  
]
```

```
"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"  
}  
}  
]
```

Sample 2

Request:

```
curl -X POST https://<qualys_base_url>/fim/v2/events/search -H  
'authorization: Bearer ' -H 'content-type:  
application/json' -d @request.json
```

Contents of request.json:

```
{  
    "pageSize":100,  
    "filter":"reputationStatus: MALICIOUS"  
}
```

Response:

```
[  
    {  
        "sortValues": [],  
        "data": {  
            "dateTime": "2021-01-25T17:33:29.806+0000",  
            "fullPath":  
                "\\\Device\\\\HarddiskVolume2\\\\Windows\\\\System32\\\\config\\\\systemprofile\\\\Terminator.exe",  
            "severity": 4,  
            "profiles": [  
                {  
                    "name": "Terminator.exe",  
                    "rules": [  
                        {  
                            "severity": 4,  
                            "description": null,  
                            "id": "d6eb7f77-3726-47b3-90d8-3ecc8d8978e9",  
                            "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": "update.exe",
    "processID": 11280,
    "imagePath": "C:\\Windows\\system32\\update.exe",
    "userName": "NT AUTHORITY\\SYSTEM",
    "userID": "S-1-5-18"
  },
  "newContent": null,
  "customerId": "58b888be-a90f-e3be-838d-88877aee572b",
  "name": "ntuser.dat",
  "action": "Create",
  "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 PRO/1000 MT Network Connection"
      }
    ],
    "lastCheckedIn": "2018-04-26T05:52:19.000Z",
    "created": 1523941162000,
    "hostId": null,
    "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A
Build 10586",
    "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",
"fileContentHash":
"50dc26047f5572a38aa7adb4e9b140dc301ea41d1f4bed5095a1ed7fc1d03fbcb",
{
    "reputationStatus": "MALICIOUS",
    "fileCertificateHash": [
        "d12bed1761e1b2c244db23cebe4185c2b0839eee",
        "7ade32c9b68b944bf291d1fcc59faef061a6d2f2"
    ],
    "trustStatus": "UNTRUSTED"
}
}
]
```

Sample 3

Request:

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

Contents of request.json:

```
{
  "pageSize":100,
  "filter":"registryKey.name: Data"
}
```

Response:

```
[
  {
    "sortValues": [],
    "data": {
      "dateTime": "2021-03-05T11:28:36.455+0000",
      "fullPath":
        "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
        NT\\CurrentVersion\\Image File Execution Options\\Data",
      "type": "Value",
      "platform": "WINDOWS",
      "oldContent": null,
      "newContent": null,
      "customerId": "00XXXX-643f-f4af-8336-b253066XXXX",
      "action": "Content",
      "id": "e115XXXX-af72-37b5-8f92-9e878bbbbba53",
      "severity": 3,
      "fileCertificateHash": null,
      "profiles": [
        {
          "name": "Profile Name",
          "rules": [
            {
              "severity": 3,
              "number": 1,
              "name": "Rule 1",
              "description": "Rule 1",
              "section": null,
              "id": "4282XXXX-cc33-49d8-82df-53a00e27XXXX",
              "type": "key"
            }
          ]
        }
      ]
    }
  }
]
```

```
],
  "id": "f99941de-2296-4044-bfca-05aeb4575ef5",
  "type": "WINDOWS",
  "category": {
    "name": "PCI",
    "id": "2dabXXXX-2fdd-11e7-93ae-92361f00XXXX"
  }
}
],
"changedAttributes": null,
"processedTime": "2021-03-05T05:37:30.311+0000",
"actor": {
  "process": "reg.exe",
  "processID": 2811,
  "imagePath": "C:\\Windows\\\\System32\\\\reg.exe",
  "userName": "MSEdgeWIN10\\\\IEUser",
  "userID": "S-1-5-21-3461203602-4096304019-2269080069-1000"
},
"name": null,
"asset": {
  "agentId": "7c99XXXX-92fa-4943-91ab-249e341dd10d",
  "interfaces": [
    {
      "hostname": "WIN10-122.WORKGROUP",
      "macAddress": "00:50:56:AA:5C:85",
      "address": "10.115.98.122",
      "interfaceName": "Intel(R) 82574L Gigabit Network Connection"
    }
  ],
  "lastCheckedIn": "2019-07-23T11:01:00.000Z",
  "created": "2021-01-11T06:40:09.930+0000",
  "hostId": null,
  "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A Build 10586",
  "tags": [
    "7508831",
    "7526815",
    "7593230"
  ],
  "assetType": "HOST",
  "system": {
    "lastBoot": "2019-07-23T11:01:00.000Z"
  },
  "ec2": null,
  "lastLoggedOnUser": ".\\\\Administrator",
}
```

```
"netbiosName": "WIN10-122",
"name": "WIN10-122",
"agentVersion": "3.0.0.101",
"updated": "2021-01-11T06:40:09.930+0000"
},
"fileContentHash": null,
"reputationStatus": null,
"registryPath":
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options",
"registryName": "Data",
"oldRegistryValueType": "REG_MULTI_SZ",
"oldRegistryValueContent": [
    "Multvalue string",
    "Multvalue string"
],
"newRegistryValueType": "REG_MULTI_SZ",
"newRegistryValueContent": [
    "Multvalue string1",
    "Multvalue string2"
],
"class": "Registry"
}
}
]
```

Sample 4:

API Request:

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

Contents of request.json:

```
{  
    "filter": "file.attribute.hidden: `Added`"  
}
```

Response:

```
"fileCertificateHash": null,  
"securitySettings"profiles": [  
    {  
        "name": "CR_All_Machines",  
        "rules": [  
            {  
                "severity": 5,  
                "number": 1,  
                "name": "CR_1",  
                "description": "",  
                "section": null,  
                "id": "59ffbe0d-d27d-428d-9766-  
226ede8ee015",  
                "type": "directory"  
            }  
        ],  
        "id": "0bd18efb-11d5-4a30-8b74-57fca4cdffb4",  
        "type": "WINDOWS",  
        "category": {  
            "name": "PCI",  
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"  
        }  
    }  
],  
"baseline": false,  
"registryName": null,  
"changedAttributes": [  
    2,  
    4,  
    8,  
    16  
],  
"processedTime": "2023-06-28T06:24:40.947+0000",  
"actor": {  
    "process": "explorer.exe",  
    "auditUserName": null,  
    "auditUserID": null,  
    "processID": 5864,  
    "imagePath": "C:\\WINDOWS\\explorer.exe",  
    "procTitle": null,  
    "userName": "DESKTOP-FR23SL8\\Administrator",  
    "userID": "S-1-5-21-1082135036-1977325707-  
348817062-500"  
},  
"oldRegistryValueContent": null,
```

```

    "newRegistryValueType": null,
    "fileContentHashOld": null,
    "size": null,
    "name": "wmplayer - Copy (4).exe",
    "fileContentHash": null,
    "volumeID": "0xa2121916",
    "reputationStatus": null,
    "newRegistryValueContent": null,
    "attributes": {
        "newAttribute": [
            "Archive",
            "Hidden",
            "Read Only"
        ],
        "oldAttribute": [
            "Archive"
        ]
    },
    "asset": {
        "agentId": "3f8a4d42-1f50-4557-881b-0efcbfff70ac",
        "interfaces": [
            {
                "hostname": "DESKTOP-FR23SL8",
                "macAddress": "00:50:56:AA:75:F0",
                "address": "10.115.138.119",
                "interfaceName": "Intel(R) 82574L Gigabit
Network Connection"
            },
            {
                "hostname": "DESKTOP-FR23SL8",
                "macAddress": "00:50:56:AA:75:F0",
                "address": "fe80:0:0:0:bf92:dce7:bb76:a30d",
                "interfaceName": "Intel(R) 82574L Gigabit
Network Connection"
            }
        ],
        "lastCheckedIn": "2023-06-13T06:28:13.000Z",
        "created": "2023-06-14T10:01:06.060+00:00",
        "hostId": null,
        "operatingSystem": "Windows Microsoft Windows 10 Pro
10.0.19045 Build 19045",
        "tags": [
            "8543820"
        ],
        "assetType": "HOST",
        "system": {

```

```
        "lastBoot": "2023-06-14T15:05:03.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": "qualys",
    "netbiosName": "DESKTOP-FR23SL8",
    "name": "DESKTOP-FR23SL8",
    "agentVersion": "4.9.0.16",
    "updated": "2023-06-14T10:01:06.060+00:00"
},
"incidentId": "a0e6709b-14cc-4750-97c9-b693883adfb6"
}
]
```

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' You can filter events based on the time they are generated on the asset (dateTIme) or based on the time they are processed at Qualys (processedTime). Note: For the dateTIme filter start date should not be lower than 2017-01-01. The processedTime filter can be used only for events generated post FIM release 2.0.2.
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 1:

Request:

```
curl -X POST https://<qualys_base_url>/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-8514af0a697": 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-81d6-8bdb04eed4": 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  
}  
}  
}
```

Sample 2:

API Request:

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

Contents of request.json:

```
{  
  
    "groupBy": ["file.attribute.hidden"]  
}
```

Response:

```
{  
    "Added": 13,  
    "Removed": 3  
}
```

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 1:

Request:

```
curl -X GET https://<qualys_base_url>/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\\\\systemprofile\\\\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"
}
```

Sample 2:

Request:

```
curl -X GET https://<qualys_base_url>/fim/v2/events/f589a105-0100-3dbb-a007-556fae7afea5 -H 'authorization: Bearer ' -H 'content-type: application/json'
```

Response:

```
{
  "dateTime": "2018-04-25T17:33:29.806+0000",
  "fullPath": "\Device\HarddiskVolume2\Windows\System32\config\systemprofile\Terminator.exe",
  "severity": 4,
  "profiles": [
    {
      "name": "Windows Profile - PCI(NJJ)",
      "rules": [
        {
          "severity": 4,
          "description": null,
          "id": "d6eb7f77-3726-47b3-90d8-3ecc8d8978e0",
          "type": "directory"
        }
      ],
      "id": "f589a105-0100-3dbb-a007-556fae7afea5",
      "type": "WINDOWS",
      "category": null
    }
  ],
  "type": "File",
  "changedAttributes": [
    2,
    4,
    8,
    16
  ],
  "platform": "WINDOWS",
  "oldContent": null,
  "actor": {
    "process": "update.exe",
    "processID": 11280,
    "imagePath": "C:\Windows\system32\update.exe",
    "userName": "NT AUTHORITY\SYSTEM",
    "userID": "S-1-5-18"
  },
}
```

```

"newContent": null,
"customerId": "58b888be-a90f-e3be-838d-88877aee572b",
"name": "Terminator.exe",
"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",
"fileContentHash":
"50dc26047f5572a38aa7adb4e9b140dc301ea41d1f4bed5095a1ed7fc1d03fbcb",

```

```
"reputationStatus": "MALICIOUS",
"fileCertificateHash": [
    "d12bed1761e1b2c244db23cebe4185c2b0839eee",
    "7ade32c9b68b944bf291d1fcc59faef061a6d2f2"
],
"trustStatus": "UNTRUSTED"
}
```

Sample 3:

Request:

```
curl -X GET https://<qualys_base_url>/fim/v2/events/e115XXXX-af72-37b5-8f92-9e878bbbbba53 -H 'authorization: Bearer ' -H 'content-type: application/json'
```

Response:

```
{
    "dateTime": "2021-03-05T11:28:36.455+0000",
    "fullPath": "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\Data",
    "type": "Value",
    "platform": "WINDOWS",
    "oldContent": null,
    "newContent": null,
    "customerId": "00XXXX-643f-f4af-8336-b253066XXXX",
    "action": "Content",
    "id": "e115XXXX-af72-37b5-8f92-9e878bbbbba53",
    "severity": 3,
    "fileCertificateHash": null,
    "profiles": [
        {
            "name": "Profile Name",
            "rules": [
                {
                    "severity": 3,
                    "number": 1,
                    "name": "Rule 1",
                    "description": "Rule 1",
                    "section": null,
                    "id": "4282XXXX-cc33-49d8-82df-53a00e27XXXX",
                    "type": "key"
                }
            ],
            "id": "f99941de-2296-4044-bfca-05aeb4575ef5",
            "type": "WINDOWS",
            "category": {
                "name": "PCI",
                "id": "2dabXXXX-2fdd-11e7-93ae-92361f00XXXX"
            }
        }
    ],
    "changedAttributes": null,
    "processedTime": "2021-03-05T05:37:30.311+0000",
```

