Malware Detection API

User Guide

Version 2.35

November 28, 2018
# Table of Contents

Get Started ....................................................................................................................................3

Malware Detection API ..........................................................................................................3

Making API calls ...................................................................................................................... 4

URL to Qualys API server .................................................................................................... 6

Qualys user account .............................................................................................................. 8

Output pagination and truncation ................................................................................... 9

JSON support ......................................................................................................................... 12

Know your portal version................................................................................................. 16

MD APIs ......................................................................................................................................... 18

  Current malware detection count ................................................................................... 18

  Search malware detections .............................................................................................. 20

  View malware detection details ..................................................................................... 23

Troubleshooting ........................................................................................................................ 25

  MD error messages ............................................................................................................. 25
Get Started

Malware Detection API

The Malware Detection API supports the download of information from the Malware Detection module, when this module is enabled your Qualys account.

Modules supported

MD

Authentication

Authentication to your Qualys account with valid Qualys credentials is required for making Qualys API requests to the Qualys API servers. Learn more about authentication to your Qualys account.

Get API Notifications

We recommend you join our Community and subscribe to our API Notifications RSS Feeds for announcements and discussions.

https://community.qualys.com/community/developer/notifications-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 Cloud Apps deliver businesses critical security intelligence continuously, enabling them to automate the full spectrum of auditing, compliance and protection for IT systems and web applications on premises, on endpoints and elastic clouds. For more information, please visit www.qualys.com

Qualys and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.
Making API calls

Curl samples in our API doc

We use curl in our API documentation to show an example how to form REST API calls, and it is not meant to be an actual production example of implementation.

GET and POST Methods

Qualys API functions allow API users to submit parameters (name=value pairs) using the GET and/or POST method. There are known limits for the amount of data that can be sent using the GET method, and these limits are dependent on the toolkit used. Please refer to the individual descriptions of the API function calls to learn about the supported methods for each function.

Parameters in URLs

API parameters, as documented in this user guide, should be specified one time for each URL. In the case where the same parameter is specified multiple times in a single URL, the last parameter takes effect and the previous instances are silently ignored. URL elements are case sensitive.

Date format in API Results

The Qualys API has adopted a date/time format to provide consistency and interoperability of the Qualys API with third-party applications. The date format follows standards published in RFC 3339 and ISO 8601, and applies throughout the Qualys API. The date format is: yyyy-mm-ddThh-mm-ssZ This represents a UTC value (GMT time zone).

URL Encoding in API Code

You must URL encode variables when using the Qualys API. This is standard practice for HTTP communications. If your application passes special characters, like the single quote (‘), parentheses, and symbols, they must be URL encoded. For example, the pound (#) character cannot be used as an input parameter in URLs. If “#” is specified, the Qualys API returns an error. To
specify the “#” character in a URL you must enter the encoded value “%23”. The “#” character is considered by browsers and other Internet tools as a separator between the URL and the results page, so whatever follows an un-encoded “#” character is not passed to the Qualys API server and returns an error.

Making requests with URL payload

While it is still possible to create simple API requests using the GET method, you can create API requests using the POST method with an XML payload to make an advanced request.

The XML payloads can be compared to a scripting language that allows user to make multiple actions within one single API request, like adding a parameter to an object and updating another parameter.

The XML structure of the payload is described in the XSD files.
URL to Qualys API server

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

<table>
<thead>
<tr>
<th>Account location</th>
<th>API server URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://qualysapi.qualys.com">https://qualysapi.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.com">https://qualysapi.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://qualysapi.qg3.apps.qualys.com">https://qualysapi.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://qualysapi.qualys.eu">https://qualysapi.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://qualysapi.qg2.apps.qualys.eu">https://qualysapi.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://qualysapi.qg1.apps.qualys.in">https://qualysapi.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>Qualys Private Cloud Platform</td>
<td><a href="https://qualysapi">https://qualysapi</a>.&lt;customer_base_url&gt;</td>
</tr>
</tbody>
</table>

Looking for your API server URL for your account? You can find this easily. Just log in to your Qualys account and go to Help > About. You’ll see this information under Security Operations Center (SOC).
Qualys user account

The application must authenticate using Qualys account credentials (user name and password) as part of the HTTP request. The credentials are transmitted using the “Basic Authentication Scheme” over HTTPS.

For more information, see the “Basic Authentication Scheme” section of RFC #2617:

http://www.faqs.org/rfcs/rfc2617.html

The exact method of implementing authentication will vary according to which programming language is used.

