



# Indication of Compromise API

User Guide  
Version 2.0

August 19, 2019

Copyright 2019 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



# Table of Contents

<b>Preface</b> .....	<b>4</b>
About Qualys .....	4
Contact Qualys Support.....	4
<b>Chapter 1 - Welcome</b> .....	<b>5</b>
Qualys API Framework .....	5
Introduction to IOC API Paradigm .....	7
<b>Chapter 2 - IOC Events API</b> .....	<b>9</b>
Fetch events within a date range .....	9
Get event count for a date range .....	13
Fetch event details .....	14

# Preface

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

## About Qualys

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

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

## Contact Qualys Support

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

# Chapter 1 - Welcome

Welcome to Indication of Compromise API.

## Get Started

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

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

## Get API Notifications

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

### From our Community

[Join our Community](#)

[API Notifications RSS Feeds](#)

## Qualys API Framework

The Qualys Indication of Compromise API uses the following framework.

### Request URL

The URL for making API requests respects the following structure:

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

where the components are described below.

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

## Base URL to the Qualys API Server

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

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

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

## Introduction to IOC API Paradigm

### Authentication

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

For example,

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

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

- **username** and **password** are the credentials of the user account for which you want to fetch IOC data
- **token** should be true
- **Content-Type** should be "application/x-www-form-urlencoded"

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

### Using Curl

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

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

The following Curl options are used according to different situations:

Option	Description
-G	The GET method is required for all IOC API requests.
-H "Authorization: Bearer <token>"	This option is used to provide a custom HTTP request header parameter for authentication. Provide the JSON Web Token (JWT) received from Qualys authentication API in the following format: Authorization: Bearer <token> For information about Qualys authentication API, see <a href="#">Authentication</a> .
--data-urlencode	Used to encode spaces and special characters in the URL/Parameter values.

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

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



# Chapter 2 - IOC Events API

Use these API functions to fetch IOC event data.

[Fetch events within a date range](#)

[Get event count for a date range](#)

[Fetch event details](#)

## Fetch events within a date range

`/ioc/events`

[GET]

Get IOC events in the user account filtered by date range.

### Input Parameters

<code>fromDate</code> (String)	Show events logged after a certain date. Supports epoch time / unix timestamp. See <a href="https://en.wikipedia.org/wiki/Unix_time">https://en.wikipedia.org/wiki/Unix_time</a> 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 drill down further by applying the time value.
<code>toDate</code> (String)	Show events logged until a certain date. Supports epoch time / unix timestamp. See <a href="https://en.wikipedia.org/wiki/Unix_time">https://en.wikipedia.org/wiki/Unix_time</a> 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.
<code>filter</code> (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 - <code>event.datetime : ['2017-01-01T05:33:34' .. '2017-01-31T05:33:34'] AND action: 'Created'</code> Note: It is recommended to use the "event.datetime" parameter if you want to fetch events by date AND time.
<code>pageNumber</code> (String)	The page to be returned. Starts from zero.
<code>pageSize</code> (String)	The number of records per page to be included in the response. Default is 10.
<code>sort</code> (String)	Sort the results using a Qualys token. For example - <code>[{"action": "asc"}]</code>

---

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.
state (Boolean)	Set state to "true" if you want to fetch events only from the current state.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken.

---

## Sample

### Request:

```
curl -G --data-urlencode "state=true" --data-urlencode  
"filter=type:file"  
"https://gateway.qg2.apps.qualys.com/ioc/events" -H  
"Authorization:Bearer <token>"
```

