# Table of Contents

**Preface**......................................................................................................................................................... 4
About Qualys .................................................................................................................................................. 4
Contact Qualys Support .......................................................................................................................... 4

**Chapter 1 - Welcome**.................................................................................................................................. 5
Qualys API Framework .............................................................................................................................. 5
Qualys API Gateway URL .......................................................................................................................... 6
Introduction to SEM API Paradigm ........................................................................................................... 7
API Rate Limits ........................................................................................................................................... 8

**Chapter 2 - API to export assets and vulnerabilities data**...................................................................... 10
  Query Parameters ..................................................................................................................................... 10
  Request ................................................................................................................................................... 15
  Response ............................................................................................................................................... 15

**Appendix**.................................................................................................................................................. 17
Error Messages ........................................................................................................................................... 17
Preface

This user guide is intended for application developers who will use the Qualys Secure Enterprise Mobility (SEM).

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 SEM 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.

SEM would expose the APIs via the QGateway (API-Gateway). QGateway provides features like:

Authentication: SEM would use the JWT based authentication. The client will first have to call the /auth API to fetch the token and then make actual API calls while passing the token in the headers as Bearer.

Get API Notifications

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

Qualys API Framework

The Qualys SEM 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.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baseurl&gt;</td>
<td>The Qualys API server URL that you should use for API requests. The base URL depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: <a href="https://gateway.qg1.apps.qualys.com">https://gateway.qg1.apps.qualys.com</a></td>
</tr>
<tr>
<td>&lt;module&gt;</td>
<td>The API module.</td>
</tr>
<tr>
<td>&lt;object&gt;</td>
<td>The module specific object.</td>
</tr>
<tr>
<td>&lt;object_id&gt;</td>
<td>(Optional) The module specific object ID, if appropriate.</td>
</tr>
<tr>
<td>&lt;operation&gt;</td>
<td>The request operation, such as count.</td>
</tr>
</tbody>
</table>
Chapter 1 - Welcome

Qualys API Gateway 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 SEM API Paradigm

Authentication

You must authenticate to the Qualys SEM using Qualys account credentials (user name and password) and get the JSON Web Token (JWT). Use the Qualys Authentication API to get the JWT. The client will first have to call the /auth API to fetch the token and then make actual API calls while passing the token in the headers as Bearer.

Auth request: Refer, Product / Service / API On-boarding#Authentication

For example,

Auth request
Path: /auth
HTTP: Get

Header:
Content/Type - application/x-www-form-urlencoded

Body
username: <provide username>
password: <provide password>
token: true
permissions: true

where
- Get is the HTTP method.
- username and password are the credentials of the user account for which you want to fetch SEM data
- token and permissions should be true

The Authentication API returns a JSON Web Token (JWT) which you can use for authentication in SEM.

Rate limit: Qgateway provides a facility of rate limiting based on the configurations done in QWeb BO. SEM would ride on this already existing feature

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-X &quot;GET&quot;</td>
<td>The GET method is required for the SEM API request.</td>
</tr>
</tbody>
</table>
| -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>
Note: For information about Qualys authentication API, see Authentication. |

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

curl -X GET

API Rate Limits

The Qualys API enforces limits on the API calls a customer can make based on their subscription settings. The limits apply to the use of all Qualys APIs except “auth” API (JWT Token Generation API). Default API control settings are provided by the service. Note these settings may be customized per subscription by Qualys Support.

The rate count and period are calculated dynamically each time an API call is received. The rate period represents a rolling window when API calls are counted.

API Controls Definition

**X-RateLimit-Remaining**: This indicates the total API calls remaining in current rate limit window.

**X-RateLimit-ToWait-Sec**: This time indicates the wait time for the rate limit to be reset. The customer has to wait for that time to execute next API calls.

**X-RateLimit-Window-Sec**: This value indicates the total time window assigned for the APIs to be executed.

**X-RateLimit-Limit**: This indicates the max number of API calls that can be executed in that particular rate limit window.

Sample Request

curl -X GET

Note: Provide "-i" in the curl request as shown in the example returns the response headers which includes the rate limit related parameters.
Example: A subscription for Standard API Service has the default API control settings. Consider that the API rate limit set for a customer is 300 API calls for a time window of 3600 seconds. If 300 API calls are received in a 5 minute period and none are blocked by any API limiting rules, then you need to wait 55 minutes before making the next call to the API. During the wait period API calls will be blocked by the rate limiting rule.

Sample HTTP Response Headers
Name : X-Content-Type : application/xml

Permissions
- Enable the 'SEM API Access' permission to default 'SEM User' role i.e. the users with SEM User role will have access to SEM APIs.

Note: The existing superuser and the manager user have permission to access SEM APIs.
Chapter 2 - API to export assets and vulnerabilities data

Customer needs API to export assets and vulnerabilities data from SEM to integrate the data in their existing ecosystem.

/sem/v1/assetList

[GET]

Query Parameters

Use these API functions to get host data from SEM.