Basic authentication - recommended option:

curl -u "USERNAME:PASSWORD"
https://qualysapi.qualys.com/qps/rest/1.0/download/cm/alert

where qualysapi.qualys.com is the base URL to the Qualys API server where your account is located.
Output pagination and truncation

The XML output of a search API request is paginated and the default page size is 100 object records. The page size can be customized to a value between 1 and 1,000. If the number of records is greater than the page size then the <ServiceResponse> element shows the response code SUCCESS with the element <hasMoreRecords>true</hasMoreRecords> as shown below.

Follow the simple process below to obtain the first two the XML pages for an API request. Please apply the same logic to get all the next (n+1) pages until all records are returned. This is indicated when <hasMoreRecords>false</hasMoreRecords>.

Step 1 - Search for malware detection alerts of type behavioral.

**API request**

```bash
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/search/md/detection/" < file.xml
Note: “file.xml” contains the request POST data.
```

**Request POST data**

```xml
<ServiceRequest>
  <preferences>
    <limitResults>5</limitResults>
  </preferences>
  <filters>
    <Criteria field="type" operator="EQUALS">BEHAVIORAL</Criteria>
  </filters>
</ServiceRequest>
```

In the response, the number of records is greater than the default pagination value so the <ServiceResponse> element identifies the last ID of the object in the current page output.
Response

```xml
<ServiceResponse ...>
  <responseCode>SUCCESS</responseCode>
  <COUNT>5</COUNT>
  <hasMoreRecords>true</hasMoreRecords>
  <lastId>123</lastId>
  <data>
    <!-- here you will find 5 alert records -->
  </data>
</ServiceResponse>
```

Step 2 - Search alerts and get next batch of results

To get the next page of results, you need to edit your service request in “file.xml” that will be passed to API request as a POST payload. According to the `<lastId>` element returned in the first page, you want the next page of results to start with the object ID 124 or greater.

**API request**

```bash
curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST"
--data-binary @-
"https://qualysapi.qualys.com/ps/rest/1.0/search/md/detection/" < file.xml
```

Note: “file.xml” contains the request POST data.

You’ll notice the operator field value is set to 123, which is the value returned in `<lastId>` of the previous page output. The GREATER operator is a logical “greater than” (it does not mean greater than or equal to).

**Request POST data**

```xml
<ServiceRequest>
  <filters>
    <Criteria field="type" operator="EQUALS">BEHAVIORAL</Criteria>
    <Criteria field="id" operator="GREATER">123</Criteria>
  </filters>
</ServiceRequest>
```
Set custom page size

The service request needs to contain the <preferences> section with the <limitResults> parameter. For the <limitResults> parameter you can enter a value from 1 to 1,000.

Response

```xml
<ServiceRequest>
    <filters>
        <Criteria> ... </Criteria>
    </filters>
    <preferences>
        <limitResults>200</limitResults>
    </preferences>
</ServiceRequest>
```
JSON support

The Qualys Malware Detection API supports JSON requests and responses. Headers used in samples below.

Send JSON request - "Content-Type: application/json"

Get response in JSON - "Accept: application/json"

Sample - Search Malware Detections

**API request**

```
```

**Request POST data**

```
{
    "ServiceRequest": {
        "preferences": { "limitResults": "100" },
        "filters": {
            "Criteria": [
                { "-field": "id", 
                  "-operator": "EQUALS",
                  "#text": "37747097"
                },
                { "-field": "url",
                  "-operator": "CONTAINS",
                  "#text": "http://www.mwtest.info/malware-demos-named/"
                },
                { "-field": "type",
                  "-operator": "EQUALS",
                  "#text": "BEHAVIORAL"
                }
            ]
        }
    }
}
```
Response
{
    "ServiceResponse": {
        "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
        "xsi:noNamespaceSchemaLocation": "https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd",
        "responseCode": "SUCCESS",
        "count": "1",
        "hasMoreRecords": "false",
        "data": {
            "Detection": {
                "id": "37747097",
                "qid": "206012",
                "name": "A Malicious Process Launch Was Detected",
                "type": "BEHAVIORAL",
                "severity": "HIGH",
                "url": "http://www.mwtest.info/malware-demos-named/MS06-014-RemotePayload/MS06-014-DEMO.html"
            }
        }
    }
}

Sample - Get details for malware detection

API request

curl -X GET -s -k -H "Accept: application/json" -n -u "{USERNAME}:{PASSWORD}" "https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/37747097"

Response
{
    
}
A Malicious Process Launch Was Detected

Upon visiting the Web page, a process launch was detected by the malware detection service. External process launches should never occur in normal Web browsing activity. This is an indication of malicious behavior. The process launched is noted in the Results section.

