Qualys Endpoint Detection and Response v3.x

API Release Notes

Version 3.0

November 30, 2023

Qualys Endpoint Detection and Response API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

Paginate Search Results Using SearchAfter API

Retrieve Asset Details using Asset API

Block Malicious Host using BlockFeature API

Quarantine or Kill File or Process Using Remediation API

URL to the Qualys API Server

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.

Paginate Search Results Using SearchAfter API

APIs affected	/ioc/events/searchAfter /ioc/incidents/searchAfter /ioc/incidents/events/searchAfter
New or Updated APIs	New
Operator	GET
DTD or XSD changes	No

Use this API to retrieve a large number of the search results in smaller sections or batches.

Input Parameters for Fetch Events

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
fromDate	Optional	String	fromDate parameter lists events logged after a certain date. It supports epoch time or Unix timestamp. **For example:** 1483228800 **Note:** This parameter is used in conjunction with the "toDate" parameter to fetch events for a specific date. Time value is not considered in this parameter. Use the filter parameter to further filter by applying the time value.
toDate	Optional	String	toDate parameter lists events that are logged until a certain date. It supports epoch time or Unix timestamp. **For example:** 1514764799 **Note:** This parameter is used in conjunction with the "fromDate" parameter to fetch events for a specific date. Time value is not considered in this parameter. Use the filter parameter to further filter by applying the time value.

Parameter	Mandatory/ Optional	Format	Description
filter	Optional	String	The filter parameter filters the events list by providing a query using the Qualys syntax. **For example:** event.dateTime : ['2017-01-01T05:33:34' .. '2017-01- 31T05:33:34'] AND action: 'Created' For more information see EDR Online Help. You can filter events based on the time they are generated on the asset (event.dateTime) or based on the time they are processed at Qualys Cloud Platform (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date AND time.
pageNumber	Optional	String	The pageNumber parameter returns the page to be returned. It starts from the value zero.
pageSize	Optional	String	The pageSize parameter mentions the number of records per page to be included in the response. The default value is 10.
include_attributes	Optional	String	include_attribute parameter includes certain attributes in the search. The search results generated are provided using a comma-separated list. The API response fetches only the included attributes. **For example:** include_attributes = _type, _id, processName
exclude_attributes	Optional	String	exclude_attribute parameter excludes certain attributes from the search. The search results generated are provided using a comma-separated list. **For example:** exclude_attributes = _type, _id, processName **Note:** You need not exclude attributes if you have included specific attributes using the include_attributes parameter. Attributes that are not included are by default excluded.
searchAfterValues	Optional	Array	The searchAfterValues sort the values in array format. **For example:** value1,value2 **Note:** This parameter is only for the next request. You will be able to get these values from previous request's header.

Sample - Fetch Events Using SearchAfter

API request:

```
curl -X GET "<qualys_base_url>/ioc/events/searchAfter" --header "accept:
*/*" --header "Authorization: Bearer <token>"
```

