File Integrity Monitoring API

User Guide

Version 1.9

March 18, 2019

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

Table of Contents

Preface **4**
About Qualys 4
Contact Qualys Support 4

Chapter 1 - Welcome **5**
Qualys API Framework 5
Introduction to FIM API Paradigm 7

Chapter 2 - FIM Events API **8**
Fetch events 8
Get event count 11
Fetch event details 12

Chapter 3 - Ignored FIM Events API **15**
Fetch ignored events 15
Get ignored events count 17
Fetch ignored event details 18

Chapter 4 - FIM Incidents API **21**
Fetch incidents 21
Fetch events for an incident 23
Get event count for an incident 26
Get incident count 27

Preface

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

About Qualys

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

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

Contact Qualys Support

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

Chapter 1 - Welcome

Welcome to File Integrity Monitoring API.

Get Started

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

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

Get API Notifications

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

From our Community

Join our Community

API Notifications RSS Feeds

Qualys API Framework

The Qualys File Integrity Monitoring API uses the following framework.

Request URL

The URL for making API requests respects the following structure:

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

where the components are described below.

<baseurl>	The Qualys API server URL that you should use for API requests depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: https://gateway.qg1.apps.qualys.com
<module>	The API module. For the FIM API, the module is: “fim”.
<object>	The module specific object.
<object_id>	(Optional) The module specific object ID, if appropriate.
<operation>	The request operation, such as count.

Base URL to the Qualys API Server

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

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

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

Introduction to FIM API Paradigm

Authentication

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

For example,

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

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

- **username** and **password** are the credentials of the user account for which you want to fetch FIM data

- **token** should be true

- **Content-Type** should be "application/x-www-form-urlencoded"

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

Using Curl

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

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

The following Curl options are used according to different situations:

Option	Description
-G	The GET method is required for all FIM API requests.
-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.

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

curl -G "https://gateway.qg1.apps.qualys.com/fim/v1/incidents" -H "Authorization: Bearer <token>"

Chapter 2 - FIM Events API

Use these API functions to fetch FIM event data.

Fetch events

Get event count

Fetch event details

Fetch events

/fim/v1/events

[GET]

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'
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
incidentContext (Boolean)	Search within incidents. Default is false.
incidentIds (String)	List of incident IDs to be included while searching for events in incidents.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G --data-urlencode "incidentContext=false" --data-urlencode
"pageSize=1" "https://gateway.qg1.apps.qualys.com/fim/v1/events" -
H "Authorization: Bearer <token>"
```

Response:


```
[
  {
    "dateTime": "2019-02-26T10:16:28.163+0000",
    "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\Temp\\8F621E57-A9B6-410E-
B396-EC0BDCCC5C0C\\API-MS-Win-security-provider-L1-1-0.dll",
    "severity": 5,
    "profiles": [
      {
        "name": "Windows Profile - PCI John",
        "rules": [
          {
            "severity": 5,
            "description": null,
            "id": "82531aac-a627-40bd-9a13-201a0917217e",
            "type": "directory"
          }
        ],
        "id": "0d0a12f7-6472-4288-b126-aab5e8328ebf",
        "type": "WINDOWS",
        "category": {
          "name": "PCI",
          "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
        }
      }
    ],
    "type": "File",
    "changedAttributes": [
      2
    ],
    "platform": "WINDOWS",
    "oldContent": null,
    "actor": {
      "process": "powershell.exe",
      "processID": 7108,
      "imagePath":
"\\Device\\HarddiskVolume2\\WINDOWS\\system32\\WindowsPowerShell\\
v1.0\\powershell.exe",
      "userName": "NT AUTHORITY\\SYSTEM",
      "userID": "S-1-5-18"
    },
    "newContent": null,
    "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
    "name": "API-MS-Win-security-provider-L1-1-0.dll",
```