Process creation was attempted on application C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\hgivV.exe with parameters (Undefined)

http://www.mwtest.info/malware-demos-named/MS06-014-RemotePayload/MS06-014-DEMO.html
Know your portal version

/qps/rest/portal/version/

[GET] [POST]

Using the Version API you can find out the installed version of Portal and its sub-modules that are available in your subscription.

Sample XML

API request


Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <data>
    <Portal-Version>
      <WAS-VERSION>6.0.0.0</WAS-VERSION>
      <FIM-VERSION>1.5.1</FIM-VERSION>
      <VM-VERSION>1.0.3</VM-VERSION>
      <CERTVIEW-VERSION>1.1.0.0</CERTVIEW-VERSION>
      <CM-VERSION>1.20.1</CM-VERSION>
      <MDS-VERSION>2.11.7.0</MDS-VERSION>
      <CA-VERSION>2.9.1.0</CA-VERSION>
      <IOC-VERSION>1.1.0</IOC-VERSION>
      <AV2-VERSION>0.1.0</AV2-VERSION>
      <QUESTIONNAIRE-VERSION>2.14.0.4</QUESTIONNAIRE-VERSION>
      <WAF-VERSION>2.7.0.0</WAF-VERSION>
    </Portal-Version>
  </data>
</ServiceResponse>
```
Sample JSON

**API request**

**Response**
```json
{
    "ServiceResponse": {
        "data": [
            {
                "Portal-Version": {
                    "WAS-VERSION": "6.0.0.0",
                    "VM-VERSION": "1.0.3",
                    "CM-VERSION": "1.20.1",
                    "MDS-VERSION": "2.11.7.0",
                    "CA-VERSION": "2.9.1.0",
                    "QUESTIONNAIRE-VERSION": "2.14.0.4",
                    "WAF-VERSION": "2.7.0.0"
                },
                ...
            }
        ],
        "responseCode": "SUCCESS",
        "count": 1
    }
}
```
MD APIs

Current malware detection count

/qps/rest/1.0/count/md/detection/

[POST]

Returns the total number of malware detections in the user’s account. Input elements are optional and are used to filter the number of detections in the count.

Permissions required - Managers with full scope. Other users must have these permissions: Access Permission “API Access” and Asset Management Permission “Read Asset”. Output includes web sites within the user's scope.

Input Parameters

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

Available operators

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>(integer)</td>
</tr>
<tr>
<td>qid</td>
<td>(integer)</td>
</tr>
<tr>
<td>url</td>
<td>(text)</td>
</tr>
<tr>
<td>type</td>
<td>(keyword)</td>
</tr>
<tr>
<td>showDeactivatedSite</td>
<td>(boolean)</td>
</tr>
</tbody>
</table>
Sample - Get malware detection count

**API request**

curl -u "USERNAME:PASSWORD" -H "content-type: text/xml" -X "POST" --data-binary @-
"https://qualysapi.qualys.com/qps/rest/1.0/count/md/detection" < file.xml
Note: “file.xml” contains the request POST data.

**Request POST data**

```
<ServiceRequest>
  <filters>
    <Criteria field="id" operator="GREATER">37747097</Criteria>
  </filters>
</ServiceRequest>
```

**Response**

```
<?xml version="1.0" encoding="UTF-8"?>
<ServiceResponse xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="https://qualysapi.qualys.com/qps/xsd/1.0/md/detection.xsd">
  <responseCode>SUCCESS</responseCode>
  <count>41</count>
</ServiceResponse>
```

**XSD**

`<platform_API_server>/qps/xsd/2.0/md/detection.xsd`
Search malware detections

/qps/rest/1.0/search/md/detection/

[POST]

Returns a list of malware detections in the user’s account.

Limit your results - Use the optional “fields” parameter to limit the amount of information returned. Learn more about limiting your results

Permissions required - Managers with full scope. Other users must have requested asset in their scope and these permissions: Access Permission “API Access” and Asset Management Permission “Read Asset”

Input Parameters

Allowed input elements are listed below. The associated data type for each element appears in parentheses. These elements are optional and act as filters. When multiple elements are specified, parameters are combined using a logical AND.

Available operators

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>(integer)</td>
</tr>
<tr>
<td>qid</td>
<td>(integer)</td>
</tr>
<tr>
<td>url</td>
<td>(text)</td>
</tr>
<tr>
<td>type</td>
<td>(keyword)</td>
</tr>
<tr>
<td>showDeactivatedSite</td>
<td>(boolean)</td>
</tr>
<tr>
<td>severity</td>
<td>(keyword)</td>
</tr>
</tbody>
</table>
Sample - Search detections

**API request**

**Request POST data**

