Qualys API Release Notes

Version 8.10.1

Qualys 8.10.1 includes improvements to the Qualys API, giving you more ways to integrate your programs and API calls with Qualys Vulnerability Management (VM) and Qualys Policy Compliance (PC). Looking for our API user guides? Just log in to your Qualys account and go to Help > Resources.

What's New

URL to the Qualys API Server

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

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

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

New Scanner Role Extended Permissions

Your subscription may now be configured to allow users with a Scanner user role to be granted these extended permissions:

- Manage virtual scanner appliances. When granted, this allows the user to create, edit and delete virtual scanner appliances from the UI and API.

- Create/edit authentication records/vaults. When granted, this allows the user to create and edit authentication records and vaults from the UI and API.

How to grant a user extended permissions

These permissions may be granted on a per user basis by a Manager or Unit Manager (with the same permission). Simply edit the user's account from the Qualys UI by going to the Users list and choosing Edit from the Quick Actions menu. These permissions may already be granted to Unit Managers.

Not seeing these permissions for Scanner users?

Your subscription must be configured to allow Scanner users to be granted these additional permissions. Please contact your Technical Account Manager or Support to have this enabled for you. Once enabled, you'll be able to grant these permissions to any Scanner user in your subscription.

New Input Parameter for Create Virtual Scanner

When users with the Unit Manager or Scanner role create a virtual scanner appliance, they must add the virtual scanner to an asset group in their account. Simply provide the asset group ID as part of the API request.

Good to Know

- Unit Manager and Scanner users must be granted the "Manage virtual scanner appliances" permission to create/manage virtual scanners. This permission is only available to Scanner users when your subscription is configured to allow it.

- There are no DTD changes.

New Input Parameter

Use this new parameter to specify the asset group.

Parameter	Description
asset_group_id={value}	(Required for Unit Managers and Scanners for Create request) The ID of an asset group the virtual scanner will be assigned to.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&name=API_Scanner&polling_interval=60&asset_group_id=149762
2" "https://qualysapi.qualys.com/api/2.0/fo/appliance/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE APPLIANCE_CREATE_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/appliance/appliance_create_outpu
t.dtd">
<APPLIANCE_CREATE_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-06-16T07:46:31Z</DATETIME>
    <APPLIANCE>
      <ID>867192</ID>
      <FRIENDLY_NAME>API_Scanner</FRIENDLY_NAME>
      <ACTIVATION_CODE>15309017243793</ACTIVATION_CODE>
      <REMAINING_QVSA_LICENSES>40</REMAINING_QVSA_LICENSES>
    </APPLIANCE>
  </RESPONSE>
</APPLIANCE_CREATE_OUTPUT>
```

VM - Detection API - New Value for Active Kernels Only input parameter

The existing parameter “active_kernels_only” helps you identify detections related to running and non-running Linux kernels. You can now specify active_kernels_only=3 in your request to only include vulnerabilities found on running Linux kernels.

active_kernels_only Parameter

The behavior of the input parameter is described below.

Parameter	Description
{unspecified}	When unspecified, vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> does not appear in the output for kernel related vulnerabilities.
active_kernels_only=0	Vulnerabilities are not filtered based on kernel activity. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities.
active_kernels_only=1	Exclude vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output for kernel related vulnerabilities.
active_kernels_only=2	Only include vulnerabilities found on non-running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 0 for all vulnerabilities.
active_kernels_only=3	Only include vulnerabilities found on running Linux kernels. <AFFECT_RUNNING_KERNEL> appears in the output with a value of 1 for all vulnerabilities.

<AFFECT_RUNNING_KERNEL> values

The value for <AFFECT_RUNNING_KERNEL> will be:

1 if QID applies to a Running Kernel, or

0 if QID applies to a Non-Running Kernel

Sample API call with XML output

API request:

```
curl -u "username:password" -H "X-Requested-With:curl demo2"  -d
"action=list&truncation_limit=50&ips=10.10.26.88&active_kernels_only=3"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

XML output:

```
....
<DETECTION>
            <QID>122069</QID>
            <TYPE>Confirmed</TYPE>
            <SEVERITY>4</SEVERITY>
            <SSL>0</SSL>
            <RESULTS><![CDATA[Package   Installed Version       Required
Version
kernel  2.6.32-71.29.1.el6.x86_64       2.6.32-431.17.1.el6
kernel  2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6
kernel  2.6.32-131.0.15.el6.x86_64      2.6.32-431.17.1.el6
kernel-devel    2.6.32-131.0.15.el6.x86_64      2.6.32-431.17.1.el6
kernel-devel    2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6
kernel-firmware 2.6.32-279.el6.noarch   2.6.32-431.17.1.el6
kernel-headers  2.6.32-279.el6.x86_64   2.6.32-431.17.1.el6]]></RESULTS>
            <STATUS>Active</STATUS>
            <FIRST_FOUND_DATETIME>2016-02-
25T20:09:55Z</FIRST_FOUND_DATETIME>
            <LAST_FOUND_DATETIME>2016-05-
17T22:00:37Z</LAST_FOUND_DATETIME>
            <LAST_TEST_DATETIME>2016-05-17T22:00:37Z</LAST_TEST_DATETIME>
            <LAST_UPDATE_DATETIME>2016-05-
17T22:07:45Z</LAST_UPDATE_DATETIME>
            <IS_IGNORED>0</IS_IGNORED>
            <IS_DISABLED>0</IS_DISABLED>
            <TIMES_FOUND>3</TIMES_FOUND>
            <AFFECT_RUNNING_KERNEL>1</AFFECT_RUNNING_KERNEL>
          </DETECTION>
...
```

