Qualys File Integrity Monitoring

API Release Notes

Version 3.7.1

June 30, 2023 (Updated on 28 July 2023)

Qualys File Integrity Monitoring API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

Introduced Two Fields in FIM Events APIs

New Add-on Fields in Response of Event Search APIs

Added Validation on Event Count for Manual Incident API

Qualys API URL

Qualys FIM supports both API server URLs and API gateway URLs for API requests.

The Qualys API server or gateway 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 Additional Values in Input Parameters in Approve the Given Incident API

This documentation uses the API URL for Qualys US Platform 2 (https://gateway.qg2.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

Introduced Two Fields in FIM Events APIs

APIs affected	/fim/v2/events/search /fim/v2/events/ignore/search /fim/v2/events/count /fim/v2/events/ignore/count /fim/v2/incidents/{incidentId}/events/count /fim/v2/incidents/{incidentId}/events/search
Method	POST
New or Updated APIs	Updated

We have introduced two fields for event search and event count APIs. Using the additional fields, you can now filter the events based on changes made in the attributes of a file or directory.

Input Parameters

Following are the newly supported values for the 'filter' parameter:

Parameter	Mandatory/Optional	Data Type	Description
file.attribute.hidden	Optional	String	Displays attribute event for file or directory for which hidden attribute is checked or unchecked.
file.attribute.readonly	Optional	String	Displays attribute event for file or directory for which readonly attribute is checked or unchecked.

For details of existing parameters refer to FIM API user guide

New Add-on Fields in Response of Event Search APIs

APIs affected	/fim/v2/events/search /fim/v2/events/ignore/search /fim/v2/incidents/{incidentId}/events/search
Method	POST
New or Updated APIs	Updated

We have added new fields in the response of event search and event count APIs. The fields are volumeID, fileID, securitySettings, fileContentHashOld, size, attributes, permissions, ownerShip, group, and fileAttribute. With these fields user can see the data of Event Detail in search.

Note: The values in bold indicate the new value added for the fields.

Sample: Fetch Events API

API Request:

```
curl -X POST
https://<QualysBaseURL>/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:

```
{
    {
        "sortValues": [],
        "data": {
            "dateTime": "2023-06-28T06:18:50.548+0000",
           "fullPath": "C:\\CR_FIM_TEST\\All_Machines\\wmplayer -
Copy (4).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": "622d5688-6880-38fb-8ca8-1a1700d6f2ea",
            "class": "Disk",
```

```
            "fileID": "0xb400002ad30",
            "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": "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"
        }
    }
]
```

Sample: Fetch Ignored Events API

API Request:

```
curl -X POST
https://<QualysBaseURL>/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": "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": "2023-06-14T06:21:45.685+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
        }
    }
]
```

Sample: Get Event Count API

API Request:

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

Sample: Get Ignored Events Count API

API Request:

```
curl -X POST
https://<QualysBaseURL>/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

}
```

Sample: Get Event Count for an Incident API

Request:

```
curl -X POST
https://<QualysBaseURL>/fim/v2/incidents/{incidentI
d}/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
}
```

Sample: Fetch Events for an Incident API

API Request:

```
curl -X POST
https://<QualysBaseURL>/fim/v2/incidents/{incidentI
d}/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": "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": "2023-06-28T06:24:41.347+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,
"fileContentHashOld": null,
"size": null,
"name": "wmplayer - Copy (6) - Copy.exe",
"fileContentHash": null,
```

```
            "volumeID": "0xa2121916",
            "reputationStatus": null,
            "newRegistryValueContent": null,
            "attributes": {
                "newAttribute": [
                    "Archive",
                    "Hidden",
                    "Read Only"
                ],
                "oldAttribute": null
            },
            "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"
```

```
            }
        }
    ]
```

Added Validation on Event Count for Manual Incident API

APIs affected	/fim/v3/incidents/create
Method	POST
New or Updated APIs	Updated

We noticed performance issues due to an unrestricted count of events in manual incident. Additionally, it affected the processing of FIM events on the platform. Therefore we added limitation on the number of events while creating manual incident. With this release, manual incident can be created with up to 100k events.