Response:


```
[
    {
     "dateTime": "2023-10-02T00:00:12.299+0000",
     "eventProcessedTime": "2023-10-01T23:58:06.530+0000",
     "file": {
         "fullPath":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000001\\S-1-5-21-3853312163-935010464-3409451040-500-
Keyboard.reg",
         "extension": "reg",
         "fileName": "S-1-5-21-3853312163-935010464-3409451040-500-
Keyboard.reg",
         "sha256":
"X1XXbc0834586XX785df94a468ab7d6XXXXX320df08a9a60f1eXXXXb95c529XX",
         "writeDate": "2023-10-01T23:59:58.018+0000",
         "macroEmbedded": false,
         "path":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000001",
         "createdDate": "2023-10-01T23:59:58.018+0000",
         "size": 4848,
         "accessDate": "2023-10-01T23:59:58.018+0000",
         "nonPEFile": true,
         "fileType": "Registration Entries",
         "md5": "aXX30a3XX7ebf6376XXb4325af2daXXX"
     },
     "eventSource": "EDR",
     "action": "CREATED",
     "indicator2": [
         {
          "sha256":
"X1XXbc0834586XX785df94a468ab7d6XXXXX320df08a9a60f1eXXXXb95c529XX",
          "verdict": "UNKNOWN",
          "rowId": "-3516754699100620536"
         }
     ],
     "id": "RTF_c58XXX14-5cXX-3f47-9XXX-dXXX675588XX_2-10-2023",
     "type": "FILE",
     "asset": {
         "fullOSName": "Microsoft Windows 10 Pro 10.0.18362 Build 18362",
```

```
          "hostName": "PN-POD1-RD",
          "agentId": "eXX6820d-6XXe-XXa2-a458-6833XX88bXX7",
          "interfaces": [
           {
            "macAddress": "xx:50:xx:xx:xx:BE",
            "ipAddress": "10.xx.xx.210",
            "interfaceName": "Intel(R) 82574L Gigabit Network Connection",
            "gatewayAddress": "10.xx.xx.1"
           }
          ],
          "netBiosName": "PN-POD1-RD",
          "isQuarantineHost": false,
          "platform": "Windows",
          "assetType": "HOST",
          "tags": [
           {
            "name": "Cloud Agent",
            "uuid": "XXe676XX-XX78-4fXX-XX5f-6XXX0bc2XX1b"
           },
           {
            "name": "Dynamic One",
            "uuid": "6aXXfeaX-4XXe-4XX9-82XX-46XX132dXXX6"
           },
           {
            "name": "DynamicTag",
            "uuid": "XXX788fX-fXX4-XX3b-abXX-XX2d85X08XX8"
           }
          ]
     },
     "uniqueId": "-3516754699100620536"
    },
    {
     "dateTime": "2023-10-02T00:00:12.627+0000",
     "eventProcessedTime": "2023-10-01T23:58:06.531+0000",
     "file": {
         "fullPath":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000000\\S-1-5-21-3853312163-935010464-3409451040-1001-
CTF.reg",
         "extension": "reg",
         "fileName": "S-1-5-21-3853312163-935010464-3409451040-1001-
CTF.reg",
         "sha256":
"X1XXbc0834586XX785df94a468ab7d6XXXXX320df08a9a60f1eXXXXb95c529XX",
         "writeDate": "2023-10-02T00:00:03.939+0000",
         "macroEmbedded": false,
         "path":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000000",
```

```
          "createdDate": "2023-10-02T00:00:03.939+0000",
          "size": 10926,
          "accessDate": "2023-10-02T00:00:03.939+0000",
          "nonPEFile": true,
          "fileType": "Registration Entries",
          "md5": "dXXfc2071c05828XXX93b2XXX62bbXXX"
      },
      ...
           {
            "name": "Dynamic One",
"uuid": "6aXXfeaX-4XXe-4XX9-82XX-46XX132dXXX6"
           },
           {
            "name": "DynamicTag",
            "uuid": "XXX788fX-fXX4-XX3b-abXX-XX2d85X08XX8"
           }
          ]
      },
      "uniqueId": "-6530935410104234747"
     },
{
      "dateTime": "2023-10-02T00:00:12.799+0000",
      "score": "0",
      "scoreSource": "REVERSING_LAB",
      ..
      },
      "uniqueId": "-8065662183459215061"
     },
     {
      "dateTime": "2023-10-02T00:00:12.361+0000",
      "eventProcessedTime": "2023-10-01T23:58:07.467+0000",
      "file": {
          "fullPath":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000001\\S-1-5-21-3853312163-935010464-3409451040-500-
CTF.reg",
          "extension": "reg",
          "fileName": "S-1-5-21-3853312163-935010464-3409451040-500-
CTF.reg",
          .. [
           {
            "name": "Cloud Agent",
            "uuid": "XXe676XX-XX78-4fXX-XX5f-6XXX0bc2XX1b"
           },
           {
            "name": "Dynamic One",
            "uuid": "6aXXfeaX-4XXe-4XX9-82XX-46XX132dXXX6"
           },
           {
```

```
            "name": "DynamicTag",
            "uuid": "XXX788fX-fXX4-XX3b-abXX-XX2d85X08XX8"
           }
          ]
     },
     "uniqueId": "2520718635903176326"
    }
]
```


Next API Request:

```
curl -X GET
"<qualys_base_url>/ioc/events/searchAfter?searchAfterValues=1696204830256
,RTF_XX87dc71-bXXX-3XXX-8940-c297XXXf3c57_2-10-2023" --header "accept:
*/*" --header "Authorization: Bearer <token>"
```