Sample API call with CSV output

API request:

```
curl -u "username:password" -H "X-Requested-With:curl demo2" -d
"action=list&truncation_limit=50&ips=10.10.31.98&active_kernels_only=3&ou
tput_format=CSV"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/vm/detection/"
```

CSV output:

```
----BEGIN_RESPONSE_HEADER_CSV
----END_RESPONSE_HEADER_CSV
----BEGIN_RESPONSE_BODY_CSV
"Host ID","IP Address","Tracking Method","Network ID","Operating
System","DNS Name","Netbios Name","QG HostID","Ec2 Instance ID","Last Scan
Datetime","OS CPE","Last VM Scanned Date","Last VM Scanned Duration","Last
```

```
VM Auth Scanned Date","Last VM Auth Scanned Duration","Last PC Scanned
Date","QID","Type","Port","Protocol","FQDN","SSL","Instance","Status","Se
verity","First Found Datetime","Last Found Datetime","Last Test
Datetime","Last Update Datetime","Last Fixed
Datetime","Results","Ignored","Disabled","Times Found","Service","Affect
Running Kernel"

........

"3036262","10.10.31.98","IP","0","Red Hat Enterprise Linux Server
6.3",,,,,"2016-05-17T22:07:23Z",,"2016-05-17T22:10:30Z","238","2016-05-
17T22:10:30Z","238",,"120662","Confirmed",,,,"0",,"Active","3","2016-02-
25T20:09:55Z","2016-05-17T22:00:37Z","2016-05-17T22:00:37Z","2016-05-
17T22:07:39Z",,"Package  Installed Version  Required Version
kernel  2.6.32-71.29.1.el6.x86_64  2.6.32-279.14.1.el6
kernel  2.6.32-279.el6.x86_64  2.6.32-279.14.1.el6
kernel  2.6.32-131.0.15.el6.x86_64  2.6.32-279.14.1.el6
kernel-devel  2.6.32-131.0.15.el6.x86_64  2.6.32-279.14.1.el6
kernel-devel  2.6.32-279.el6.x86_64  2.6.32-279.14.1.el6
kernel-firmware  2.6.32-279.el6.noarch  2.6.32-279.14.1.el6
kernel-headers  2.6.32-279.el6.x86_64  2.6.32-
279.14.1.el6","0","0","3",,"1"

..........

----END_RESPONSE_BODY_CSV
----BEGIN_RESPONSE_FOOTER_CSV
"Status Message"
"Finished"
----END_RESPONSE_FOOTER_CSV
```

PC - Enhancement to File Integrity Checks

With this release you're no longer required to manually set the default expected value when defining File Integrity checks. Now you can pick the "Use scan data as expected value" option in the UDC and we'll set the expected value for you based on the actual value returned by the scan. Note that you'll also need to select the "Auto Update expected value" option in your compliance profile.

Good to Know

- You'll see USE_SCAN_VALUE for all File Integrity checks when you list controls and when you export controls and policies from your account. This tag indicates whether the "Use scan data as expected value" option is enabled for the control. A value of "1" means it is enabled. A value of "0" means it's not enabled.

- We made updates to the Control List Output DTD, Policy Export Output DTD and to the ImportableControl.xsd schema to include the new USE_SCAN_VALUE element.

List Compliance Controls

We added the USE_SCAN_VALUE element to the XML output for Compliance Control List and updated the DTD.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/?action=list&
ids=103423"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
output.dtd">
<CONTROL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2017-06-19T17:25:36Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>103423</ID>
        <UPDATE_DATE>2017-06-19T17:22:37Z</UPDATE_DATE>
        <CREATED_DATE>2017-06-19T17:22:37Z</CREATED_DATE>
        <CATEGORY>Anti-Virus/Malware</CATEGORY>
        <SUB_CATEGORY><![CDATA[Virus/Malware Prevention]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[FIM]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[UNDEFINED]]></LABEL>
```

