Qualys Endpoint Detection and Response v2.x

API Release Notes

Version 2.4

April 5, 2023

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

What's New

Updated Input Parameter for Fetch Events

Fetch Events Using Scroll APIs

Fetch Incident Events Using Scroll APIs

Fetch Incidents Using Scroll APIs

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.

Updated Input Parameter for Fetch Events

With this release, the **state** input parameter for Fetch events has been set to the **false** value. Previously, the state parameter supported the Boolean value. Now, the true value is not supported for Fetch events.

Input Parameter

Parameter	Description
state	Set state to "false" to fetch events.

Fetch Events Using Scroll APIs

Scroll APIs are the mandatory APIs for Windows.

Use the following API to fetch events using Scroll APIs:

API affected	/ioc/events/scroll
New or Updated APIs	New
DTD or XSD changes	No

Input Parameters

Use the following input parameters to fetch events in the API output:

Parameter	Description
fromDate(String)	Events logged after a certain date. Supports epoch time/unix timestamp. For example-14283228800 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 drill down further by applying the time value.
toDate (String)	Events logged until a certain date. Supports epoch time / 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 drill down further by applying the time value
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 while creating your query. For example - event.dateTime : ['2017-01-01T05:33:34' .. '2017-01-31T05:33:34'] and action: 'Created' 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 (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date and time.
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - agentId
sort (String)	Sort the results using a Qualys token. For example - [{"action":"asc"}]
include_attributes (String)	Include certain attributes in search (provide comma separated list). Only included attributes are fetched in the API response. For example, include_attributes = _type, _id, processName

Parameter	Description
exclude_attributes (String)	Exclude certain attributes from search (provide 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. Not-included attributes are excluded by default.
scrollId (String)	Identifier for the search. Its retrieve the next batch of search results for the request. For example - scrollId=<scroll_id> Note: This parameter is only for the Next API Request and onwards. We will get scroll_id from header of fresh request.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer <authToken>

Sample- GET Event using Scroll APIs

API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/events/scroll?filter
=type:MUTEX' --header 'Authorization: Bearer <token> \
```

Response header:

```
{
    "transfer-encoding": "chunked",
    "date": "Tue, 24 Jan 2023 09:08:43 GMT",
    "content-type": "application/json",
    "count": "3254",
    "scroll_id":"XXXXXXXXXXXXXXXXXXXXX"
    "strict-transport-security": "max-age=15724800; includeSubDomains",
    "cache-control": "no-cache, no-store, max-age=0, must-revalidate",
    "pragma": "no-cache",
    "expires": "0",
    "referrer-policy": "no-referrer"
}
```

Response:

```
[
    {
        "dateTime": "2023-01-17T02:34:50.573+0000",
        "process": {
            "fullPath": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe\\Microsoft.Photos.exe",
```

```
            "parentProcessName": "svchost.exe",
            "processFile": {
                "fullPath": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe\\Microsoft.Photos.exe",
                "path": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe",
                "sha256":
"xa9xxx5a9aaxxxxx36e721exxx7d00aa2438xxd800xxxxx172axxx2f8xxx88a",
                "size": 756736,
                "moduleName": "Microsoft.Photos.exe",
                "md5": "3d8bxxxea865fxxx6d755bxxxd67aaca"
            },
            "processEventId": "RTP_xxxx0e2f-4ea0-3xx2-xxx0-
9cxxxx60e227_17-1-2023",
            "processName": "Microsoft.Photos.exe",
            "elevated": true,
            "parentPid": 912,
            "arguments": "-
ServerName:App.AppXzst44mncqdg84v7sv6p7yznqwssy6f7f.mca",
            "pid": 6008,
            "parentEventId": "RTP_2xxxxxe0-xxx4-3xx7-8xxx-eaxxxxxfe0x4_11-
1-2023",
            "userName": "DESKTOP-SF6JTIO\\Administrator",
            "integrityLevel": "ML_LOW"
        },
        "eventProcessedTime": "2023-01-17T02:41:25.383+0000",
        "eventSource": "EDR",
        "mutex": {
            "mutexName": "\\Sessions\\2\\AppContainerNamedObjects\\S-1-15-
2-222XXXX697-XXXXX7180-2301XXX-42489XXXXX-2024719031-23XXXXX081-
291XXXXXX\\SessionImmersiveColorMutex"
        },
        "indicator2": [
            {
                "score": "0",
                "sha256":
"xa9xxx5a9aaxxxxx36e721exxx7d00aa2438xxd800xxxxx172axxx2f8xxx88a",
                "verdict": "KNOWN",
                "rowId": "41844119948680912 97"
            }
        ],
        "type": "MUTEX",
        "score": "0",
        "scoreSource": "REVERSING_LAB",
        "action": "RUNNING",
        "id": "RTM_xxxx0f3x-xxx5-3xxd-bxxx-060xxxdxx20x_17-1-2023",
        "asset": {
```

