Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.6

December 8, 2020

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.

Policy Export Shows Control Status for Different Control Types and Formats

APIs affected	/api/2.0/fo/compliance/policy/?action=export /api/2.0/fo/compliance/policy/?action=import
New or Updated API	Updated
DTD or XSD changes	Yes

When you export a compliance policy (from the UI or API) we indicate the status for each control in the policy so you know whether the control is disabled or not. We were already showing control status in XML format for service-defined controls, and now you'll also see the status for user-defined controls. When you export a policy to CSV format, you'll notice a new column for showing the control status for all control types, including service-defined controls and user-defined controls. This change provides consistency across formats. The control status appears under IS_CONTROL_DISABLE with a value of 1 when the control is disabled and a value of 0 when the control is enabled.

Keep in Mind

When exporting a policy, all the service-defined controls in the policy are exported by default, and you must choose to export the user-defined controls. You do this by specifying "show_user_controls=1" as part of the export request (using API) or by selecting the export option "Include UDCs and QCCs" (from UI).

When you import an XML policy with user-defined controls into your account, we'll now include the control status for each UDC. You must choose to import the UDCs from the policy XML by specifying "create_user_controls=1" as part of the import request (using API) or by selecting the import option "Create user-defined controls" (from UI).

API Sample - Policy Export to XML

In the USER_DEFINED_CONTROL section you'll now see IS_CONTROL_DISABLE for each control with a value of 1 (disabled) or 0 (enabled).

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=export&id=221469&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

Response:

```
...
<USER_DEFINED_CONTROL>
                    <ID>100111</ID>
                    <UDC_ID>a9d7e4b1-236f-40c4-823e-f030cb2efa1d</UDC_ID>
                    <CHECK_TYPE>PostgreSQL Database Check</CHECK_TYPE>
```

```
                         <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                          <CATEGORY>
                              <ID>8</ID>
                              <NAME><![CDATA[Database Settings]]></NAME>
                          </CATEGORY>
...
```

DTD update:

The Policy Export Output DTD (policy_export_output.dtd) was updated to show IS_CONTROL_DISABLE as part of the element USER_DEFINED_CONTROL.

```
<!-- QUALYS POLICY_EXPORT_OUTPUT DTD -->
<!-- $Revision: 62328 $ -->
<!ELEMENT POLICY_EXPORT_OUTPUT (REQUEST?, RESPONSE)>

...

<!ELEMENT USER_DEFINED_CONTROL (ID, UDC_ID, CHECK_TYPE,
IS_CONTROL_DISABLE?, CATEGORY, SUB_CATEGORY, STATEMENT, CRITICALITY?,
COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?, IGNORE_ERROR,
(IGNORE_ITEM_NOT_FOUND|ERROR_SET_STATUS)?, SCAN_PARAMETERS?,
REFERENCE_TEXT?, TECHNOLOGIES, REFERENCE_LIST)>

...
```

API Sample - Policy Import from XML

When you import a policy from XML into your account and include UDCs, the control status is included for each UDC.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -H Content-
Type:text/xml --data-binary "@policy.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=import
&title=ImportedPolicy1&create_user_controls=1"
```

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>2020-11-16T22:51:16Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
```

```
          <KEY>ID</KEY>
          <VALUE>1867541</VALUE>
        </ITEM>
        <ITEM>
            <KEY>TITLE</KEY>
            <VALUE>ImportedPolicy1</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

ImportableControl.xsd Schema update:

The ImportableControl.xsd schema was also updated to include IS_CONTROL_DISABLE so that when you import UDCs from a policy, the status for each UDC is included.

```
...
    <xs:element name="CONTROL">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="UDC_ID" minOccurs="0" maxOccurs="1" />
                <xs:element ref="CHECK_TYPE" maxOccurs="1" />
                <xs:element ref="IS_CONTROL_DISABLE" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="CATEGORY" minOccurs="0" maxOccurs="1" />
               <xs:element ref="SUB_CATEGORY" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="STATEMENT" maxOccurs="1" />
                <xs:element ref="CRITICALITY" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="COMMENT" minOccurs="0" maxOccurs="1" />
                <xs:element ref="USE_AGENT_ONLY" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="AUTO_UPDATE" minOccurs="0" maxOccurs="1"
/>
               <xs:element ref="IGNORE_ERROR" minOccurs="0" maxOccurs="1"
/>
                <xs:element ref="ERROR_SET_STATUS" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="IGNORE_ITEM_NOT_FOUND" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="SCAN_PARAMETERS" minOccurs="0"
maxOccurs="1" />
                <xs:element ref="TECHNOLOGY_LIST" maxOccurs="1" />
                <xs:element ref="REFERENCE_LIST" maxOccurs="1" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
```

```
...

    <xs:element name="IS_CONTROL_DISABLE">
        <xs:simpleType>
            <xs:restriction base="xs:integer"/>
        </xs:simpleType>
    </xs:element>

...
```

API Sample - Policy Export to CSV (from UI)

You can export policies to CSV format from the Policies list in the UI. When you view your CSV report, you'll see the new column "Is Control Disable" with a value of 1 (disabled) or 0 (enabled) for each control.

Sample CSV report:

```
Policy Information,,,,,,,,,,,,
Title,Cover Page,,,,,,,,,,,
Postgre_Policy,,,,,,,,,,,,
,,,,,,,,,,,,
Technologies (6),,,,,,,,,,,,
ID,Name,,,,,,,,,,,
114,PostgreSQL 9.x,,,,,,,,,,,
143,PostgreSQL 10.x,,,,,,,,,,,
192,PostgreSQL 11.x,,,,,,,,,,,
201,Pivotal Greenplum 5.x,,,,,,,,,,,
228,PostgreSQL 12.x,,,,,,,,,,,
230,Pivotal Greenplum 6.x,,,,,,,,,,,
,,,,,,,,,,,,
Control Information,,,,,,,,,,,,
Section No.,Section
Heading,Reference,CID,UDC_ID,Statement,Description,Technology
ID,Technology Name,Criticality Label,Criticality Value,Evaluation,Is
Control Disable
1,postgre,,10979,N/A,Status of the UNIX/Linux ownership and permissions
set for the log directory specified in the 'log_directory' parameter,"The
log directory specified in the 'log_directory' parameter designates the
directory in which the log files will be stored.  Log files play an
important role in security auditing, incident response, troubleshooting
and system maintenance.  To maintain integrity, and prevent any
unauthorized access, misuse or tampering, ownership and permissions for
the log directory should be restricted as appropriate to the
business/organization needs.",114,PostgreSQL 9.x,CRITICAL,4,"The
following List string value of X indicates the UNIX/Linux ownership and
permissions set for the log directory specified in the 'log_directory'
parameter of the server.  The result consists of user ownership, group
```

```
ownership, directory permissions, followed by the directory name (absolute
path).

* * * * * Expected Value(s) * * * * *
matches regular expression list
.*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x]:.*
OR, any of the selected values below:
[x] Setting not found
[x] File not found",1
1,postgre,,10979,N/A,Status of the UNIX/Linux ownership and permissions
set for the log directory specified in the 'log_directory' parameter,"The
log directory specified in the 'log_directory' parameter designates the
directory in which the log files will be stored.  Log files play an
important role in security auditing, incident response, troubleshooting
and system maintenance.  To maintain integrity, and prevent any
unauthorized access, misuse or tampering, ownership and permissions for
the log directory should be restricted as appropriate to the
business/organization needs.",143,PostgreSQL 10.x,CRITICAL,4,"The
following List string value of X indicates the UNIX/Linux ownership and
permissions set for the log directory specified in the 'log_directory'
parameter of the server.  The result consists of user ownership, group
ownership, directory permissions, followed by the directory name (absolute
path).