```
            <VALUE>0</VALUE>
          </CRITICALITY>
          <CHECK_TYPE><![CDATA[Window File Integrity Check]]></CHECK_TYPE>
          <COMMENT><![CDATA[]]></COMMENT>
          <IGNORE_ERROR>0</IGNORE_ERROR>
          <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
          <SCAN_PARAMETERS>
              <FILE_PATH><![CDATA[C:\Windows]]></FILE_PATH>
              <HASH_TYPE><![CDATA[MD5]]></HASH_TYPE>
              <DATA_TYPE>String</DATA_TYPE>
              <DESCRIPTION><![CDATA[Windows file integrity]]></DESCRIPTION>
          </SCAN_PARAMETERS>
          <TECHNOLOGY_LIST>
            <TECHNOLOGY>
              <ID>12</ID>
              <NAME>Windows 2000</NAME>
              <RATIONALE><![CDATA[Windows file integrity]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>no cd</CARDINALITY>
                  <OPERATOR>re</OPERATOR>
                  <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
              <USE_SCAN_VALUE>0</USE_SCAN_VALUE>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>91</ID>
              <NAME>Windows 10</NAME>
              <RATIONALE><![CDATA[test]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>no cd</CARDINALITY>
                  <OPERATOR>re</OPERATOR>
                  <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
              <USE_SCAN_VALUE>0</USE_SCAN_VALUE>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

DTD update:

We updated the Control List Output DTD (control_list_output.dtd) to include the new element USE_SCAN_VALUE.

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->
...
<!ELEMENT TECHNOLOGY (ID, NAME, RATIONALE, DATAPOINT?, USE_SCAN_VALUE?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT DATAPOINT (CARDINALITY, OPERATOR, DEFAULT_VALUES)>
<!ELEMENT USE_SCAN_VALUE (#PCDATA)>
...
```

Export Policy to XML

You can export a compliance policy from your account to an XML file. You must specify the input parameter show_user_controls=1 to include UDCs in the output. You'll see USE_SCAN_VALUE in the output for each File Integrity check.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=export&ids=991742279&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
...
                        <TECHNOLOGY>
                            <ID>91</ID>
                            <NAME>Windows 10</NAME>

<EVALUATE><CTRL><DP><K>custom.file_integrity_check.1835288</K><L>0</L><OP
>re</OP><V><![CDATA[USE_SCAN_VALUE]]></V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[Check for changes to
File.txt]]></RATIONALE>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>re</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                            <USE_SCAN_VALUE>1</USE_SCAN_VALUE>
...
```

DTD update:

The Policy Export Output DTD (policy_export_output.dtd) was updated to include the new element USE_SCAN_VALUE.

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
...
<!ELEMENT TECHNOLOGY (ID, NAME?, EVALUATE?, RATIONALE?, DATAPOINT?,
                      USE_SCAN_VALUE?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EVALUATE (CTRL*)>
<!ELEMENT RATIONALE (#PCDATA)>
...
<!ELEMENT USE_SCAN_VALUE (#PCDATA)>
...
```

Export Policy to CSV (UI Only)

You can export a policy to CSV format from the Qualys UI. Select the option "Include UDCs and QCCs" to include UDCs in the output. You'll see USE_SCAN_VALUE as the expected value for File Integrity checks with "Use scan data as expected value" selected in the control when the control has not yet been evaluated (meaning the value has not yet been updated with the scan value).

CSV output:

```
"Policy Information"
"Title","Cover Page"
"File Integrity Monitoring - Windows",

"Technologies (1)"
"ID","Name"
"91","Windows 10"

"Control Information"
"Section No.","Section
Heading","Reference","CID","UDC_ID","Statement","Description","Technology
ID","Technology Name","Criticality Label","Criticality
Value","Evaluation"
"1","File Integrity",,"103405","4b73b464-335b-40e5-82d6-
3888f4a9bf75","File Integrity Check for File.txt","Check for changes to
File.txt","91","Windows 10","UNDEFINED","0","Check for changes to
File.txt.

* * * * * Expected Value(s) * * * * *
regular expression match
USE_SCAN_VALUE"
```

Export Control to XML

When you export a File Integrity Check UDC from your account to XML you'll see USE_SCAN_VALUE in the output.

XML output:

```
...
            <TECHNOLOGY>
                <ID>91</ID>
                <TECH_NAME><![CDATA[Windows 10]]></TECH_NAME>
                <RATIONALE><![CDATA[Check for changes to
File.txt]]></RATIONALE>
                <DATAPOINT>
                    <CARDINALITY>no cd</CARDINALITY>
                    <OPERATOR>re</OPERATOR>
                    <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[USE_SCAN_VALUE]]></DEFAULT_VALUE>
                    </DEFAULT_VALUES>
                </DATAPOINT>
                <USE_SCAN_VALUE>1</USE_SCAN_VALUE>
            </TECHNOLOGY>
...
```

Schema update:

The ImportableControl.xsd schema is used when importing and exporting controls. It was updated to include the new element USE_SCAN_VALUE.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified"

...

<xs:element name="TECHNOLOGY">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" maxOccurs="1"/>
                <xs:element ref="TECH_NAME" maxOccurs="1" />
                <xs:element ref="RATIONALE" maxOccurs="1" />
                <xs:element ref="DATAPOINT" maxOccurs="1" />
                <xs:element ref="USE_SCAN_VALUE" minOccurs="0"
maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
```

```
...
    <xs:element name="USE_SCAN_VALUE" default="0">
        <xs:simpleType>
            <xs:restriction base="xs:integer">
                <xs:enumeration value="0" />
                <xs:enumeration value="1" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
```