Response:


```
[
    {
     "dateTime": "2023-10-02T00:00:12.768+0000",
     "score": "0",
     "scoreSource": "REVERSING_LAB",
     "eventProcessedTime": "2023-10-01T23:58:07.467+0000",
     "file": {
         "fullPath":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000002\\S-1-0-0-Keyboard.reg",
         "extension": "reg",
         "fileName": "S-1-0-0-Keyboard.reg",
         "sha256":
"X1XXbc0834586XX785dfxxxxab7d6XXXXX320df08a9a60f1eXXXXb95c529XX",
         "writeDate": "2023-10-02T00:00:09.533+0000",
         "macroEmbedded": false,
         "path":
"C:\\$WINDOWS.~BT\\Work\\MachineIndependent\\Working\\agentmgr\\CCSIAgent
\\005A4BDD\\USER00000002",
         "createdDate": "2023-10-02T00:00:09.533+0000",
         "size": 2662,
         "accessDate": "2023-10-02T00:00:09.533+0000",
         "nonPEFile": true,
         "fileType": "Registration Entries",
         "md5": "d60xxxxx556axxxxxxa9e3f10b"
     },
     "eventSource": "EDR",
     "action": "CREATED",
     "indicator2": [
         {
          "score": "0",
```

```
          "sha256":
"X1XXbc0834586XX785df94a468ab7d6XXXXX320df08a9a60f1eXXXXb95c529XX",
          "verdict": "KNOWN",
          "rowId": "-696544353557563093"
         }
     ],
     "id": "RTF_XXX84f19-XXXf-30XX-a2XX-43dXXXb1eXX7_2-10-2023",
     "type": "FILE",
     "asset": {
         "fullOSName": "Microsoft Windows 10 Pro 10.0.18362 Build 18362",
         "hostName": "<host_name>",
 "agentId": "eXX6820d-6XXe-XXa2-a458-6833XX88bXX7",
            "interfaces": [
                {
                 "macAddress": "00:xx:56:xx:31:xx",
                 "ipAddress": "10.xx.xx.210",
                 "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                 "gatewayAddress": "10.113.226.1"
                }
            ],
            "netBiosName": "<net_bios_name>",
            "isQuarantineHost": false,
            "platform": "Windows",
            "assetType": "HOST",
            "tags": [
                {
                 "name": "Cloud Agent",
                 "uuid": "XXe676XX-XX78-4fXX-XX5f-6XXX0bc2XX1b"
                },
                {
                 "name": "Dynamic One",
                 "uuid": "6aXXfeaX-4XXe-4XX9-82XX-46XX132dXXX6"
                },
                {
                 "name": "DynamicTag",
                 "uuid": "XXX788fX-fXX4-XX3b-abXX-XX2d85X08XX8"
                }
            ]
        },
        "uniqueId": "-696544353557563093"
    },
    ..
]
```

Sample - Fetch Incidents Using SearchAfter

API Request:

```
curl -X GET "<qualys_base_url>/ioc/incidents/searchAfter" --header
"accept: */*" --header "Authorization: Bearer <token>
```

Response:


```
[
    {
     "hostName": "<host_name>",
     "agentId": "XX76XXXa-bab5-4XXe-95XX-9XXX2eeXX66X",
     "malwareFamilies": [
         null,
         "Heur.BZC.PZQ.Boxter.919.2F8E3E9D"
     ],
     "sha256":
"XX953a4XXXcfd39d7b7XXX8d92e9a8fXX849d52c64036c2f6XXXfb2XX5a52XXX",
     "malwareCategories": [
         null,
         "VIRUS"
     ],
     "eventSource": "Anti-malware",
     "fileEventCount": 1,
     "operatingSystem": "Microsoft Windows 10 Enterprise 10.0.19045 Build
19045",
     "detectedOn": "2023-08-10T07:31:47.000+0000",
     "scoreSource": "Anti-malware",
     "mutexEventCount": 0,
     "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
     "riskScore": 9,
     "id": "XXc42aXX-03XX-XXdd-aXX8-42fXXXd7cXXX",
     "behavior": 0,
     "incidentStatus": "CLOSED",
     "networkEventCount": 0,
     "registryEventCount": 0,
     "updatedOn": "2023-08-10T08:21:28.719Z",
     "userName": "Unassigned",
     "eventTypes": [
         "FILE",
         "PROCESS"
     ],
     "sha256Set": [
         null,

"XX953a4XXXcfd39d7b7XXX8d92e9a8fXX849d52c64036c2f6XXXfb2XX5a52XXX"
     ],
     "incidentId": "XXc42aXX-03XX-XXdd-aXX8-42fXXXd7cXXX",
```

```
     "exploit": 0,
     "incidentNumber": 21657,
     "incidentDescription": "Heur.BZC.PZQ.Boxter.919.2F8E3E9D",
     "processEventCount": 1
    },
..
]
```


Next API Request:

```
curl -X GET "<qualys_base_url>/ioc/incidents/searchAfter
?pageSize=50&searchAfterValues= 1691705672299,XdeXX9Xe-50XX-XX24-b4XX-
dXX2XX187XdX" --header "accept: */*" --header "Authorization: Bearer
<token>"
```