* * * * * Expected Value(s) * * * * *
matches regular expression list
.*:.*:[-r][-w][-x][-r][-w][-x][-r][-w][-x]:.*
OR, any of the selected values below:
[x] Setting not found
[x] File not found",1
...
```

More Regions Supported for EC2 and Cloud Perimeter Scans

APIs affected	/api/2.0/fo/scan/ /api/2.0/fo/scan/compliance/ /api/2.0/fo/scan/cloud/perimeter/job /api/2.0/fo/schedule/scan/
New or Updated API	Updated
DTD or XSD changes	No

We support the following new regions when launching vulnerability and compliance scans on EC2 instances, and when launching cloud perimeter scans: Europe (Milan) and Africa (Cape Town). You need to set the input parameter to the respective region and include it in the scan request.

Input Parameters

Refer to the Qualys API (VM,PC) User Guide for full details on all the parameters.

Parameter	Description
EC2 Vulnerability or Compliance Scan	
ec2_endpoint= {value}	(Required for EC2 vulnerability and compliance scans) The EC2 region code or the ID of the Virtual Private Cloud (VPC) zone. When specifying a region code, you can now include these newly supported regions: eu-south-1 (EU-Milan) af-south-1 (Africa-Cape Town)
Cloud Perimeter Scan	
region_code={value}	(Optional) The region code. You can now include these newly supported regions: eu-south-1 (EU-Milan) af-south-1 (Africa-Cape Town)
	One of these parameters must be specified in the request: region_code or vpc_id. These are mutually exclusive and cannot be specified in the same request.

Check out these examples for launching various types of scans in different regions.

Sample - Launch Vulnerability Scan on EC2 instances in Cape Town region

Sample - Launch Compliance Scan on EC2 instances in Milan region

Sample - Schedule Vulnerability Scan on EC2 instances in Cape Town region

Sample - Create Cloud Perimeter Scan Job in Cape Town region for VM

Sample - Create Cloud Perimeter Scan Job in Milan region for PC

Sample - Create VM EC2 Scan on instance ID for Cape Town region

Sample - Create PC EC2 Scan on instance ID for Milan region

Sample - Launch Vulnerability Scan on EC2 instances in Cape Town region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=launch&scan_title=API_OnDemand_CapeTown&target_from=tags&tag_set_
by=name&tag_include_selector=any&tag_set_include=CapeTown&connector_name=
AWS_Connector&ec2_endpoint=af-south-1&option_title=Initial
Options&iscanner_name=EC2_Scanner"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:

```
<?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>2020-11-20T06:27:07Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>11845838</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1605853625.45838</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch Compliance Scan on EC2 instances in Milan region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=launch&scan_title=API_OnDemand_Milan_PC&target_from=tags&tag_set_
by=name&tag_include_selector=any&tag_set_include=Milan&connector_name=AWS
_Connector&ec2_endpoint=eu-south-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:


```
<?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>2020-11-20T06:33:40Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>11845850</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1605854018.45850</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```


Sample - Schedule Vulnerability Scan on EC2 instances in Cape Town region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=create&scan_title=API_Schedule_CapeTown_VM&target_from=tags&tag_s
et_by=name&tag_include_selector=any&tag_set_include=CapeTown&connector_na
me=AWS_Connector&ec2_endpoint=af-south-
1&active=1&occurrence=daily&start_date=11/21/2020&start_hour=9&start_minu
te=00&time_zone_code=IN&option_title=Initial
Options&frequency_days=364&end_after=1&observe_dst=no&iscanner_name=EC2_S
canner" "https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/"
```

XML output:


```
<?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>2020-11-20T06:37:43Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3546443</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```


Sample - Create Cloud Perimeter Scan Job in Cape Town region for VM

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"action=create&scan_title=API_CPS_VM_CapeTown&module=vm&active=1&schedule
=now&tag_set_include=Live_EC2_Assets&tag_set_by=name&platform_type=vpc_pe
ered&option_id=646656&connector_name=AWS_Connector&region_code=af-south-
1&iscanner_id=573747"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

XML output:


```
<?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>2020-11-20T06:47:19Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3546445</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Create Cloud Perimeter Scan Job in Milan region for PC

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"action=create&scan_title=API_CPS_PC_Milan&module=pc&active=1&schedule=no
w&tag_set_include=Live_EC2_Assets&tag_set_by=name&platform_type=vpc_peere
d&option_id=646660&connector_name=AWS_Connector&region_code=eu-south-
1&iscanner_id=573747"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

XML output:


```
<?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>2020-11-20T06:51:03Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3546448</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```


Sample - Create VM EC2 Scan on instance ID for Cape Town region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=launch&scan_title=API_VM_OnDemand_InstanceID_CapeTown&connector_n
ame=AWS_Connector&ec2_endpoint=af-south-1&option_title=Initial
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-05a961c6033d62bd5"
"https://qualysapi.qualys.com/api/2.0/fo/scan/"
```

XML output:


```
<?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>2020-11-20T07:03:08Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
```

```
      <KEY>ID</KEY>
      <VALUE>11845893</VALUE>
    </ITEM>
    <ITEM>
      <KEY>REFERENCE</KEY>
      <VALUE>scan/1605855787.45893</VALUE>
    </ITEM>
  </ITEM_LIST>
</RESPONSE>
```

Sample - Create PC EC2 Scan on instance ID for Milan region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=launch&scan_title=API_PC_OnDemand_InstanceID_Milan&connector_name
=AWS_Connector&ec2_endpoint=eu-south-1&option_title=Initial PC
Options&iscanner_name=EC2_Scanner&ec2_instance_ids=i-003ee800c064aeb4a"
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/"
```

XML output:

```
<?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>2020-11-20T07:05:46Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>11845901</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1605855945.45901</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Choose Data Scope for Asset Purge

APIs affected	/api/2.0/fo/asset/host/?action=purge
New or Updated API	Updated
DTD or XSD changes	No

With this release, we've introduced a new input parameter called "data_scope" that allows you to specify the type of data to purge from a host. You can specify "vm" to purge vulnerability data, "pc" to purge compliance data, or "vm,pc" (irrespective of order) to purge both types of data.

Note that you can continue to use the existing input parameter "compliance_enabled" to purge compliance data along with vulnerability data or vulnerability data only. This existing option did not allow you to purge compliance data only but now you can achieve that with the new data_scope option.

You can combine compliance_enabled and data_scope in the same request. Note, however, that anytime compliance_enabled=1 is specified, then both vulnerability and compliance data is purged regardless of the data_scope value. See the table below to understand the different combinations and the type of data purged.

compliance_enabled value	data_scope value	type of data purged
1	unspecified	vulnerability + compliance data
0	unspecified	vulnerability data only
unspecified or 0	vm	vulnerability data only
unspecified or 0	pc	compliance data only
unspecified or 0	vm,pc	vulnerability + compliance data
1	vm	vulnerability + compliance data
1	pc	vulnerability + compliance data
1	vm,pc	vulnerability + compliance data

Permissions

Managers can purge assessment data for all hosts in the subscription, including vulnerability data and/or compliance data.

Auditors can purge compliance data only for all compliance hosts in the subscription (vulnerability data will not be removed).

Unit Managers, Scanners, and Readers can purge vulnerability data and/or compliance data in their user account if granted the permission "Purge host information/history". The permission "Manage compliance" is required to purge compliance data.

Input Parameters

Refer to the Qualys API (VM,PC) User Guide for details on all the possible input parameters for purging assets. There are several additional inputs which are not listed here.

Parameter	Description
action=purge	(Required)
data_scope={value}	(Optional) The type of data to purge. Specify "vm" to purge vulnerability data, specify "pc" to purge compliance data, or specify both as a comma separated list to purge both types of data. If compliance_enabled=1 is specified in the same request, then vulnerability and compliance data will both be purged regardless of the data_scope value.
compliance_enabled={0|1}	(Optional) This parameter is valid only when the policy compliance module is enabled for the user account. Specify 1 to purge compliance hosts in the user's account. These hosts are assigned to the PC module. When selected, the service will remove vulnerability data and compliance data associated with the selected hosts. Specify 0 to purge hosts which are not assigned to the PC module. When specified (without data_scope), the service will remove only vulnerability information associated with the selected hosts. Note: A sub-account (Unit Manager, Scanner or Reader) can specify this parameter only when the user account is granted permissions to purge compliance information. An Auditor does not have permission to set compliance_enabled=0.