```
    "action": "Create",
    "id": "c1e96d55-cdef-37ac-973b-f23bf9b0238b",
    "asset": {
      "agentId": "efee083e-1da3-41f4-b814-58871c16da45",
      "interfaces": [
        {
          "hostname": null,
          "macAddress": "00-00-00-00-00-00-00-E0",
          "address": "fe80:0:0:0:28c5:194e:f58c:b413",
          "interfaceName": "Teredo Tunneling Pseudo-Interface"
        },
        {
          "hostname": "SHISHU-WIN10-VM",
          "macAddress": "00:50:56:AA:DC:C1",
          "address": "10.115.75.236",
          "interfaceName": "Intel(R) 82574L Gigabit Network
           Connection"
        }
      ],
      "lastCheckedIn": "2019-02-22T02:40:47.000Z",
      "created": 1529296486000,
      "hostId": null,
      "operatingSystem": "Microsoft Windows 10 Pro 10.0.16299 N/A
        Build 16299",
      "tags": [
        "7509812",
        "7509619"
      ],
      "assetType": "HOST",
      "system": {
        "lastBoot": "2019-02-18T17:42:08.000Z"
      },
      "ec2": null,
      "lastLoggedOnUser": ".\\Administrator",
      "netbiosName": "SHISHU-WIN10-VM",
      "name": "SHISHU-WIN10-VM",
      "agentVersion": "2.0.6.1",
      "updated": 1529635248743
    },
    "class": "Disk"
  }
]
```

Get event count

/fim/v1/events/count

[GET]

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'
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 Note: An interval lower than a second is not supported.
incidentContext (Boolean)	Search within incidents. Default is false.
incidentIds (String)	List of incident IDs to be included while searching for events in incidents.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G --data-urlencode "incidentContext=false" --data-urlencode
"groupBy=action"
"https://gateway.qg1.apps.qualys.com/fim/v1/events/count" -H
"Authorization: Bearer <token>"
```

Response:

```
{
"Rename": 9030024, "Attributes": 541520, "Delete": 340857,
"Create": 265141, "Security": 189813, "Content": 29497
}
```

Fetch event details

/fim/v1/events/{eventId}

[GET]

Fetch details for an event.

Input Parameters

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

Sample

Request:

```
curl -G
"https://gateway.qg1.apps.qualys.com/fim/v1/events/c1e96d55-cdef-
37ac-973b-f23bf9b0238b" -H "Authorization: Bearer <token>"
```

Response:

```
{
"dateTime": "2019-02-15T15:09:00.023+0000",
"fullPath": "\\Device\\HarddiskVolume2\\Windows\\System32\\sru
SRU.log ",
"severity": 3,
"profiles": [{
  "name": "Just Test",
  "rules": [{
    "severity": 3,
    "number": 6,
    "name": "name 2",
    "description": "",
    "section": {
      "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
      "id": "733ef4ff-0d4c-4124-8b07-6cc5098e0356",
      "name": "section 001",
      "profileId": "d4fe6f29-b798-4637-ae15-ea40bc5b8de9",
      "references": [{
        "links": [
          "test.abc",
          "test2.abc"
        ],
       "description": "test ref"
```

```
      }],
      "deleted": false,
      "categoryId": "4e4d7131-a96a-4427-9c68-d444413e4904",
      "createdBy": {
        "date": 1543225080098
      },
      "updatedBy": {
        "date": 1543225080098
      }
    },
    "id": "b16c97ad-ef21-46c7-8a4d-428b71d36189",
    "type": "directory"
  }],
  "id": "d4fe6f29-b798-4637-ae15-ea40bc5b8de9",
  "type": "WINDOWS",
  "category":
  {
    "name": "test0",
    "id": "aed6533e-f110-4b9b-b586-7777cbc0ea07"
  }
}],
"type": "File",
"changedAttributes": null,
"platform": "WINDOWS",
"oldContent": null,
"actor":
{
  "process": "svchost.exe",
  "processID": 3016,
  "imagePath":
  "\\Device\\HarddiskVolume2\\windows\\system32\\
    svchost.exe",
  "userName": "NT AUTHORITY\\LOCAL SERVICE",
  "userID": "S-1-5-19"
},
"newContent": null,
"customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
"name": "SRU.log",
"action": "Content",
"id": "e29a283d-39bf-397b-9044-a9004b5941f8",
"asset": {
  "agentId": "47a9921f-c0e2-4663-9c31-a109dfaf2bf8",
  "interfaces": [

    {
      "hostname": "FIMTEST1",
```

```
      "macAddress": "00:50:56:AA:75:71",
      "address": "10.115.78.231",
      "interfaceName": "Intel(R) 82574L Gigabit Network Connection"
    }
],
  "lastCheckedIn": "2019-02-14T07:35:23.000Z",
  "created": "2019-02-21T11:09:33.000+0000",
  "hostId": "12042",
  "operatingSystem": "Microsoft Windows 10 Pro 10.0.17134 N/A
    Build 17134",
   "tags": [
     "7509619",
     "7538812"
  ],
  "assetType": "HOST",
  "system":

  {
    "lastBoot": "2019-02-28T21:18:33.000Z"
  },
  "ec2": null,
  "lastLoggedOnUser": ".
  Administrator ",
  "netbiosName": "FIMTEST1",
  "name": "FIMTESTab",
  "agentVersion": "2.0.6.1",
  "updated": "2019-02-14T07:35:23.949+0000"
 },
 "incidentId": "fe19d6c2-27e2-4096-bd62-a8798d9f0673",
 "class": "Disk"
}
```

Chapter 3 - 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/v1/events/ignore

[GET]

Get FIM events that are ignored.