Response:


```
[
    {
     "hostName": "DESKTOP-2KJTVJO",
     "agentId": "XX76XXXa-bab5-4XXe-95XX-9XXX2eeXX66X",
     "sha256":
"XXX1d6b2a6684b4c5XXf0335e61546d998XXX680378ff11a8XXbbf7XXa7aXXd",
     "techniqueNames": [
         "Unusual Parent-Child Relationship"
     ],
     "eventSource": "EDR",
     "fileEventCount": 1,
     "operatingSystem": "Microsoft Windows 10 Enterprise 10.0.19045 Build
19045",
     "detectedOn": "2023-08-10T08:11:24.025+0000",
     "scoreSource": "SIDDHI",
     "mutexEventCount": 0,
     "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
     "techniqueIds": [
         "Q0016"
     ],
     "riskScore": 9,
     "id": "a2XX5d3X-dXXa-3bXX-bXXe-a7aaXXX94XXX",
     "behavior": 0,
     "incidentStatus": "OPEN",
     "networkEventCount": 0,
     "registryEventCount": 0,
     "softwareNames": [
         "certutil"
     ],
     "mitreRuleNames": [
         "RM10001"
     ],
```

```
      "tacticIds": [
          "TA0005"
      ],
      "updatedOn": "2023-08-10T08:38:26.614+0000",
      "userName": "Unassigned",
      "eventTypes": [
          "FILE"
      ],
      "sha256Set": [
         "XXX1d6b2a6684b4c5XXf0335e61546d998XXX680378ff11a8XXbbf7XXa7aXXd"
      ],
      "tacticNames": [
          "Defense Evasion"
      ],
      "incidentId": "a2XX5d3X-dXXa-3bXX-bXXe-a7aaXXX94XXX",
      "exploit": 0,
      "incidentNumber": 21664,
      "processEventCount": 0
     },
..
]
```

Input Parameters for Incident Events

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. For example - Bearer authToken.
filter	Optional	String	The filter parameter filters the events list by providing a query using the Qualys syntax. **For example:** event.dateTime : ['2017-01-01T05:33:34' .. '2017-01- 31T05:33:34'] AND action: 'Created' For more information see EDR Online Help. You can filter events based on the time they are generated on the asset (event.dateTime) or based on the time they are processed at Qualys Cloud Platform (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date AND time.
pageNumber	Optional	String	The pageNumber parameter returns the page to be returned. It starts from the value zero.
pageSize	Optional	String	The pageSize parameter mentions the number of records per page to be included in the response. The default value is 10.
include_attributes	Optional	String	include_attribute parameter includes certain attributes in the search. The search results generated are provided using a comma-separated list. The API response fetches only the included attributes. **For example:** include_attributes = _type, _id, processName
exclude_attributes	Optional	String	exclude_attribute parameter excludes certain attributes from the search. The search results generated are provided using a comma-separated list. **For example:** exclude_attributes = _type, _id, processName **Note:** You need not exclude attributes if you have included specific attributes using the include_attributes parameter. Attributes that are not included are by default excluded.

Parameter	Mandatory/ Optional	Format	Description
searchAfterValues	Optional	Array	The searchAfterValues sort the values in array format. **For example:** value1,value2 **Note:** This parameter is only for the next request. You will be able to get these values from previous request's header.

Sample - Fetch Incident Events Using SearchAfter

API Request:

```
curl -X GET "<qualys_base_url>/ioc/incidents/events/searchAfter" --header
"accept: */*" --header "Authorization: Bearer <token>"
```

Response:


```
[
    {
     "dateTime": "2021-05-22T07:14:01.924+0000",
     "eventProcessedTime": "2021-05-22T08:22:17.210+0000",
     "workflow": 1,
     "eventSource": "EDR",
    "stateDocumentId": "RTF_2XXX2-XXX8-482e-aXX-e71c9dXX4_74XX87XX19XX4",
     "indicator2": [
         {
          "score": "1",
          "sha256":
"2da4XXXXXa1c206db6eXXX4bXX654e47XXXX308dab0XX5ff0ebXXX5f9d22XX5",
          "familyName": "test-knowntomal",
          "verdict": "REMEDIATED",
          "threatName": "test-threat",
          "category": "test-type",
          "rowId": "7405876919274160783"
         }
     ],
     "type": "FILE",
     "actor": {
        "processEventId": "RTP_XXX66462-ff28-48X-eXX671cXXX94_612XXX07X",
         "processUniqueId": "6124620742717860794",
         "processId": 19400,
         "processName": "powershell.exe",
         "userName": "NT AUTHORITY\\SYSTEM",
         "imageFullPath":
"C:\\Windows\\system32\\WindowsPowerShell\\v1.0\\powershell.exe"
     },
     "score": "1",
```

```
        "file": {
            "extension": "exe",
            "fileName": "123dsad_MALICIOUS - Copy.exe",
            "sha256": "xxxc953e80xxxxxc37eb0xxxxxd97fa71bxxxx9d05f8xxx29",
            "size": 180736,
            "nonPEFile": false,
            "macroEmbedded": false,
            "fileType": "Regular File",
            "md5": "ee59d4xxxxxx578cf8fxxxxx436d"
        },
    "verdict": [
            "REMEDIATED"
        ],
        "familyName": [
            "test-knowntomal"
        ],
        "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
        "action": "DELETED",
        "id": "RTF_c8xxxxxxb-d622-xx-b02b-xxxxxxxxx_22-5-2021",
        "category": [
            "test-type"
        ],
        "incidentId": "7af49e37-4b5a-3912-8715-1f8fe325ea29",
        "asset": {
           "fullOSName":"Microsoft Windows Server 2019 Standard 10.0.17763",
            "hostName": "<host_name>",
            "agentId": "X1aXX462-fXX8-482e-a0XX-e0eXXXX9dd9X",
            "interfaces": [
             {
              "macAddress": "00:xx:56:xx:98:xx",
              "ipAddress": "10.xx.98.162",
              "interfaceName": "Intel(R) 82574L Gigabit Network Connection",
              "gatewayAddress": "xx.xx.98.1"
             }
            ],
            "netBiosName": "<net_bios_name>",
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
            "platform": "Windows",
            "tags": [
             {
              "name": "Cloud Agent",
              "uuid": "X4e67XXX-XX78-4f32-bfXX-Xe480bc24XXX"
             }
            ]
        },
        "uniqueId": "7405876919274160783"
       },
    ..
]
```