Asset List Detection

API Request

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=list</td>
<td>(Required)</td>
</tr>
<tr>
<td>echo_request={0</td>
<td>1}</td>
</tr>
<tr>
<td>show_asset_id={0</td>
<td>1}</td>
</tr>
</tbody>
</table>
## Detection Filters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action=list</td>
<td>(Required)</td>
</tr>
<tr>
<td>echo_request=[0</td>
<td>1]</td>
</tr>
<tr>
<td>show_results=[0</td>
<td>1]</td>
</tr>
<tr>
<td>show_reopened_info=[0</td>
<td>1]</td>
</tr>
<tr>
<td>output_format={XML}</td>
<td>(Optional) Specifies the format of the asset detection list output. When not specified, the output format is XML by default.</td>
</tr>
<tr>
<td>truncation_limit={value}</td>
<td>(Optional) Specifies the maximum number of asset records processed per request. When not specified, the truncation limit is set to 1000 asset records. You may specify a value less than the default (1-999) or greater than the default (1001-1000000). If the requested list identifies more asset records than the truncation limit and output_format=XML, then the XML output includes the element and the URL for making another request for the next batch of asset records. If the requested list identifies more asset records than the truncation limit and output_format=CSV, then the CSV output includes &quot;Truncated&quot; in the FOOTER_CSV section and the URL for making another request for the next batch of asset records. <strong>Note:</strong> When 0 is specified, the truncation limit is set to 1000.</td>
</tr>
<tr>
<td>max_days_since_detection_updated={value}</td>
<td>(Optional) Show only detections whose detection status changed since some maximum number of days you specify. For detections that have never changed the maximum number of days is applied to the last detection date. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated</td>
</tr>
</tbody>
</table>
### Chapter 2 - API to export assets and vulnerabilities data

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detection_updated_since={value}</td>
<td>(Optional) Show only detections whose detection status changed after a certain date and time. For detections that have never changed the date is applied to the last detection date. Valid date format is: <code>YYYY-MMDD[THH:MM:SSZ]</code> format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. <strong>Tip:</strong> You can use this parameter in conjunction with the detection_updated_before parameter to limit the detections are shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated</td>
</tr>
<tr>
<td>detection_updated_before={value}</td>
<td>(Optional) Show only detections whose detection status changed before a certain date and time. Valid date format is: <code>YYYY-MMDD[THH:MM:SSZ]</code> format (UTC/GMT), like “2017-02-15” or “2017-02-15T23:15:00Z”. <strong>Tip:</strong> You can use this parameter in conjunction with the detection_updated_since parameter to limit the detections shown to a specific date range. One of these parameters may be specified in the same request: detection_updated_since, max_days_since_detection_updated</td>
</tr>
</tbody>
</table>

### Asset Filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ids={value}</td>
<td>(Optional) Show only certain asset IDs/ranges. One or more asset IDs/ranges may be specified. Multiple entries are comma-separated. An asset ID range is specified with a hyphen (for example 190-400). Valid asset IDs are required.</td>
</tr>
<tr>
<td>status={value}</td>
<td>(Optional) Show only assets with one or more of these status values: Enrolled, Deenrolled, Ready for Re-enrollment. Multiple status values are entered as a comma-separated list. If this parameter is not passed to the API, by default, the output contains detections with Enrolled only.</td>
</tr>
<tr>
<td>os_pattern={expression}</td>
<td>(Optional) Show only assets which have an operating system matching a certain regular expression. An empty value cannot be specified. Use “%5E%24” to match an empty string. <strong>Important:</strong> The regular expression string you enter must follow the PCRE standard and it must be URL encoded.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>qids={value}</td>
<td>(Optional) Show only detection records with certain QIDs.</td>
</tr>
<tr>
<td></td>
<td>One or more QIDs may be specified. A range is specified with a dash (for example: 68518-68522). Multiple entries are comma-separated. Valid QIDs are required.</td>
</tr>
<tr>
<td>severities={value}</td>
<td>(Optional) Show only detection records which have certain severities. One or more levels may be specified. A range is specified with a dash (for example 1-3). Multiple entries are comma-separated.</td>
</tr>
</tbody>
</table>
## Asset Tags Filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>use_tags={0</td>
<td>1}</td>
</tr>
<tr>
<td>(tag_set_by={id</td>
<td>name}</td>
</tr>
<tr>
<td>tag_include_selector={any</td>
<td>all}</td>
</tr>
<tr>
<td>tag_exclude_selector={any</td>
<td>all}</td>
</tr>
<tr>
<td>tag_set_include={value}</td>
<td>(Optional when use_tags=1) Specify a tag set to include. Assets that match these tags will be included. You identify The tag set by providing tag names or IDs. Multiple entries are comma separated.</td>
</tr>
<tr>
<td>tag_set_exclude={value}</td>
<td>(Optional when use_tags=1) Specify a tag set to exclude. Assets that match these tags will be excluded. You identify the tag set by providing tag names or IDs. Multiple entries are comma-separated.</td>
</tr>
<tr>
<td>show_tags={0</td>
<td>1}</td>
</tr>
</tbody>
</table>

Note: Expect 'show_tags' all the tags filled required the 'use_tags' set to 1 i.e. use_tags=1