```
          "fullOSName": "Microsoft Windows 10 Enterprise 10.0.19044 Build
19044",
            "hostName": "DESKTOP-SF6JTIO",
            "agentId": "xxxa98xx-xxx5-4xx8-8xx3-xxxd76xx02x",
            "interfaces": [
                {
                    "macAddress": "xx:xx:xx:xx:xx:xx",
                    "ipAddress": "xx.xxx.xxx.xx",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                    "gatewayAddress": "xx.xxx.xxx.x"
                }
            ],
            "netBiosName": "xxxxx-xxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-6xx5-xxx1-8xxx-xx008f55xxx3",
            "platform": "Windows",
            "assetType": "HOST",
            "tags": [
                {
                    "name": "Cloud Agent",
                    "uuid": "xxx676fe-cxxx-4xxx-xx5f-xx48xxcxxx1b"
                }
            ]
        },
        "uniqueId": "x18xxxxxxxxx09xxx7"
    },
    {
        "dateTime": "2023-01-17T02:34:50.573+0000",
        "process": {
            "fullPath": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe\\Microsoft.Photos.exe",
            "parentProcessName": "svchost.exe",
            "processFile": {
                "fullPath": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe\\Microsoft.Photos.exe",
                "path": "C:\\Program
Files\\WindowsApps\\Microsoft.Windows.Photos_2022.30120.12007.0_x64__8wek
yb3d8bbwe",
                "sha256":
"xa9xxx5a9aaxxxxx36e721exxx7d00aa2438xxd800xxxxx172axxx2f8xxx88a",
                "size": 756736,
                "moduleName": "Microsoft.Photos.exe",
                "md5": "3xxxxxxxxx5fad7xxxxxxxx6d67xxxx"
            },
            "processEventId": "RTP_xxxx0e2f-4ea0-3xx2-xxx0-
9cxxxx60e227_17-1-2023",
```

```
            "processName": "Microsoft.Photos.exe",
            "elevated": true,
            "parentPid": 912,
            "arguments": "-
ServerName:App.AppXzst4xxxcqdxxxxxyznqwsxxx7f.mca",
            "pid": 6008,
           "parentEventId": "RTP_2xxxxxe0-xxx4-3xx7-8xxx-eaxxxxxfe0x4_11-
1-2023",
            "userName": "xxxx-xxxxx\\Administrator",
            "integrityLevel": "ML_LOW"
        },
        "eventProcessedTime": "2023-01-17T02:41:25.383+0000",
        "eventSource": "EDR",
        "mutex": {
           "mutexName": "\\Sessions\\2\\AppContainerNamedObjects\\S-1-15-
2-2226957697-3030467180-2301525-4248967783-2024719031-2325529081-
2915787518\\SM0:6008:120:WilError_03"
        },
        "indicator2": [
            {
                "score": "0",
                "sha256":
"xa9xxx5a9aaxxxxx36e721exxx7d00aa2438xxd800xxxxx172axxx2f8xxx88a",
                "verdict": "KNOWN",
                "rowId": "-744512xxxxxxx98913"
            }
        ],
        "type": "MUTEX",
        "score": "0",
        "scoreSource": "REVERSING_LAB",
        "action": "RUNNING",
        "id": "RTM_bxxx1397-4xxx-3xxc-xxx9-xx2f0xxx8axx_17-1-2023",
        "asset": {
          "fullOSName": "Microsoft Windows 10 Enterprise 10.0.19044 Build
19044",
            "hostName": "xxxx-xxxx",
            "agentId": "xxxa98xx-xxx5-4xx8-8xx3-xxxd76xx02x",
            "interfaces": [
                {
                    "macAddress": "XX:XX:XX:XX:XX:XX",
                    "ipAddress": "XX.XXX.XXX.X",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                    "gatewayAddress": "XX.XXX.XXX.X"
                }
            ],
            "netBiosName": "xxxx-xxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-6xx5-xxx1-8xxx-xx008f55xxx3",
```

```
                "platform": "Windows",
                "assetType": "HOST",
                "tags": [
                    {
                        "name": "Cloud Agent",
                        "uuid": "xxx676fe-cxxx-4xxx-xx5f-xx48xxcxxx1b"
                    }
                ]
            },
            "uniqueId": "-xxxx1xx6xxx27xxxx1x"
        }
    ]
```


Next API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/events/scroll?scroll
Id=<scroll_id>' --header 'Authorization: Bearer <token> \
```