Next API Request:

```
curl -X GET
"<qualys_base_url>/ioc/incidents/events/searchAfter?searchAfterValues=163
9811976662,RTF_fXX871e0-c2fc-3XXc-XXbf-4XXXXe63ef47_15-12-2021" --header
"accept: */*" --header "Authorization: Bearer <token>"
```

Response:


```
[
    {
     "dateTime": "2021-12-15T16:26:32.593+0000",
     "eventProcessedTime": "2021-12-18T06:11:16.553+0000",
     "workflow": 1,
     "eventSource": "EDR",
     "stateDocumentId": "RTF_XXd4eac4-1XX7-4XX8-8eXX-XXXd61dc7XXX_-
3003943943815049134",
     "indicator2": [
         {
          "score": "0",
          "sha256": "xxxc953xxxx79b5dec3xxx8173d9xxxx1b1599529xxxf82cd7",
          "verdict": "KNOWN",
          "rowId": "-3003943943815049134"
         }
     ],
     "type": "FILE",
     "actor": {
         "processEventId": "RTP_XXd4eac4-1XX7-4XX8-8eXX-
XXXd61dc7XXX_3511148714510205520_1648",
         "processUniqueId": "3511148714510205520",
         "processId": 1648,
         "processName": "mscorsvw.exe",
         "userName": "NT AUTHORITY\\SYSTEM",
         "imageFullPath":
"C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\mscorsvw.exe"
     },
     "score": "0",
     "file": {
         "fullPath":
"C:\\Windows\\assembly\\temp\\MX3WY8LDDL\\System.Configuration.Install.ni
.dll",
         "extension": "dll",
         "copyright": "© Microsoft Corporation.All rights reserved.",
         "product": "Microsoft® .NET Framework",
         "fileName": "System.Configuration.Install.ni.dll",
         "sha256": "xxxc953xxxx79b5dec37ebxxx8173d91b1599529xxxf82cd74x",
         "writeDate": "2021-10-12T23:18:01.643+0000",
         "macroEmbedded": false,
         "version": "4.8.4084.0",
```

```
          "path": "C:\\Windows\\assembly\\temp\\MX3WY8LDDL",
"createdDate": "2021-10-12T23:18:01.643+0000",
          "size": 174592,
          "accessDate": "2021-11-19T16:12:24.745+0000",
          "nonPEFile": false,
          "company": "Microsoft Corporation",
          "fileType": "dll",
          "md5": "8xxx0d6xxxxxxd2b7065xxxxx38f1"
      },
      "verdict": [
          "KNOWN"
      ],
      "familyName": [
          ""
      ],
      "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
      "action": "DELETED",
      "id": "RTF_1496bf78-0c22-3df6-ba2f-12df0de2d7fc_15-12-2021",
      "category": [
          ""
      ],
      "incidentId": "e4c2b959-1036-38bc-b9c4-9577af9c8014",
      "asset": {
          "fullOSName": "Microsoft Windows 10 Enterprise 10.0.19042 Build
19042",
          "hostName": "<host_name>",
          "agentId": "XXd4eac4-1XX7-4XX8-8eXX-XXXd61dc7XXX",
          "interfaces": [
           {
            "macAddress": "00:xx:56:xx:xx:D7",
            "ipAddress": "10.xx.xx.67",
            "interfaceName": "Intel(R) 82574L Gigabit Network Connection",
            "gatewayAddress": "10.xx.127.xx"
           }
          ],
          "netBiosName": "<net_bios_name>",
          "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
          "platform": "Windows",
          "tags": [
           {
            "name": "Cloud Agent",
            "uuid": "X4e67XXX-XX78-4f32-bfXX-Xe480bc24XXX"
           }
          ]
      },
      "uniqueId": "-3003943943815049134"
     },
..
]
```