Input Parameters

filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z']
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G "https://gateway.qg1.apps.qualys.com/fim/v1/events/ignore"
-H "Authorization: Bearer <token>"
```

Response:

```
[
  {
    "dateTime": "2019-02-14T18:29:22.668+0000",
    "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\ServiceProfiles\\LocalService
\\AppData\\Local\\lastalive1.dat",
```

```
    "severity": 4,
    "profiles": [
      {
        "name": "UW_FIM_Profile",
        "rules": [
          {
            "severity": 4,
            "description": null,
            "id": "06fedb6f-47f0-4edf-94c2-b08fd92f2c75",
            "type": "directory"
          }
        ],
        "id": "1cbdf2f2-f9b3-4d94-a22c-07945aa9507b",
        "type": "WINDOWS",
        "category": {
          "name": "PCI",
          "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
        }
      }
    ],
    "type": "File",
    "changedAttributes": null,
    "platform": "WINDOWS",
    "oldContent": null,
    "actor": {
      "process": "svchost.exe",
      "processID": 660,
      "imagePath":
"\\Device\\HarddiskVolume2\\Windows\\System32\\svchost.exe",
      "userName": "NT AUTHORITY\\LOCAL SERVICE",
      "userID": "S-1-5-19"
    },
    "newContent": null,
    "ignoreDate": "2019-02-13",
    "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
    "name": "lastalive1.dat",
    "action": "Delete",
    "id": "e442fd5c-0c11-3b0d-b927-62e1c9e1f870",
    "asset": {
      "agentId": "e8a3cbf5-f617-4d58-a975-f40bc29daac2",
      "interfaces": [
        {
          "hostname": "WIN-890BLRMESC6",
          "macAddress": "00:50:56:AA:F6:02",
          "address": "10.115.74.175",
          "interfaceName": "Intel(R) 82574L Gigabit Network
```

```
            Connection"
          }
        ],
        "lastCheckedIn": "2019-02-14T09:05:09.000Z",
        "created": 1534229941000,
        "hostId": "12029",
       "operatingSystem": "Microsoft Windows Server 2012 R2 Standard
          6.3.9600 N/A Build 9600",
        "tags": [
          "7532413",
          "7509619"
        ],
        "assetType": "HOST",
        "system": {
          "lastBoot": "2019-02-07T11:30:11.000Z"
        },
        "ec2": null,
        "lastLoggedOnUser": "administrator",
        "netbiosName": "WIN-890BLRMESC6",
        "name": "UW_WIN-2012_SERV",
        "agentVersion": "2.2.0.40",
        "updated": 1534242468684
      },
      "class": "Disk"
    }
  ]
```


Get ignored events count

/fim/v1/events/ignore/count

[GET]

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'
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 Note: An interval lower than a second is not supported.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G
"https://gateway.qg1.apps.qualys.com/fim/v1/events/ignore/count" -
H "Authorization: Bearer <token>"
```

Response:

```
{
  "count": 31
}
```

Fetch ignored event details

/fim/v1/events/ignore/{ignoredEventId}

[GET]

Fetch details for an ignored event.

Input Parameters

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

Sample

Request:

```
curl -G
"https://gateway.qg1.apps.qualys.com/fim/v1/events/ignore/e442fd5c
-0c11-3b0d-b927-62e1c9e1f870" -H "Authorization: Bearer <token>"
```