### Detection Time-stamp

Use these parameters to view various time-stamp values in the output.
Chapter 2 - API to export assets and vulnerabilities data

Request


Response

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE ASSET_LIST_VM_DETECTION_OUTPUT SYSTEM "https://gateway.qg1.apps.qualys.com/sem/xapi/v1/asset/asset_list_output.dtd">
<ASSET_LIST_VM_DETECTION_OUTPUT>
  <RESPONSE>
    <DATETIME>2021-10-18T07:58:11.268Z</DATETIME>
    <ASSET_LIST>
      <ASSET>
        <ID>231</ID>
        <IP>192.168.1.101</IP>
        <IPV6>2401:4900:52b8:8433:204a:25d7:89b0:1a51</IPV6>
        <ASSET_FRIENDLY_NAME>abhi123abhi123_iOS_Apple_5</ASSET_FRIENDLY_NAME>
        <OS>iOS</OS>
        <OS_VERSION>14.5</OS_VERSION>
        <ASSET_STATUS>Enrolled</ASSET_STATUS>
        <LAST_SEEN>2021-04-28 12:01:06</LAST_SEEN>
        <OWNERSHIP>Corporate - Owned</OWNERSHIP>
        <MODEL_NAME>iPad (5th generation)</MODEL_NAME>
        <MANUFACTURER>Apple, Inc.</MANUFACTURER>
        <USERNAME>abhi123abhi123</USERNAME>
        <DETECTION_LIST>
          <DETECTION>
            <QID>610100</QID>
            <TYPE>Information</TYPE>
            <SEVERITY>1</SEVERITY>
            <RESULTS>
```

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>first_found_datetime={date}</td>
<td>The date/time when the vulnerability was first found</td>
</tr>
<tr>
<td>last_found_datetime={date}</td>
<td>The most recent date/time when the vulnerability was found.</td>
</tr>
<tr>
<td>last_update_datetime={date}</td>
<td>The most recent date/time when the detection record was updated.</td>
</tr>
<tr>
<td>last_fixed_datetime={date}</td>
<td>The date/time when the vulnerability was verified fixed by a scan.</td>
</tr>
</tbody>
</table>

Parameter Description

- `first_found_datetime`: The date/time when the vulnerability was first found.
- `last_found_datetime`: The most recent date/time when the vulnerability was found.
- `last_update_datetime`: The most recent date/time when the detection record was updated.
- `last_fixed_datetime`: The date/time when the vulnerability was verified fixed by a scan.
Chapter 2 - API to export assets and vulnerabilities data

<![CDATA[iOS Device Details : iOS : 14.5 Model : iPad (5th generation)]> ]>
</RESULTS>
<STATUS>Active</STATUS>
<FIRST_FOUND_DATETIME>2021-04-28 05:01:36</FIRST_FOUND_DATETIME>
<LAST_FOUND_DATETIME>2021-04-28 12:01:07</LAST_FOUND_DATETIME>
<TIMES_FOUND>21</TIMES_FOUND>
<LAST_UPDATE_DATETIME>2021-04-28 12:01:07</LAST_UPDATE_DATETIME>
</DETECTION>
</DETECTION_LIST>
</ASSET>
</ASSET_LIST>
<WARNING>
<CODE>1980</CODE>
<TEXT>1 record limit exceeded. Use URL to get next batch of results.</TEXT>
<URL>
<![CDATA[https://gateway.p04.eng.sjc01.qualys.com/sem/v1/assetList?id_min=643&action=list&truncation_limit=1]]>
</URL>
</WARNING>
</RESPONSE>
</ASSET_LIST_VM_DETECTION_OUTPUT>
<--
CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the QualysGuard Service "As Is," without any warranty of any kind. Qualys makes no warranty that the information contained in this report is complete or error-free. Copyright 2021, Qualys, Inc.-->
Appendix

This appendix describes the types of error messages returned from SEM API requests.

## Error Messages

<table>
<thead>
<tr>
<th>Condition</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>User enters unsupported parameters</td>
<td>Unrecognized parameter(s): (name of the parameters) (action=list allows: List of allowed attributes)</td>
</tr>
<tr>
<td>Required parameter missing in the request</td>
<td>Missing required parameter(s): (name of the parameters)</td>
</tr>
<tr>
<td>Invalid value received for any query parameter</td>
<td>parameter (parameter) has invalid value: {value} (please specify one of the following: {allowed values} )</td>
</tr>
<tr>
<td></td>
<td>For example: parameter use_tags has invalid value: 76 (please specify one of the following: 1,0 )</td>
</tr>
<tr>
<td>API failed due to any errors or problems in SEM</td>
<td>Internal Error</td>
</tr>
<tr>
<td>User doesn’t have SEM.API.Access permission</td>
<td>User is not authorized to run the SEM API.</td>
</tr>
<tr>
<td>Module not allowed to the User</td>
<td>User doesn’t have SEM access.</td>
</tr>
<tr>
<td>Exception occurred while decoding token</td>
<td>Error occurred while decoding token</td>
</tr>
<tr>
<td>Any Exception occurred while checking authorization (checking permission or module access)</td>
<td>Error occurred while checking user access</td>
</tr>
</tbody>
</table>