API Samples

Sample 1 - Purge only compliance data

In this example, data_scope=pc so only compliance data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=pc"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:


```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:51:57Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (compliance data) for Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```


Sample 2 - Purge only vulnerability data

In this example, data_scope=vm so only vulnerability data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:


```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:51:45Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability data) for Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 3 - Purge vulnerability and compliance data

In this example, data_scope=pc,vm so both vulnerability and compliance data will be purged for the host.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.152&data_scope=pc,vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T10:52:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability + compliance data) for
Purging</TEXT>
        <ID_SET>
          <ID>3971339</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 4 - Purge vulnerability and compliance data (using compliance_enabled)

In this example, compliance_enabled=1 and data_scope=pc. Both vulnerability and compliance data will be purged for the host since compliance_enabled=1 takes precedence.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.154&compliance_enabled=1&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T11:25:12Z</DATETIME>
    <BATCH_LIST>
```

```
      <BATCH>
        <TEXT>Hosts Queued (vulnerability + compliance data) for
Purging</TEXT>
        <ID_SET>
          <ID>3971340</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample 5 - Purge only vulnerability data (using compliance_enabled)

In this example, compliance_enabled=0 and data_scope=vm so only vulnerability data will be purged.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -X "POST" -d
"action=purge&ips=10.20.32.154&compliance_enabled=0&data_scope=vm"
"https://qualysapi.qualys.com/api/2.0/fo/asset/host/"
```

Response:

```
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-11-19T11:25:12Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Hosts Queued (vulnerability data) for Purging</TEXT>
        <ID_SET>
          <ID>3971340</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

More Details in Authentication Reports: Host ID and All Asset Tags

APIs affected	/api/2.0/fo/report/
New or Updated API	Updated
DTD or XSD changes	Yes

Now you have the option to include additional details in authentication reports. When you generate an authentication report in the UI (from VM or PC), you'll see new options for including Host ID and All Asset Tags in the Details Section of the report. These are optional details that are not included by default. The details you pick will appear in all report formats, including XML and CSV.

Use the API to download any saved report from your account. See samples below.

Changes to the CSV format of the report:

- We added the column "Host Id" where you'll see the host Id for each host in the report. This column only appears in the report when the user selected the Host ID option at the time the report was generated.

- We added the column "All Asset Tags" where you'll see a complete list of tags associated with the asset. This column only appears in the report when the user selected the All Asset Tags option at the time the report was generated.

- We changed the value in the existing "Asset Tags" column. This column used to show the text "Selected Tags". Now you'll see the tag names for the tags associated with the asset that also match the report target.

Changes to the XML format of the report:

- We added the element HOST_ID where you'll see the host Id for each host in the report. This only appears in the report when the user selected the Host ID option at the time the report was generated.

- We added the element ALL_ASSET_TAGS where you'll see a complete list of tags associated with the asset. This only appears in the report when the user selected the All Asset Tags option at the time the report was generated.

API Sample - Authentication Report in CSV

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4121141&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:

```
My Auth Report,12/04/2020 at 20:11:10 (GMT+0530),,,,,,,,,,,,,
"Qualys, Inc.","919 E Hillsdale Blvd, 4th Floor",,Foster
City,California,United States of America,94404,,,,,,,,
Joe User,Manager,,,,,,,,,,,,,
SUMMARY,,,,,,,,,,,,,,
Asset Tags,Passed Authentications,Insufficient Authentications,Failed
Authentications,Not Attempted Authentications,Not Installed
Authentication,Total Authentications,Passed Percentage,Failed
Percentage,Not Attempted Percentage,,,,,,
"Included(any): Tag123,TagXYZ, TagABC;
Excluded(any);",7,0,0,0,0,7,100,0,0,,,,,,
RESULTS,,,,,,,,,,,,,,
Asset Tags,Technology,Host Technology,Instance,Host IP,DNS
Hostname,NetBIOS Hostname,Tracking Method,Network,Status,Failure
Reason,OS,Last Auth,Last Success,Host Id,All Asset Tags
Tag123,Windows,Windows 2003 Server,,10.10.25.224,ora10105-win-25-
224,ORA10105-WIN-25,IP,Global Default Network,Passed,'-,Windows Server
2003 Service Pack 2,11/5/2020,11/5/2020,4411605,"Demo, Windows, Tag123"
TagABC,Unix/Cisco/Checkpoint Firewall,CentOS 6.x,,10.10.32.227,centos-60-
32-227.qualys.com,,IP,Custom Network 1,Passed,'-,CentOS Linux
6.0,12/3/2020,12/3/2020,4797608,"BU1, AG1, TagABC, CentOS6"
...
```

API Sample - Authentication Report in XML

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=4119485&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_AUTHENTICATION_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_authentication_report.dtd">
<COMPLIANCE_AUTHENTICATION_REPORT>
  <HEADER>
    <NAME><![CDATA[My Auth Report]]></NAME>
    <GENERATION_DATETIME>2020-12-03T14:21:06Z</GENERATION_DATETIME>
    <COMPANY_INFO>
      <NAME><![CDATA[Qualys, Inc.]]></NAME>
      <ADDRESS><![CDATA[919 E Hillsdale Blvd, 4th Floor]]></ADDRESS>
      <CITY><![CDATA[Foster City]]></CITY>
      <STATE><![CDATA[California]]></STATE>
      <COUNTRY><![CDATA[United States of America]]></COUNTRY>
      <ZIP_CODE><![CDATA[94404]]></ZIP_CODE>
```

```
      </COMPANY_INFO>
      <USER_INFO>
        <NAME><![CDATA[Joe User]]></NAME>
        <ROLE>Manager</ROLE>
      </USER_INFO>
      <FILTERS>
        <ASSET_TAG_LIST>
          <INCLUDED_TAGS scope="any">
            <TAG_ITEM><![CDATA[TagABC]]></TAG_ITEM>
            <TAG_ITEM><![CDATA[TagXYZ]]></TAG_ITEM>
            <TAG_ITEM><![CDATA[Tag123]]></TAG_ITEM>
          </INCLUDED_TAGS>
        </ASSET_TAG_LIST>
      </FILTERS>
    </HEADER>
    <ASSET_TAG_LIST>
      <ASSET_TAG>
        <INCLUDED_TAGS scope="any">
            <TAG_ITEM><![CDATA[TagABC]]></TAG_ITEM>
            <TAG_ITEM><![CDATA[TagXYZ]]></TAG_ITEM>
            <TAG_ITEM><![CDATA[Tag123]]></TAG_ITEM>
        </INCLUDED_TAGS>
        <AUTH_PASSED>7</AUTH_PASSED>
        <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
        <AUTH_FAILED>0</AUTH_FAILED>
        <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
        <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
        <AUTH_TOTAL>7</AUTH_TOTAL>
        <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
        <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
        <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <NAME><![CDATA[Windows]]></NAME>
            <HOST_LIST>
              <HOST>
                <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
                <IP><![CDATA[10.10.25.224]]></IP>
                <DNS><![CDATA[ora10105-win-25-224]]></DNS>
                <NETBIOS><![CDATA[ORA10105-WIN-25]]></NETBIOS>
                <HOST_TECHNOLOGY><![CDATA[Windows 2003
  Server]]></HOST_TECHNOLOGY>
                <STATUS><![CDATA[Passed]]></STATUS>
                <NETWORK><![CDATA[Global Default Network]]></NETWORK>
                <OS><![CDATA[Windows Server 2003 Service Pack 2]]></OS>
                <LAST_AUTH><![CDATA[11/05/2020]]></LAST_AUTH>
                <LAST_SUCCESS><![CDATA[11/05/2020]]></LAST_SUCCESS>
                <HOST_ID><![CDATA[4411605]]></HOST_ID>
                <ALL_ASSET_TAGS><![CDATA[Demo, Windows,
```

