Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.22

April 03, 2023

This new version of the Qualys Cloud Platform (VM, PC) includes improvements to the Qualys API. You'll find all the details in our user guides, available at the time of release. Just log in to your Qualys account and go to Help > Resources.

What's New

Qualys API Server 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 server URL for Qualys US Platform 1 (https://qualysapi.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

VM/PC: New Scan API to List the Last 'N' Scan References

APIs affected	api/2.0/fo/scan/schedules/runhistory/
New or Updated API	New
DTD or XSD changes	Yes

This release introduces a new API which will provide the Last 'n' scan references for the given schedule scan ID. Customers can fetch scan references launched through a specific schedule scan id.

Note: This API will not work for MAP schedule scan ids.

Input Parameters

Use the following input parameters to list the last 'n' scan references for the given schedule scan ID.

Parameter	Description
action=list	(Required) Specify value as “list” in action input parameter.
schedule_scan_ids	(Required) Specify schedule scan ids in a comma-separated list. Maximum 500 schedule ids are supported.
output_format	(Optional) Specify output file format. Default value is “xml” format. Supported values are “xml” & “json”.
schedule_executions_count	(Optional) Specify count value form 1 to 10. When not specified, 3 scan launch information of the particular schedule will be listed in output.

API Sample

Sample - List the Last 'n' scan references for the given schedule scan IDs.

API Request:

```
curl --location
'<qualys_base_url>/api/2.0/fo/scan/schedules/runhistory/?action=list&outp
ut_format=xml&schedule_executions_count=4&schedule_scan_ids=99446%2C85403
%2C144180%2C144181%2C6666%2C657657%2C125485' \
--header 'X-Requested-With: test' \
--header 'Authorization: Basic <token>'
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<!DOCTYPE SCHEDULES_RUN_HISTORY SYSTEM
"http://10.20.30.40:29000/api/2.0/fo/scan/schedules/runhistory/output.dtd
">
<SCHEDULES_RUN_HISTORY>
    <RESPONSE>
        <DATETIME>2023-01-09T14:57:51Z</DATETIME>
        <SCHEDULE_LIST>
            <SCHEDULE id="85403">
                <SCHEDULE_ID>85403</SCHEDULE_ID>
                <SCHEDULE_RUN_HISTORY>
                    <SCHEDULE_RUN>
                        <SCAN_LAUNCH_INFO>
                            <SCAN_ID>99408</SCAN_ID>

<SCAN_REFERENCE>scan/1634824016.99408</SCAN_REFERENCE>
                            <LAUNCH_DATETIME>2021-10-21
13:46:56</LAUNCH_DATETIME>
                            <TITLE>test9090</TITLE>
                            <TARGET>10.20.30.40</TARGET>
                            <STATUS>FINISHED</STATUS>
                            <DURATION>86 Seconds</DURATION>
                            <NBHOST>0</NBHOST>
                            <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                            <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                            <IS_PROCESSED>1</IS_PROCESSED>
                        </SCAN_LAUNCH_INFO>
                    </SCHEDULE_RUN>
                </SCHEDULE_RUN_HISTORY>
            </SCHEDULE>
            <SCHEDULE id="99446">
                <SCHEDULE_ID>99446</SCHEDULE_ID>
                <SCHEDULE_RUN_HISTORY>
                    <SCHEDULE_RUN>
                        <SCAN_LAUNCH_INFO>
                            <SCAN_ID>99561</SCAN_ID>

<SCAN_REFERENCE>scan/1635442781.99561</SCAN_REFERENCE>
                            <LAUNCH_DATETIME>2021-10-28
17:39:41</LAUNCH_DATETIME>
                            <TITLE>test_555</TITLE>
                            <TARGET>list of target ips</TARGET>
                            <STATUS>FINISHED</STATUS>
                            <DURATION>434 Seconds</DURATION>
                            <NBHOST>0</NBHOST>
                            <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                            <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                            <IS_PROCESSED>1</IS_PROCESSED>
```

```
                            </SCAN_LAUNCH_INFO>
                        </SCHEDULE_RUN>
                        <SCHEDULE_RUN>
                            <SCAN_LAUNCH_INFO>
                                <SCAN_ID>99554</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99554</SCAN_REFERENCE>
                                <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                                <TITLE>test_898</TITLE>
                                <TARGET>10.20.30.40</TARGET>
                                <STATUS>FINISHED</STATUS>
                                <DURATION>9 Seconds</DURATION>
                                <NBHOST>0</NBHOST>
                                <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                                <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                                <IS_PROCESSED>1</IS_PROCESSED>
                            </SCAN_LAUNCH_INFO>
                        </SCHEDULE_RUN>
                        <SCHEDULE_RUN>
                            <SCAN_LAUNCH_INFO>
                                <SCAN_ID>99553</SCAN_ID>

<SCAN_REFERENCE>scan/1635431408.99553</SCAN_REFERENCE>
                                <LAUNCH_DATETIME>2021-10-28
14:30:08</LAUNCH_DATETIME>
                                <TITLE>test9090</TITLE>
                                <TARGET>10.20.30.40</TARGET>
                                <STATUS>FINISHED</STATUS>
                                <DURATION>79 Seconds</DURATION>
                                <NBHOST>0</NBHOST>
                                <SUBSCRIPTION_ID>237630</SUBSCRIPTION_ID>
                                <OPTION_PROFILE_TITLE>Initial
Options</OPTION_PROFILE_TITLE>
                                <IS_PROCESSED>1</IS_PROCESSED>
                            </SCAN_LAUNCH_INFO>
                        </SCHEDULE_RUN>
                    </SCHEDULE_RUN_HISTORY>
                </SCHEDULE>
            </SCHEDULE_LIST>
        </RESPONSE>
</SCHEDULES_RUN_HISTORY>
```