Response:


```
[
    {
        "dateTime": "2023-01-23T13:06:28.992+0000",
        "process": {
            "fullPath": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher\\FNPLicensingService64.exe",
            "parentProcessName": "services.exe",
            "processFile": {
               "fullPath": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher\\FNPLicensingService64.exe",
                "path": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher",
                "sha256":
"xxxc953e80xxxxxc37eb0xxxxxd97fa71bxxxx9d05f8xxxxd36xxxx29",
                "size": 1519440,
                "certificates": [
                    {
                        "certificateSigned": true,
                       "certificateIssuer": "Symantec Class 3 SHA256 Code
Signing CA",
                        "certificateValid": true,
                        "certificateIssuedTo": "Flexera Software LLC",
                        "certificateSignedDate": "2018-09-
13T00:00:00.000+0000",
                        "certificateHash":
"xxx0dxxb23f9a2xxx4d22b2f7xxx32e7c934xxx8"
                    }
```

```
                ],
                "moduleName": "FNPLicensingService64.exe",
                "md5": "xxxc890f8539d4d3689xxx73cd52ac5"
            },
            "processEventId": "RTP_xxx26173-8axx-3xx6-8xxx-
41xxxbe55xxx_22-12-2022",
            "processName": "FNPLicensingService64.exe",
            "elevated": true,
            "parentPid": 816,
            "pid": 3280,
           "parentEventId": "RTP_xxxd8a66-xxx0-3fxx-xxx5-xxxad8d62xxx_22-
12-2022",
            "userName": "NT AUTHORITY\\SYSTEM",
            "integrityLevel": "ML_SYSTEM"
        },
        "eventProcessedTime": "2023-01-23T13:03:24.731+0000",
        "eventSource": "EDR",
        "mutex": {
            "mutexName": "\\BaseNamedObjects\\{xxxxxxxx-ef71-4xxf-axxx-
91dcaxxxf13}-cxx-s_tpm_init"
        },
        "indicator2": [
            {
                "score": "0",
                "sha256":
"xxxc953xxxx79b5dec37ebxxx8173d9xxxx1b1599529xxxf82cd74xxx6291xxx",
                "verdict": "KNOWN",
                "rowId": "-32xx86xxxxxxx76x5x"
            }
        ],
        "type": "MUTEX",
        "score": "0",
        "scoreSource": "REVERSING_LAB",
        "action": "TERMINATED",
        "id": "RTM_xxxx2ecd-xxxc-33f0-b2xx-0xxxx60adexx_23-1-2023",
        "asset": {
            "fullOSName": "Microsoft Windows 10 Pro 10.0.19045 Build
19045",
            "hostName": "xxx-xxx-xxxx",
            "agentId": "xxxx7a51-xxx7-xxx1-xxx1-xxx0e7b33xxx",
            "interfaces": [
                {
                    "macAddress": "xx:xx:xx:xx:xx:xx",
                    "ipAddress": "xxxx:0:0:0:xxxx:xxxx:xxxx:xxxx",
                    "interfaceName": "VirtualBox Host-Only Ethernet
Adapter"
                },
                {
                    "macAddress": "xx:xx:xx:xx:xx:xx",
```

```
                    "ipAddress": "xx.xx.xxx.xxx",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                    "gatewayAddress": "xx.xx.xxx.x
                },
                {
                    "macAddress": "xx:xx:xx:00:00:xx",
                    "ipAddress": "xxx.xxx.xxx.xx",
                    "interfaceName": "VirtualBox Host-Only Ethernet
Adapter"
                },
                {
                    "macAddress": "xx:xx:xx:xx:xx:xx",
                    "ipAddress": "xxxx:0:0:0:xxxx:xxxx:xxxx:xxxx",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                    "gatewayAddress": "xx.xx.xxx.x"
                }
            ],
            "netBiosName": "xxx-xxxx-xxxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
            "platform": "Windows",
            "assetType": "HOST",
            "tags": [
                {
                    "name": "Cloud Agent",
                    "uuid": "xxx676fe-xxx8-xxx2-xxxf-xxx80bc2411b"
                }
            ]
        },
        "uniqueId": "-xxxx38xxxxxxx61xxx"
    },
    {
        "dateTime": "2023-01-23T13:06:28.941+0000",
        "process": {
            "fullPath": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher\\FNPLicensingService64.exe",
            "parentProcessName": "services.exe",
            "processFile": {
               "fullPath": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher\\FNPLicensingService64.exe",
                "path": "C:\\Program Files\\Common Files\\Macrovision
Shared\\FlexNet Publisher",
                "sha256": "xxxx953e803d9xxxxxb1599xxxxx46d3xxxx29",
                "size": 1519440,
                "certificates": [
                    {
                        "certificateSigned": true,
```

```
                        "certificateIssuer": "Symantec Class 3 SHA256 Code
Signing CA",
                         "certificateValid": true,
                         "certificateIssuedTo": "Flexera Software LLC",
                         "certificateSignedDate": "2018-09-
13T00:00:00.000+0000",
                         "certificateHash":
"xxxxd07b23xxx25e2xxx2f7bxxx7c9xx2f98"
                    }
                ],
                "moduleName": "FNPLicensingService64.exe",
                "md5": "xxxx90f8539dxxxx68928327xxx52ac5"
            },
            "processEventId": "RTP_x26173-xxx2-xxx6-xxx3-xxx93abe5xxx_22-
12-2022",
            "processName": "FNPLicensingService64.exe",
            "elevated": true,
            "parentPid": 816,
            "pid": 3280,
            "parentEventId": "RTP_xxxd8a66--xxxad8d62xxx_22-12-2022",
            "userName": "NT AUTHORITY\\SYSTEM",
            "integrityLevel": "ML_SYSTEM"
        },
        "eventProcessedTime": "2023-01-23T13:03:24.732+0000",
        "eventSource": "EDR",
        "mutex": {
            "mutexName": "\\BaseNamedObjects\\{xxxxxxxx-exxx-xxxf-xxxx-
91xxxx37xxxx}-cxx-s_wxx_init"
        },
        "indicator2": [
            {
                "score": "0",
               "sha256":"xxxc953e37eb0xxxx73d97faxxxx99529d05f82cd74xxx6",
                "verdict": "KNOWN",
                "rowId": "-4893206851394137947"
            }
        ],
        "type": "MUTEX",
        "score": "0",
        "scoreSource": "REVERSING_LAB",
        "action": "TERMINATED",
        "id": "RTM_xxx0c057-xxx8-xxxf-xxxf-xxx921a7fxxx_23-1-2023",
        "asset": {
          "fullOSName": "Microsoft Windows 10 Pro 10.0.19045 Build 19045",
            "hostName": "xxx-xxxx-xxxx",
            "agentId": "xxxd7a51-xxx7-xxx1-xxx1-xxx0e7b33xxx",
            "interfaces": [
                {
                    "macAddress": "xx:xx:xx:xx:00:xx",
```

```
                    "ipAddress": "xxxx:0:0:0:xxxx:xxxx:xxxx:xxxx",
                    "interfaceName": "VirtualBox Host-Only Ethernet
Adapter"
                },
                {
                    "macAddress": "xx:xx:xx:xx:00:xx",
                    "ipAddress": "xx:xx:xx:xx",
                    "interfaceName": "Intel(R) 82574L Gigabit Network
Connection",
                    "gatewayAddress": "xx:xx:xx:x"
                },
                {
                    "macAddress": "xx:xx:xx:xx:00:xx",
                    "ipAddress": "xxx:xx:xx:x",
                    "interfaceName": "VirtualBox Host-Only Ethernet
Adapter"
                },
                {
                    "macAddress": "xx:xx:xx:xx:00:xx",
                    "ipAddress": "xxxx:0:0:0:xxxx:xxxx:xxxx:xxxx",
                    "interfaceName": "Intel(R)82574L Gigabit Network
Connection",
                    "gatewayAddress": "xx:xx:xx:x"
                }
            ],
            "netBiosName": "xxx-xxxx-xxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bce3",
            "platform": "Windows",
            "assetType": "HOST",
            "tags": [
                {
                    "name": "Cloud Agent",
                    "uuid": "xxxx67xx-xxx8-xxx2-xxxf-xxx80bc2411b"
                }
            ]
        },
        "uniqueId": "-4xx32xxxxx94137xxx"
    }
]
```