```
Tag123]]></ALL_ASSET_TAGS>
            </HOST>
          </HOST_LIST>
        </TECHNOLOGY>
        <TECHNOLOGY>
          <NAME><![CDATA[Unix/Cisco/Checkpoint Firewall]]></NAME>
          <HOST_LIST>
            <HOST>
              <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
              <IP><![CDATA[10.10.32.227]]></IP>
              <DNS><![CDATA[centos-60-32-227.qualys.com]]></DNS>
              <NETBIOS><![CDATA[]]></NETBIOS>
              <HOST_TECHNOLOGY><![CDATA[CentOS 6.x]]></HOST_TECHNOLOGY>
              <STATUS><![CDATA[Passed]]></STATUS>
              <NETWORK><![CDATA[Custom Network 1]]></NETWORK>
              <OS><![CDATA[CentOS Linux 6.0]]></OS>
              <LAST_AUTH><![CDATA[12/03/2020]]></LAST_AUTH>
              <LAST_SUCCESS><![CDATA[12/03/2020]]></LAST_SUCCESS>
              <HOST_ID><![CDATA[4797608]]></HOST_ID>
              <ALL_ASSET_TAGS><![CDATA[BU1, AG1, TagABC,
CentoOS6]]></ALL_ASSET_TAGS>
            </HOST>
...
          </HOST_LIST>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
    </ASSET_TAG>
  </ASSET_TAG_LIST>
  <APPENDIX />
</COMPLIANCE_AUTHENTICATION_REPORT>
```

DTD Update:

<base_url>compliance_authentication_report.dtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE AUTHENTICATION REPORT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_AUTHENTICATION_REPORT (ERROR | (HEADER,
(BUSINESS_UNIT_LIST | ASSET_GROUP_LIST | ASSET_TAG_LIST | IPS_LIST),
APPENDIX?))>
...
<!ELEMENT TECHNOLOGY_LIST (TECHNOLOGY*)>
<!ELEMENT TECHNOLOGY (NAME, HOST_LIST)>
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, HOST_TECHNOLOGY?,
INSTANCE?, STATUS, CAUSE?, NETWORK?, OS?, LAST_AUTH?,
LAST_SUCCESS?,HOST_ID?,ALL_ASSET_TAGS?)>
<!ELEMENT TRACKING_METHOD (#PCDATA)>
```

```
<!ELEMENT IP (#PCDATA)>
<!ELEMENT DNS (#PCDATA)>
<!ELEMENT HOST_TECHNOLOGY (#PCDATA)>
<!ELEMENT NETBIOS (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CAUSE (#PCDATA)>
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT OS (#PCDATA)>
<!ELEMENT LAST_AUTH (#PCDATA)>
<!ELEMENT LAST_SUCCESS (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT ALL_ASSET_TAGS (#PCDATA)>
...
```

New SAP IQ Authentication API

APIs affected	/api/2.0/fo/auth/
New or Updated API	Updated
DTD or XSD changes	Yes
APIs affected	/api/2.0/fo/auth/sapiq/
New or Updated API	New
DTD or XSD changes	New

SAP IQ authentication is now supported for compliance scans (using PC or SCA). The new SAP IQ API (api/2.0/fo/auth/sapiq/) lets you list, create, update and delete SAP IQ authentication records. User permissions for this API are the same as other authentication record APIs.

List all record types

Use the Authentication Record List API (/api/2.0/fo/auth/ with action=list) to list authentication records for all types. You'll see <AUTH_SAP_IQ_IDS> in the output when you have SAP IQ records in your account.

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With:curl' -d
"action=list" "https://qualysapi.qualys.com/api/2.0/fo/auth/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_RECORDS_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/auth_records.dtd">
<AUTH_RECORDS_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-12-05T06:46:07Z</DATETIME>
        <AUTH_RECORDS>
            <AUTH_UNIX_IDS>
                <ID_SET>
                    <ID>75275</ID>
                </ID_SET>
            </AUTH_UNIX_IDS>
            <AUTH_WINDOWS_IDS>
                <ID_SET>
                    <ID>75272</ID>
                    <ID>83173</ID>
                    <ID>85175</ID>
                </ID_SET>
            </AUTH_WINDOWS_IDS>
```

```
                <AUTH_SAP_IQ_IDS>
                    <ID_SET>
                        <ID>96170</ID>
                    </ID_SET>
                </AUTH_SAP_IQ_IDS>
            </AUTH_RECORDS>
        </RESPONSE>
    </AUTH_RECORDS_OUTPUT>
```

Updated DTD

<base_url>/api/2.0/fo/auth/auth_records.dtd

The element AUTH_SAP_IQ_IDS has been added to identify SAP IQ record IDs.

```
<!-- QUALYS AUTH_RECORDS_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_RECORDS_OUTPUT (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 urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, AUTH_RECORDS?, WARNING_LIST?)>

<!ELEMENT AUTH_RECORDS (AUTH_UNIX_IDS?, AUTH_WINDOWS_IDS?,
AUTH_ORACLE_IDS?, AUTH_ORACLE_LISTENER_IDS?, AUTH_SNMP_IDS?,
AUTH_MS_SQL_IDS?, AUTH_IBM_DB2_IDS?, AUTH_VMWARE_IDS?, AUTH_MS_IIS_IDS?,
AUTH_APACHE_IDS?, AUTH_IBM_WEBSPHERE_IDS?, AUTH_HTTP_IDS?,
AUTH_SYBASE_IDS?, AUTH_MYSQL_IDS?, AUTH_TOMCAT_IDS?,
AUTH_ORACLE_WEBLOGIC_IDS?, AUTH_DOCKER_IDS?, AUTH_POSTGRESQL_IDS?,
AUTH_MONGODB_IDS?, AUTH_PALO_ALTO_FIREWALL_IDS?, AUTH_VCENTER_IDS?,
AUTH_JBOSS_IDS?, AUTH_MARIADB_IDS?, AUTH_INFORMIXDB_IDS?,
AUTH_MS_EXCHANGE_IDS?, AUTH_ORACLE_HTTP_SERVER_IDS?, AUTH_GREENPLUM_IDS?,
AUTH_MICROSOFT_SHAREPOINT_IDS?, AUTH_KUBERNETES_IDS?, AUTH_SAP_IQ_IDS? )>

<!ELEMENT AUTH_UNIX_IDS (ID_SET)>
<!ELEMENT AUTH_WINDOWS_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_LISTENER_IDS (ID_SET)>
<!ELEMENT AUTH_SNMP_IDS (ID_SET)>
<!ELEMENT AUTH_MS_SQL_IDS (ID_SET)>
```

```
<!ELEMENT AUTH_IBM_DB2_IDS (ID_SET)>
<!ELEMENT AUTH_VMWARE_IDS (ID_SET)>
<!ELEMENT AUTH_MS_IIS_IDS (ID_SET)>
<!ELEMENT AUTH_APACHE_IDS (ID_SET)>
<!ELEMENT AUTH_IBM_WEBSPHERE_IDS (ID_SET)>
<!ELEMENT AUTH_HTTP_IDS (ID_SET)>
<!ELEMENT AUTH_SYBASE_IDS (ID_SET)>
<!ELEMENT AUTH_MYSQL_IDS (ID_SET)>
<!ELEMENT AUTH_TOMCAT_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_WEBLOGIC_IDS (ID_SET)>
<!ELEMENT AUTH_DOCKER_IDS (ID_SET)>
<!ELEMENT AUTH_POSTGRESQL_IDS (ID_SET)>
<!ELEMENT AUTH_MONGODB_IDS (ID_SET)>
<!ELEMENT AUTH_PALO_ALTO_FIREWALL_IDS (ID_SET)>
<!ELEMENT AUTH_VCENTER_IDS (ID_SET)>
<!ELEMENT AUTH_JBOSS_IDS (ID_SET)>
<!ELEMENT AUTH_MARIADB_IDS (ID_SET)>
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
<!ELEMENT AUTH_GREENPLUM_IDS (ID_SET)>
<!ELEMENT AUTH_MICROSOFT_SHAREPOINT_IDS (ID_SET)>
<!ELEMENT AUTH_KUBERNETES_IDS (ID_SET)>
<!ELEMENT AUTH_SAP_IQ_IDS (ID_SET)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>