```
"actor": {
    "process": "reg.exe",
    "processID": 2811,
    "imagePath": "C:\\Windows\\System32\\reg.exe",
    "userName": "MSEdgeWIN10\\IEUser",
    "userID": "S-1-5-21-3461203602-4096304019-2269080069-1000"
},
"name": null,
"asset": {
    "agentId": "7c99XXXX-92fa-4943-91ab-249e341dd10d",
    "interfaces": [
        {
            "hostname": "WIN10-122.WORKGROUP",
            "macAddress": "00:50:56:AA:5C:85",
            "address": "10.115.98.122",
            "interfaceName": "Intel(R) 82574L Gigabit Network
Connection"
        }
    ],
    "lastCheckedIn": "2019-07-23T11:01:00.000Z",
    "created": "2021-01-11T06:40:09.930+0000",
    "hostId": null,
    "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A
Build 10586",
    "tags": [
        "7508831",
        "7526815",
        "7593230"
    ],
    "assetType": "HOST",
    "system": {
        "lastBoot": "2019-07-23T11:01:00.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
    "netbiosName": "WIN10-122",
    "name": "WIN10-122",
    "agentVersion": "3.0.0.101",
    "updated": "2021-01-11T06:40:09.930+0000"
},
    "fileContentHash": null,
    "reputationStatus": null,
    "registryPath": "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options",
    "registryName": "Data",
}
```

```
"oldRegistryValueType": "REG_MULTI_SZ",
"oldRegistryValueContent": [
    "Multvalue string",
    "Multvalue string"
],
"newRegistryValueType": "REG_MULTI_SZ",
"newRegistryValueContent": [
    "Multvalue string1",
    "Multvalue string2"
],
"class": "Registry"
}
```

Ignored FIM Events API

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

[Fetch ignored events](#)

[Get ignored events count](#)

[Fetch ignored event details](#)

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 - <code>dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z']</code> You can filter events based on the time they are generated on the asset (dateTime) or based on the time they are processed at Qualys (processedTime). Note: For the dateTime filter start date should not be lower than 2017-01-01. The processedTime filter can be used only for events generated post FIM release 2.0.2.
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 - <code>[{"action":"asc"}]</code>
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample 1:

Request:

```
curl -X POST https://<qualys_base_url>/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,
  "lastLoggedInUser": ".\\Administrator",
  "netbiosName": "CAAUTOMATION-PC",
  "name": "IOC-104",
  "agentVersion": "2.0.6.1",
  "updated": 1531408044017
},
  "class": "Disk"
}
}
]
```

Sample 2:

Request:

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

Contents of request.json:

```
{
  "pageSize":100,
  "filter":"reputationStatus: MALICIOUS"
}
```

Response:

```
{
  "dateTime": "2021-01-19T07:09:07.116+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": "f589a105-0100-3dbb-a007-556fae7afea5"
      }
    }
  ],
  "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": "2021-01-19",  
"customerId": "58b888be-a90f-e3be-838d-88877aee572b",  
"name": "ProdCerts",  
"action": "Create",  
"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": "2021-01-19T07:02:08.000Z",  
    "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",  
"fileContentHash":  
"50dc26047f5572a38aa7adb4e9b140dc301ea41d1f4bed5095a1ed7fc1d03fbc"
```

```
'  
    "reputationStatus": "KNOWN",  
    "fileCertificateHash": [  
        "d12bed1761e1b2c244db23cebe4185c2b0839eee",  
        "7ade32c9b68b944bf291d1fcc59faef061a6d2f2"  
    ],  
    "trustStatus": "TRUSTED"  
}
```

Sample 3:

Request:

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

Contents of request.json:

```
{
  "pageSize":100,
  "filter":"registryKey.name: Data"
}
```

Response:

```
[
  {
    "sortValues": [],
    "data": {
      "dateTime": "2021-03-05T11:28:36.455+0000",
      "fullPath":
      "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
      NT\\CurrentVersion\\Image File Execution Options\\Data",
      "type": "Value",
      "platform": "WINDOWS",
      "oldContent": null,
      "newContent": null,
      "customerId": "00XXXX-643f-f4af-8336-b253066XXXX",
      "action": "Content",
      "id": "e115XXXX-af72-37b5-8f92-9e878bbbba53",
      "severity": 3,
      "fileCertificateHash": null,
      "profiles": [
        {
          "name": "Profile Name",
          "rules": [
            {
              "severity": 3,
              "number": 1,
              "name": "Rule 1",
              "description": "Rule 1",
              "section": null,
              "id": "4282XXXX-cc33-49d8-82df-53a00e27XXXX",
              "type": "key"
            }
          ]
        }
      ]
    }
  }
]
```

```
        ],
        "id": "f99941de-2296-4044-bfca-05aeb4575ef5",
        "type": "WINDOWS",
        "category": {
            "name": "PCI",
            "id": "2dabXXXX-2fdd-11e7-93ae-92361f00XXXX"
        }
    }
],
"changedAttributes": null,
"processedTime": "2021-03-05T05:37:30.311+0000",
"actor": {
    "process": "reg.exe",
    "processID": 2811,
    "imagePath": "C:\\Windows\\System32\\reg.exe",
    "userName": "MSEdgeWIN10\\IEUser",
    "userID": "S-1-5-21-3461203602-4096304019-2269080069-1000"
},
"name": null,
"asset": {
    "agentId": "7c99XXXX-92fa-4943-91ab-249e341dd10d",
    "interfaces": [
        {
            "hostname": "WIN10-122.WORKGROUP",
            "macAddress": "00:50:56:AA:5C:85",
            "address": "10.115.98.122",
            "interfaceName": "Intel(R) 82574L Gigabit Network Connection"
        }
    ],
    "lastCheckedIn": "2019-07-23T11:01:00.000Z",
    "created": "2021-01-11T06:40:09.930+0000",
    "hostId": null,
    "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A Build 10586",
    "tags": [
        "7508831",
        "7526815",
        "7593230"
    ],
    "assetType": "HOST",
    "system": {
        "lastBoot": "2019-07-23T11:01:00.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
}
```

```
"netbiosName": "WIN10-122",
"name": "WIN10-122",
"agentVersion": "3.0.0.101",
"updated": "2021-01-11T06:40:09.930+0000"
},
"ignoreDate": "2021-01-12",
"fileContentHash": null,
"reputationStatus": null,
"registryPath":
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
NT\\CurrentVersion\\Image File Execution Options",
"registryName": "Data",
"oldRegistryValueType": "REG_MULTI_SZ",
"oldRegistryValueContent": [
    "Multvalue string",
    "Multvalue string"
],
"newRegistryValueType": "REG_MULTI_SZ",
"newRegistryValueContent": [
    "Multvalue string1",
    "Multvalue string2"
],
"class": "Registry"
}
}
]
```

Sample 4:

API Request:

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

Contents of request.json:

```
{  
  
    "filter": "file.attribute.readOnly: `Removed`",  
    "pageSize": 1  
  
}
```

Response:

```
[  
    {  
        "sortValues": [],  
        "data": {  
            "dateTime": "2023-06-14T06:20:01.269+0000",  
            "fullPath":  
                "C:\\\\CR_FIM_TEST\\\\All_Machines\\\\test_3\\\\1_event.json",  
            "fileAttribute": {  
                "readonly": "Removed",  
                "hidden": "Added",  
                "encrypted": null,  
                "compressed": null  
            },  
            "ownerShip": null,  
            "registryPath": null,  
            "contentId": null,  
            "type": "File",  
            "platform": "WINDOWS",  
            "oldContent": null,  
            "contentStatus": null,  
            "oldRegistryValueType": null,  
            "newContent": null,  
            "ignoreDate": "2023-06-28",  
            "permissions": null,  
            "customerId": "25a14e60-80c1-4c25-8166-6653a4e2b094",  
            "action": "Attributes",  
            "id": "e6b9a72b-0eb6-3143-896f-b9c9edd87013",  
            "class": "Disk",  
            "fileID": "0x90000147d4",  
            "group": null,  
            "severity": 5,  
            "trustStatus": null,  
            "fileCertificateHash": null,  
            "lastModified": "2023-06-14T06:20:01.269+0000",  
            "lastAccessed": "2023-06-14T06:20:01.269+0000",  
            "lastWritten": "2023-06-14T06:20:01.269+0000",  
            "size": 0, "sizeUnit": "B",  
            "modificationTime": "2023-06-14T06:20:01.269+0000",  
            "creationTime": "2023-06-14T06:20:01.269+0000",  
            "lastModifiedBy": null, "lastAccessedBy": null,  
            "lastWrittenBy": null, "lastModifiedTime": null,  
            "lastAccessedTime": null, "lastWrittenTime": null  
        }  
    }  
]
```

```

"securitySettings": null,
"profiles": [
    {
        "name": "CR_All_Machines",
        "rules": [
            {
                "severity": 5,
                "number": 1,
                "name": "CR_1",
                "description": "",
                "section": null,
                "id": "59ffbe0d-d27d-428d-9766-226ede8ee015",
                "type": "directory"
            }
        ],
        "id": "0bd18efb-11d5-4a30-8b74-57fca4cdfbf4",
        "type": "WINDOWS",
        "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
        }
    }
],
"baseline": false,
"registryName": null,
"changedAttributes": [
    2,
    4,
    8,
    16
],
"processedTime": "2023-06-14T06:21:45.685+0000",
"actor": {
    "process": "Explorer.EXE",
    "auditUserName": null,
    "auditUserID": null,
    "processID": 1588,
    "imagePath": "C:\\Windows\\Explorer.EXE",
    "procTitle": null,
    "userName": "WIN7QWB3\\Administrator",
    "userID": "S-1-5-21-122566442-3410611961-1220210811-500"
},
"oldRegistryValueContent": null,
"newRegistryValueType": null,
"fileContentHashOld": null,
"size": null,
"name": "1_event.json",
"fileContentHash": null,
"volumeID": "0xa677df9e",
"reputationStatus": null,
"newRegistryValueContent": null,
"attributes": {
    "newAttribute": [
        "Archive",

```

```
        "Encrypted",
        "Hidden"
    ],
    "oldAttribute": [
        "Archive",
        "Encrypted",
        "Read Only"
    ]
},
"asset": {
    "agentId": "789b2ded-fa94-436d-99d3-7db7f30662d4",
    "interfaces": [
        {
            "hostname": "WIN7QWB3",
            "macAddress": "00:50:56:AA:ED:CD",
            "address": "10.115.106.43",
            "interfaceName": "Intel(R) PRO/1000 MT Network
Connection"
        }
    ],
    "lastCheckedIn": "2023-06-13T16:02:38.000Z",
    "created": "2023-05-30T11:04:56.931+00:00",
    "hostId": "3577425",
    "operatingSystem": "Microsoft Windows 7 Professional
6.1.7601 64-bit Service Pack 1 Build 7601",
    "tags": [
        "8543820"
    ],
    "assetType": "HOST",
    "system": {
        "lastBoot": "2023-05-03T07:01:47.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": "Administrator",
    "netbiosName": "WIN7QWB3",
    "name": "Win7qwb3",
    "agentVersion": "5.2.0.10",
    "updated": "2023-05-30T11:04:56.931+00:00"
},
"incidentId": null
}
]
}
```

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' You can filter events based on the time they are generated on the asset (dateTIme) or based on the time they are processed at Qualys (processedTime). Note: For the dateTIme filter start date should not be lower than 2017-01-01. The processedTime filter can be used only for events generated post FIM release 2.0.2.
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 1:

Request:

```
curl -X POST https://<qualys_base_url>/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  
}
```

Sample 2:

API Request:

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

Contents of request.json:

```
{  
  
    "filter": "file.attribute.hidden: `Added`"  
  
}
```

Response:

```
{  
  
    "count": 13  
  
}
```

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 1:

Request:

```
curl -X GET  
https://<qualys_base_url>/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"
}
```

Sample 2:

Request:

```
curl -X GET
https://<qualys_base_url>/fim/v2/events/ignore/f589a105-0100-3dbb-
a007-556fae7afea5 -H 'authorization: Bearer <token>' -H
'content-type: application/json'
```

Response:

```
{
  "dateTime": "2021-01-19T07:09:07.116+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": "f589a105-0100-3dbb-a007-556fae7afea5"
      }
    }
  ],
  "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": "2021-01-19",
"customerId": "58b888be-a90f-e3be-838d-88877aee572b",
"name": "ProdCerts",
"action": "Create",
"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": "2021-01-19T07:02:08.000Z",
  "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",
"fileContentHash":
```

```
"50dc26047f5572a38aa7adb4e9b140dc301ea41d1f4bed5095a1ed7fc1d03fb" ,  
    "reputationStatus": "KNOWN",  
    "fileCertificateHash": [  
        "d12bed1761e1b2c244db23cebe4185c2b0839eee",  
        "7ade32c9b68b944bf291d1fcc59faef061a6d2f2"  
    ],  
    "trustStatus": "TRUSTED"  
}
```

Sample 3:

Request:

```
curl -X GET
https://<qualys_base_url>/fim/v2/events/ignore/e115XXXX-af72-37b5-
8f92-9e878bbbbba53 -H 'authorization: Bearer <token>' -H
'content-type: application/json'
```

Response:

```
{
    "dateTime": "2021-03-05T11:28:36.455+0000",
    "fullPath":
    "HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
    NT\\CurrentVersion\\Image File Execution Options\\Data",
    "type": "Value",
    "platform": "WINDOWS",
    "oldContent": null,
    "newContent": null,
    "customerId": "00XXXX-643f-f4af-8336-b253066XXXX",
    "action": "Content",
    "id": "e115XXXX-af72-37b5-8f92-9e878bbbbba53",
    "severity": 3,
    "fileCertificateHash": null,
    "profiles": [
        {
            "name": "Profile Name",
            "rules": [
                {
                    "severity": 3,
                    "number": 1,
                    "name": "Rule 1",
                    "description": "Rule 1",
                    "section": null,
                    "id": "4282XXXX-cc33-49d8-82df-53a00e27XXXX",
                    "type": "key"
                }
            ],
            "id": "f99941de-2296-4044-bfca-05aeb4575ef5",
            "type": "WINDOWS",
            "category": {
                "name": "PCI",
                "id": "2dabXXXX-2fdd-11e7-93ae-92361f00XXXX"
            }
        }
    ],
    "changedAttributes": null,
```

```
"processedTime": "2021-03-05T05:37:30.311+0000",
"actor": {
    "process": "reg.exe",
    "processID": 2811,
    "imagePath": "C:\\Windows\\System32\\reg.exe",
    "userName": "MSEdgeWIN10\\IEUser",
    "userID": "S-1-5-21-3461203602-4096304019-2269080069-1000"
},
"name": null,
"asset": {
    "agentId": "7c99XXXX-92fa-4943-91ab-249e341dd10d",
    "interfaces": [
        {
            "hostname": "WIN10-122.WORKGROUP",
            "macAddress": "00:50:56:AA:5C:85",
            "address": "10.115.98.122",
            "interfaceName": "Intel(R) 82574L Gigabit Network
Connection"
        }
    ],
    "lastCheckedIn": "2019-07-23T11:01:00.000Z",
    "created": "2021-01-11T06:40:09.930+0000",
    "hostId": null,
    "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A
Build 10586",
    "tags": [
        "7508831",
        "7526815",
        "7593230"
    ],
    "assetType": "HOST",
    "system": {
        "lastBoot": "2019-07-23T11:01:00.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
    "netbiosName": "WIN10-122",
    "name": "WIN10-122",
    "agentVersion": "3.0.0.101",
    "updated": "2021-01-11T06:40:09.930+0000"
},
"ignoreDate": "2021-01-12",
"fileContentHash": null,
"reputationStatus": null,
"registryPath":
"HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows
```

```
NT\\CurrentVersion\\Image File Execution Options",
  "registryName": "Data",
  "oldRegistryValueType": "REG_MULTI_SZ",
  "oldRegistryValueContent": [
    "Multvalue string",
    "Multvalue string"
  ],
  "newRegistryValueType": "REG_MULTI_SZ",
  "newRegistryValueContent": [
    "Multvalue string1",
    "Multvalue string2"
  ],
  "class": "Registry"
}
```

Sample 4:

API Request:

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

Contents of request.json:

```
{  
  
    "filter": "file.attribute.readOnly: `Removed`",  
    "pageSize": 1  
  
}  
}
```

Response:

```
[  
    {  
        "sortValues": [],  
        "data": {  
            "dateTime": "2023-06-14T06:20:01.269+0000",  
            "fullPath":  
                "C:\\\\CR_FIM_TEST\\\\All_Machines\\\\test_3\\\\1_event.json",  
            "fileAttribute": {  
                "readonly": "Removed",  
                "hidden": "Added",  
                "encrypted": null,  
                "compressed": null  
            },  
            "ownerShip": null,  
            "registryPath": null,  
            "contentId": null,  
            "type": "File",  
            "platform": "WINDOWS",  
            "oldContent": null,  
            "contentStatus": null,  
            "oldRegistryValueType": null,  
            "newContent": null,  
            "ignoreDate": "2023-06-28",  
            "permissions": null,  
            "customerId": "25a14e60-80c1-4c25-8166-6653a4e2b094",  
            "action": "Attributes",  
            "id": "e6b9a72b-0eb6-3143-896f-b9c9edd87013",  
            "class": "Disk",  
            "fileID": "0x90000147d4",  
            "group": null,  
            "severity": 5,  
            "trustStatus": null,  
            "fileCertificateHash": null,  
        }  
    }  
]
```

```

"securitySettings": null,
"profiles": [
    {
        "name": "CR_All_Machines",
        "rules": [
            {
                "severity": 5,
                "number": 1,
                "name": "CR_1",
                "description": "",
                "section": null,
                "id": "59fffbe0d-d27d-428d-9766-226ede8ee015",
                "type": "directory"
            }
        ],
        "id": "0bd18efb-11d5-4a30-8b74-57fca4cdfbf4",
        "type": "WINDOWS",
        "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
        }
    }
],
"baseline": false,
"registryName": null,
"changedAttributes": [
    2,
    4,
    8,
    16
],
"processedTime": "2023-06-14T06:21:45.685+0000",
"actor": {
    "process": "Explorer.EXE",
    "auditUserName": null,
    "auditUserID": null,
    "processID": 1588,
    "imagePath": "C:\\Windows\\Explorer.EXE",
    "procTitle": null,
    "userName": "WIN7QWB3\\Administrator",
    "userID": "S-1-5-21-122566442-3410611961-1220210811-500"
},
"oldRegistryValueContent": null,
"newRegistryValueType": null,
"fileContentHashOld": null,
"size": null,
"name": "1_event.json",
"fileContentHash": null,
"volumeID": "0xa677df9e",
"reputationStatus": null,
"newRegistryValueContent": null,
"attributes": {
    "newAttribute": [
        "Archive",

```

```
        "Encrypted",
        "Hidden"
    ],
    "oldAttribute": [
        "Archive",
        "Encrypted",
        "Read Only"
    ]
},
"asset": {
    "agentId": "789b2ded-fa94-436d-99d3-7db7f30662d4",
    "interfaces": [
        {
            "hostname": "WIN7QWB3",
            "macAddress": "00:50:56:AA:ED:CD",
            "address": "10.115.106.43",
            "interfaceName": "Intel(R) PRO/1000 MT Network
Connection"
        }
    ],
    "lastCheckedIn": "2023-06-13T16:02:38.000Z",
    "created": "2023-05-30T11:04:56.931+00:00",
    "hostId": "3577425",
    "operatingSystem": "Microsoft Windows 7 Professional
6.1.7601 64-bit Service Pack 1 Build 7601",
    "tags": [
        "8543820"
    ],
    "assetType": "HOST",
    "system": {
        "lastBoot": "2023-05-03T07:01:47.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": "Administrator",
    "netbiosName": "WIN7QWB3",
    "name": "Win7qwb3",
    "agentVersion": "5.2.0.10",
    "updated": "2023-05-30T11:04:56.931+00:00"
},
"incidentId": null
}
]
}
```

FIM Incidents API

Use these API functions to fetch FIM Incident data.

[Fetch incident count](#)

[Fetch incidents](#)

[Get event count for an incident](#)

[Fetch events for an incident](#)

[Create manual incident](#)

[Approve incidents](#)

Fetch incident count

/fim/v2/incidents/count

[POST]

Get number of Incidents in an user account.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

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 - status:'OPEN'
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
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.
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [\"name\":\"asc\"]

Sample

Request:

```
curl -X POST https://<qualys_base_url>/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-d6f4e31fcfd6e": 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
}
}
```

Fetch incidents

/fim/v3/incidents/search

[POST]

Get FIM incidents for an user account.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

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 - status:‘OPEN’
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 - "sort": "[{\\"name\\":\"asc\\"}]"
attributes (String)	Search based on certain attributes (provide comma separated list).
SearchAfter	(Required) This parameter is required to fetch more than 10,000 rows.

Sample

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/incidents/search -H  
'authorization: Bearer <token>' -H 'content-type:  
application/json' -d @request.json
```

Contents of request.json:

```
{  
    "attributes": "reviewers, name",  
    "filter": "changeType:AUTOMATED",  
    "pageSize": 2,  
    "pageNumber": 0,  
    "sort": "[{\\"name\\":\"asc\\"}]"  
}
```

Response:

```
[  
  {  
    "sortValues": [  
      "incident_01"  
    ],  
    "data": {  
      "name": "incident_01",  
      "id": "xxx9xx4x-2x73-4x6x-95x6-29x3x4x4x013",  
      "reviewers": [  
        "quays_fa"  
      ]  
    }  
  },  
  {  
    "sortValues": [  
      "incident_02"  
    ],  
    "data": {  
      "name": "incident)2",  
      "id": "7992xxxx-x161-494x-x761-323xx67844x8",  
      "reviewers": [  
        "quays_fa"  
      ]  
    }  
  }]
```

Get event count for an incident

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

[POST]

Get number of events logged for an incident.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

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 - status: 'OPEN'
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 - [{"name": "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 1:

Request:

```
curl -X POST
https://<qualys_base_url>/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  
  }  
}
```

Sample 2:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v2/incidents/{incidentId}/events/count -H 'authorization: Bearer <token>' -H
'contenttype: application/json' -d @request.json
```

Contents of request.json:

```
{
  "filter": "file.attribute.readonly: `Added`"
}
```

Response:

```
{
  "count": 10
}
```

Fetch events for an incident

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

[POST]

Get events logged under an incident.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

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 - status:OPEN
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 - [{"name": "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 1:

Request:

```
curl -X POST
https://<qualys_base_url>/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": "8x340728-411x-37x1-x028-0xxx41362xxx"  
    }  
  },  
  {  
    "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": "87x0x9x7-0518-3974-86x3-x48712323147"  
    }  
  }
```

```
},
{
  "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-03f45eec137"
    }
}
]
```

Sample 2:

API Request:

```
curl -X POST
https://<qualys_base_url>/fim/v2/incidents/{incidentId}/events/search -H 'authorization: Bearer <token>' -H
'contenttype: application/json' -d @request.json
```

Contents of request.json:

```
{
  "filter": "file.attribute.readonly:'Added'",
  "pageSize": 1
}
```

Response:

```
[
  {
    "sortValues": [],
    "data": {
      "dateTime": "2023-06-28T06:22:36.938+0000",
      "fullPath": "C:\\CR_FIM_TEST\\All_Machines\\wmplayer - Copy (6) - Copy.exe",
      "fileAttribute": {
        "readonly": "Added",
        "hidden": "Added",
        "encrypted": null,
        "compressed": null
      },
      "ownerShip": null,
      "registryPath": null,
      "contentId": null,
      "type": "File",
      "platform": "WINDOWS",
      "oldContent": null,
      "contentStatus": null,
      "oldRegistryValueType": null,
      "newContent": null,
      "permissions": null,
      "customerId": "25a14e60-80c1-4c25-8166-6653a4e2b094",
      "action": "Attributes",
      "id": "8ce8a4ae-80b2-3b17-a42d-ff9c488a7714",
      "class": "Disk",
      "fileID": "0x6600002b53c",
      "group": null,
      "severity": 5,
      "trustStatus": null,
      "fileCertificateHash": null,
      "securitySettings": null,
      "profiles": [
        {
          "name": "CR_All_Machines",
        }
      ]
    }
  }
]
```