Fetch Incident Events Using Scroll APIs

Use the following API to fetch incident events using Scroll APIs.

API affected	ioc/incidents/events/scroll
New or Updated APIs	New
DTD or XSD changes	No

Input Parameters

Use the following input parameters to fetch events in the API output:

Parameter	Description
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 - event.dateTime : ['2017-01-01T05:33:34' .. '2017-01-31T05:33:34'] and action: 'Created' 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 (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date and time.
sort (String)	Sort the results using a Qualys token. For example - [{"action":"asc"}]
include_attributes (String)	Include certain attributes in search (provide comma separated list). Only included attributes are fetched in the API response. For example, include_attributes = _type, _id, processName
exclude_attributes (String)	Exclude certain attributes from search (provide 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. Not-included attributes are excluded by default.
scrollId (String)	Identifier for the search. Its retrieve the next batch of search results for the request. For example - scrollId=<scroll_id> Note: This parameter is only for the Next API Request and onwards. We will get scroll_id from header of fresh request.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer <authToken>

Sample- GET Incident Events Using Scroll APIs

API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/incidents/scroll?fil
ter=(incident.files>0) and incident.process>0' --header 'Authorization:
Bearer <token> \
```

Response header:


```
{
    "transfer-encoding": "chunked",
    "date": "Tue, 24 Jan 2023 09:18:23 GMT",
    "content-type": "application/json",
    "count": "3254",
    "scroll_id": "
VhUxxxxxxxpMTWt4S3VfZxxxxxxxxxxxxxxxxVmWxxxxx0UAAQmlxxxxxxxxxxx5rV193dxxx
xxxxxxxxxxeVFsNxxxxxJWTVhfxxxxxxxxxxxxxZRAAAA"
    "strict-transport-security": "max-age=15724800; includeSubDomains",
    "cache-control": "no-cache, no-store, max-age=0, must-revalidate",
    "pragma": "no-cache",
    "expires": "0",
    "referrer-policy": "no-referrer"
}
```


Response:


```
[
    {
        "hostName": "xxx-xx-xxx-xxxx",
        "agentId": "xxx5f0c4-xxxa-xxx1-xxx4-xxxee204bxxx",
        "malwareFamilies": [
            "Generic",
            "fam_trojan"
        ],
       "sha256": "xxx488fcca1c206xxxxxxxxx82308dab03c5ff0ebf605f9d2xxxx",
        "techniqueNames": [
            "Command and Scripting Interpreter: Windows Command Shell",
            "Signed Binary Proxy Execution: Regsvr32"
        ],
        "malwareCategories": [
            "Trojan",
            "trojan"
        ],
        "fileEventCount": 3,
        "operatingSystem": "Microsoft Windows 10 Pro 10.0.17763 Build
17763",
        "detectedOn": "2022-07-14T22:00:10.745+0000",
```

```
    "scoreSource": "SIDDHI",
    "mutexEventCount": 0,
    "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
    "techniqueIds": [
        "Txxxx.0x0",
        "Txxxx.xx3"
    ],
    "riskScore": 8,
    "id": "xxx7aed0-xxx7-xxx6-xxxe-xxxed62128a4",
    "behavior": 0,
    "networkEventCount": 0,
    "registryEventCount": 0,
    "softwareNames": [
        "cmd"
    ],
    "mitreRuleNames": [
        "T1059_003_1",
        "T1218_010_2"
    ],
    "tacticIds": [
        "TA0005",
        "TA0002"
    ],
    "updatedOn": "2022-07-14T22:03:14.586+0000",
    "eventTypes": [
        "PROCESS",
        "FILE"
    ],
    "incidentId": "xxx7aed0-xxx7-xxx6-xxxe-xxxed6212xxx",
    "exploit": 0,
    "incidentDescription": "fam_trojan",
    "processEventCount": 1
},
{
    "hostName": "xxx-xx-xxx-xxxx",
    "agentId": "xxx5f0c4-xxxa-xxx1-xxx4-xxxee204bxxx",
    "malwareFamilies": [
        "Generic",
        "fam_trojan"
    ],
   "sha256": "xxxcb4081f34xxx669a65x3653f63fce0b8b4xxxb018772fddxxx",
    "techniqueNames": [
        "Command and Scripting Interpreter: Windows Command Shell",
        "Signed Binary Proxy Execution: Regsvr32"
    ],
    "malwareCategories": [
        "Trojan",
        "trojan"
    ],
```

```
            "fileEventCount": 4,
            "operatingSystem": "Microsoft Windows 10 Pro Build 17763",
            "detectedOn": "2022-07-15T04:00:13.040+0000",
            "scoreSource": "SIDDHI",
            "mutexEventCount": 0,
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
            "techniqueIds": [
                "T1218.010",
                "T1059.003"
            ],
            "riskScore": 8,
            "id": "xxx49269-xxx7-xxx9-xxxf-xxx3a9b30xxx",
            "behavior": 0,
            "networkEventCount": 0,
            "registryEventCount": 0,
            "softwareNames": [
                "cmd"
            ],
            "mitreRuleNames": [
                "T1059_003_1",
                "T1218_010_2"
            ],
            "tacticIds": [
                "TA0005",
                "TA0002"
            ],
            "updatedOn": "2022-07-15T04:04:12.134+0000",
            "eventTypes": [
                "PROCESS",
                "FILE"
            ],
            "incidentId": "xxx49269-xxx7-xxx9-xxxf-xxx3a9b30xxx",
            "exploit": 0,
            "incidentDescription": "Generic",
            "processEventCount": 1
        }
    ]
```


Next API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/incidents/Scroll?scr
ollId=<scroll_id>'  --header 'Authorization: Bearer <token> \
```

Response:


```
[
    {
        "hostName": "xxxxxxx.xxx.xxx.xxxx.qualys.com",
```

```
        "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
        "sha256":
"xxxxxxb076caa8xxxxx922xxxxdeec0542xxxxx6a2e53aa968055fxxx",
        "techniqueNames": [
            "System Information Discovery",
            "Ingress Tool Transfer"
        ],
        "fileEventCount": 11,
        "operatingSystem": "CentOS Linux 7.9.2009",
        "detectedOn": "2022-10-01T08:45:01.000+0000",
        "scoreSource": "SIDDHI",
        "mutexEventCount": 0,
        "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
        "techniqueIds": [
            "T1082",
            "T1105"
        ],
        "riskScore": 5,
        "id": "xxx227f4-xxxf-xxxa-xxx9-xxx99b9c5xxx",
        "behavior": 0,
        "networkEventCount": 0,
        "registryEventCount": 0,
        "mitreRuleNames": [
            "AK1001",
            "AK1002"
        ],
        "tacticIds": [
            "TA0007",
            "TA0011"
        ],
        "updatedOn": "2022-10-01T08:49:44.008+0000",
        "eventTypes": [
            "PROCESS",
            "FILE"
        ],
        "tacticNames": [
            "Command and Control"
        ],
        "incidentId": "xxx227f4-xxxf-xxxa-xxx9-xxx99b9c5xxx",
        "exploit": 0,
        "processEventCount": 4
    },
    {
        "hostName": "xxxxxxxx.xxx.xxx.xxxx.qualys.com",
        "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
        "sha256":
"xxxxx376xxx65a48527b52ca23xxxx825c54dff1xxxf01exxxxxx1161",
        "techniqueNames": [
            "System Information Discovery",
```

```
            "Ingress Tool Transfer"
        ],
        "fileEventCount": 1,
        "operatingSystem": "CentOS Linux 7.9.2009",
        "detectedOn": "2022-10-01T09:15:02.000+0000",
        "scoreSource": "SIDDHI",
        "mutexEventCount": 0,
        "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
        "techniqueIds": [
            "T1082",
            "T1105"
        ],
        "riskScore": 5,
        "id": "xxx4aca-8xxd-8669-3xxx6bxx2xx0",
        "behavior": 0,
        "networkEventCount": 0,
        "registryEventCount": 0,
        "mitreRuleNames": [
            "AK1001",
            "AK1002"
        ],
        "tacticIds": [
            "TA0007",
            "TA0011"
        ],
        "updatedOn": "2022-10-01T09:20:02.659+0000",
        "eventTypes": [
            "PROCESS",
            "FILE"
        ],
        "tacticNames": [
            "Command and Control"
        ],
        "incidentId": "xxxb4aca-xxxf-xxxd-xxx9-xxx6b5452xxx",
        "exploit": 0,
        "processEventCount": 6
    }
]
```