<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT ID_RANGE (#PCDATA)>


<!-- EOF -->
```

List SAP IQ records

Use these parameters to list SAP IQ authentication records.

Parameter	Description
action={action}	(Required) Specify list (using GET or POST) to list records.
details={value}	(Optional) Default value is Basic. You can choose from None, Basic, and All.
ids={value}	(Optional) SAP IQ auth record IDs to list. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.

Sample - List SAP IQ Records with All Details

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=list&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_SAP_IQ_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/auth_sap_iq_list_outp
ut.dtd">
<AUTH_SAP_IQ_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-11-20T06:59:40Z</DATETIME>
        <AUTH_SAP_IQ_LIST>
            <AUTH_SAP_IQ>
                <ID>96170</ID>
                <TITLE>
                    <![CDATA[sap iq]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <DATABASE>
                    <![CDATA[sapiqdb]]>
                </DATABASE>
                <PORT>123</PORT>
                <IP_SET>
                    <IP>10.10.10.55</IP>
                </IP_SET>
                <DATABASE>
                    <![CDATA[sapiqdb]]>
                </DATABASE>
```

```
                    <PORT>123</PORT>
                    <LOGIN_TYPE>
                        <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2020-11-20T06:40:42Z</DATETIME>
                        <BY>quays_rd4</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-11-20T06:40:42Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_SAP_IQ>
            </AUTH_SAP_IQ_LIST>
            <GLOSSARY>
                <USER_LIST>
                    <USER>
                        <USER_LOGIN>joe_user</USER_LOGIN>
                        <FIRST_NAME>Joe</FIRST_NAME>
                        <LAST_NAME>User</LAST_NAME>
                    </USER>
                </USER_LIST>
            </GLOSSARY>
        </RESPONSE>
    </AUTH_SAP_IQ_LIST_OUTPUT>
```

<u>New DTD</u>

<base_url>/api/2.0/fo/auth/sapiq/auth_sap_iq_list_output.dtd

```
<!-- QUALYS AUTH_SAP_IQ_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_SAP_IQ_LIST_OUTPUT (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 urlencoded -->
<!ELEMENT POST_DATA (#PCDATA)>

<!ELEMENT RESPONSE (DATETIME, (AUTH_SAP_IQ_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_SAP_IQ_LIST (AUTH_SAP_IQ+)>
```

```
<!ELEMENT AUTH_SAP_IQ (ID, TITLE, USERNAME, DATABASE, PORT,
INSTALLATION_DIR?, PASSWORD_ENCRYPTION?, IP_SET?, LOGIN_TYPE?,
DIGITAL_VAULT?, NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT INSTALLATION_DIR (#PCDATA)>
<!ELEMENT PASSWORD_ENCRYPTION (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>

<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_USERNAME?, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?,
VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_NS_TYPE (#PCDATA)>
<!ELEMENT VAULT_NS_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>

<!ELEMENT NETWORK_ID (#PCDATA)>

<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT COMMENTS (#PCDATA)>

<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
```

```
<!ELEMENT ID_RANGE (#PCDATA)>

<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>

<!-- EOF -->
```

Create/Update SAP IQ Authentication Records

Use these parameters to create or update SAP IQ authentication records.

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
echo_request={**0**|1}	(Optional) Specify 1 to view (echo) input parameters in the XML output. By default these are not included.
ids={value}	(Required to update or delete record) Record IDs to update/delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
SAP IQ	
database={value}	(Required for create request) The name of the database you want to authenticate to.
port={value}	(Required for create request) The port the database is on.
installation_dir={value}	(Required for create request when this record will be used for scanning Unix hosts) The database installation directory for scanning Unix hosts.
Login credentials	
username={value}	(Required for create request) The username of the account to be used for authentication. If password is specified this is the username of a SAP IQ account. If login_type=vault is specified, this is the username of a vault account. Maximum 255 characters (ascii).
password={value}	(For create request, password or login_type=vault is required) The password of the SAP IQ account to be used for authentication. Maximum 100 characters (ascii).

Parameter	Description
password_encryption={**0**|1}	(Optional to create or update record) Enable this option when your database instance requires an encrypted password for successful login. If password encryption is required and you do not enable this option then authentication will fail. When set to 1, password encryption is enabled in the record. When set to 0 (the default), password encryption is not enabled.
login_type={value}	(For create request, password or login_type=vault is required) Login type can be basic (default) or vault. Set to vault if a third party vault will be used to retrieve the password. Vault parameters need to be provided in the record. See "Vault Definition" in the API user guide.
vault_id={value}	(Required if login_type=vault) The ID of the vault to be used to retrieve the password for login.
vault_type={value}	(Required if login_type=vault) The third party vault to be used to retrieve the password for login. Certain vaults support this capability. See "Vault Support Matrix" in the API user guide.
Target Hosts	
ips={value}	(Required to create record) The IP address(es) the server will log into using the record's credentials. Multiple entries are comma separated. (Optional to update record) IPs specified will overwrite existing IPs in the record, and existing IPs will be removed. This parameter and the add_ips parameter or the remove_ips parameter cannot be specified in the same request.
add_ips={value}	(Optional to update record) Add IPs and/or ranges to the IPs list for this record. Multiple IPs/ranges are comma separated. This parameter and the ips parameter cannot be specified in the same request.
remove_ips={value}	(Optional to update record) IPs to be removed from your record. You may enter a combination of IPs and ranges. Multiple entries are comma separated. This parameter and the ips parameter cannot be specified in the same request.
network_id={value}	(Optional to create or update record, and valid only when the networks feature is enabled) The network ID for the record.

Sample - Create SAP IQ Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=create&title=sapiq&username=root&password=root&database=sapDb&por
t=123&&ips=11.11.11.11"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-12-05T12:04:32Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>96171</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```


Sample - Update SAP IQ Record

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=update&ids=10002&title=SAP IQ new title"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-12-05T12:09:25Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>10002</ID>
                </ID_SET>
```

```
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Delete SAP IQ Records

Use the following parameter to delete one or more SAP IQ authentication records.

Parameter	Description
ids={value}	(Required to delete record) SAP IQ auth record IDs to delete. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.

Sample - Delete SAP IQ Records

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl' -d
"action=delete&ids=10002"
"https://qualysapi.qualys.com/api/2.0/fo/auth/sapiq/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-12-05T12:10:16Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Deleted</TEXT>
                <ID_SET>
                    <ID>10002</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

New Database UDC for SAP IQ

APIs affected	/api/2.0/fo/compliance/posture/info/?action=list /api/2.0/fo/compliance/control/?action=list /api/2.0/fo/compliance/policy/?action=export /api/2.0/fo/subscription/option_profile/pc
New or Updated API	Updated
DTD or XSD changes	Yes

We've introduced a new Database UDC for SAP IQ. For this new database control type, we added new settings in the compliance option profile. You'll see API changes for create, update, list, and export option profiles. We've also added new elements to the XML output and DTDs for Control List Output, Policy Export Output, Posture Info List Output, Option Profiles, and the ImportableControl.xsd schema.