```
"rules": [
    {
        "severity": 5,
        "number": 1,
        "name": "CR_1",
        "description": "",
        "section": null,
        "id": "59fffbe0d-d27d-428d-9766-226ede8ee015",
        "type": "directory"
    }
],
"id": "0bd18efb-11d5-4a30-8b74-57fca4cdfbf4",
"type": "WINDOWS",
"category": {
    "name": "PCI",
    "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
}
},
"baseline": false,
"registryName": null,
"changedAttributes": [
    2,
    4,
    8,
    16
],
"processedTime": "2023-06-28T06:24:41.347+0000",
"actor": {
    "process": "explorer.exe",
    "auditUserName": null,
    "auditUserID": null,
    "processID": 5864,
    "imagePath": "C:\\WINDOWS\\explorer.exe",
    "procTitle": null,
    "userName": "DESKTOP-FR23SL8\\Administrator",
    "userID": "S-1-5-21-1082135036-1977325707-348817062-500"
},
"oldRegistryValueContent": null,
"newRegistryValueType": null,
"fileContentHashOldsizevolumeIDattributes
```

```
        },
        "asset": {
            "agentId": "3f8a4d42-1f50-4557-881b-0efcbfff70ac",
            "interfaces": [
                {
                    "hostname": "DESKTOP-FR23SL8",
                    "macAddress": "00:50:56:AA:75:F0",
                    "address": "10.115.138.119",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection"
                },
                {
                    "hostname": "DESKTOP-FR23SL8",
                    "macAddress": "00:50:56:AA:75:F0",
                    "address": "fe80:0:0:0:bf92:dce7:bb76:a30d",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection"
                }
            ],
            "lastCheckedIn": "2023-06-13T06:28:13.000Z",
            "created": "2023-06-14T10:01:06.060+00:00",
            "hostId": null,
            "operatingSystem": "Windows Microsoft Windows 10 Pro
10.0.19045 Build 19045",
            "tags": [
                "8543820"
            ],
            "assetType": "HOST",
            "system": {
                "lastBoot": "2023-06-14T15:05:03.000Z"
            },
            "ec2": null,
            "lastLoggedOnUser": "qualys",
            "netbiosName": "DESKTOP-FR23SL8",
            "name": "DESKTOP-FR23SL8",
            "agentVersion": "4.9.0.16",
            "updated": "2023-06-14T10:01:06.060+00:00"
        },
        "incidentId": "a0e6709b-14cc-4750-97c9-b693883adfb6"
    }
]
```

Create manual incident

/fim/v3/incidents/create

[POST]

Create manual incidents of type "DEFAULT".

Response Code

- 201: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

comment (String)	Comments for approval of the Incidents.
filters	(Required) 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 - "filters": ["dateTime: ['2020-05-17T18:30:00.000Z'..'2020-05-18T18:29:59.999Z'] and (action:'Attributes')"],
name (String)	(Required) The name of the incident. Accepted length: Between 1 to 128 characters.
reviewers (String)	Reviewers who will approve the incident.
type	This is set to "DEFAULT" always.
userInfo	Information about the user.

Note: Manual incident is created with up to 100K events

Sample

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/incidents/create -H  
'authorization: Bearer <token>' -H 'content-type:  
application/json' -d @request.json
```

Content of request.json:

```
{
  "name": "<INCIDENT NAME>",
  "reviewers": [
    "<USERNAME>", "<USER EMAIL ID>"
  ],
  "filters": [
    "dateTime: ['2020-01-14T18:30:00.000Z'..'2022-12-
```

```
16T09:29:59.999Z'] and action:`Create`"
],
"comment": "<COMMENT>",
"type": "DEFAULT",
"userInfo": {
    "user": {
        "name": "<USERNAME>",
        "id": "<INCIDENT ID>"
    }
}
}
```

Response:

```
{
    "comment": "comment for an incident",
    "approvalType": "MANUAL",
    "type": "DEFAULT",
    "id": "INCIDENT ID",
    "userInfo": {
        "date": 1671188983383
    },
    "customerId": "<CUSTOMER ID>",
    "name": "<INCIDENT NAME>",
    "filters": [
        "dateTime: ['2020-01-14T18:30:00.000Z'..'2022-12-
16T09:29:59.999Z'] and action:`Create`"
    ],
    "reviewers": [
        "<USERNAME>",
        "<USER EMAIL ID>"      ]
}
```

Approve incidents

`/fim/v3/incidents/{incidentId}/approve`

[POST]

For approving an incident.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not found
- 503: Service unavailable

Input Parameters

approvalStatus	(Required) The approval status of the incident created by the rule. Allowed values: "APPROVED", "POLICY_VIOLATION", "UNAPPROVED", "PENDING".
changeType	(Required) Type of Incidents created by the rule. Allowed values: "MANUAL", "AUTOMATED", "COMPROMISE", "STANDARD_CHANGE", "EMERGENCY_CHANGE", "NORMAL_CHANGE", "OTHER".
comment (String)	(Required) Comments for the incidents created by rule.
dispositionCategory	(Required) The category of the Incident created by the rule. Allowed values: "PATCHING", "PRE_APPROVED_CHANGE_CONTROL", "CONFIGURATION_CHANGE", "HUMAN_ERROR", "DATA_CORRUPTION", "EMERGENCY_CHANGE", "CHANGE_CONTROL_VIOLATION", "GENERAL_HACKING", "MALWARE", "MALICIOUS_INTENT", "UNAUTHORIZED_ACCESS", "INAPPROPRIATE_USAGE_OR_FRAUD", "DATA LOSS OR THEFT", "DISREGARD_OF_ORGANIZATIONAL_POLICY", "FALSE_POSITIVE", "OTHER".

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/incidents/{incidentId}/approve -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Content of request.json:

```
{
    "approvalStatus": "PENDING",
    "changeType": "NORMAL_CHANGE",
    "comment": "With additional approval values",
    "dispositionCategory": "DISREGARD_OF_ORGANIZATIONAL_POLICY"
}
```

Response:

```
{
    "customerId": "<CUSTOMER ID>",
    "type": "DEFAULT",
    "id": "<ID>",
    "filterFromDate": "2022-11-15T16:07:00.000+0000",
    "filterToDate": "2022-12-15T16:07:00.000+0000",
    "name": "TEST WITH SPECIAL CHARS",
    "filters": [
        "dateTime: ['2022-11-15T16:07:00.000Z'..'2022-12-
15T16:07:00.000Z'] AND (action:Content)"
    ],
    "status": "CLOSED",
    "reviewers": [
        "<REVIEWER USERNAME OR EMAIL ID>"
    ],
    "comment": "With additional approval values",
    "assignDate": "2022-12-15T16:08:19.560+0000",
    "approvalDate": "2022-12-16T06:33:19.224+0000",
    "approvalStatus": "PENDING",
    "dispositionCategory": "DISREGARD_OF_ORGANIZATIONAL_POLICY",
    "changeType": "NORMAL_CHANGE",
    "approvalType": "MANUAL",
    "createdById": "<USER ID>",
    "createdByName": "<USER NAME>",
    "createdDate": "2022-12-15T16:08:19.560+0000",
    "lastUpdatedById": "<USER ID>",
    "lastUpdatedByName": "USER NAME",
    "lastUpdatedDate": "2022-12-16T06:17:36.953+0000",
    "filterUpdatedDate": "2022-12-15T16:08:19.560+0000",
```

```
"deleted": false,  
"marked": true,  
"moved": null,  
"markupStatus": "COMPLETED",  
"ruleId": null,  
"ruleName": null
```

FIM Alerting API

Use these API functions to fetch FIM Alerting data.

Alerting Action API

[Fetch all Alert Actions](#)

[Fetch Alert Actions for an Action ID](#)

Fetch all Alert Actions

`/fim/v3/alert/actions/search`

[POST]

To search all the Alert actions created.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/actions/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
  "customerId": "x5x0514x-x211-x1x4-809x-x3x2xx667xxx",
  "applicationName": "FIM",
  "id": "xxx13x40-11x0-11xx-x12x-xx6083x5x695",
  "name": "Email - Alerting regression",
  "description": "Alerting regression",
  "actionType": "qemail",
  "createdBy": "John Doe",
  "createdById": "quays_jd2",
  "updatedBy": "John Doe",
  "updatedById": "quays_jd2",
  "created": 1574919350308,
```

```
"updated": 1574919362952,  
"alert": "Email- Alerting regression",  
"subject": "Email- Alerting regression",  
"smtpHost": "mta01.eng.sjc01.qualys.com",  
"smtpPort": 25,  
"emailRecipients": [  
  "jd2@qualys.com",  
  "jd1@qualys.com",  
  "jd@qualys.com"  
,  
  "emailFromAddress": "noreply@qualys.com",  
  "emailReplyTo": "noreply@qualys.com",  
  "slackWebhookUri": null,  
  "slackChannel": null,  
  "pagerdutyServiceKey": null,  
  "pagerdutyEventType": null,  
  "pagerdutyClient": null,  
  "activeRules": 1,  
  "disabledRules": 2,  
  "smtpUser": null  
}
```

Fetch Alert Actions for an Action ID

/fim/v3/alert/actions/{actionId}

[GET]

To search the Alert actions for an Action ID.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not found
- 503: Service unavailable

Input Parameters

actionId	(Required) ID of the action you want to fetch the action for.
----------	---

Sample

Request:

```
curl -X GET  
https://<qualys_base_url>/fim/v3/alert/actions/{actionId} -  
H'authorization: Bearer <token>' -H 'content-type:  
application/json'
```

Response:

```
{  
    "customerId": "x5x0514x-x211-x1x4-809x-x3x2xx667xxx",  
    "applicationName": "FIM",  
    "id": "xxx13x40-11x0-11xx-x12x-xx6083x5x695",  
    "name": "Email - Alerting regression",  
    "description": "Alerting regression",  
    "actionType": "qemail",  
    "createdBy": "John Doe",  
    "createdById": "quays_jd2",  
    "updatedBy": "John Doe",  
    "updatedById": "quays_jd2",  
    "created": 1574919350308,  
    "updated": 1574919362952,  
    "alert": "Email- Alerting regression",  
    "subject": "Email- Alerting regression",  
    "smtpHost": "mta01.eng.sjc01.qualys.com",  
    "smtpPort": 25,  
    "emailRecipients": [
```

```
"jd2@qualys.com",
"jd1@qualys.com",
"jd@qualys.com"
],
"emailFromAddress": "noreply@qualys.com",
"emailReplyTo": "noreply@qualys.com",
"slackWebhookUri": null,
"slackChannel": null,
"pagerdutyServiceKey": null,
"pagerdutyEventType": null,
"pagerdutyClient": null,
"activeRules": 1,
"disabledRules": 2,
"smtpUser": null
}
```

Alerting Rules API

[Fetch Alert Rules](#)

[Fetch details for Alert Rule](#)

[Enable Alert Rule](#)

[Disable Alert Rule](#)

[Delete a Alert Rule](#)

Fetch Alert Rules

/fim/v3/alert/rules/search

[POST]

To search all the alert rules.

Note: The API will return the default value for the following fields:

For Single Match: slideTime, matchCount, aggregate, aggregationKeys.

For Time-Window Scheduled Match: slideTime, matchCount.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Sample

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/alert/rules/search -  
H 'authorization: Bearer <token>' -H 'content-type:  
application/json'
```

Response:

```
{  
    "customerId": "x5x0514x-x211-x1x4-809x-x3x2xx667xxx",  
    "applicationName": "FIM",  
    "id": "8xx98x30-xx5x-11x9-9036-339x439x1x4x",  
    "datasource": "EVENTS",  
    "ruleType": "simple_alert",  
    "name": "Rule - Alerting 2.1.2 testing updating",  
    "description": "Rule - Alerting 2.1.2 testing",  
    "qql": "(file fullPath:'*\\"\\System32\\*' and action:Attributes  
)",
```

```
"windowTime":0,
"slideTime":900000,
"matchCount":3,
"fromHour":0,
"fromMinute":0,
"duration":0,
"aggregate":true,
"aggregationKeys": [
    "tokens"
],
"actions": [
    {
        "id":"54x62750-xx5x-11x9-9525-51f120x87xx9",
        "actionType":"qemail",
        "name":"Alerting 2.1.2 Testing",
        "subject":"Alerting 2.1.2 Testing",
        "alert":"Alerting 2.1.2 Testing",
        "emailRecipients": [
            "jd1@qualys.com",
            "jd2@qualys.com",
            "jd@qualys.com"
        ],
        "slackChannel":null,
        "subjectParameters": [
            ,
            "bodyParameters": [
                ]
        }
    ],
    "created":1569172952451,
    "createdBy":"John Doe",
    "createdById":"quays_jd2",
    "updated":1569332877053,
    "updatedBy":"John Doe",
    "updatedById":"quays_jd2",
    "lastRun":1569312595868,
    "active":false,
    "ruleState":"DISABLED",
    "actionNames": [
        "Alerting 2.1.2 Testing"
    ],
    "trigger":"Single Match"
}
```

Fetch details for Alert Rule

/fim/v3/alert/rules/{ruleId}

[GET]

To search the details for the given rule id.