Response:


```
{
  "dateTime": "2019-02-14T18:29:22.668+0000",
  "fullPath":
"\\Device\\HarddiskVolume2\\Windows\\ServiceProfiles\\LocalService
\\AppData\\Local\\lastalive1.dat",
  "severity": 4,
  "profiles": [
    {
      "name": "UW_FIM_Profile",
      "rules": [
        {
          "severity": 4,
          "description": null,
          "id": "06fedb6f-47f0-4edf-94c2-b08fd92f2c75",
          "type": "directory"
        }
      ],
      "id": "1cbdf2f2-f9b3-4d94-a22c-07945aa9507b",
      "type": "WINDOWS",
      "category": {
        "name": "PCI",
        "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
      }
    }
  ],
  "type": "File",
  "changedAttributes": null,
  "platform": "WINDOWS",
  "oldContent": null,
  "actor": {
    "process": "svchost.exe",
    "processID": 660,
    "imagePath":
"\\Device\\HarddiskVolume2\\Windows\\System32\\svchost.exe",
    "userName": "NT AUTHORITY\\LOCAL SERVICE",
    "userID": "S-1-5-19"
  },
  "newContent": null,
  "ignoreDate": "2019-02-13",
  "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
  "name": "lastalive1.dat",
  "action": "Delete",
  "id": "e442fd5c-0c11-3b0d-b927-62e1c9e1f870",
```

```
  "asset": {
    "agentId": "e8a3cbf5-f617-4d58-a975-f40bc29daac2",
    "interfaces": [
      {
        "hostname": "WIN-890BLRMESC6",
        "macAddress": "00:50:56:AA:F6:02",
        "address": "10.115.74.175",
        "interfaceName": "Intel(R) 82574L Gigabit Network
         Connection"
      }
    ],
    "lastCheckedIn": "2019-02-14T09:05:09.000Z",
    "created": 1534229941000,
    "hostId": "12029",
    "operatingSystem": "Microsoft Windows Server 2012 R2 Standard
6.3.9600 N/A Build 9600",
    "tags": [
      "7532413",
      "7509619"
    ],
    "assetType": "HOST",
    "system": {
      "lastBoot": "2019-02-07T11:30:11.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": "administrator",
    "netbiosName": "WIN-890BLRMESC6",
    "name": "UW_WIN-2012_SERV",
    "agentVersion": "2.2.0.40",
    "updated": 1534242468684
  },
  "class": "Disk"
}
```

Chapter 4 - FIM Incidents API

Use these API functions to fetch FIM incident data.

Fetch incidents

Fetch events for an incident

Get event count for an incident

Get incident count

Fetch incidents

/fim/v1/incidents

[GET]

Get FIM incidents for an user account.

Input Parameters

filter (String)	Filter the incidents list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z']
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
attributes (String)	Search based on certain attributes (provide comma separated list).
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G "https://gateway.qg1.apps.qualys.com/fim/v1/incidents" -H
"Authorization: Bearer <token>"
```

Response:


```
[
  {
    "approvalStatus": null,
    "dateTime": "2019-02-03T18:30:00.000+0000",
    "lastUpdatedBy": {
      "date": 1541396385773,
      "user": {
        "name": "John Doe",
        "id": "b888f3e6-9956-d7be-8354-bc49e6df4daf"
      }
    },
    "filterToDate": "2019-02-04T18:29:59.999+0000",
    "approvalDate": null,
    "assignDate": "2019-02-04T08:43:01.687+0000",
    "changeType": null,
    "approvalType": "MANUAL",
    "filters": [
      "dateTime: ['2019-02-03T18:30:00.000Z'..'2019-02-
       04T18:29:59.999Z'] and action:\"Security\""
    ],
    "reviewers": [
      "quays_dr"
    ],
    "deleted": false,
    "filterFromDate": "2019-02-03T18:30:00.000+0000",
    "createdBy": {
      "date": 1538642581681,
      "user": {
        "name": "John Doe",
        "id": "b888f3e6-9956-d7be-8354-bc49e6df4daf"
      }
    },
    "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
    "name": "Security incident",
    "comment": "patch\n",
    "dispositionCategory": null,
    "id": "4989f531-ce9d-4d35-a4c8-1edcdd1d1ce6",
    "status": "REOPENED"
  }
]
```

Fetch events for an incident

/fim/v1/incidents/{incidentId}/events

[GET]

Get events logged under an incident.

Input Parameters

incidentId (String)	(Required) ID of the incident you want to fetch the events for.
filter (String)	Filter the events list by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z']
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.
sort (String)	Sort the results using a Qualys token. For example - [{\"action\":\"asc\"}]
attributes (String)	Search based on certain attributes (provide comma separated list).
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G --data-urlencode "pageSize=1"
"https://gateway.qg1.apps.qualys.com/fim/v1/incidents/4989f531-
ce9d-4d35-a4c8-1edcdd1d1ce6/events" -H "Authorization: Bearer
<token>"
```