DTD Output:

```
<!ELEMENT SCHEDULES_RUN_HISTORY (REQUEST?,RESPONSE)>
<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
```

```
POST_DATA?)>
<!ELEMENT DATETIME (#PCDATA)>
<!ELEMENT USER_LOGIN (#PCDATA)>
<!ELEMENT RESOURCE (#PCDATA)>
<!ELEMENT PARAM_LIST (PARAM+)>
<!ELEMENT PARAM (KEY, VALUE)>
<!ELEMENT KEY (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!-- if returned, POST_DATA will be url encoded -->
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, SCHEDULE_LIST?)>
<!ELEMENT SCHEDULE_LIST (SCHEDULE+)>
<!ELEMENT SCHEDULE (SCHEDULE_ID, SCHEDULE_RUN_HISTORY?)>
<!ATTLIST SCHEDULE id CDATA #IMPLIED>
<!ELEMENT SCHEDULE_ID (#PCDATA)>
<!ELEMENT SCHEDULE_RUN_HISTORY (SCHEDULE_RUN+)>
<!ELEMENT SCHEDULE_RUN ((SCHEDULE_RUN_INFO?, SCAN_LAUNCH_INFO?)+)>
<!ELEMENT SCHEDULE_RUN_INFO (ACTION_TEXT)>
<!ELEMENT ACTION_TEXT (#PCDATA)>
<!ELEMENT SCAN_LAUNCH_INFO (SCAN_ID, SCAN_REFERENCE, LAUNCH_DATETIME,
TITLE, TARGET, SCAN_TYPE?, STATUS, DURATION, NBHOST, SUBSCRIPTION_ID,
OPTION_PROFILE_TITLE, IS_PROCESSED, CONNECTOR_UUID?, ENDPOINT_UUID?)>
<!ELEMENT SCAN_ID (#PCDATA)>
<!ELEMENT SCAN_REFERENCE (#PCDATA)>
<!ELEMENT LAUNCH_DATETIME (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TARGET (#PCDATA)>
<!ELEMENT SCAN_TYPE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT DURATION (#PCDATA)>
<!ELEMENT NBHOST (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT OPTION_PROFILE_TITLE (#PCDATA)>
<!ELEMENT IS_PROCESSED (#PCDATA)>
<!ELEMENT CONNECTOR_UUID (#PCDATA)>
<!ELEMENT ENDPOINT_UUID (#PCDATA)>
<!-- EOF -->
```