Fetch Incidents Using Scroll APIs

Use the following fetch incidents using Scroll APIs:

API affected	ioc/incidents/scroll
New or Updated APIs	New
DTD or XSD changes	No

Input Parameters

Use the following input parameters to fetch events in the API output:

Parameter	Description
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 - event.dateTime : ['2017-01-01T05:33:34' .. '2017-01-31T05:33:34'] and action: 'Created' 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 (event.eventProcessedTime). It is recommended to use the "event.dateTime" or "event.eventProcessedTime" parameter if you want to fetch events by date and time.
sort (String)	Sort the results using a Qualys token. For example - [{"action":"asc"}]
include_attributes (String)	Include certain attributes in search (provide comma separated list). Only included attributes are fetched in the API response. For example, include_attributes = _type, _id, processName
exclude_attributes (String)	Exclude certain attributes from search (provide 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. Not-included attributes are excluded by default.
scrollId (String)	Identifier for the search. Its retrieve the next batch of search results for the request. For example - scrollId=<scroll_id> Note: This parameter is only for the Next API Request and onwards. We will get scroll_id from header of fresh request.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer <authToken>

Sample- GET Incidents Using Scroll APIs

API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/incidents/events/scr
oll?filter=incident.id:"xxx676ad-xxxe-34b8-axxx-e0xxxbefxxx9" --header
'Authorization: Bearer <token>'
```

Response header:

```
{
    "transfer-encoding": "chunked",
    "date": "Tue, 24 Jan 2023 09:40:03 GMT",
    "content-type": "application/json",
    "count": "3254",
    "scroll_id": "
J3Ad1hUbWFEZkpMxxxxxxxxxxxxxxxxxxxiY255MlZRATWXY3YXVabkAAAASUKv8WYk5rV193
wMmM1aURTJWTVhxxxxxxxxxxx55MlZRAAAAt4S3VfZxZzYk16cXFGbFJ6dXI3Y"
    "strict-transport-security": "max-age=15724800; includeSubDomains",
    "cache-control": "no-cache, no-store, max-age=0, must-revalidate",
    "pragma": "no-cache",
    "expires": "0",
    "referrer-policy": "no-referrer"
}
```

Response:

```
[
    {
        "dateTime": "2022-10-04T11:56:47.000+0000",
        "eventProcessedTime": "2022-10-04T12:00:54.149+0000",
        "workflow": 4,
        "eventSource": "EDR",
        "stateDocumentId": "RTF_xxxf627e-xxx3-xxxc-xxx3-
xxx863c3fxxx_6902519366503004772",
        "type": "FILE",
        "actor": {
            "processEventId": "RTP_xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx_-
7833919771257568865_32386",
            "processUniqueId": "-7833919771257568865",
            "processId": 32386,
            "processName": "/usr/sbin/syslog-ng",
            "userName": "root",
            "imageFullPath": "/usr/sbin/syslog-ng"
        },
        "score": "5",
        "scoreSource": "SIDDHI",
        "file": {
            "fullPath": "/var/log/secure",
            "path": "/var/log",
```