```xml
<ServiceRequest>
  <preferences>
    <limitResults>100</limitResults>
  </preferences>
  <filters>
    <Criteria field="id" operator="EQUALS">37747097</Criteria>
    <Criteria field="url" operator="CONTAINS">http://www.mwtest.info/malware-demos-named/</Criteria>
    <Criteria field="type" operator="EQUALS">BEHAVIORAL</Criteria>
  </filters>
</ServiceRequest>
```

**Response**

```xml
<?xml version="1.0" encoding="UTF-8"?>
  <responseCode>SUCCESS</responseCode>
  <count>1</count>
  <hasMoreRecords>false</hasMoreRecords>
  <data>
    <Detection>
      <id>37747097</id>
      <qid>206012</qid>
      <name><![CDATA[A Malicious Process Launch Was Detected]]></name>
      <type>BEHAVIORAL</type>
      <severity>HIGH</severity>
      <url>
```
<![CDATA[http://www.mwtest.info/malware-demos-named/MS06-014-RemotePayload/MS06-014-DEMO.html]]>
</url>
</Detection>
</data>
</ServiceResponse>

XSD

<platform API server>/qps/xsd/2.0/md/detections.xsd
View malware detection details

/qps/rest/1.0/get/md/detection/<id>

[GET] [POST]

Returns details of a malware detection.

Limit your results - Use the optional “fields” parameter to limit the amount of information returned. Learn more about limiting your results

Permissions required - Managers with full scope. Other users must have requested asset in their scope and these permissions: Access Permission “API Access” and Asset Management Permission “Read Asset”. Output includes web sites in the user’s scope.

Input Parameter

The element “id” (Integer) is required, where “id” identifies the alert.

Sample - Get detection details

API request

curl -u "USERNAME:PASSWORD" -X GET
https://qualysapi.qualys.com/qps/rest/1.0/get/md/detection/37747097

Response

<?xml version="1.0" encoding="UTF-8"?>
    responseCode="SUCCESS"
    count="1"
    data
        <Detection>
            <id>37747097</id>
            <qid>206012</qid>
            <name>
<![CDATA[A Malicious Process Launch Was Detected]]>

<type>BEHAVIORAL</type>
<description>
<!CDATA[Upon visiting the Web page, a process launch was detected by the malware detection service. External process launches should never occur in normal Web browsing activity. This is an indication of malicious behavior. The process launched is noted in the Results section.]]>
</description>
<severity>HIGH</severity>
<url>
 <![CDATA[http://www.mwtest.info/malware-demos-named/MS06-014-RemotePayload/MS06-014-DEMO.html]]>
</url>
<result>
 <![CDATA[Process creation was attempted on application C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\hgivV.exe with parameters (Undefined)]]>
</result>
<asset>
 <id>2688083</id>
 <name>
  <![CDATA[http://www.mwtest.info/malware-demos-named/]]>
 </name>
 <deactivated>false</deactivated>
</asset>
</Detection>
</data>
</ServiceResponse>

XSD

<platform_API_server>/qps/xsd/2.0/md/detection.xsd
# Troubleshooting

## MD error messages

Error messages returned from MD API requests are described below by category.

Error categories: [Element](#) | [Criteria](#) | [Authorization](#) | [Report Storage Limit](#)

### Element

<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>url: Invalid URL format (&lt;value&gt;)</td>
<td>URL format must be as follows: http://&lt;baseUrl&gt;/rest/1.0/?parameters</td>
</tr>
<tr>
<td>Url: Element is required</td>
<td>Element “Url” is required.</td>
</tr>
<tr>
<td>uris.&lt;field&gt;: Invalid URL format (&lt;value&gt;).</td>
<td>For the uri.&lt;field&gt; sub element, specify a URL like <a href="http://domain.name/base/url/?parameters">http://domain.name/base/url/?parameters</a></td>
</tr>
<tr>
<td>uris.&lt;field&gt;: Length of the field must not be greater than 2048 characters. (&lt;value&gt;).</td>
<td>For the uri.&lt;field&gt; sub element, the maximum field length is 2048 characters.</td>
</tr>
<tr>
<td>Attribute.category: Element is required.</td>
<td>The element Attribute.category is required.</td>
</tr>
<tr>
<td>Attribute.category:</td>
<td>Element Attribute.category must be set to one of</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Invalid value (&lt;value&gt;).</td>