Retrieve Asset Details using Asset API

APIs affected	/ioc/asset/count /ioc/asset/{assetId} /ioc/asset/all
New or Updated APIs	New
Operator	GET
DTD or XSD changes	No

Use this API to retrieve asset details.

Input Parameters for Fetch Asset Count

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
filter	Optional	String	The filter parameter sorts the fields in the JSON format. **For example:** [{"asset.lastupdatedtime":"asc"}]
sort	Optional	String	The sort parameter filters the asset by providing a query using Qualys syntax. For more information see EDR Online Help. **For example:** asset.platform: 'WINDOWS'

Sample - Fetch Asset Count

API Request:

```
curl -X GET "<qualys_base_url>/ioc/asset/count" --header "accept: */*" --
header "Authorization: Bearer <token>"
```

Response:

```
{
  "count": 228
}
```

Input Parameters for Fetch Asset Data

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
assetId	Mandatory	String	Use the assetId paramter to retrieve the asset details.

Sample - Fetch Asset Data

API Request:

```
curl -X GET "<qualys_base_url>/ioc/asset/XXX44XX6-XXf8-4XX2-bfXX-
XX8ba6XX2ebX" --header "accept: */*" --header "Authorization: Bearer
<token>"
```

Response:

```
{
"addedHashes": [
"string"
],
"feature": "EDR_FEATURE"
"isEnabled
"hostName": "<host_name>",
"interfaces": [
{
 "macAddress": "00:00:00:XX:00:00",
 "ipAddress": "fXX0:0:0:0:XXX9:1XX9:2XXb:XXed",
 "interfaceName": "Intel(R) XXX74X Gigabit Network Connection",
 "gatewayAddress": "XX.XX.X0X.X"
},
{
 "macAddress": "00:X0:XX:0X:00:00",
 "ipAddress": "X0.1X.XX1.00",
 "interfaceName": "Intel(R) XXX74X Gigabit Network Connection",
 "gatewayAddress": "XX.XX.X0X.X"
}
],
"avStatus": false,
"avProfile": {
"name": "Default",
"id": "XXX8a87X-XXbb-4XX9-XX74-XXX08f6XX54X",
"status": "ASSIGNED"
},
```

```
"operatingSystem": "Microsoft Windows 10",
"platform": "WINDOWS",
"isAVUpToDate": false,
"assetType": "HOST",
"tags": [
{
 "name": "Cloud Agent",
 "uuid": "XXX676fX-cXX8-XX32-bfXX-XXX8XbcXXX1b"
}
],
"timeStamp": "2022-08-30T06:19:26.999+0000",
"system": {
"lastBoot": "2022-07-17 19:02:42",
"timezone": "+05:30",
"model": "VMware Virtual Platform",
"manufacturer": "VMware, Inc."
},
"lastLoggedOnUser": "Administrator",
"infections": 0,
"id": "XXX44XX6-XXf8-4XX2-bfXX-XX8ba6XX2ebX"}
```

Input Parameters for Fetch Asset List

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
filter	Optional	String	The filter parameter filters the events list by providing a query using the Qualys syntax. **For example:** event.dateTime : ['2017-01-01T05:33:34' .. '2017-01- 31T05:33:34'] AND action: 'Created' For more information see EDR Online Help. You can filter events based on the time they are generated on the asset (event.dateTime) or based on the time they are processed at Qualys Cloud Platform (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date AND time.
pageNumber	Optional	String	The pageNumber parameter returns the page to be returned. It starts from the value zero.
pageSize	Optional	String	The pageSize parameter mentions the number of records per page to be included in the response. The default value is 10.
include_attributes	Optional	String	include_attribute parameter includes certain attributes in the search. The search results generated are provided using a comma-separated list. The API response fetches only the included attributes. **For example:** include_attributes = _type, _id, processName
exclude_attributes	Optional	String	exclude_attribute parameter excludes certain attributes from the search. The search results generated are provided using a comma-separated list. **For example:** exclude_attributes = _type, _id, processName **Note:** You need not exclude attributes if you have included specific attributes using the include_attributes parameter. Attributes that are not included are by default excluded.

sort	Optional	String	The sort parameter filters the asset by providing a query using Qualys syntax. For more information see EDR Online Help. **For example:** asset.platform: 'WINDOWS'