```
            "fileName": "secure",
            "createdDate": "2022-10-04T10:52:11.000+0000",
            "sha256": "xxxddcb5a776652xxxx97xxxxxx941xxx23d1bxxxx66",
            "size": 14910,
            "accessDate": "2022-10-04T10:52:11.000+0000",
            "nonPEFile": false,
            "writeDate": "2022-10-04T11:56:47.000+0000",
            "macroEmbedded": false,
            "fileType": "regularfile",
            "md5": "xxx4exxx7cxxxfebxxxx75aaxxxx20dx6"
        },
        "techniques": [
            {
                "techniqueName": "Ingress Tool Transfer",
                "techniqueScore": 5,
                "techniqueId": "T1105"
            }
        ],
        "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
        "action": "WRITE",
        "tactics": [
            {
                "tacticName": "Command and Control",
                "tacticId": "TA0011"
            }
        ],
        "ruleNames": [
            "AK1001"
        ],
        "id": "RTF_xxx2c622-xxx3-xxxf-xxx8-xxx29b20fxxx_4-10-2022",
        "incidentId": "xxx676ad-xxxe-34b8-axxx-e0xxxbefxxx9"",
        "asset": {
            "fullOSName": "CentOS Linux 7.9.2009",
            "hostName": "xxxxxxx.xxxx.xxx.xxxx.xxxx.com",
            "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
            "platform": "LINUX",
            "assetType": "HOST"
        },
        "nodeId": "xxx036f5-xxx5-xxxf-xxx4-xxx4276fcxxx",
        "uniqueId": "xxx25xxxx0300xxx2"
    },
    {
        "dateTime": "2022-10-01T02:45:03.000+0000",
        "eventSource": "EDR",
        "type": "FILE",
        "score": "5",
        "scoreSource": "SIDDHI",
```

```
        "file": {
            "fullPath": "/var/log//maillog",
            "path": "/var/log/",
            "fileName": "maillog",
            "createdDate": "2022-10-01T02:32:02.000+0000",
            "sha256": "xxxxc1bexxxefb21ba2xxxx1200b5xxxdb26xxxx9d7e",
            "size": 81139,
            "accessDate": "2022-10-01T02:32:02.000+0000",
            "nonPEFile": false,
            "writeDate": "2022-10-01T02:45:03.000+0000",
            "macroEmbedded": false,
            "fileType": "regularfile",
            "md5": "xxx9109aabxxx17xxxebxx86cxxxa"
        },
        "familyName": [
            ""
        ],
        "customerId": "xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxx",
        "action": "WRITE",
        "id": "RTF_xxxc1476-xxx3-xxx8-xxxb-xxxa88bb2xxx_30-9-2022",
        "eventProcessedTime": "2022-10-01T02:58:39.093+0000",
        "workflow": 2,
        "stateDocumentId": "RTF_xxxf627e-xxx3-xxxc-xxx3-
xxx863c3fff4_6561786300176718951",
        "indicator2": [
            {
                "sha256": "xxxxx8cfxxxx2565xxf6z7xxxx551xxx458xx299xx1",
                "verdict": "UNKNOWN",
                "rowId": "6561786300176718951"
            },
            {
                "sha256": "xxxxb11e8a826489xxxd9fxxx6c6xxx003d",
                "verdict": "UNKNOWN",
                "rowId": "6561786300176718951"
            },
            {
                "sha256": "xxx5b20eaa35ec27xxx90a4adxxx15470xxxa8xxb",
                "verdict": "UNKNOWN",
                "rowId": "6561786300176718951"
            }
        ],
        "actor": {
            "processEventId": "RTP_xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx_-
78xxxxxx756xxx_32xxx",
            "processUniqueId": "-xx3xxxxxxxxx8865",
            "processId": 32386,
            "processName": "/usr/sbin/syslog-ng",
            "userName": "root",
            "imageFullPath": "/usr/sbin/syslog-ng"
```

```
            },
            "techniques": [
                {
                    "techniqueName": "Ingress Tool Transfer",
                    "techniqueScore": 5,
                    "techniqueId": "T1105"
                }
            ],
            "verdict": [
                "UNKNOWN"
            ],
            "tactics": [
                {
                    "tacticName": "Command and Control",
                    "tacticId": "TA0011"
                }
            ],
            "ruleNames": [
                "AK1001"
            ],
            "incidentId": "xxx676ad-xxxe-34b8-axxx-e0xxxbefxxx9"",
            "asset": {
                "fullOSName": "CentOS Linux 7.9.2009",
                "hostName": "xxxxx.xxx.xxx.xxxx.xxxx.com",
                "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
                "isQuarantineHost": false,
                "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
                "platform": "LINUX",
                "assetType": "HOST"
            },
            "category": [
                ""
            ],
            "nodeId": "xxx5056f-xxx9-xxx5-xxxb-xxx826773xxx",
            "uniqueId": "6561xxxxxxxx71xxxxx"
        }
    ]
```


Next API request:

```
curl --location --request GET
'https://'https://gateway.xxx.eng.xxx.qualys.com/ioc/incidents/events/scr
oll?scrollId=<scroll_id>' --header 'Authorization: Bearer <token> \
```

Response:


```
[
    {
        "dateTime": "2022-10-01T15:30:01.000+0000",
        "eventProcessedTime": "2022-10-01T15:34:54.785+0000",
```