### Response:

```
[  
  {  
    "dateTime": "2019-06-10T07:34:01.000+0000",  
    "file": {  
      "fullPath": "C:\\WINDOWS\\WinSxS\\amd64_netfx4-  
system.resources.writer_b03f5f7f11d50a3a_4.0.15671.0_none_86de4e43  
19dba14f\\System.Resources.Writer.dll",  
      "path": "C:\\WINDOWS\\WinSxS\\amd64_netfx4-  
system.resources.writer_b03f5f7f11d50a3a_4.0.15671.0_none_86de4e43  
19dba14f",  
      "extension": "dll",  
      "fileName": "System.Resources.Writer.dll",  
      "createdDate": "2018-04-11T23:35:16.825+0000",  
      "sha256":  
"ff0ea5d10cb04dac122e0768fbed2dd1f022ebee91b1ab51295c0ceb300b0c3c"  
,  
      "md5": "21647807ce1396e6aa9cd54435a63afb"  
    },  
    "timeSeriesId": "F_7dc23490-dcc6-3654-bd27-b3140c226eac_10-6-  
2019",
```

```
    "action": "CREATED",
    "id": "F_50f17eea-8963-4a33-8b8e-bd56bc970f54_-
8414843404120473211",
    "type": "FILE",
    "asset": {
      "fullOSName": "Microsoft Windows 10 Pro 10.0.17134 Build
17134",
      "hostName": "WIN10-95-107",
      "agentId": "50f17eea-8963-4a33-8b8e-bd56bc970f54",
      "interfaces": [
        {
          "ipAddress": "10.115.95.107"
        }
      ],
      "netBiosName": "WIN10-95-107",
      "customerId": "e468ee44-ee1e-e89f-8239-5c264e797471",
      "platform": "WINDOWS"
    }
  },
  {
    "dateTime": "2019-06-10T07:33:12.000+0000",
    "file": {
      "fullPath": "C:\\WINDOWS\\WinSxS\\amd64_microsoft-windows-
wmi-
scripting_31bf3856ad364e35_10.0.17134.1_none_4691c4ee5be79e17\\wbe
mdisp.tlb",
      "path": "C:\\WINDOWS\\WinSxS\\amd64_microsoft-windows-wmi-
scripting_31bf3856ad364e35_10.0.17134.1_none_4691c4ee5be79e17",
      "extension": ".tlb",
      "fileName": "wbemdisp.tlb",
      "createdDate": "2018-04-11T23:34:40.369+0000",
      "sha256":
"9b45cef2a114457656f0221ab11ecce497c8749af8916706050e35d789ffb6e4"
,
      "md5": "a4f85f017eada091bb1f828bbe354335"
    },
    "timeSeriesId": "F_f80f4e9f-ed6b-3280-8518-d7b4be619d8f_10-6-
2019",
    "action": "CREATED",
    "id": "F_8c95026d-c8c8-4502-b3c4-
0e79ad8ec846_751402726227817552",
    "type": "FILE",
    "asset": {
      "fullOSName": "Microsoft Windows 10 Pro 10.0.17134 Build
17134",
      "hostName": "WIN10-95-107",
```

```
"agentId": "8c95026d-c8c8-4502-b3c4-0e79ad8ec846",
"interfaces": [
  {
    "ipAddress": "10.115.95.107"
  }
],
"netBiosName": "WIN10-95-107",
"customerId": "e468ee44-ee1e-e89f-8239-5c264e797471",
"platform": "WINDOWS"
}
},
{
  "dateTime": "2019-06-10T08:19:04.000+0000",
  "file": {
    "fullPath": "C:\\WINDOWS\\System32\\en-US\\fltlib.dll.mui",
    "path": "C:\\WINDOWS\\System32\\en-US",
    "extension": ".mui",
    "fileName": "fltlib.dll.mui",
    "createdDate": "2018-04-12T09:15:04.125+0000",
    "sha256":
"325cb3d1326890efd1212f6cc53ce30c6103e4f01d6ed8252d1130d6b018a4c6"
,
    "md5": "71994230ebcae5a23f1288f4e21e799e"
  },
  "timeSeriesId": "F_d184b469-2748-3f5e-aa95-18b3597c2e3c_10-6-
2019",
  "action": "CREATED",
  "id": "F_6a743abf-3b8e-463d-b089-deeb9dbb5129_-
8493612420176684885",
  "type": "FILE",
  "asset": {
    "fullOSName": "Microsoft Windows 10 Pro 10.0.17134 Build
17134",
    "hostName": "WIN10-95-107",
    "agentId": "6a743abf-3b8e-463d-b089-deeb9dbb5129",
    "interfaces": [
      {
        "ipAddress": "10.115.95.107"
      }
    ],
    "netBiosName": "WIN10-95-107",
    "customerId": "e468ee44-ee1e-e89f-8239-5c264e797471",
    "platform": "WINDOWS"
  }
}
}
]
```

## Get event count for a date range

`/ioc/events/count`

[GET]

Get number of events logged within a date range.

### Input Parameters

<code>fromDate</code> (String)	Events logged after a certain date. Supports epoch time / unix timestamp. See <a href="https://en.wikipedia.org/wiki/Unix_time">https://en.wikipedia.org/wiki/Unix_time</a> 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 drill down further by applying the time value.
<code>toDate</code> (String)	Events logged until a certain date. Supports epoch time / unix timestamp. See <a href="https://en.wikipedia.org/wiki/Unix_time">https://en.wikipedia.org/wiki/Unix_time</a> 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.
<code>filter</code> (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' Note: It is recommended to use the "event.datetime" parameter if you want to fetch events by date AND time.
<code>groupBy</code> (String)	Group results based on certain parameters (provide comma separated list). For example - agentId
<code>limit</code> (String)	Limit the number of rows fetched by the groupBy function.
<code>sort</code> (String)	Sort the results using a Qualys token. For example - [{"action": "asc"}]
<code>interval</code> (String)	GroupBy interval for date fields. Valid values are y(year), q(quarter), M(month), w(week), d(day), h(hour), m(minute), s(second). For example - 1d
<code>state</code> (Boolean)	Set state to "true" if you want to fetch events only from the current state.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