Sample - Fetch Asset List

API Request:

```
curl -X GET "<qualys_base_url>/ioc/asset/all" --header "accept: */*" --
header "Authorization: Bearer <token>"
```

Response:


```
[
  {
    "lastReportedTime": "2023-08-28T06:37:54.011+0000",
    "id": "XX79XXXa-2aXX-XX0b-bXXd-Xc0XXXfbcXXc"
  },
  {
    "timeStamp": "2022-07-20T10:14:37.721+0000",
    "avStatus": false,
    "id": "4XX9aXX9-XXa7-4XX1-b2XX-XXX5cb2badXX",
    "isAVUpToDate": false
  },
  {
    "hostName": "DESKTOP-ABCNXYZ",
    "interfaces": [
      {
        "macAddress": "00:00:00:XX:00:00",
        "ipAddress": "fXX0:0:0:0:XXX9:1XX9:2XXb:XXed",
        "interfaceName": "Intel(R) XXX74X Gigabit Network Connection",
        "gatewayAddress": "XX.XX.X0X.X"
      },
      {
        "macAddress": "00:X0:XX:0X:00:00",
        "ipAddress": "X0.1X.XX1.00",
        "interfaceName": "Intel(R) XXX74X Gigabit Network Connection",
        "gatewayAddress": "XX.XX.X0X.X"
      }
    ],
    "avStatus": false,
    "avProfile": {
      "name": "Default",
      "id": "XXX8a87X-XXbb-4XX9-XX74-XXX08f6XX54X",
      "status": "ASSIGNED"
    },
    "operatingSystem": "Microsoft Windows 10",
```

```
    "platform": "WINDOWS",
    "isAVUpToDate": false,
    "assetType": "HOST",
    "tags": [
      {
        "name": "Cloud Agent",
        "uuid": "XXX676fX-cXX8-XX32-bfXX-XXX8XbcXXX1b"
      }
    ],
...
]
```

Block Malicious Host using BlockFeature API

APIs affected	/ioc/blockfeature/feature /ioc/blockfeature/hash
New or Updated APIs	New
Operator	GET
DTD or XSD changes	No

The BlockFeature API blocks the Endpoint's Malicious or Suspicious Artifacts and quarantine the malicious host.

Input Parameters for Feature Policy

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
platform	Mandatory	String	Use the platform parameter to specify the platform type - Linux, Mac, or Windows.

Sample - Fetch Block Feature Policy

API Request:

```
curl -X GET "<qualys_base_url>/ioc/blockfeature/feature?platform=WINDOWS"
--header "accept: */*" --header "Authorization: Bearer <token>"
```

Response:

```
{
  "customerPolicyId": 1004,
  "hashBlocked": true,
  "urlBlocked": false,
  "ipBlocked": false
}
```

Input Parameters for Block Hash Features

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
platform	Mandatory	String	Use the platform parameter to specify the platform type - Linux, Mac, or Windows.
limit	Optional	Integer	The limit parameter lists the number of records to be included in the response. The default value is 10.
offset	Optional	Integer	The offset parameter returns the value of the page to be returned. It starts from the value zero.

Sample - Fetch Block Feature

API Request:

```
curl -X GET "<qualys_base_url>/ioc/blockfeature/hash?platform=WINDOWS" --
header "accept: */*" --header "Authorization: Bearer <token>"
```

Response:

```
[
  {
    "id": 12003,
    "type": "SHA256",
    "hash": "396861axx5xxc493xxxd9451x18xa4xx72exxcb28XX8c0xc07cxxxd693"
  },
  {
    "id": 17003,
    "type": "SHA256",
    "hash": "xxfd6021xxxbdxxxafxxx290x09xx3ax3191xxx1c7f70axxx8688axxx1"
  }
]
```

Quarantine or Kill File or Process Using Remediation API

APIs affected	/ioc/remediation-actions/{remediationID} /ioc/remediation-actions/performQuarantineHostAction /ioc/remediation-actions/performAction
New or Updated APIs	New
Operator	[GET][POST]
DTD or XSD changes	No

The new Remediation API allows you to kill or quarantine any process or file and perform remote isolation of the host.