Response:

```
[
  {
    "dateTime": "2019-02-10T10:11:35.009+0000",
    "fullPath": "\\Device\\HarddiskVolume2\\Program Files
(x86)\\Google\\Chrome\\Application\\68.0.3440.106\\Locales",
    "severity": 5,
    "profiles": [
      {
        "name": "My Test Recommended Baseline for Windows OS",
        "rules": [
```

```
            {
              "severity": 5,
              "description": null,
              "id": "13a8f363-cdc1-4d7a-a978-c1dc3dca6cad",
              "type": "directory"
            }
          ],
          "id": "c3a98bb0-4217-4ccd-9ea5-f5f5366453b3",
          "type": "WINDOWS",
          "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
          }
        },
        {
          "name": "My Test Minimum Baseline for PCI for Windows OS",
          "rules": [
            {
              "severity": 5,
              "description": null,
              "id": "b30eb36f-2921-40da-aad5-a5849695cea5",
              "type": "directory"
            }
          ],
          "id": "faa130d3-37b5-4d7b-bca8-2cab9fc0b552",
          "type": "WINDOWS",
          "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
          }
        }
      ],
      "type": "Directory",
      "changedAttributes": [
        1
      ],
      "platform": "WINDOWS",
      "oldContent": null,
      "actor": {
        "process": "setup.exe",
        "processID": 15220,
        "imagePath":
"\\Device\\HarddiskVolume2\\WINDOWS\\TEMP\\CR_7C2AD.tmp\\setup.exe
",
        "userName": "NT AUTHORITY\\SYSTEM",
        "userID": "S-1-5-18"
```

```
  },
  "newContent": null,
  "customerId": "f59b9543-51f8-7130-83c6-b8a2fd457509",
  "name": "Locales",
  "action": "Security",
  "id": "582f946a-44b0-388b-9605-74a23a37f893",
  "asset": {
    "agentId": "47a9921f-c0e2-4663-9c31-a109dfaf2bf8",
    "interfaces": [
      {
        "hostname": "FIMTEST1",
        "macAddress": "00:50:56:AA:75:71",
        "address": "10.115.78.231",
        "interfaceName": "Intel(R) 82574L Gigabit Network
         Connection"
      }
    ],
    "lastCheckedIn": "2019-02-10T10:21:52.000Z",
    "created": 1529579373000,
    "hostId": "12042",
    "operatingSystem": "Microsoft Windows 10 Pro 10.0.17134 N/A
     Build 17134",
    "tags": [
      "7509619",
      "7523616",
      "7526812",
      "7523614",
      "7523615",
      "7509812",
      "7529412"
    ],
    "assetType": "HOST",
    "system": {
      "lastBoot": "2019-02-29T16:49:24.000Z"
    },
    "ec2": null,
    "lastLoggedOnUser": ".\\Administrator",
    "netbiosName": "FIMTEST1",
    "name": "FIMTESTabc",
    "agentVersion": "2.0.6.1",
    "updated": 1536574912853
  },
  "incidentId": "4989f531-ce9d-4d35-a4c8-1edcdd1d1ce6",
  "class": "Disk"
}]
```

Get event count for an incident

/fim/v1/incidents/{incidentId}/events/count

[GET]

Get number of events logged for an incident.

Input Parameters

incidentId (String)	(Required) ID of the incident you want to fetch the events for.
filter (String)	Filter the incidents list by providing a query using Qualys syntax. Refer to the "How to Search" topic in the online help for assistance with creating your query. For example - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] AND action: 'Content'
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]
interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d Note: An interval lower than a second is not supported.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G
"https://gateway.qg1.apps.qualys.com/fim/v1/incidents/4989f531-
ce9d-4d35-a4c8-1edcdd1d1ce6/events/count" -H "Authorization:
Bearer <token>"
```

Response:

```
{
  "count": 339
}
```

Get incident count

/fim/v1/incidents/count

[GET]

Get number of incidents in an user account.

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 - dateTime:['2019-02-25T18:30:00.000Z'..'2019-02-26T18:29:59.999Z'] AND action: 'Content'
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - action
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{\"dateTime\":\"asc\"}]
interval (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d Note: An interval lower than a second is not supported.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample

Request:

```
curl -G
"https://gateway.qg1.apps.qualys.com/fim/v1/incidents/count" -H
"Authorization: Bearer <token>"
```

Response:

```
{
  "count": 9
}
```