Note: The API will return the default value for the following fields:

For Single Match: slideTime, matchCount, aggregate, aggregationKeys.

For Time-Window Scheduled Match: slideTime, matchCount.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not found
- 503: Service unavailable

Input Parameters

ruleId	(Required) ID of the alert rule you want the details for.
--------	---

Sample

Request:

```
curl -X GET https://<qualys_base_url>/fim/v3/alert/rules/{ruleId}  
-H 'authorization: Bearer <token>' -H 'content-type:  
application/json'
```

Response:

```
{  
    "customerId": "x5x0514x-x211-x1x4-809x-x3x2xx667xxx",  
    "applicationName": "FIM",  
    "id": "8xx98x30-xx5x-11x9-9036-339x439x1x4x",  
    "datasource": "EVENTS",  
    "ruleType": "simple_alert",  
    "name": "",  
    "description": "",  
    "qql": "(file fullPath:'*\\"System32\\*' and action:Attributes  
)",  
    "windowTime": 0,  
    "slideTime": 900000,  
    "matchCount": 3,  
    "fromHour": 0,  
    "fromMinute": 0,
```

```
"duration": 0,  
"aggregate": true,  
"aggregationKeys": [  
    "tokens"  
,  
    "actions": [{  
        "id": "54x62750-xx5x-11x9-9525-51x120x87xx9",  
        "actionType": "qemail",  
        "name": "Alerting 2.1.2 Testing",  
        "subject": "Alerting 2.1.2 Testing",  
        "alert": "Alerting 2.1.2 Testing",  
        "emailRecipients": [  
            "jd1@qualys.com",  
            "jd2@qualys.com",  
            "jd@qualys.com"  
,  
            "slackChannel": null,  
            "subjectParameters": [],  
            "bodyParameters": []  
        }  
,  
        "created": 1569172952451,  
        "createdBy": "John Doe",  
        "createdById": "quays_jd2",  
        "updated": 1569332877053,  
        "updatedBy": "John Doe",  
        "updatedById": "quays_jd2",  
        "lastRun": 1569312595868,  
        "active": false,  
        "ruleState": "DISABLED",  
        "actionNames": [  
            "Alerting 2.1.2 Testing"  
,  
        "trigger": "Single Match"  
    }]
```

Enable Alert Rule

`/fim/v3/alert/rules/{ruleId}/enable`

[POST]

To enable an Alert rule.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not Found
- 503: Service unavailable

Input Parameters

ruleId	(Required) ID of the alert rule you want to enable.
--------	---

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/rules/{ruleId}/enable -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
  "enabled": true
}
```

Disable Alert Rule

/fim/v3/alert/rules/{ruleId}/disable

[POST]

To disable an alert rule.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not Found
- 503: Service unavailable

Input Parameters

ruleId	(Required) ID of the alert rule you want to disable.
--------	--

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/rules/{ruleId}/disable -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
    "disabled": true
}
```

Delete a Alert Rule

/fim/v3/alert/rules/{ruleId}/delete

[POST]

To delete an alert rule.

Response Code

- 201: Successful
- 401: Unauthorized
- 404: Not Found
- 503: Service unavailable

Input Parameters

ruleId	(Required) ID of the alert rule you want to delete.
--------	---

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/rules/{ruleId}/delete -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
    "deleted": true
}
```

Alerting Activities API

Fetch the generated alerts for FIM

Count Number of Alerts Generated for FIM

Fetch the generated alerts for FIM

/fim/v3/alert/activities/search

[POST]

To search all the Alerting activities for FIM.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

filter (String)	Filter the alerts 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: ruleName:`POD12: Email Rule`
pageNumber	The page number to be returned. The number starts from zero.
pageSize	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 - "sort":"[\"status\":\"desc\"]"

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/activities/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "filter": "string",
  "pageNumber": {},
  "pageSize": {},
  "sort": "string"
```

}

Response:

```
[  
    "statusDate": 1560569128488,  
    "subject": "PagerDuty Test Action with John's Service Key",  
    "identifiers": [  
        "xx18x49x-1x2x-3xxx-x7x1-4787xxx5xxxx"  
    ],  
    "emailRecipients": [],  
    "matches": 1,  
    "ruleDescription": "Rule to test PagerDuty account",  
    "aggregate": true,  
    "actionType": "pagerduty",  
    "createdBy": "John Doe",  
    "alert": "Testing the pager duty account, to check the calls  
and sms\nSecurity\xxx5026x1-0xx8-4x4x-9xx4-64x8x1xx905f\nJohn  
Linux FIM\nCentOS Linux 7.5.1804\nn2\n[Linux Profile]\n[[f0534cd2-  
8f19-4a1d-986f-  
414d8ef5825d]]\nchgrp\n/usr/bin/chgrp\nn2.4.0.72\n\n[7701016,  
7905815]\nxxx18x49x-1x2x-3xxx-x7x1-4787xxx5xxxx\n[My category JD]",  
    "datasource": "EVENTS",  
    "customerId": "x5x0514x-x211-x1b4-809x-x3x2xx667xxx",  
    "actionId": "xx3xx0x0-8x68-11x9-9xx1-058683x890x9",  
    "ruleName": "Rule to test PagerDuty account",  
    "id": "x51xxxx1-8x91-11x9-88x1-x97xx3100467",  
    "ruleId": "x5xx0190-8x68-11x9-x24x-87456x2x93x3",  
    "applicationName": "FIM",  
    "createdById": "quays_jd2",  
    "actionName": "PagerDuty Test Action",  
    "status": "SUCCESS"  
]
```

Count Number of Alerts Generated for FIM

/fim/v3/alert/activities/count

[POST]

To count the alerting activities for FIM.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

filter (String)	Filter the alerts 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 - ruleName:‘POD12: Email Rule`
-----------------	---

Sample

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/alert/activities/count -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "filter": "string"

}
```

Response:

```
{
  "count": 86457

}
```

FIM Correlation API

Use these API functions to fetch FIM Correlation data.

- [Fetch all Correlation Rules](#)
- [Fetch Correlation Rule Details for a particular Rule ID](#)
- [Fetch the count of Correlation Rules](#)
- [Create Correlation Rules](#)
- [Update Correlation Rule](#)
- [Activate Correlation Rule](#)
- [Deactivate Correlation Rule](#)
- [Delete Correlation Rule](#)

Fetch all Correlation Rules

/fim/v3/autocorrelation/rules/search

[POST]

To search all the Correlation rules.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

attributes (String)	(Optional) The list of comma-separated attributes that you want to include in the response.
filter (String)	(Optional) Filter the correlation rules 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 - scheduleType: DAILY
pageNumber	(Optional) The page number to be returned. The number starts from zero.
pageSize	(Optional) The number of records per page to be included in the response. Default is 10.
sort (String)	(Optional) Sort the results using correlation rule attributes. Example: "sort": "[{\\"ruleName\\":\\"asc\\"}]"

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/autocorrelation/rules/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "pageSize":1,
  "pageNumber":1,
  "filter":"approvalType:`MANUAL` ",
  "sort":"[{\\"ruleName\\":\\"asc\\"}]"
}
```

Response:

```
[  
  {  
    "fixDate": "2020-03-27",  
    "approvalStatus": null,  
    "updatedBy": {  
      "date": 1585289546339  
    },  
    "changeType": null,  
    "approvalType": "MANUAL",  
    "description": "",  
    "reviewers": [  
      "quays_fa"  
    ],  
    "deletedBy": null,  
    "deleted": false,  
    "scheduleType": "ONETIME",  
    "dayOfMonth": null,  
    "createdBy": {  
      "date": 1585289546339  
    },  
    "customerId": "25x14x60-80x1-4x25-8166-6653x4x2x094",  
    "ruleName": "*",  
    "days": [],  
    "startTime": "06:30:00",  
    "dispositionCategory": null,  
    "comment": "",  
    "id": "1xxx7x30-x730-4x94-xx03-xx98x4xx28x1",  
    "endTime": "08:00:00",  
    "filterQuery": "action>Create",  
    "status": "ACTIVATED"  
  }  
]
```

Fetch Correlation Rule Details for a particular Rule ID

/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}

[GET]

To search Correlation rule details for a particular Rule ID

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not found
- 503: Service unavailable

Input Parameters

RuleId	(Required) ID of the correlation rule you want to fetch the details for.
--------	--

Sample:

Request:

```
curl -X GET  
https://<qualys_base_url>/fim/v3/autocorrelation/rules/{autoCorrelationRuleId} -H 'authorization: Bearer <token>' -H 'content-type: application/json'
```

Response:

```
{  
  "customerId": "003x084-643x-x4xx-8336-x2530663x0x2",  
  "id": "479886xx-0xx7-46xx-x00x-1xxx9x07x58x",  
  "ruleName": "dyno_007",  
  "filterQuery": "file.name:yesyes.txt",  
  "description": "",  
  "startTime": "11:32:00",  
  "endTime": "11:33:00",  
  "scheduleType": "DAILY",  
  "days": null,  
  "fixDate": null,  
  "changeType": "MANUAL",  
  "dispositionCategory": "PATCHING",  
  "approvalType": "AUTOMATED",  
  "approvalStatus": "UNAPPROVED",  
  "reviewers": [  
    "quays_hs"
```

```
],  
  "deleted": false,  
  "status": "ACTIVATED",  
  "dayOfMonth": null,  
  "comment": ".",  
  "createdById": null,  
  "createdByName": null,  
  "createdDate": "2020-05-04T05:56:11.497+0000",  
  "updatedById": null,  
  "updatedByName": null,  
  "updatedDate": "2020-05-04T05:56:11.497+0000",  
  "deletedById": null,  
  "deletedByName": null,  
  "deletedDate": null  
}
```

Fetch the count of Correlation Rules

/fim/v3/autocorrelation/rules/count

[POST]

To get the count of Correlation rules.

Response Code

- 200: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

filter (String)	(Optional) Filter the rule 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 - scheduleType: DAILY
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - ruleName
interval (String)	(Optional) 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.
limit	(Optional) Limit the number of rows fetched by the groupBy function.
sort (String)	(Optional) Sort the results using a Qualys token. For example - [{"ruleName": "asc"}]

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/autocorrelation/rules/count -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
```

```
"groupBy": ["approvalType"],  
"limit": 2,  
"filter": "reviewers:quays_fa"  
}
```

Response:

```
{  
    "MANUAL": 105,  
    "AUTOMATED": 10  
}
```

Create Correlation Rules

/fim/v3/autocorrelation/rules/create

[POST]

To create Correlation rules.

Response Code

- 201: Successful
- 401: Unauthorized
- 503: Service unavailable

Input Parameters

ruleName (String)	(Required) The name of the correlation rule. The length should be between 1 to 112 characters.
description (String)	The description for the correlation rule.
filterQuery (String)	(Required) Filter query using Qualys syntax to match the events with the incidents. Refer to the "How to Search" topic in the Online help for assistance with creating your query.
reviewers (String)	(Required) A list of comma separated user names to review the incidents created from the rule.
approvalType	(Required) Approval Type of the Incident created by this rule. Allowed values: "AUTOMATED" or "MANUAL"
approvalStatus	(Required if the Approval Type is Automated) The approval status of the incident created by the rule. Allowed values: "APPROVED", "POLICY_VIOLATION", "UNAPPROVED", "NA".
changeType	(Required if approval type is Automated) Type of Incidents created by the rule. Allowed values: "MANUAL", "AUTOMATED", "COMPROMISE", "OTHER".
comment (String)	(Required if approval type is Automated) Comments for Incidents created by rule.
dispositionCategory	(Required if approval type is Automated). The category of the Incident created by the rule. Allowed values: "PATCHING", "PRE_APPROVED_CHANGE_CONTROL", "CONFIGURATION_CHANGE", "HUMAN_ERROR", "DATA_CORRUPTION", "EMERGENCY_CHANGE", "CHANGE_CONTROL_VIOLATION", "GENERAL_HACKING", "MALWARE"
scheduleType	(Required) The schedule for the rule: Allowed values: "ONETIME", "DAILY", "WEEKLY", "MONTHLY"

startTime	(Required) Time when the Correlation rule must start. Format: "HH:mm:ss" Note: The time must be mentioned in UTC format.
endTime	(Required if Schedule Type is selected as "ONETIME") Time when the Correlation rule should end. Format: "HH:mm:ss". Note: The time must be mentioned in UTC format.
fixDate	(Required if Schedule Type is selected as "ONETIME") The date on which the rule is executed. Format: "yyyy-MM-dd". Note: Value should not be a past date. Note: The date must be mentioned in UTC format.
dayOfMonth	(Required if Schedule Type is selected as "MONTHLY") The days of the month on which rule is executed. Allowed values: integer (1-31).
days	For recurring weekly schedules, it is the list of days on which rule is executed. Allowed values: Allowed values: integer (1-7), where Sunday (1) and Saturday (7). Default value is 1 (Sunday).

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/autocorrelation/rules/create -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Content of request.json:

```
{
  "fixDate": "2020-06-04",
  "approvalStatus": "APPROVED",
  "changeType": "AUTOMATED",
  "approvalType": "AUTOMATED",
  "description": "test",
  "reviewers": [
    "<REVIEWER USERNAME OR EMAIL ID>"
  ],
  "scheduleType": "ONETIME",
  "ruleName": "<CORRELATION RULE NAME>",
  "startTime": "12:00:00",
  "dispositionCategory": "PRE_APPROVED_CHANGE_CONTROL",
  "comment": "<USER COMMENT>",
  "endTime": "23:59:00",
  "filterQuery": "action>Create"
}
```

Response:

```
{  
    "customerId": "<CUSTOMER ID>",  
    "id": "<RULE ID>",  
    "ruleName": "<CORRELATION RULE NAME>",  
    "filterQuery": "action:Create",  
    "description": "<CORRELATION RULE DESCRIPTION>",  
    "startTime": "12:00:00",  
    "endTime": "23:59:00",  
    "scheduleType": "ONETIME",  
    "days": [],  
    "fixDate": "2023-06-04",  
    "changeType": "NORMAL_CHANGE",  
    "dispositionCategory": "DISREGARD_OF_ORGANIZATIONAL_POLICY",  
    "approvalType": "AUTOMATED",  
    "approvalStatus": "PENDING",  
    "reviewers": [  
        "<USERNAME>",  
        "USER EMAIL ID"  
    ],  
    "comment": "<COMMENT>",  
    "createdBy": {  
        "user": {  
            "id": "<USER ID>",  
            "name": "<USER NAME>"  
        },  
        "date": 1671187879859  
    },  
    "updatedBy": {  
        "user": {  
            "id": "<USER ID>",  
            "name": "<USER NAME>"  
        },  
        "date": 1671187879859  
    }  
}
```

Update Correlation Rule

/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/update

[POST]

To update a Correlation rule.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Not found
- 503: Service unavailable

Input Parameters

description (String)	The description for the correlation rule.
reviewers (String)	A list of comma separated user names to review the incidents created from the rule.
approvalType	Approval Type of the Incident created by this rule. Allowed values: "AUTOMATED" or "MANUAL"
approvalStatus	(Required if the Approval Type is Automated) The approval status of the incident created by the rule. Allowed values: "APPROVED", "POLICY_VIOLATION", "UNAPPROVED", "NA".
changeType	(Required if approval type is Automated) Type of Incidents created by the rule. Allowed values: "MANUAL", "AUTOMATED", "COMPROMISE", "OTHER".
comment (String)	(Required if approval type is Automated) Comments for Incidents created by rule.
dispositionCategory	(Required if approval type is Automated). The category of the Incident created by the rule. Allowed values: "PATCHING", "PRE_APPROVED_CHANGE_CONTROL", "CONFIGURATION_CHANGE", "HUMAN_ERROR", "DATA_CORRUPTION", "EMERGENCY_CHANGE", "CHANGE_CONTROL_VIOLATION", "GENERAL_HACKING", "MALWARE"
scheduleType	The schedule for the rule: Allowed values: "ONETIME", "DAILY", "WEEKLY", "MONTHLY" Note: This parameter cannot be updated from: -ONETIME to WEEKLY, MONTHLY, DAILY or -WEEKLY, MONTHLY, DAILY to ONETIME Also, ONETIME Rule cannot be updated after END time is over.

startTime	Time when the Correlation rule must start. Format: "HH:mm:ss" Note: The time must be mentioned in UTC format.
endTime	(Required if Schedule Type is selected as "ONETIME") Time when the Correlation rule should end. Format: "HH:mm:ss" Note: The time must be mentioned in UTC format.
fixDate	(Required if Schedule Type is selected as "ONETIME") The date on which the rule is executed. Format: "yyyy-MM-dd" Note: Its value should not be past date. The date must be mentioned in UTC format.
dayOfMonth	(Required if Schedule Type is selected as "MONTHLY") The days of the month on which rule is executed. Allowed values: integer (1-31).
days	For recurring weekly schedules, it is the list of days on which rule is executed. Allowed values: Allowed values: integer (1-7), where Sunday (1) and Saturday (7). Default value is 1 (Sunday).

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/update -H 'authorization: Bearer <token>' -H
'content-type: application/json' -d @request.json
```

Content of request.json:

```
{
  "fixDate": "2020-06-09",
  "endTime": "13:00:00",
  "startTime": "06:30:00",
  "description": "<DESCRIPTION>",
  "reviewers": [
    "<REVIEWER WHO UPDATED RULE>"
  ]
}
```

Response:

```
{
  "customerId": "<CUSTOMER ID>",
  "id": "RULE ID",
  "ruleName": "Testing_reviewerField",
  "filterQuery": "action>Create",
  "description": "update description",
```

```
"startTime": "06:30:00",
"endTime": "13:00:00",
"scheduleType": "ONETIME",
"days": null,
"fixDate": "2023-06-09",
"changeType": "NORMAL_CHANGE",
"dispositionCategory": "DISREGARD_OF_ORGANIZATIONAL_POLICY",
"approvalType": "AUTOMATED",
"approvalStatus": "PENDING",
"reviewers": [
    "<REVIEWER NAME>",
    "<REVIEWER EMAIL ID>"
],
"deleted": false,
"status": "ACTIVATED",
"dayOfMonth": null,
"comment": "<COMMENT>",
"createdById": "<USER ID>",
"createdByName": "<USERNAME>",
"createdDate": "2022-12-16T10:51:19.859+0000",
"updatedById": "<USER ID>",
"updatedByName": "<USERNAME>",
"updatedDate": "2022-12-16T10:58:29.096+0000",
"deletedById": null,
"deletedByName": null,
"deletedDate": null
}
```

Activate Correlation Rule

`/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/activate`

[POST]

To update the Correlation rule to activate state.

Note: After a Correlation rule is created, it is default in an active state.

Response Code

- 201: Successful
 - 404: Not found
 - 401: Unauthorized
 - 503: Service unavailable

Input Parameters

`autoCorrelationRuleId` (Required) ID of the rule you want to activate.

Sample:

Request:

```
curl -X POST  
https://<qualys_base_url>/fim/v3/autocorrelation/rules/{autoCorrela-  
tionRuleId}/activate -H 'authorization: Bearer <token>' -H  
'content-type: application/json'
```

Response:

```
{  
    "status": "ACTIVATED"  
}
```

Deactivate Correlation Rule

`/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/deactivate`

[POST]

To deactivate auto correlation rule.

Response Code

- 200: Successful
 - 404: Not found
 - 401: Unauthorized
 - 503: Service unavailable

Input Parameters

`autoCorrelationRuleId` (Required) ID of the rule you want to deactivate.

Sample:

Request:

```
curl -X POST  
https://<qualys_base_url>//fim/v3/autocorrelation/rules/{autoCorre  
lationRuleId}/deactivate -H 'authorization: Bearer <token>' -H  
'content-type: application/json'
```

Response:

```
{  
    "status": "DEACTIVATED"  
}
```

Delete Correlation Rule

`/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/delete`

[POST]

To delete Correlation rule.

Response Code

- 200: Successful
 - 404: Not found
 - 401: Unauthorized
 - 503: Service unavailable

Input Parameters

`autoCorrelationRuleId` (Required) ID of the rule you want to delete.

Sample

Request:

```
curl -X POST  
https://<qualys_base_url>/fim/v3/autocorrelation/rules/{autoCorrel  
ationRuleId}/delete -H 'authorization: Bearer <token>' -H  
'content-type: application/json'
```

Response:

```
{  
    "deleted": true  
}
```

FIM Profile APIs

Use these API functions to fetch FIM Profile data.

[Search a Profile](#)

[Activate a Profile](#)

[Assign an Asset to a Profile](#)

[Assign Tags to a Profile](#)

[Export the Profile in XML Format](#)

[Export a Profile in JSON format](#)

[Import a Profile from XML File Inputs](#)

[Import a Profile from JSON File Inputs](#)

[List the Profile Categories](#)

[Deactivate a Profile](#)

[Import Profile from CSV](#)

[Export Profile into CSV](#)

[Bulk Delete Profiles](#)

Search a Profile

/fim/v3/profiles/search

[POST]

To search Profile.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

attributes (String)	(Required) The list of comma-separated attributes that you want to include in the response. By default, all attributes will be returned in the result.
filter (String)	(Required) Filter the Profile rules 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	(Required) The page number to be returned. The number starts from zero.
pageSize	(Required) The number of records per page to be included in the response. Default is 10.
sort (String)	(Required) Sort the results using Profile rule attributes.

Sample:

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/profiles/search -H  
'authorization: Bearer <token>' -H 'content-type:  
application/json' -d @request.json
```

Contents of request.json:

```
{  
    "attributes": "string",  
    "filter": "string",  
    "pageNumber": "number",  
    "pageSize": "number",  
    "sort": "string",  
}
```

Response:

```
{  
    "updatedBy": {  
        "date": 1582023188082,  
        "user": {  
            "name": "John Doe",  
            "id": "x37x1x6x-x023-x948-80xx-2xx6022x3436"  
        }  
    },  
    "assetTagIds": [],  
    "assetIds": [],  
    "type": "LINUX",  
    "version": "1.0",  
    "syncFromId": "00000000-0000-0001-0000-000000000001",  
    "deletedBy": null,  
    "deleted": false,  
    "importRegistryRules": false,  
    "registryProfile": false,  
    "createdBy": {  
        "date": 1581935157993,  
        "user": {  
            "name": "John Doe",  
            "id": "x37x1x6x-x023-x948-80xx-2xx6022x3436"  
        }  
    },  
    "name": "Linux testing FIM-3387 ",  
    "customerId": "x5x0514x-x211-x1x4-809x-x3x2xx667xxx",  
    "id": "x444920x-81xx-4xx6-x018-x44b0xx2xx22",  
    "category": {  
        "name": "PCI",  
        "id": "2xxx5022-2xxx-11x7-93xx-92361f002671"  
    },  
    "syncType": "NOT_APPLICABLE",  
    "status": "DEACTIVATED"  
}
```

Activate a Profile

/fim/v3/profiles/{profileId}/activate

[POST]

To activate a Profile

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Profile not found
- 409: Conflict if the profile is activated.
- 500: Internal Server error

Input Parameters

profileId	(Required) ID of the profile that is to be activated.
-----------	---

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/activate -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
    "status": "ACTIVATED"
}
```

Assign an Asset to a Profile

/fim/v3/profiles/{profileId}/assets

[POST]

To assign an asset to a Profile.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

assetIdsForProfile	(Required) The UUID of the asset you want to assign to the profile.
--------------------	---

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/assets -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "assetIdsForProfile": [
    "asset uuid 1", "asset uuid2"
  ]
}
```

Response:

```
{
  "assetsAdded": true
}
```

Assign Tags to a Profile

/fim/v3/profiles/{profileId}/assettags

[POST]

To assign a tag to a Profile.

Note: Using this API, only tags that contain FIM activated assets can be assigned to profile.

Response Code

- 200: Successful
- 400: Profile ID does not exist
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

assetTagIdsForProfile	(Required) List of asset tag ids to which you want to assign to the profiles.
-----------------------	---

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/assettags -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "assetTagIdsForProfile": [
    "tag id 1", "tag id 2"
  ]
}
```

Response:

```
{
  "assetTagsAdded": true
}
```

Export the Profile in XML Format

/fim/v3/profiles/{profileId}/exportxml

[POST]

To export the Profile in XML format.