Input Parameters for Remediation Event

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
remediationId	Mandatory	String	Enter Remediation ID. **For example:** RTF_5XX96XXeXX6b-XX6b-4XX4-90XX-349XXXfcXbc_10-2023_XX22e6XX-5XXd-XX61-9X6X-c8XX8eXXc26X

Sample - Fetch Remediation Event Details

API Request:

```
curl -X GET "<qualys_base_url>/ioc/remediation-actions/RTF_5XX96XXe-XX6b-
4XX4-90XX-349XXXfcXbcX_10-2023_XX22e6XX-5XXd-XX61-9X6X-c8XX8eXXc26X" --
header "accept: */*" --header "Authorization: Bearer <token>"
```

Response:

```
{
  "customerId": "XXXcadeX-XX35-6XX1-82XX-aXX08fXXbceX",
  "dateTime": "2023-09-14T12:33:09.498+0000",
  "type": "FILE",
  "action": "CREATED",
  "asset": {
    "agentId": "XXXX69XX-cXXb-XX14-90XX-3XXX17fX7bX7",
    "platform": "WINDOWS",
    "interfaces": [
      {
```

```
        "ipAddress": "X0.0X.00.00"
      }
    ],
    "hostName": "<host_name>"
  },
  "file": {
    "path": "C:",
    "fullPath": "C:\\AM2_MALICIOUS.exe",
    "md5": "ee59d4xxxxx40578cfxxxxf1436d",
    "sha256": "2dXX88XXca1X20XXb6eXXX844b16X4e4XXX82308daXX3c5fX0dXX60X",
    "size": 180736,
    "macroEmbedded": false,
    "nonPEFile": false,
    "writeDate": "2021-10-06T10:46:26.192+0000",
    "accessDate": "2023-09-14T12:32:52.117+0000",
    "fileName": "AM2_MALICIOUS.exe",
    "createdDate": "2023-09-14T12:32:52.117+0000"
  },
  "response": {
    "action": "Unquarantine File",
    "status": "success",
    "executionTime": "2023-10-04T07:16:45.000+0000",
    "user": "ABC XYZ",
    "userId": "user",
    "comments": "test",
    "statusMessage": "Success: UnQuarantine Successful.\n0\r\n",
    "timestamp": "2023-10-04T07:16:55.432+0000"
  }
}
```

Input Parameters for Remediation Action on Event

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
user	Mandatory	String	Name of the user associated with the action.
userId	Mandatory	String	User Id of the user associated with the action.
comment	Optional	String	Use the comment parameter to mention the reason behind the action.

Sample - Perform Remediation Action on Event

API Request:

```
curl -X POST "<qualys_base_url>/ioc/remediation-
actions/performAction?user=username&userId=XXc42aXX-03XX-XXdd-aXX8-
42fXXXd7cXXX" --header "accept: */*" --header "Authorization: Bearer
<token>"-H "Content-Type: application/json" -d "<JSON payload>"
```

Sample JSON Payload:

```
[
  {
    "actionId": 0,
    "agentId": "XXX85f64-5XX7-XX62-b3XX-XX963f6XXfaX",
    "eventId": "string",
    "eventType": "string",
    "pid": 0,
    "uniqueId": "string"
  }
]
```

Response:

```
{
  "HttpStatus": "OK"
}
```

Input Parameters for Quarantine Host Action on Event

Parameter	Mandatory/ Optional	Format	Description
Authorization	Mandatory	String	Authorization parameter authenticates the Qualys Cloud Platform. Prepend token with "Bearer" and a space. **For example:** Bearer authToken.
user	Mandatory	String	Name of the user associated with the action.
userId	Mandatory	String	User Id of the user associated with the action.
comment	Optional	String	Use the comment parameter to mention the reason behind the action.
remediationSource	Optional	String	The Remediation Source values are event, asset, or incident.
sourceEventId	Optional	String	Use the sourceEventId parameter for event, asset, and incident from which remediation is performed on end point.

Prerequisite:

- Linux Cloud Agent: 6.0.0.0.x and above

- Windows Cloud Agent: 4.9.0.x and above

Note: If the prerequisites are not met for Quarantine Host Action on Event API, the process might be stuck in the In-Progress or Failed state.

Sample - Quarantine Host Action on Event

API Request:

```
curl -X POST "<qualys_base_url>/ioc/remediation-
actions/performQuarantineHostAction?user=username&userId=XXc42aXX-03XX-
XXdd-aXX8-42fXXXd7cXXX" --header "accept: */*" --header "Authorization:
Bearer <token>"-H "Content-Type: application/json" -d "<JSON payload>"
```

Sample JSON Payload:

```
{
  "actions": [
    {
      "actionId": 0,
      "agentId": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
      "eventId": "string",
      "eventType": "string",
      "pid": 0,
```

```
        "uniqueId": "string"
      }
    ],
    "host": {
      "configuration": {
        "allow": {
          "application": [
            "string"
          ]
        },
        "block": {
          "application": [
            "string"
          ]
        },
        "notification": {
          "emailId": "string",
          "message": "string",
          "phone": "string",
          "title": "string"
        }
      }
    }
  }
```

Response:

```
{
  "HttpStatus": "OK"
}
```