Endpoint Detection and Response API

User Guide
Version 1.0

September 21, 2020

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

Table of Contents

Preface

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

EDR is an evolved superset of the IOC app. EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

The IOC endpoints documented in this guide will work with the new EDR 1.0 release.

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.

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/.

Chapter 1 - Welcome

Welcome to Endpoint Detection and Response 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 EDR 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 Endpoint Detection and Response 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.

<baseurl>	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: https://gateway.qg1.apps.qualys.com
<module>	The API module.
<object>	The module specific object.
<object_id>	(Optional) The module specific object ID, if appropriate.
<operation>	The request operation, such as count.

Qualys API URL

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

Click here to identify your Qualys platform and get the API URL

This documentation uses the API gateway URL for Qualys US Platform 1 (https://gateway.qg1.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate gateway URL for your account.

Introduction to EDR 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 EDR 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 EDR 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 EDR API calls. The token expires in 4 hours. You must regenerate the token to continue using the EDR 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 EDR 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 Authentication.
--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 - EDR Events API

Use these API functions to fetch EDR event data.

Fetch events within a date range

/ioc/events

[GET]

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

Input Parameters

fromDate (String)	Show events logged after a certain date. Supports epoch time / unix timestamp. See https://en.wikipedia.org/wiki/Unix_time 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.
toDate (String)	Show events logged until a certain date. Supports epoch time / unix timestamp. See https://en.wikipedia.org/wiki/Unix_time 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 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.
pageNumber (String)	The page to be returned. Starts from zero.
pageSize (String)	The number of records per page to be included in the response. Default is 10.

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.
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": "2020-08-17T04:15:06.000+0000",
    "actor": {
      "processId": 1612,
      "processName": "svchost.exe",
      "type": "PROCESS",
      "userName": "NT AUTHORITY\\LOCAL SERVICE",
      "imageFullPath": "C:\\Windows\\System32\\svchost.exe",
      "userId": "LOCAL SERVICE",
      "createDate": "1970-01-01T00:00:00.000+0000"
    },
    "score": "0",
    "eventProcessedTime": "2020-08-22T08:17:53.202+0000",
    "file": {
      "fullPath": "C:\\Windows\\System32",
      "path": "C:\\Windows\\System32",
```

```
      "extension": "dll",
      "fileName": "energyprov.dll",
      "createdDate": "2019-03-19T04:43:45.586+0000",
      "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364f60x3x81x24217x433x10x"
,
      "certificates": [
        {
          "certificateSigned": true,
          "certificateIssuer": "DigiCert High Assurance Code
Signing CA-1",
          "certificateValid": true,
          "certificateIssuedTo": "Xxxxx Operations XxxX & Co. KG",
          "certificateSignedDate": "2019-12-16T00:00:00.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA 2010",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2019-05-02T21:25:42.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Windows Production PCA
2011",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Windows",
          "certificateSignedDate": "2019-03-27T19:21:43.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2008-10-22T21:24:55.000+0000"
        },
        {
          "certificateSigned": true,
          "certificateIssuer": "Microsoft Code Signing PCA 2011",
          "certificateValid": true,
          "certificateIssuedTo": "Microsoft Corporation",
          "certificateSignedDate": "2020-03-04T18:39:48.000+0000"
        }
      ],
      "md5": "684475093x4x806350x80xxxx3x11332"
```

```
    },
    "action": "CREATED",
    "indicator2": [
      {
        "score": 0,
        "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x"
,
        "familyName": " ",
        "verdict": "KNOWN",
        "category": " ",
        "rowId": "-3836563445362934026"
      }
    ],
    "id": "RTF_x82xx34x-5xxx-4110-9878-x91x5x476f47_-
3836563445362934026",
    "type": "FILE",
    "asset": {
      "fullOSName": "Microsoft Windows 10 Enterprise 10.0.18363
Build 18363",
      "hostName": "132017-T490.corp.qualys.com",
      "agentId": "x82xx34x-5xxx-4110-9878-x91x5x476f47",
      "netBiosName": "132017-T490",
      "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
      "platform": "WINDOWS"
    }
  }
]
```

Get event count for a date range

/ioc/events/count

[GET]

Get number of events logged within a date range.

Input Parameters

fromDate (String)	Events logged after a certain date. Supports epoch time / unix timestamp. See https://en.wikipedia.org/wiki/Unix_time 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.
toDate (String)	Events logged until a certain date. Supports epoch time / unix timestamp. See https://en.wikipedia.org/wiki/Unix_time 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 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.
groupBy (String)	Group results based on certain parameters (provide comma separated list). For example - agentId
limit (String)	Limit the number of rows fetched by the groupBy function.
sort (String)	Sort the results using a Qualys token. For example - [{"action":"asc"}]
interval (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
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/count" -H
"Authorization:Bearer <token>"
```

