Qualys File Integrity Monitoring v2.x

API Release Notes

Version 2.0.2

December 19, 2019

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

What's New

Filtering events by processed time

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.

Filtering events by processed time

APIs affected	/fim/v2/events/search /fim/v2/events/{eventId} /fim/v2/events/ignore/search /fim/v2/events/ignore/{ignoredEventId}
New or Updated APIs	Updated

You can use the processedTime filter to fetch all events processed at Qualys within a certain time duration.

Usually a time lag occurs between the time the events are generated on the asset and the time when they get processed at Qualys. You now have the option to filter events either based on the time they are generated on the asset (dateTime) or based on the time they are processed at Qualys (processedTime).

Note: Processed time is available only for newly generated events.

Sample 1 - Fetch FIM events based on the processed time

Events are fetched for the processedTime duration provided in the API request.

Request:

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

Contents of request.json

```
{
    "pageSize": 2,
    "pageNumber":0,
    "sort": "[{\"processedTime\": \"asc\"}, {\"id\": \"desc\"}]",
    "filter": "processedTime: ['2019-11-20T00:00:00Z'..'2019-11-
    20T23:59:59Z']"
}
```

Response:

```
[
  {
    "sortValues": [
      1574224099908,
      "b9f095e3-a872-3445-989b-1943f5a1e9b1"
    ],
    "index": "fim_003b9084-643f-f4af-8336-b2530663a0b2",
```

```
    "type": "fim",
    "shardId": 0,
    "node": null,
    "matchedQueries": null,
    "data": {
      "dateTime": "2019-11-20T04:28:06.942+0000",
      "fullPath":
"\\Device\\HarddiskVolume2\\Users\\Public\\Documents\\profile_test\\Secur
ity",
      "severity": 3,
      "profiles": [
        {
          "name": "New 001",
          "rules": [
            {
              "severity": 3,
              "number": 2,
              "name": "New rule 34",
              "description": "asdsd",
              "section": null,
              "id": "ab619d60-38ac-465a-bcef-0d0c9723dfb5",
              "type": "directory"
            }
          ],
          "id": "b8c1c229-8a9a-4de3-895e-e6f4bb4fe247",
          "type": "WINDOWS",
          "category": {
            "name": "PCI",
            "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
          }
        }
      ],
      "type": "Directory",
      "changedAttributes": null,
      "platform": "windows",
      "oldContent": null,
      "processedTime": "2019-11-20T04:28:19.908+0000",
      "actor": {
        "process": "DllHost.exe",
        "processID": 2684,
        "imagePath":
"\\Device\\HarddiskVolume2\\Users\\Public\\Documents\\profile_test\\DllHo
st.exe",
        "userName": "john_doe",
        "userID": "S-1-5-21-3910453560-944185229-3986553578-500"
      },
      "newContent": null,
      "customerId": "003b9084-643f-f4af-8336-b2530663a0b2",
      "name": "Security",
```

```
      "action": "Create",
      "id": "b9f095e3-a872-3445-989b-1943f5a1e9b1",
      "asset": {
        "agentId": "435ca55c-9b63-4795-b32a-462ff96a4f9c",
        "interfaces": [],
        "lastCheckedIn": null,
        "created": "2019-10-23T09:14:31.056+0000",
        "hostId": null,
       "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A Build
        10586",
        "tags": [],
        "assetType": "HOST",
        "system": {
          "lastBoot": null
        },
        "ec2": null,
        "lastLoggedOnUser": "",
        "netbiosName": "WIN10-121",
        "name": "WIN10-121",
        "agentVersion": null,
        "updated": "2019-10-23T09:14:31.120+0000"
      },
      "incidentId": null,
      "class": "Disk"
    }
  },
  {
    "sortValues": [
      1574224099908,
      "400c6805-8eb4-37db-b304-8e7817551e73"
    ],
    "index": "fim_003b9084-643f-f4af-8336-b2530663a0b2",
    "type": "fim",
    "shardId": 0,
    "node": null,
    "matchedQueries": null,
    "data": {
      "dateTime": "2019-11-20T04:28:06.969+0000",
      "fullPath":
"\\Device\\HarddiskVolume2\\Users\\Public\\Documents\\profile_test\\8F621
E57-A9B6-410E-B396-EC0BDCCC5C0C\\security_run.dll",
      "severity": 3,
      "profiles": [
        {
          "name": "New 001",
          "rules": [
            {
              "severity": 3,
              "number": 2,
```

```
        "name": "New rule 34",
        "description": "asdsd",
        "section": null,
        "id": "ab619d60-38ac-465a-bcef-0d0c9723dfb5",
        "type": "directory"
      }
    ],
    "id": "b8c1c229-8a9a-4de3-895e-e6f4bb4fe247",
    "type": "WINDOWS",
    "category": {
      "name": "PCI",
      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
    }
  }
],
"type": "File",
"changedAttributes": null,
"platform": "windows",
"oldContent": null,
"processedTime": "2019-11-20T04:28:19.908+0000",
"actor": {
  "process": "DllHost.exe",
  "processID": 2684,
  "imagePath":
   "\\Device\\HarddiskVolume2\\WINDOWS\\system32\\DllHost.exe",
  "userName": "john_doe",
  "userID": "S-1-5-21-3910453560-944185229-3986553578-500"
},
"newContent": null,
"customerId": "003b9084-643f-f4af-8336-b2530663a0b2",
"name": "security_run.dll",
"action": "Rename",
"id": "400c6805-8eb4-37db-b304-8e7817551e73",
"asset": {
  "agentId": "435ca55c-9b63-4795-b32a-462ff96a4f9c",
  "interfaces": [],
  "lastCheckedIn": null,
  "created": "2019-10-23T09:14:31.056+0000",
  "hostId": null,
  "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A Build
  10586",
  "tags": [],
  "assetType": "HOST",
  "system": {
    "lastBoot": null
  },
  "ec2": null,
  "lastLoggedOnUser": "",
  "netbiosName": "WIN10-121",
```

```
        "name": "WIN10-121",
        "agentVersion": null,
        "updated": "2019-10-23T09:14:31.120+0000"
      },
      "incidentId": null,
      "class": "Disk"
    }
  }
]
```