You'll see these changes:

- We added new input parameters sapiq_db_udc_restriction and sapiq_db_udc_limit to the Option Profile API to help you set a limit on the number of rows returned per scan for a SAP IQ UDC. The default value is 256 and maximum allowed limit is 10000 rows.

- We added a new CHECK_TYPE element to the XML output for Control List API: SAP IQ Database Check.

- We added support for SAP IQ 16.x technology for the UDC, and you'll see this technology in Posture API and Policy Export API.

- We updated the ImportableControl.xsd schema to include a new enumeration value for the CHECK_TYPE element: SAP IQ Database Check.

Sample - Option Profile API: Create

In this sample, you'll create an option profile and specify the new parameters for SAP IQ: sapiq_db_udc_restriction and sapiq_db_udc_limit.

<u>API request:</u>

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=create&title=SAPIQ_OP&scan_ports=targeted&sapiq_db_udc_restrictio
n=1&sapiq_db_udc_limit=5000"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:


```
<?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>2020-12-05T09:05:39Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>4561564</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```


Sample - Option Profile API: Update

In this sample, you'll update an option profile and specify the new parameters for SAP IQ: sapiq_db_udc_restriction and sapiq_db_udc_limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=update&title=UpdatedAPI_OP&id=4561564&sapiq_db_udc_restriction=1&
sapiq_db_udc_limit=7000"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:


```
<?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>2020-12-05T10:42:14Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>4561564</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Option Profile API: List

When you list option profiles, you'll see the database preference keys and their corresponding values for SAP IQ.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&id=4561564"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>4561564</ID>
      ...

      <DATABASE_PREFERENCE_KEY>
        <SAPIQ>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>7000</DB_UDC_LIMIT>
        </SAPIQ>
      </DATABASE_PREFERENCE_KEY>
...
```

Sample - Options Profile API: Export

When you export an option profile, you'll see the database preference keys and their corresponding values for SAP IQ.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=export&output_format=xml&option_profile_type=compliance&option_profil
e_id=4561564"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
```

```
<OPTION_PROFILE>
  <BASIC_INFO>
    <ID>4561564</ID>
    ...

    <DATABASE_PREFERENCE_KEY>
      <SAPIQ>
        <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
        <DB_UDC_LIMIT>7000</DB_UDC_LIMIT>
      </SAPIQ>
    </DATABASE_PREFERENCE_KEY>
...
```

DTD update:

We updated the option_profile_info.dtd to include SAP IQ in Database Preference Key and corresponding elements.

DTD: <platform>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>
<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
...

<!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?, ORACLE?, SYBASE?, POSTGRESQL?,
SAPIQ?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)>

...
```

Schema update (option_profiles.xsd):

The option_profiles.xsd schema is used when importing and exporting option profiles. We added new elements for the SAP IQ database control type.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="OPTION_PROFILES" type="OPTION_PROFILESType"/>
...
    <xs:complexType name="DATABASE_PREFERENCE_KEYType">
        <xs:sequence>
            <xs:element type="MSSQLType" name="MSSQL" minOccurs="0"/>
```

```
            <xs:element type="ORACLEType" name="ORACLE" minOccurs="0"/>
            <xs:element type="SYBASEType" name="SYBASE" minOccurs="0"/>
            <xs:element type="POSTGRESQLType" name="POSTGRESQL"
minOccurs="0"/>
            <xs:element type="SAPIQType" name="SAPIQ" minOccurs="0"/>

        </xs:sequence>
    </xs:complexType>
...

    <xs:complexType name="SAPIQType">
        <xs:sequence>
            <xs:element name="DB_UDC_RESTRICTION">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:enumeration value="1"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="DB_UDC_LIMIT">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="10000"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
...
```

Sample - Control List API for SAP IQ

We added a new CHECK_TYPE element to the XML output for Control List API: SAP IQ Database Check.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&details=All&ids=100005"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

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>2020-12-03T06:18:41Z</DATETIME>
      <CONTROL_LIST>
        <CONTROL>
          <ID>100005</ID>
          <UPDATE_DATE>2020-11-27T10:42:07Z</UPDATE_DATE>
          <CREATED_DATE>2020-11-27T10:42:07Z</CREATED_DATE>
          <CATEGORY>Database Settings</CATEGORY>
          <SUB_CATEGORY><![CDATA[DB Specific Settings]]></SUB_CATEGORY>
          <STATEMENT><![CDATA[SAP IQ UDC 3 - AR]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[SERIOUS]]></LABEL>
            <VALUE>3</VALUE>
          </CRITICALITY>
          <CHECK_TYPE><![CDATA[SAP IQ Database Check]]></CHECK_TYPE>
          <COMMENT><![CDATA[SAP IQ - 3]]></COMMENT>
          <IGNORE_ERROR>0</IGNORE_ERROR>
          <ERROR_SET_STATUS></ERROR_SET_STATUS>
          <TECHNOLOGY_LIST>
            <TECHNOLOGY>
              <ID>270</ID>
              <NAME>SAP IQ 16.x</NAME>
              <RATIONALE><![CDATA[Rationale 3]]></RATIONALE>
              <DB_QUERY><![CDATA[select @@servername as dbservername,
'201910' as fortidbversion]]></DB_QUERY>
              <DESCRIPTION><![CDATA[Desc 3]]></DESCRIPTION>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </RESPONSE>
```


Sample - Posture API

We added support for SAP IQ 16.x technology for the UDC, and you'll see this technology in the Posture API, when applicable.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -X "POST" -d
"action=list&policy_id=3549551&details=All&host_ids=5090108"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
```

```
    <DATETIME>2020-12-03T07:07:14Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>11269075</ID>
        <HOST_ID>5090108</HOST_ID>
        <CONTROL_ID>100000</CONTROL_ID>
        <TECHNOLOGY_ID>270</TECHNOLOGY_ID>
        <INSTANCE>SAP IQ 16:2638:pca-rhel68x64-70-
52_iqdemo:iqdemo</INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
30T07:54:32Z</POSTURE_MODIFIED_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-30T07:06:23Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2020-12-02T17:50:26Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[(((:dp_7 in #fv_4 or :dp_7 matches $tp_7
)))]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2020-12-02T09:39:30Z">
              <LABEL>:dp_7</LABEL>
              <V />
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
          <BOOLEAN_EXPR><![CDATA[(((:dp_7 in #fv_4 or :dp_7 matches $tp_7
)))]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2020-12-02T09:39:30Z">
              <LABEL>:dp_7</LABEL>
              <V />
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
    </INFO_LIST>
...
      <TECHNOLOGY_LIST>
        <TECHNOLOGY>
          <ID>270</ID>
          <NAME><![CDATA[SAP IQ 16.x]]></NAME>
        </TECHNOLOGY>
      </TECHNOLOGY_LIST>
...
```

Sample - Policy Export API

We added support for SAP IQ 16.x technology for the UDC, and you'll see this technology in the Policy Export API, when applicable.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=export
&id=354955&show_user_controls=1"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-12-05T17:08:54Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[SAP IQ - Policy]]></TITLE>
    <EXPORTED><![CDATA[2020-12-05T06:57:19Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>270</ID>
            <NAME>SAP IQ 16.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="2">
        <SECTION>
            <NUMBER>1</NUMBER>
            <HEADING><![CDATA[UDCs]]></HEADING>
            <CONTROLS total="6">
                <USER_DEFINED_CONTROL>
                    <ID>100000</ID>
                    <UDC_ID>bb99f909-0797-dbc9-809e-4ad3041da631</UDC_ID>
                    <CHECK_TYPE>SAP IQ Database Check</CHECK_TYPE>
                   <IS_CONTROL_DISABLE><![CDATA[0]]></IS_CONTROL_DISABLE>
                    <CATEGORY>
                        <ID>3</ID>
                     <NAME><![CDATA[Access Control Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1010</ID>
                        <NAME><![CDATA[Account Creation/User
Management]]></NAME>
                    </SUB_CATEGORY>
```