<td>these values: Business Function, Business Location, Business Description.</td>
</tr>
<tr>
<td>Attribute.value: Element is required.</td>
<td>Element Attribute.category must be set to one of these values: Business Function, Business Location, Business Description.</td>
</tr>
<tr>
<td>Attribute.value: Element is required.</td>
<td>Provide a value for the attribute in the Attribute.value element: function, location or description.</td>
</tr>
<tr>
<td>The attribute length cannot be greater than 64 characters.</td>
<td>The value for this attribute cannot exceed 64 characters.</td>
</tr>
<tr>
<td>The attribute length cannot be greater than 2048 characters.</td>
<td>The value for this attribute cannot exceed 2048 characters.</td>
</tr>
<tr>
<td>&lt;element&gt;: Element must not be set.</td>
<td>This element does not apply to this request.</td>
</tr>
<tr>
<td>set: Element must contain at least one child.</td>
<td>The set element requires at least one sub element.</td>
</tr>
<tr>
<td>headers: Length of all headers cannot exceed 2048 characters.</td>
<td>The values of all headers cannot exceed 2048 characters.</td>
</tr>
<tr>
<td>At least one of the following elements must be set: set, add, remove.</td>
<td>For an “update” request you must set at least one of these elements: set, add or remove.</td>
</tr>
<tr>
<td>UrlEntry: Element</td>
<td>The element UrlEntry must be provided.</td>
</tr>
</tbody>
</table>
is required.

**UrlEntry: Invalid URL format (value).**
Specify a URL like http://domain.name/base/url/?parameters

**<parent>: Length of all [URLs, regular expressions] cannot exceed 2048 characters**
The list of entries for a given type shall not exceed 2048 characters.

**UrlEntry: Only regular expressions are accepted for this element.**
You must provide regular expressions for the element postDataBlackList.

**tags.<element>: Element must not be set.**
The tags element does not apply for this request.

**tags.set: Element must contain at least one child.**
At least one sub element must be provided for the element tag.set.

**Tag.id: Element is required.**
Provide a value for the element Tag.id

**Tag.id: Invalid value (value).**
Value must be an integer set at least to 1.

**Tag: Tag specified by ID <id> does not exist or is not available.**
Provide a value for the element id that corresponds to a valid tag.
## Criteria

<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria: Field is required.</td>
<td>Specify the name of the criteria to search against.</td>
</tr>
<tr>
<td>Criteria: Invalid criteria (&lt;field name&gt;).</td>
<td>Please search against one of the following criteria: %s.</td>
</tr>
<tr>
<td>Criteria: Invalid operator for criteria '&lt;field&gt;' (&lt;operator&gt;).</td>
<td>Allowed operations for this criteria are: %s.</td>
</tr>
<tr>
<td>Criteria: Value is required for criteria '&lt;field&gt;'.</td>
<td>Specify a value for a field name for search criteria.</td>
</tr>
<tr>
<td>Criteria: Invalid value format for criteria '&lt;field&gt;':</td>
<td>Boolean (true, false). Date and Time in UTC format.</td>
</tr>
<tr>
<td>&lt;value&gt;.</td>
<td>Enumeration (allowed options separated by comma). Other: Specify criteria value(s) as &lt;type&gt;.</td>
</tr>
</tbody>
</table>

## Authorization

<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You are not authorized to access the application through the API.</td>
<td>You must be granted the API Access permission in your roles and scopes.</td>
</tr>
<tr>
<td>No data shall be passed for this</td>
<td>The POST request does not specify a data element.</td>
</tr>
</tbody>
</table>
User is not authorized to perform this operation on specified object(s).

You must be granted access to these objects in your user scope.

Operation %s does not support search filters.

Do not provide search filters for this operation.

Report storage limit

<table>
<thead>
<tr>
<th>Error message</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your [subscription</td>
<td>user] storage limit of &lt;NB&gt; Mb has been reached.</td>
</tr>
</tbody>
</table>