A New API Input Parameter for Enabling IPv6 on LAN

APIs affected	api/2.0/fo/appliance/
New or Updated API	Updated
DTD or XSD changes	No

With this release, customer can enable or disable IPv6 on LAN through API itself without login on QWEB FO to manually enable it. A new API input parameter is introduced to enable IPV6 on LAN for recently added IPV6 VLAN feature.

Input Parameter

Use the following input parameter to enable/disable IPv6 on LAN..

Parameter	Description
enable_ipv6=0	(Optional) Specify value as “1” or “0” (enable=1, disable=0) in input parameter. By default value is “0”.

API Sample

Sample - Enable IPV6 on LAN for the specified scan ID .

.API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&id=972162&set_vlans=1|10.20.30.40|111.222.333.0|Testvlan1&
enable_ipv6=1"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-02-16T09:27:54Z</DATETIME>
        <TEXT>Virtual scanner updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>972162</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Extended CVE Search Ability in Knowledge Base for "Exact Match" and "Contains"

APIs affected	api/2.0/fo/qid/search_list/dynamic
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, customer can use the extended CVE search options "Exact Match" and "Contains" that allows user to filter the QIDS based on selected search criteria

- "The “Exact Match” option shows the QIDs that exactly matches with the CVEs provided in the search criteria.

- The "Contains" option shows the QIDS that exactly matches with the CVE’s & the CVE's that contains the given CVE's name in the search criteria.

This option is provided in KnowledgeBase Search option. User can create new Dynamic Search List that can be imported in different sections such as Reports, Scans and Remediation. It is available to user on KnowledgeBase and Dynamic Search List Pages.

Create, Update and List Dynamic Serach List API

There is one new input parameter for Dynamic Search List API to indicate QIDS search criteria. Refer to the Qualys API (VM,PC) User Guide for details on all input parameters.

Parameter	Description
cve_ids_filter	(Optional) Specify value as 1(EXACT MATCH) or 2(CONTAINS).

Sample: Create Dynamic Search List

.API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=API_dynamic_filer&cve_ids_filter=1&cve_ids=CVE-2019-
3813%2CCVE-2017-7506\"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
     <RESPONSE>
          <DATETIME>2023-02-21T10:37:50Z</DATETIME>
          <TEXT>New search list created successfully</TEXT>
          <ITEM_LIST>
```

```
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>1283280</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Update Dynamic Search List

.API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&title=API_dynamic_filer_default&cve_ids_filter=2&cve_ids=C
VE-2019-3813%2CCVE-2017-7506&id=1283283"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2023-02-21T10:55:02Z</DATETIME>
        <TEXT>search list updated successfully</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>1283283</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample: List Dynamic Search List

.API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=1282246"
```

XML Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/qid/search_list/dynamic/dynamic_
list_output.dtd">
<DYNAMIC_SEARCH_LIST_OUTPUT>
```

```
<RESPONSE>
     <DATETIME>2023-02-21T10:26:21Z</DATETIME>
     <DYNAMIC_LISTS>
          <DYNAMIC_LIST>
               <ID>1282246</ID>
               <TITLE>
                    <![CDATAcve_id_contains]>
               </TITLE>
               <GLOBAL>Yes</GLOBAL>
               <OWNER>
                    <![CDATA]>
               </OWNER>
               <CREATED>2023-02-20T07:19:54Z</CREATED>
               <MODIFIED_BY>
                    <![CDATA]>
               </MODIFIED_BY>
               <MODIFIED>2023-02-21T09:23:56Z</MODIFIED>
               <QIDS>
                    <QID>150646</QID>
                    <QID>150647</QID>
                    <QID>150648</QID>
                    <QID>150649</QID>
                    <QID>151019</QID>
                    <QID>672596</QID>
                    <QID>672597</QID>
                    <QID>672598</QID>
                    <QID>672600</QID>
                    <QID>672601</QID>
                    <QID>672602</QID>
                    <QID>672603</QID>
               </QIDS>
               <CRITERIA>
                    <DISCOVERY_METHOD>
                         <![CDATAAll]>
                    </DISCOVERY_METHOD>
                    <CVE_ID>
                         <![CDATACVE-2022]>
                    </CVE_ID>
                    <CVE_ID_FILTER>
                         <![CDATAContains]>
                    </CVE_ID_FILTER>
               </CRITERIA>
          </DYNAMIC_LIST>
     </DYNAMIC_LISTS>
</RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>
```