```
                    <STATEMENT><![CDATA[SAP IQ UDC 1 - AR]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[URGENT]]></LABEL>
                        <VALUE>5</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[SAP IQ ]]></COMMENT>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                    <ERROR_SET_STATUS></ERROR_SET_STATUS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>270</ID>
                            <NAME>SAP IQ 16.x</NAME>

<EVALUATE><CTRL><AND><OR><DP><K>custom.sapiq_query.2691389</K><OP>xre</OP
><CD>matches</CD><FV set="1">No data
found</FV><DT>5</DT><V><![CDATA[.*]]></V><DBCOL><![CDATA[]]></DBCOL></DP>
</OR></AND></CTRL></EVALUATE>
                          <RATIONALE><![CDATA[Rationale 1]]></RATIONALE>
                            <REMEDIATION><![CDATA[Remediation
1]]></REMEDIATION>
                         <DB_QUERY><![CDATA[select user_name from sysuser
where expire_password_on_login=1;]]></DB_QUERY>
                            <DESCRIPTION><![CDATA[Description
1]]></DESCRIPTION>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
...
```

Option to Scan Multiple Slices in a Single Scan

APIs affected	/api/2.0/fo/subscription/option_profile/
New or Updated API	Updated
DTD or XSD changes	Yes

With this release, we have added scan_multiple_slices_per_scanner parameter under scan performance for option profile. This will reduce scan completion time and increase the scanner capacity utilization.

To use this option, “Enable Scan Job Management Service” feature must be enabled for your subscription.

Input Parameter

The following table shows new input parameter used for listing, creating, updating, importing and exporting option profile to scan multiple slices in a single scan.

Parameter	Description
scan_multiple_slices_per_scanner={0|1}	(Optional) When unspecified or set to 0, scan using multiple slices are not used. Specify 1 to scan multiple slices in a single scan.

Sample - List Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/?
action=list&title=VM_API_Option234"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>103274</ID>
            <GROUP_NAME>
                <![CDATA[VM_API_Option234]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
...
```

```
               </BASIC_INFO>
               <SCAN>
                   <PORTS>
                       <TCP_PORTS>
                           <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                           <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
                       </TCP_PORTS>
...
                   </PORTS>
                   <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
                   <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
                   <PERFORMANCE>
                       <PARALLEL_SCALING>0</PARALLEL_SCALING>
                       <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                       <HOSTS_TO_SCAN>
                           <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                           <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                       </HOSTS_TO_SCAN>
                       <PROCESSES_TO_RUN>
                           <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                           <HTTP_PROCESSES>10</HTTP_PROCESSES>
                       </PROCESSES_TO_RUN>
                       <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                       <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                       <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                       <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>1</SCAN_MULTIPLE_SLICES_PER_SCANNER>
                   </PERFORMANCE>
                   <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
...

<IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                   </PACKET_OPTIONS>
             </ADDITIONAL>
         </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Create Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/?
action=create&title=VM_API_Opt234&scan_tcp_ports=none&scan_udp_ports=none
&authoritative_option=1&basic_information_gathering=none&vulnerability_de
tection=complete&map_overall_performance=custom&map_external_scanners=16&
map_scanner_appliances=16&scan_multiple_slices_per_scanner=1"
```

XML output:


```
<?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>2020-11-30T04:53:18Z</DATETIME>
        <TEXT>Option profile successfully added.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>103635</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```


Updated DTD:

DTD: <platform API server>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID,
SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?,
UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>
...

<!ELEMENT PERFORMANCE (PARALLEL_SCALING?, OVERALL_PERFORMANCE,
HOSTS_TO_SCAN, PROCESSES_TO_RUN, PACKET_DELAY,
PORT_SCANNING_AND_HOST_DISCOVERY, EXTERNAL_SCANNERS_TO_USE?,
HOST_CGI_CHECKS?, MAX_CGI_CHECKS?, MAX_TARGETS_PER_SLICE?,
MAX_NUMBER_OF_TARGETS?, CONF_SCAN_LIMITED_CONNECTIVITY?,
SKIP_PRE_SCANNING?, SCAN_MULTIPLE_SLICES_PER_SCANNER?)>
<!ELEMENT PARALLEL_SCALING (#PCDATA)>
```

```
<!ELEMENT OVERALL_PERFORMANCE (#PCDATA)>
<!ELEMENT HOSTS_TO_SCAN (EXTERNAL_SCANNERS, SCANNER_APPLIANCES)>
<!ELEMENT EXTERNAL_SCANNERS (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCES (#PCDATA)>
<!ELEMENT PROCESSES_TO_RUN (TOTAL_PROCESSES, HTTP_PROCESSES)>
<!ELEMENT TOTAL_PROCESSES (#PCDATA)>
<!ELEMENT HTTP_PROCESSES (#PCDATA)>
<!ELEMENT PACKET_DELAY (#PCDATA)>
<!ELEMENT PORT_SCANNING_AND_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT EXTERNAL_SCANNERS_TO_USE (#PCDATA)>
<!ELEMENT HOST_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_TARGETS_PER_SLICE (#PCDATA)>
<!ELEMENT MAX_NUMBER_OF_TARGETS (#PCDATA)>
<!ELEMENT CONF_SCAN_LIMITED_CONNECTIVITY (#PCDATA)>
<!ELEMENT SKIP_PRE_SCANNING (#PCDATA)>
<!ELEMENT SCAN_MULTIPLE_SLICES_PER_SCANNER (#PCDATA)>
<!ELEMENT LOAD_BALANCER_DETECTION (#PCDATA)>
...

<!ELEMENT PACKET_OPTIONS (IGNORE_FIREWALL_GENERATED_TCP_RST?,
IGNORE_ALL_TCP_RST?,  IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK?,
NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY?)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_ALL_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK (#PCDATA)>
<!ELEMENT NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY (#PCDATA)>
```

Sample - Update Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/?
action=update&id=103274&scan_tcp_ports=none&scan_udp_ports=none&authorita
tive_option=1&basic_information_gathering=none&vulnerability_detection=co
mplete&map_overall_performance=custom&map_external_scanners=16&map_scanne
r_appliances=16&scan_multiple_slices_per_scanner=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2020-11-30T04:56:40Z</DATETIME>
        <TEXT>Option profile successfully updated.</TEXT>
        <ITEM_LIST>
```

```
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>103635</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample - Import Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -H "content-type:
text/xml" -X POST --data-binary @datafile.xml
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=import""

Note: "datafile.xml" contains the request POST data
```

Request POST data:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>103274</ID>
            <GROUP_NAME>
                <![CDATA[VM_API_Option234]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Doe(quays_jd75)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>221243</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2020-11-09T06:11:31Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
...

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>
```

```
<SCAN_MULTIPLE_SLICES_PER_SCANNER>1</SCAN_MULTIPLE_SLICES_PER_SCANNER>
            </PERFORMANCE>
            <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
            <VULNERABILITY_DETECTION>
                <COMPLETE>
                    <![CDATA[complete]]>
                </COMPLETE>
                <DETECTION_INCLUDE>
                    <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                    <OVAL_CHECKS>0</OVAL_CHECKS>
                </DETECTION_INCLUDE>
            </VULNERABILITY_DETECTION>
            <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
        </SCAN>
...
                <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"http://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2020-11-30T06:19:27Z</DATETIME>
       <TEXT>Successfully imported Option profile for the subscription Id
221243</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>103636</KEY>
                <VALUE>
                    VM_API_OpTTion234
                </VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Export Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H 'X-Requested-With: curl'
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=export&option_profile_title=VM_API_Option234"
```

XML output:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/optio
n_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>103274</ID>
            <GROUP_NAME>
                <![CDATA[VM_API_Option234]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
                <![CDATA[John Doe (quays_jd75)]]>
            </USER_ID>
          ...
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>0</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>10</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
                <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>

<CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
                <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>1</SCAN_MULTIPLE_SLICES_PER_SCANNER>
```

```
                </PERFORMANCE>
                <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
                <VULNERABILITY_DETECTION>
                    <COMPLETE>
                        <![CDATA[complete]]>
                    </COMPLETE>
                    <DETECTION_INCLUDE>
                        <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
                        <OVAL_CHECKS>0</OVAL_CHECKS>
                    </DETECTION_INCLUDE>
                </VULNERABILITY_DETECTION>
                <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
            </SCAN>
...