### Sample

Request:

```
curl -G --data-urlencode "state=true" --data-urlencode  
"filter=type:file"  
"https://gateway.qg2.apps.qualys.com/ioc/events/count" -H  
"Authorization:Bearer <token>"
```

Response:

```
{
  "count": 18048196
}
```

## Fetch event details

`/ioc/events/{agentId}/{eventId}`

[GET]

Fetch details for an event.

## Input Parameters

agentId (String)	(Required) ID of the agent you want to fetch the details for.
eventId (String)	(Required) ID of the event you want to fetch the details for.
state (Boolean)	Set state to "true" if you want to fetch events only from the current state.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

## Sample

Request:

```
curl -G --data-urlencode "state=true"
"https://gateway.qg2.apps.qualys.com/ioc/events/fe1118a2-222a-
1111-abcd-28edac4ff111/F_fe1118a2-222a-1111-abcd-
28edac4ff111_111150815650803056" -H "Authorization:Bearer <token>"
```

Response:

```
{
  "customerId": "e468ee44-ee1e-e89f-8239-5c264e797471",
  "score": null,
  "familyName": null,
  "verdict": null,
  "category": null,
  "infections": null,
  "id": "F_7dc23490-dcc6-3654-bd27-b3140c226eac_10-6-2019",
  "dateTime": "2019-06-10T07:34:01.000+0000",
  "type": "FILE",
  "action": "CREATED",
  "asset": {
    "agentId": "50f17eea-8963-4a33-8b8e-bd56bc970f54",
```

```

    "customerId": "e468ee44-ee1e-e89f-8239-5c264e797471",
    "netBiosName": "WIN10-95-107",
    "platform": "WINDOWS",
    "fullOSName": "Microsoft Windows 10 Pro 10.0.17134 Build
17134",
    "assetType": null,
    "tags": null,
    "interfaces": [
      {
        "ipAddress": "10.115.95.107"
      }
    ],
    "lastLoggedOnUser": null,
    "hostName": "WIN10-95-107"
  },
  "file": {
    "path": "C:\\WINDOWS\\WinSxS\\amd64_netfx4-
system.resources.writer_b03f5f7f11d50a3a_4.0.15671.0_none_86de4e43
19dba14f",
    "fullPath": "C:\\WINDOWS\\WinSxS\\amd64_netfx4-
system.resources.writer_b03f5f7f11d50a3a_4.0.15671.0_none_86de4e43
19dba14f\\System.Resources.Writer.dll",
    "md5": "21647807ce1396e6aa9cd54435a63afb",
    "sha256":
"ff0ea5d10cb04dac122e0768fbed2dd1f022ebee91b1ab51295c0ceb300b0c3c"
  },
  "fileType": null,
  "owner": null,
  "extension": "dll",
  "size": 28808,
  "accessDate": "2019-02-21T07:23:47.870+0000",
  "writeDate": "2018-04-11T23:35:16.825+0000",
  "devicePath": null,
  "deviceLetter": "C",
  "company": "Microsoft Corporation",
  "copyright": "© Microsoft Corporation. All rights reserved.",
  "description": "System.Resources.Writer",
  "publisher": null,
  "version": "4.7.3056.0",
  "product": "Microsoft® .NET Framework",
  "permission": null,
  "securityAttributes": "O:S-1-5-80-956008885-3418522649-
1831038044-1853292631-2271478464G:S-1-5-80-956008885-3418522649-
1831038044-1853292631-2271478464D:PAI(A;;FA;;;S-1-5-80-956008885-
3418522649-1831038044-1853292631-
2271478464)(A;;0x1200a9;;;BA)(A;;0x1200a9;;;SY)(A;;0x1200a9;;;BU)(

```

```
A;;0x1200a9;;;AC) (A;;0x1200a9;;;S-1-15-2-  
2)S:AI (AU;SAFA;DCLCRPCRSWDWO;;;WD) ",  
  "manifestId": null,  
  "fileName": "System.Resources.Writer.dll",  
  "createdDate": "2018-04-11T23:35:16.825+0000"  
},  
"registry": null,  
"indicator1": null,  
"indicator2": null,  
"process": null,  
"mutex": null,  
"network": null  
}
```