Revised Rate Limits for PC Posture Streaming APIs

We have revised the rate limits for the following PC posture streaming APIs:

- **Get Policy List**: /pcrs/1.0/posture/policy/list?lastEvaluationDate=<evaluation date>

- **Resolve Host IDs**: /pcrs/1.0/posture/hostids?policyId=<policy ids>

- **Get Posture Info**: /pcrs/1.0/posture/postureInfo?evidenceRequired=0&compressionRequired=1&lastEvaluationDate=<date>

For each of these APIs, you can now send a maximum of 25 API requests per Qualys PC subscription in a 60-second timeframe.

Get Posture Information of Assets Scanned between Two Dates

APIs affected	/pcrs/1.0/posture/postureInfo
New or Updated API	Updated
DTD or XSD changes	NA

We have introduced two new input parameters to get the posture information of assets scanned between specified dates. These parameters provide an effective way to retrieve and analyze posture data for your assets scanned during a particular time frame.

Input Parameter

The following input parameters are added:

Parameter	Mandatory?	Data Type	Description
lastScanDateFrom lastScanDateTo	Optional	string	Provides compliance posture information of the assets scanned between these two dates, both dates included. The format for dates is: lastScanDateFrom=2022-09-30 or 2022-09-30T18:48:16Z lastScanDateTo=2022-12-27 or 2022-12-27T20:48:16Z **Notes**: - You must specify both dates. - You must not use these parameters with lastScanDate.

Sample: Get Posture Info of Assets Scanned between Two Dates

.API Request:

```
curl -X POST
"<qualys_base_url>/pcrs/1.0/posture/postureInfo?evidenceRequired=0&compre
ssionRequired=0&lastScanDateFrom=2021-12-23&lastScanDateTo=2022-12-27"
-H "accept: /"
-H "Authorization: Bearer <token>"
-H "Content-Type: application/json"
-d "[
{\"policyId\":\"<POLICYID>\",\"subscriptionId\":\"<SUBSCRIPTIONI
D>\",\"hostIds\":[\"<HOST ID1>\",\"<HOST ID2>\"]}
]"
```