Response Code

- 200: Successful
- 400: Profile ID does not exist
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

profileId	(Required) The ID for the profile that needs to be exported.
-----------	--

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/exportxml -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
<?xml version="1.0" encoding="UTF-8"?>
<profile>
  <id>20x213xx-xx2x-44x0-xxx3-x95940x49x62</id>
  <name>FIM-2998 windows</name>
  <version>1.0</version>
  <description />
  <type>WINDOWS</type>
  <category>
    <id>9xx0154x-70x8-4807-90xx-xxxxx6xx59xx</id>
    <name>PCI</name>
  </category>
  <rules>
    <rule>
      <id>32xxx356-xx8x-4334-x972-33x6x428xx79</id>
      <type>directory</type>
      <imagePath>C:\\Windows\\System32\\</imagePath>
      <description>Rule Description</description>
```

```
<recursiveDepth>2</recursiveDepth>
<notifyFor>
    <directory>
        <notify>rename</notify>
        <notify>modifyMetadata</notify>
        <notify>delete</notify>
        <notify>modifySecuritySettings</notify>
        <notify>create</notify>
    </directory>
    <file>
        <notify>rename</notify>
        <notify>modifyContent</notify>
        <notify>delete</notify>
        <notify>modifyMetadata</notify>
        <notify>create</notify>
        <notify>modifySecuritySettings</notify>
    </file>
</notifyFor>
<inclusions>
    <inclusion>
        <objectType>file</objectType>
        <patterns>
            <pattern>C:\Windows\*.txt</pattern>
        </patterns>
    </inclusion>
</inclusions>
<exclusions>
    <exclusion>
        <objectType>file</objectType>
        <patterns>
            <pattern>C:\Windows\*.log</pattern>
        </patterns>
    </exclusion>
</exclusions>
<severity>3</severity>
<name>Rule Name 2</name>
</rule>
<rule>
    <id>32xxx356-xx8x-4334-x972-33x6x428xx78</id>
    <type>key</type>

    <imagePath>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run</imagePath>
    <description>
    </description>
    <recursiveDepth>2</recursiveDepth>
```

```
<notifyFor>
    <directory/>
    <file/>
    <key>
        <notify>rename</notify>
        <notify>delete</notify>
        <notify>create</notify>
        <notify>modifySecuritySettings</notify>
    </key>
    <value>
        <notify>delete</notify>
        <notify>modifyContent</notify>
    </value>
</notifyFor>
<inclusions>
    <inclusion>
        <objectType>key</objectType>
        <patterns>
            <pattern>childkey</pattern>
        </patterns>
    </inclusion>
    <inclusion>
        <objectType>value</objectType>
        <patterns>
            <pattern>childvalue</pattern>
        </patterns>
    </inclusion>
</inclusions>
<exclusions/>
<severity>3</severity>
<name>Registry Rule</name>
</rule>
<rule>
    <id>32xxx356-xx8x-4334-x972-33x6x428xx87</id>
    <type>value</type>

<imagePath>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run</imagePath>
    <description>
    </description>
    <notifyFor>
        <directory/>
        <file/>
        <key/>
        <value>
            <notify>delete</notify>
```

```
    <notify>modifyContent</notify>
    </value>
  </notifyFor>
  <inclusions/>
  <exclusions/>
  <severity>3</severity>
  <name>Registry Rule 2</name>
  <valueName>TeamsMachineInstaller</valueName>
</rule>
</rules>
</profile>
```

Export the Profile in JSON Format

/fim/v3/profiles/{profileId}/exportjson

[POST]

To export the profile in JSON format.

Response Code

- 200: Successful
- 400: Profile ID does not exist
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

profileId	(Required) The ID for the profile that needs to be exported.
-----------	--

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/exportjson -
H 'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
  "id": "20x213xx-xx2x-44x0-xxx3-x95940x49x62",
  "name": "FIM-2998 windows",
  "version": "1.0",
  "description": "Profile Description",
  "type": "WINDOWS",
  "category": {
    "id": "9xx0154x-70x8-4807-90xx-xxxxx6xx59xx",
    "name": "PCI 1"
  },
  "rules": [
    {
      "id": "32xxx356-xx8x-4334-x972-33x6x428xx79",
      "type": "directory",
      "imagePath": "C:\\Windows",
      "description": "",
      "recursiveDepth": "2",
      "order": 1
    }
  ]
}
```

```
"notify": {  
    "directory": [  
        "rename",  
        "modifyMetadata",  
        "delete",  
        "modifySecuritySettings",  
        "create"  
    ],  
    "file": [  
        "rename",  
        "modifyContent",  
        "delete",  
        "modifyMetadata",  
        "create",  
        "modifySecuritySettings"  
    ]  
},  
"monitorOwnership": false,  
"inclusionFilter": [  
    {  
        "objectType": "file",  
        "patterns": [  
            "C:\\Windows\\*.txt"  
        ]  
    },  
    {  
        "objectType": "file",  
        "patterns": [  
            "C:\\Windows\\*.log"  
        ]  
    }  
],  
"exclusionFilter": [],  
"severity": 3,  
"name": "Rule 1"  
},  

```

```
        "delete"
    ],
    "file": [
        "delete"
    ]
},
"monitorOwnership": false,
"inclusionFilter": [
{
    "objectType": "file",
    "patterns": [
        "C:\\Windows\\*.txt"
    ]
},
{
    "objectType": "file",
    "patterns": [
        "C:\\Windows\\*.log"
    ]
}
],
"exclusionFilter": [],
"severity": 3,
"name": "Rule 2"
},
{
    "id": "140d87a6-5065-4eb9-8640-7c92665788e6",
    "type": "key",
    "imagePath":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\Cu
rrentVersion\\Run",
    "description": "Description",
    "recursiveDepth": "2",
    "notify": {
        "directory": [],
        "file": [],
        "key": [
            "rename",
            "delete",
            "create",
            "modifySecuritySettings"
        ],
        "value": [
            "delete",
            "modifyContent"
        ]
    }
}
```

```
        },
        "monitorOwnership": false,
        "inclusionFilter": [
            {
                "objectType": "key",
                "size": null,
                "operator": null,
                "attribute": null,
                "patterns": [
                    "childkey"
                ]
            },
            {
                "objectType": "value",
                "size": null,
                "operator": null,
                "attribute": null,
                "patterns": [
                    "childvalue"
                ]
            }
        ],
        "exclusionFilter": [],
        "severity": 3,
        "name": "Registry Rule"
    },
    {
        "id": "6b9aeadb-9204-42ab-afc4-231cd1dec8c3",
        "type": "value",
        "imagePath": "HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\Run",
        "description": "Description",
        "notify": {
            "directory": [],
            "file": [],
            "key": [],
            "value": [
                "delete",
                "modifyContent"
            ]
        },
        "monitorOwnership": false,
        "inclusionFilter": [],
        "exclusionFilter": [],
        "severity": 3,
```

```
        "name": "Registry Rule 2",
        "valueName": "TeamsMachineInstaller"
    }
]
}
```

Import a Profile from XML File Inputs

/fim/v3/profiles/importxml

[POST]

To create a profile from XML inputs.

Response Code

- 201: Successful
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

name (String)	The name of the profile.
description (String)	Description of the profile.
category.id	The ID of the category.
category.name	Name of the Category
type	Type of profile. Example: WINDOWS or LINUX.
rules.rule.type	Type of the Rule. Example: file/directory/key/value
rules.severity	Severity of Rule. Allowed values 1,2,3,4,5
rules.rule.imagePath	Path on the asset which needs to be monitored.
rules.rule.description	Description of the Rule.
rules.rule.recursiveDepth	Depth of directory we need to monitor. Allowed values: 1,2,3,4,5,6,7,8,9,None,All
rules.rule.valueName	If Type of the Rule is Value. Allowed Registry key value name.
rules.rule.notifyFor.directory	List of directory attributes which needs to be monitored. Allowed values: create, delete, rename, modifyMetadata ,modifySecuritySettings
rules.rule.notifyFor.file	List of file attributes which needs to be monitored. Allowed values - create, delete, rename, modifyContent, modifyMetadata, modifySecuritySettings
rules.rule.notifyFor.key	List of key attributes which needs to be monitored. Allowed values: create, delete, rename, modifySecuritySettings
rules.rule.notifyFor.value	List of value attributes which needs to be monitored. Allowed values: delete,modifyContent

rules.rule.inclusions.inclusion. objectType	Type of the object that needs to be in inclusion Filter of the rule. file/directory/key/value
rules.rule.inclusions.inclusion. patterns	List of paths to be added as inclusion filters For example: C:\System32*.log
rules.rule.exclusions.exclusion. objectType	Type of the object that needs to be added in exclusion Filter of the rule. file/directory/key/value
rules.rule.exclusions.exclusion. patterns	List of paths to be added in exclusion filters. For example: C:\System32*.log

Sample:Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/profiles/importxml -H 'authorization: Bearer <token>' -H 'content-type: application/json' -d @request.json
```

Contents of request.json:

```
<?xml version=""1.0"" encoding=""UTF-8""?>
<profile>
    <id>20x213xx-xx2x-44x0-xxx3-x95940x49x62</id>
    <name>FIM-2998 windows</name>
    <version>1.0</version>
    <description />
    <type>WINDOWS</type>
    <category>
        <id>9xx0154x-70x8-4807-90xx-xxxxx6xx59xx</id>
        <name>PCI</name>
    </category>
    <rules>
        <rule>
            <type>directory</type>
            <imagePath>C:\\Windows\\System32\\</imagePath>
            <description>Rule Description</description>
            <recursiveDepth>2</recursiveDepth>
            <notifyFor>
                <directory>
                    <notify>rename</notify>
                    <notify>modifyMetadata</notify>
                    <notify>delete</notify>
                    <notify>modifySecuritySettings</notify>
                    <notify>create</notify>
                </directory>
            </notifyFor>
        </rule>
    </rules>
</profile>
```

```
<file>
    <notify>rename</notify>
    <notify>modifyContent</notify>
    <notify>delete</notify>
    <notify>modifyMetadata</notify>
    <notify>create</notify>
    <notify>modifySecuritySettings</notify>
</file>
</notifyFor>
<inclusions>
    <inclusion>
        <objectType>file</objectType>
        <patterns>
            <pattern>C:\Windows\*.txt</pattern>
        </patterns>
    </inclusion>
</inclusions>
<exclusions>
    <exclusion>
        <objectType>file</objectType>
        <patterns>
            <pattern>C:\Windows\*.log</pattern>
        </patterns>
    </exclusion>
</exclusions>
<severity>3</severity>
<name>Rule Name 2</name>
</rule>
<rule>
    <id>32xxx356-xx8x-4334-x972-33x6x428xx78</id>
    <type>key</type>

<imagePath>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run</imagePath>
    <description>Rule Description</description>
    <recursiveDepth>2</recursiveDepth>
    <notifyFor>
        <directory/>
        <file/>
        <key>
            <notify>rename</notify>
            <notify>delete</notify>
            <notify>create</notify>
            <notify>modifySecuritySettings</notify>
        </key>
        <value>
```

```
<notify>delete</notify>
<notify>modifyContent</notify>
</value>
</notifyFor>
<inclusions>
<inclusion>
<objectType>key</objectType>
<patterns>
<pattern>childkey</pattern>
</patterns>
</inclusion>
<inclusion>
<objectType>value</objectType>
<patterns>
<pattern>childvalue</pattern>
</patterns>
</inclusion>
</inclusions>
<exclusions/>
<severity>3</severity>
<name>Registry Rule</name>
</rule>
<rule>
<id>32xxx356-xx8x-4334-x972-33x6x428xx87</id>
<type>value</type>

<imagePath>HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run</imagePath>
<description>
</description>
<notifyFor>
<directory/>
<file/>
<key/>
<value>
<notify>delete</notify>
<notify>modifyContent</notify>
</value>
</notifyFor>
<inclusions/>
<exclusions/>
<severity>3</severity>
<name>Registry Rule 2</name>
<valueName>TeamsMachineInstaller</valueName>
</rule>
</rules>
```