Sample 2 - Fetch Ignored event details

API response shows the processedTime.

Request:

```
curl -X GET
https://gateway.qg1.apps.qualys.com/fim/v2/events/ignore/ab619d60-38ac-
465a-bcef-0d0c9723dfb5 -H 'authorization: Bearer <token>' -H
'content-type: application/json'
```

Contents of request.json

```
{
    "pageSize": 2,
    "pageNumber":0,
    "sort": "[{\"processedTime\": \"asc\"}, {\"id\": \"desc\"}]",
    "filter": "processedTime: ['2019-11-20T00:00:00Z'..'2019-11-
    20T23:59:59Z']"
}
```

Response:


```
[
{

  "dateTime": "2019-11-18T11:15:57.271+0000",
  "fullPath":
"\\Device\\HarddiskVolume2\\Users\\Public\\Documents\\profile_test\\test2
9",
  "severity": 3,
  "profiles": [
    {
      "name": "New 001",
      "rules": [
        {
          "severity": 3,
          "number": 2,
          "name": "New rule 34",
```

```
        "description": "",
        "section": null,
        "id": "ab619d60-38ac-465a-bcef-0d0c9723dfb5",
        "type": "file"
      }
    ],
    "id": "b8c1c229-8a9a-4de3-895e-e6f4bb4fe247",
    "type": "WINDOWS",
    "category": {
      "name": "PCI",
      "id": "2dab5022-2fdd-11e7-93ae-92361f002671"
    }
  }
],
"type": "Directory",
"changedAttributes": null,
"platform": "windows",
"oldContent": null,
"processedTime": "2019-11-18T05:45:58.448+0000",
"actor": {
  "process": "DllHost.exe",
  "processID": 2684,
  "imagePath":
   "\\Device\\HarddiskVolume2\\WINDOWS\\system32\\DllHost.exe",
  "userName": "john_doe",
  "userID": "S-1-5-21-3910453560-944185229-3986553578-500"
},
"newContent": null,
"ignoreDate": "2019-11-18",
"customerId": "003b9084-643f-f4af-8336-b2530663a0b2",
"name": "test29",
"action": "Create",
"id": "a9413638-451b-3caf-8053-b2168a765960",
"asset": {
  "agentId": "435ca55c-9b63-4795-b32a-462ff96a4f9c",
  "interfaces": [],
  "lastCheckedIn": null,
  "created": "2019-10-23T09:14:31.056+0000",
  "hostId": null,
  "operatingSystem": "Microsoft Windows 10 Pro 10.0.10586 N/A Build
   10586",
  "tags": [],
  "assetType": "HOST",
  "system": {
    "lastBoot": null
  },
  "ec2": null,
  "lastLoggedOnUser": "",
  "netbiosName": "WIN10-121",
```

```
    "name": "WIN10-121",
    "agentVersion": null,
    "updated": "2019-10-23T09:14:31.120+0000"
  },
  "incidentId": null,
  "class": "Disk"
}
]
```