Response:

```
{
    "count": 55279
}
```

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:

```
{
  "score": 0,
  "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
  "verdict": [
    "KNOWN"
```

```
  ],
  "category": [
    ""
  ],
  "familyName": [
    ""
  ],
  "eventId": "RTF_x82xx34x-5xxx-4110-9878-x91x5x476x47_-
3836563445362934026",
  "dateTime": "2020-08-17T04:15:06.000+0000",
  "type": "FILE",
  "action": "CREATED",
  "asset": {
    "agentId": "x82xx34x-5xxx-4110-9878-x91x5x476x47",
    "customerId": "8380x005-x923-x37x-8032-42xx709x6xx7",
    "netBiosName": "132017-T490",
    "platform": "WINDOWS",
   "fullOSName": "Microsoft Windows 10 Enterprise 10.0.18363 Build
18363",
    "hostName": "132017-X490.corp.qualys.com"
  },
  "file": {
    "path": "C:\\Windows\\System32",
    "fullPath": "C:\\Windows\\System32//energyprov.dll",
    "md5": "684475093x4x806350x80xxxx3x11332",
    "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x"
,
    "extension": "dll",
    "size": 178688,
    "accessDate": "2020-02-13T07:07:44.325+0000",
    "writeDate": "2019-03-19T04:43:45.586+0000",
    "deviceLetter": "C",
    "company": "Microsoft Corporation",
    "copyright": "© Microsoft Corporation. All rights reserved.",
    "version": "10.0.18362.1",
    "product": "Microsoft® Windows® Operating System",
    "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;DCLCRPCRSDWDWO;;;WD)",
    "fileName": "energyprov.dll",
    "createdDate": "2019-03-19T04:43:45.586+0000",
```

```
    "certificates": [
      {
        "certificateHash": "3484479880440166040",
       "certificateIssuer": "DigiCert High Assurance Code Signing
CA-1",
        "certificateIssuedTo": "Avira Operations GmbH & Co. KG",
        "certificateValid": true,
        "certificateSigned": true,
        "certificateSignedDate": "2019-12-16T00:00:00.000+0000",
        "subject": "Avira Operations GmbH & Co. KG",
        "expiryDate": "2021-11-16T12:00:00.000+0000"
      },
      {
        "certificateHash": "3504057697670195553",
        "certificateIssuer": "Microsoft Code Signing PCA 2010",
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2019-05-02T21:25:42.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2020-05-02T21:25:42.000+0000"
      },
      {
        "certificateHash": "3538015942716645516",
        "certificateIssuer": "Microsoft Windows Production PCA
2011",
        "certificateIssuedTo": "Microsoft Windows",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2019-03-27T19:21:43.000+0000",
        "subject": "Microsoft Windows",
        "expiryDate": "2020-03-27T19:21:43.000+0000"
      },
      {
        "certificateHash": "3549218827299643443",
        "certificateIssuer": "Microsoft Code Signing PCA",
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": false,
        "certificateSigned": true,
        "certificateSignedDate": "2008-10-22T21:24:55.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2010-01-22T21:34:55.000+0000"
      },
      {
        "certificateHash": "3563733393992181563",
        "certificateIssuer": "Microsoft Code Signing PCA 2011",
```

```
        "certificateIssuedTo": "Microsoft Corporation",
        "certificateValid": true,
        "certificateSigned": true,
        "certificateSignedDate": "2020-03-04T18:39:48.000+0000",
        "subject": "Microsoft Corporation",
        "expiryDate": "2021-03-03T18:39:48.000+0000"
      }
    ]
  },
  "indicator2": [
    {
      "score": "0",
      "sha256":
"91511x1x0349xxxx43x1067xx627798x5038752364x60x3x81x24217x433x10x"
,
      "familyName": " ",
      "verdict": "KNOWN",
      "category": " ",
      "rowId": "-3836563445362934026"
    }
  ],
  "actor": {
    "state": "RUNNING",
    "eventId": "RTP_x82xx34x-5xxx-4110-9878-x91x5x476x47_-
7916036775084163258_1612",
    "arguments": "-k LocalServiceNetworkRestricted -p -s
TimeBrokerSvc",
    "elevated": "false",
    "userName": "NT AUTHORITY\\LOCAL SERVICE",
    "processId": 1612,
    "parentProcessId": 0,
    "processName": "svchost.exe",
    "imageFullPath": "C:\\Windows\\System32\\svchost.exe"
  }
}
```