Response:


```
[
  {
    "id": 24442834,
    "instance": "os",
    "policyId": 5266764,
    "policyTitle": "CIS Reference Policies",
    "netBios": null,
    "controlId": 1071,
    "controlStatement": "Status of the 'Minimum Password Length' setting",
    "rationale": "Among the several characteristics that make 'user
identification' via password a secure and workable solution is setting a
'minimum password length' requirement.  Each character that is added to
the password length squares the difficulty of breaking the password via
'brute force,' which attempts using every combination possible within the
password symbol set-space, in order to discover a user's password.  While
no 'minimum length' can be guaranteed secure, eight (8) is commonly
considered to be the minimum for most application access, along with
requiring other password security factors, such as increasing the size of
the symbol set-space by requiring mixed-cases, along with other forms of
password variability creation, increases the difficulty of breaking any
password by brute-force attack.",
    "remediation": "To specify password length requirements for new
accounts, edit the file \"/etc/login.defs\" and add or correct the
following lines: \n\nPASS_MIN_LEN <required
value>\n\nexample:\n\nPASS_MIN_LEN 14\n\n\nNote:\nThe DoD requirement is
\"14\". If a program consults \"/etc/login.defs\" and also another PAM
module (such as \"pam_cracklib\") during a password change operation, then
the most restrictive must be satisfied.",
    "controlReference": null,
    "technologyId": 43,
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2022-09-29T19:22:29Z",
    "lastPassDate": "2023-02-08T10:14:17Z",
    "postureModifiedDate": "2022-09-29T19:22:23Z",
    "lastEvaluatedDate": "2023-02-08T10:14:17Z",
    "created": "2023-02-08T11:29:16Z",
    "hostId": 8650108,
    "cloudResourceId": null,
    "ip": "<ip address>",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:centos:centos:6.9:::",
    "domainName": null,
    "dns": null,
```

```
    "qgHostid": null,
    "networkId": 0,
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2022-09-30T05:08:44Z",
    "customerUuid": "f1495d3b-test-fdd6-test-9ca83f5e8f8b",
    "customerId": "<customer ID>",
    "assetId": 21452756,
    "technology": {
      "id": 43,
      "name": "CentOS 6.x"
    },
    "criticality": {
      "label": "CRITICAL",
      "value": 4
    },
    "evidence": {
      "expectedValues": "\nSetting not found\n------------ OR -----------
-\nFile not found\n------------ OR ------------\ngreater than or equal
to\n0",
      "currentValues": [
        "5"
      ],
      "actualValues": null,
      "directoryFimUdc": null
    },
    "causeOfFailure": null,
    "currentDataSizeKB": "2.49",
    "totalDataSizeKB": "2.49",
    "currentBatch": 1,
    "totalBatches": 9
  },
  {
    "id": 24443419,
    "instance": "os",
    "policyId": 5266764,
    "policyTitle": "CIS Reference Policies",
    "netBios": null,
    "controlId": 12821,
    "controlStatement": "List of runtime audit rules for '/etc/issue'
file, using auditctl",
    "rationale": "The '/etc/issue' parameter monitors and logs any changes
to the message displayed prior to login. Monitoring /etc/issue and
/etc/issue.net is important, as intruders could put disinformation into
those files and trick users into providing information to the intruder.
This should be configured according to the needs of the business.",
    "remediation": "Run the following command to audit the system's
network environment events according to the business needs and
organization's security policies.\nauditctl -w <system's network
environment event> -p wa -k system-locale\n\nExample:\nauditctl -w
```

```
/etc/issue -p wa -k system-locale",
    "controlReference": null,
    "technologyId": 80,
    "status": "Passed",
    "previousStatus": "Passed",
    "firstFailDate": "",
    "lastFailDate": "",
    "firstPassDate": "2022-09-29T19:26:36Z",
    "lastPassDate": "2023-02-08T10:14:33Z",
    "postureModifiedDate": "2022-09-29T19:26:35Z",
    "lastEvaluatedDate": "2023-02-08T10:14:32Z",
    "created": "2023-02-08T10:19:37Z",
    "hostId": 8650098,
    "cloudResourceId": null,
    "ip": "<ip address>",
    "trackingMethod": "IP",
    "os": null,
    "osCpe": "cpe:/o:centos:centos_linux:7.6.1810:::",
    "domainName": null,
    "dns": null,
    "qgHostid": null,
    "networkId": 0,
    "networkName": "Global Default Network",
    "complianceLastScanDate": "2022-12-26T12:04:50Z",
    "customerUuid": "f1495d3b-test-fdd6-82cd-test",
    "customerId": "<customer ID>",
    "assetId": 21452548,
    "technology": {
      "id": 80,
      "name": "CentOS 7.x"
    },
    "criticality": {
      "label": "SERIOUS",
      "value": 3
    },
    "evidence": {
      "expectedValues": "\nSetting Not Found\n------------ OR -----------
-\nNo Rules Found\n------------ OR ------------\nmatches regular
expression list\n.*",
      "currentValues": [
        "No Rules Found"
      ],
      "actualValues": null,
      "directoryFimUdc": null
    }
  ]
```