```
</profile>
```

Import a Profile from JSON File Inputs

/fim/v3/profiles/importjson

[POST]

To create a profile from JSON file inputs.

Response Code

- 201: Successful
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Input Parameters

name (String)	The name of the profile.
type	Type of profile. Example: WINDOWS or LINUX.
category.id	The ID of the category.
category.name	Name of the Category
description (String)	Description of the profile.
rules.name	Name of the rule.
rules.description	Description of the rule
rules.type	Type of the Rule. Example: file/directory/key/value
rules.imagePath	Path which needs to be monitored.
rules.recursiveDepth	In case of directory rule, depth of directory we want to monitor. Allowed values: 1,2,3,4,5,6,7,8,9,None,All
rules.severity	Severity of Rule. Allowed values 1,2,3,4,5
rules.valueName	If Type of the Rule is Value. Allowed Registry key value name
rules.notify.directory	List of directory attributes that needs to be monitored. Allowed values: create, delete, rename, modifyMetadata, modifySecuritySettings.
rules.notify.file	List of file attributes that needs to be monitored. Allowed values: create, delete, rename, modifyContent, modifyMetadata,modifySecuritySettings.
rules.notify.key	List of value attributes which needs to be monitored. Allowed values: delete,modifyContent

rules.notify.value	List of key attributes which needs to be monitored. Allowed values: create, delete, rename, modifySecuritySettings
rules.inclusionFilter.objectType	Type of the object which needs to be in inclusion Filter of the rule. file/directory/key/value
rules.inclusionFilter.patterns	List of paths to be added as inclusion filters For example: C:\System32*.txt
rules.exclusionFilter.objectType	Type of the object which needs to be in exclusion filter of the rule. file/directory/key/value
rules.exclusionFilter.patterns	List of paths to be added as exclusion filters. For example:C:\System32*.log

Sample:

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/profiles/importjson
-H 'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{
  "name": "Profile name",
  "type": "WINDOWS",
  "category": {
    "id": "string",
    "name": "string"
  },
  "description": "Profile Description",
  "rules": [
    {
      "name": "Rule Name",
      "description": "string",
      "type": "file",
      "imagePath": "string",
      "recursiveDepth": "Nine",
      "severity": 2,
      "notify": {
        "directory": [
          "rename",
          "delete",
          "create",
          "modifyMetadata",
          "modifySecuritySettings"
        ],
        "key": [
          "create",
          "delete",
          "modifyMetadata"
        ]
      }
    }
  ]
}
```

```
"file": [
    "rename",
    "delete",
    "create",
    "modifyMetadata",
    "modifyContent",
    "modifySecuritySettings"
],
"key": [],
"value": []
},
"inclusionFilter": [
{
    "objectType": "file",
    "patterns": [
        "C:\\Windows\\*.txt"
    ]
}
],
"exclusionFilter": [
{
    "objectType": "file",
    "patterns": [
        "C:\\Windows\\*.log"
    ]
}
]
},
{
    "type": "key",
    "imagePath":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\Cu
rrentVersion\\Run",
    "description": "",
    "recursiveDepth": "2",
    "notify": {
        "directory": [],
        "file": [],
        "key": [
            "rename",
            "delete",
            "create",
            "modifySecuritySettings"
        ],
        "value": [
            "delete",
            "create"
        ]
    }
}
]
```

```
        "modifyContent"
    ]
},
"inclusionFilter": [
{
    "objectType": "key",
    "patterns": [
        "childkey"
    ]
},
{
    "objectType": "value",
    "patterns": [
        "childvalue"
    ]
}
],
"exclusionFilter": [
{
    "objectType": "key",
    "patterns": [
        "excludechildkey"
    ]
}
],
"severity": 3,
"name": "Registry Rule"
},
{
    "type": "value",
    "imagePath":
"HKEY_LOCAL_MACHINE\\SOFTWARE\\WOW6432Node\\Microsoft\\Windows\\CurrentVersion\\Run",
    "description": "Rule description",
    "notify": {
        "directory": [],
        "file": [],
        "key": [],
        "value": [
            "delete",
            "modifyContent"
        ]
    },
    "severity": 3,
    "name": "Registry Rule 2",
    "valueName": "TeamsMachineInstaller"
```

```
    }  
]  
}
```

List the Profile Categories

/fim/v3/categories/search

[POST]

To search the categories of Profile.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Profile not found
- 500: Internal Server error

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/fim/v3/categories/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Contents of request.json:

```
[
  {
    "id": "2xxx5022-2xxx-11x7-93xx-92361x002671",
    "name": "PCI",
    "createdBy": {
      "user": {
        "id": "2xxx5270-2xxx-11x7-93xx-92361x002671",
        "name": "System"
      },
      "date": 1493813100000
    },
    "system": true,
    "deleted": false
  },
  {
    "id": "2xxb5374-2xxx-11x7-93xx-92361x002671",
    "name": "HIPAA",
    "createdBy": {
      "user": {
        "id": "2xxx5270-2xxx-11x7-93xx-92361x002671",
        "name": "System"
      },
      "date": 1493813100000
    }
  }
]
```

```
    } ,  
    "system": true,  
    "deleted": false  
}  
]  
.
```

Deactivate a Profile

/fim/v3/profiles/{profileId}/deactivate

[POST]

To deactivate a Profile.

Response Code

- 200: Successful
- 401: Unauthorized
- 404: Profile not found
- 409: Conflict if profile is already deactivated.
- 500: Internal Server error

Input Parameters

profileId	(Required) ID of the profile which needs to be deactivated.
-----------	---

Sample:

Request:

```
curl -X POST
https://<qualys_base_url>/fim/v3/profiles/{profileId}/deactivate -
H 'authorization: Bearer <token>' -H 'content-type:
application/json'
```

Response:

```
{
    "status": "DEACTIVATED"
}
```

Import Profile from CSV

/fim/v3/profiles/importcsv

[POST]

Import monitoring profile from CSV.

Response Code

- 400 : Profile does not exist
- 200 : Success
- 401 : Unauthorized

Input Parameters

Parameter	Mandatory/Optional	Data Type	Description
file	Mandatory	CSV	Provide the name of the CSV file that contains all the information related to monitoring profile.
Authorization	Mandatory	String	Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken
forceUpdate	Optional	Boolean	Provide the value as "true" only if you want to update your existing profile.

Sample 1:

API Request:

```
curl -X POST '<qualys_base_url>/fim/v3/profiles/importcsv' -H
'Authorization: Bearer <JWT Token>' -H 'Content-Type:
multipart/form-data ; boundary=---
WebKitFormBoundary7MA4YWxkTrZu0gW' -F 'file=@"csvFileName.csv"'
```

Response:

```
{
  "BAD DATA" : {
    "<profilename_1>" : "profile name contains invalid character. Only
alpha numeric characters, space, '-', '_' are allowed."
  },
  "FAILED" : {},
  "SUCCESS" : {
    "<profilename_2>" : "Profile created successfully"
  }
}
```

```
        }  
    }
```

Sample 2:

API Request:

```
"curl X POST""<qualys_base_url>/fim/v3/profiles/importcsv""-  
H""Authorization:Bearer <JWT Token>" -H 'Content-Type:  
multipart/form-data ; boundary=--  
WebKitFormBoundary7MA4YWxkTrZu0gW' -F ''csvFileName.csv'' --form  
'forceUpdate="true"'
```

Response:

```
{  
    "BAD DATA" : {},  
    "FAILED" : {},  
    "SUCCESS" :  
    {  
        "Import No Restrictions Profile" : "Profile updated successfully"  
    }  
}
```

Export Profile into CSV

/fim/v3/profiles/exportcsv

[POST]

Export monitoring profile into CSV.

Response Code

- 200 : Success
- 401 : Unauthorized
- 500 : Server error

Input Parameters

Parameter	Mandatory/Optional	Data Type	Description
profileUUID	Mandatory	String	Provide the profile UUID to be exported as the CSV file. You can provide multiple profile UUIDs.
csv_filename	Mandatory	String	Provide the CSV file name where the profile data/details are exported.
Authorization	Mandatory	String	Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample:

API Request:

```
curl -X POST '<qualys_base_url>/fim/v3/profiles/exportcsv' -H
'Authorization: Bearer <JWT token>' -H 'Content-Type: application/json' -
-data-raw '[
    "<profileUUID_01>","<profileUUID_02>"
]' -k -o <csv_fileName.csv>
```

Response:

The CSV file is created according to the name and path you provided in your API request.

Note: Only one CSV is generated for all given profile UUIDs.

Bulk Delete Profiles

/fim/v3/profiles/delete

[DELETE]

This API deletes one or multiple profiles.

Response Code

- 207 : Multi-Status
- 201 : Successfully deleted profiles.
- 400 : Bad Request : When User sends bad data in request body.

Input Parameters

Parameter	Mandatory/Optional	Data Type	Description
profileIdsToDelete	Mandatory	String	Provide the profile UUID to delete the respective profile. You can provide multiple profile UUIDs too.
Authorization	Mandatory	String	Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample:

API Request:

```
curl -X DELETE '<qualys_base_url>/fim/v3/profiles/delete -H
'authorization: Bearer <JWT Token>' -H 'content-type: application/json' -
d '{"profileIdsToDelete": ["<profileUUID_01>","<profileUUID_02>"]}'
```

Response:

```
{
    "BAD DATA" : {},
    "FAILED" : {},
    "SUCCESS" : {
        "<profileUUID_01>" : "Profile successfully deleted",
        "<profileUUID_02>" : "Profile successfully deleted"
    }
}
```

FIM Assets API

Use these API functions to fetch FIM Asset data.

[Search Assets](#)

[Count the Assets](#)

Search Assets

/fim/v3/assets/search

[POST]

To search Assets based on a criteria.

Response Code

- 200: Successful
- 400: Bad Request
- 500: Internal Server error

Input Parameters

Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken
attributes (String)	(Optional) The list of comma-separated attributes that you want to include in the response. By default, all attributes will be returned in the result.
filter (String)	(Optional) Filter the Assets 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 - operatingSystem:'Microsoft Windows 10'
pageNumber	(Optional) The page number to be returned. The number starts from zero.
pageSize	(Optional) The number of records per page to be included in the response. Default is 10.
includeTagData	(Optional) Set the flag to "true" if you want the tags related information in the response. Else, set it to false.
searchAfter	(Optional) This parameter is required to fetch more than 10,000 rows.
notSentEventsForHours	(Optional) List those assets that have not sent any events in last "<enter value>" hours. This integer input e.g 10.
sort (String)	(Optional) Sort the results using Asset rule attributes.

Sample:

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/assets/search -H
'authorization: Bearer <token>' -H 'content-type:
application/json' -d @request.json
```

Contents of request.json:

```
{  
    "attributes": "name,manifest.status,operatingSystem",  
    "filter": "agentUuid:`fef2f2e0-636d-4d20-b68b-2c2967a9da5d`"  
}
```

Response:

```
[  
    {  
        "sortValues": [],  
        "data": {  
            "manifest": {  
                "status": "FIM_MANIFEST_APPLIED_SUCCESS"  
            }  
        },  
        "  
            "name": "FIM_API_AUTOMATION",  
            "id": "fef2f2e0-636d-4d20-b68b-2c2967a9da5d",  
            "operatingSystem": "Microsoft Windows 7 Professional  
6.1.7601 64-bit Service Pack 1 Build 7601"  
        }  
    }  
]
```

Count the Assets

/fim/v3/assets/count

[POST]

To count the assets based on a criteria.

Response Code

- 200: Successful
- 400: Bad Request
- 500: Internal Server error

Input Parameters

Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken
filter (String)	(Optional) Filter the Assets 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 - operatingSystem:'Microsoft Windows 10'
groupBy (String)	(Optional) Group results based on certain parameters (provide comma separated list). For example - operatingSystem
interval (String)	(Optional) 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.
limit (String)	(Optional) Limit the number of rows fetched by the groupBy function.
sort (String)	(Optional) Sort the results using a Qualys token. For example - [\"operatingSystem\":\"asc\"]

Sample:

Request:

```
curl -X POST https://<qualys_base_url>/fim/v3/assets/count -H  
'authorization: Bearer <token>' -H 'content-type:  
application/json' -d @request.json
```

Contents of request.json:

```
{  
    "filter": "interfaces.address:10.112.113.114",  
    "limit": 5,  
    "groupBy" : ["manifest.status"]  
}
```

Response:

```
{  
    "FIM_MANIFEST_PUBLISHED": 20010,  
    "FIM_ACTIVATION_REQUEST_RECEIVED": 10027  
}
```