```
        "workflow": 4,
        "eventSource": "EDR",
        "stateDocumentId": "RTF_xxxf627e-xxx3-xxxc-xxx3-
xxx863c3fxxx_7836938903773883484",
        "type": "FILE",
        "actor": {
            "processEventId": "RTP_xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx_-
7833919771257568865_32386",
            "processUniqueId": "-7833919771257568865",
            "processId": 32386,
            "processName": "/usr/sbin/syslog-ng",
            "userName": "root",
            "imageFullPath": "/usr/sbin/syslog-ng"
        },
        "score": "5",
        "scoreSource": "SIDDHI",
        "file": {
            "fullPath": "/var/log/cron",
            "path": "/var/log",
            "fileName": "cron",
            "createdDate": "2022-10-01T15:17:07.000+0000",
           "sha256": "xxxf33b5xxxa2b77625xxx078cxxx1f5xx0f0xx0xxxf8c9bf",
            "size": 28736,
            "accessDate": "2022-10-01T15:17:07.000+0000",
            "nonPEFile": false,
            "writeDate": "2022-10-01T15:30:01.000+0000",
            "macroEmbedded": false,
            "fileType": "regularfile",
            "md5": "xxx3cexxd460xx089b2xxc9fxx8710"
        },
        "techniques": [
            {
                "techniqueName": "Ingress Tool Transfer",
                "techniqueScore": 5,
                "techniqueId": "T1105"
            }
        ],
        "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
        "action": "WRITE",
        "tactics": [
            {
                "tacticName": "Command and Control",
                "tacticId": "TA0011"
            }
        ],
        "ruleNames": [
            "AK1001"
        ],
        "id": "RTF_xxx584ec-xxx3-xxx4-xxx7-xxx738330xxx_1-10-2022",
```

```
        "incidentId": "xxx676ad-xxxe-34b8-axxx-e0xxxbefxxx9",
        "asset": {
            "fullOSName": "CentOS Linux 7.9.2009",
            "hostName": "xxxxxxx.xxx.xxx.xxxx.qualys.com",
            "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcade1-xxx5-xxx1-xxx3-xxx08f55bxxx",
            "platform": "LINUX",
            "assetType": "HOST"
        },
        "nodeId": "xxxd4ea1-xxxa-xxx7-xxx4-xxxcbb193xxx",
        "uniqueId": "xxx36xxxxxx3883484"
    },
    {
        "dateTime": "2022-10-01T16:30:01.000+0000",
        "eventProcessedTime": "2022-10-01T16:35:01.803+0000",
        "workflow": 4,
        "eventSource": "EDR",
        "stateDocumentId": "RTF_xxxf627e-xxx3-xxxc-xxx3-
xxx863c3fxxx_7836xxxxxx3883484",
        "type": "FILE",
        "actor": {
            "processEventId": "RTP_xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx_-
7833xxxxxx68865_32386",
            "processUniqueId": "-xxx39xxxxx688xxx",
            "processId": 32386,
            "processName": "/usr/sbin/syslog-ng",
            "userName": "root",
            "imageFullPath": "/usr/sbin/syslog-ng"
        },
        "score": "5",
        "scoreSource": "SIDDHI",
        "file": {
            "fullPath": "/var/log/cron",
            "path": "/var/log",
            "fileName": "cron",
            "createdDate": "2022-10-01T16:17:14.000+0000",
            "sha256": "3xxx4db24868xxxxx678xxxxx3fc77xxxxxx7axxxxx83",
            "size": 31006,
            "accessDate": "2022-10-01T16:17:14.000+0000",
            "nonPEFile": false,
            "writeDate": "2022-10-01T16:30:01.000+0000",
            "macroEmbedded": false,
            "fileType": "regularfile",
            "md5": "xxxa0f9xxx29b16eba9xxxxe85c1exxx"
        },
        "techniques": [
            {
                "techniqueName": "Ingress Tool Transfer",
```

```
                "techniqueScore": 5,
                "techniqueId": "T1105"
            }
        ],
        "customerId": "xxxcxxe1-xxx5-xxx1-xxx3-xxx08f55bxxx",
        "action": "WRITE",
        "tactics": [
            {
                "tacticName": "Command and Control",
                "tacticId": "TA0011"
            }
        ],
        "ruleNames": [
            "AK1001"
        ],
        "id": "RTF_xxx806a0-xxxd-xxx9-xxx4-xxxc6a154xxx_1-10-2022",
        "incidentId": "xxx676ad-xxxe-34b8-axxx-e0xxxbefxxx9",
        "asset": {
            "fullOSName": "CentOS Linux 7.9.2009",
            "hostName": "xxxxxxx.xxxxx.xxxxx.xxxxx.xxxxx.com",
            "agentId": "xxxf627e-xxx3-xxxc-xxx3-xxx863c3fxxx",
            "isQuarantineHost": false,
            "customerId": "xxxcxxe1-xxx5-xxx1-xxx3-xxx08f55bxxx",
            "platform": "LINUX",
            "assetType": "HOST"
        },
        "nodeId": "xxxd4ea1-xxxa-xxx7-xxx4-xxxcbb193xxx",
        "uniqueId": "7836xxxxxx3883484"
    }
]
```