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>
                <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

Posture Info API - Show/Hide Evidence in XML and CSV Formats

APIs affected	/api/2.0/fo/compliance/posture/info/
New or Updated API	Updated
DTD or XSD changes	No

Note - In the earlier version of this notification we announced that the CSV format will now include the Posture Evidence section. Now we're also giving you the option to choose whether to show or hide evidence in the output.

In previous releases, the evidence section of the Posture Info API output only appeared in XML format. Now evidence information will also appear in CSV format, making the output consistent between these formats. Like with the XML format, evidence information only appears when details=All or details=Light.

We've introduced a new input parameter in this release that will allow you to hide the evidence section when details=All or details=Light. When you specify hide_evidence=1, evidence information will not appear in the output (XML or CSV). When hide_evidence=0, evidence information will appear in the output.

Input Parameters

Refer to the Qualys API (VM,PC) User Guide for full details on all input parameters for Posture Info API. There are several additional inputs which are not listed here.

Parameter	Description
action=list	(Required)
policy_id={value}	(policy_id or policy_ids is required) Show compliance posture info records for a specified policy. A valid policy ID is required. The parameters policy_id and policy_ids cannot be specified in the same request.
policy_ids={value}	(policy_id or policy_ids is required) Show compliance posture info records for multiple policies - up to 10 policies may be requested. Provide a comma-separated list of valid policy IDs. When this parameter is specified, all posture data is downloaded (and the "truncation_limit" parameter is invalid). The parameters policy_id and policy_ids cannot be specified in the same request. When policy_ids is specified, truncation_limit is invalid. For CSV output, policy_id must be specified (and policy_ids is invalid).

Parameter	Description
output_format={value}	(Optional) The output format. A valid value is: xml (default), csv (posture data and metadata i.e. summary and warning data), csv_no_metadata (posture data only, no metadata). For CSV output, you can include only one policy. For this reason, policy_id is required.
details={Basic|All|None|Light}	(Optional) Show a certain amount of information for each compliance posture info record. A valid value is: None - show posture info and minimum exception information (assignee and status) if appropriate Basic (default) - show posture info, full exception information if appropriate, and a minimum glossary (basic info for hosts and controls) Light - show posture info, exception info if appropriate, and a limited glossary (host info and last scan date/time, control ID, and evidence info All - show posture info (including the percentage of controls that passed for each host), exception info if appropriate, posture summary (the number of assets, controls, and control instances evaluated) and a glossary (host info and last scan date/time), control info, technology info, evidence info When hide_evidence=1 is specified in the same request as details=All or details=Light, then evidence info will not be shown in the output.
hide_evidence={0|1}	(Optional when details=All or details=Light) Set to 1 to hide the evidence information in the output. When set to 0 or unspecified, evidence information is shown in the output.

API Samples

Sample 1 - Show Evidence in CSV format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&details=All&policy_id=3433470&hide_evidence=0&output_format=
csv" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
"POLICY ID","DATETIME"
"3433470","11/24/2020 13:37:33"

"ID","IP","OS","DNS Name","NetBios","Tracking Method","Control
ID","Control Statement","Criticality Label","Criticality
Value","Technology ID","Technology Name","Posture","Previous
Status","First Fail Date","Last Fail Date","First Pass Date","Last Pass
Date","Evaluation Date","Qualys Host ID","Posture Evidence"
"11062330","10.10.30.115","Windows 7 Ultimate Service Pack 1","win7-30-
115","WIN7-30-115","IP","1048","Status of the 'Shutdown: Clear virtual
memory pagefile' setting","CRITICAL","4","37","Windows
7","Passed","Passed","N/A","N/A","11/11/2020 19:32:13","11/11/2020
19:32:13","08/24/2020 17:38:18",,"This Integer value <B>X</B> indicates
the current status of the setting <B>Shutdown: Clear virtual memory
pagefile</B> using the registry key path
<B>HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session
Manager\Memory Management\ClearPageFileAtShutdown</B>.  A value of
<B>0</B> indicates the setting is <B>Disabled</B>; a value of <B>1</B>
indicates the setting is <B>Enabled</B>.

======Expected Value(s)======

Disabled (0)
------------ OR ------------
Enabled (1)
------------ OR ------------
Key not found

======Current Value(s) - Last updated: 08/24/2020 at 17:38:18 (GMT)======
Disabled (0)"
...

SUMMARY
"TOTAL ASSETS","TOTAL CONTROLS","TOTAL CONTROL INSTANCES","TOTAL PASSED
CONTROL INSTANCES","TOTAL FAILED CONTROL INSTANCES","TOTAL ERROR CONTROL
INSTANCES"
"1","6","6","6","0","0"
----END_RESPONSE_BODY_CSV
```

Sample 2 - Hide Evidence in CSV format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&details=All&policy_id=3433470&hide_evidence=1&output_format=
csv" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
"POLICY ID","DATETIME"
"3433470","11/24/2020 13:38:35"

"ID","IP","OS","DNS Name","NetBios","Tracking Method","Control
ID","Control Statement","Criticality Label","Criticality
Value","Technology ID","Technology Name","Posture","Previous
Status","First Fail Date","Last Fail Date","First Pass Date","Last Pass
Date","Evaluation Date","Qualys Host ID"
"11062330","10.10.30.115","Windows 7 Ultimate Service Pack 1","win7-30-
115","WIN7-30-115","IP","1048","Status of the 'Shutdown: Clear virtual
memory pagefile' setting","CRITICAL","4","37","Windows
7","Passed","Passed","N/A","N/A","11/11/2020 19:32:13","11/11/2020
19:32:13","08/24/2020 17:38:18",
...

SUMMARY
"TOTAL ASSETS","TOTAL CONTROLS","TOTAL CONTROL INSTANCES","TOTAL PASSED
CONTROL INSTANCES","TOTAL FAILED CONTROL INSTANCES","TOTAL ERROR CONTROL
INSTANCES"
"1","6","6","6","0","0"
----END_RESPONSE_BODY_CSV
```

Sample 3 - Show Evidence in XML format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&details=All&policy_id=3433470&hide_evidence=0&output_format=
xml" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-11-24T13:40:02Z</DATETIME>
<!-- keep-alive for POSTURE_INFO_LIST_OUTPUT  -->
```

```
    <INFO_LIST>
      <INFO>
        <ID>11062330</ID>
        <HOST_ID>140608</HOST_ID>
        <CONTROL_ID>1048</CONTROL_ID>
        <TECHNOLOGY_ID>37</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
11T19:32:13Z</POSTURE_MODIFIED_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-11T19:32:13Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2020-11-11T19:32:13Z</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[(:dp_1 in #fv_1 )]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2020-08-24T17:38:18Z">
              <LABEL>:dp_1</LABEL>
              <V><![CDATA[0]]></V>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
...
```

Sample 4 - Hide Evidence in XML format

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&details=All&policy_id=3433470&hide_evidence=1&output_format=
csv" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
<!DOCTYPE POSTURE_INFO_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/posture_
info_list_output.dtd">
<POSTURE_INFO_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-11-24T13:40:54Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>11062330</ID>
        <HOST_ID>140608</HOST_ID>
        <CONTROL_ID>1048</CONTROL_ID>
        <TECHNOLOGY_ID>37</TECHNOLOGY_ID>
```

```
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2020-11-
11T19:32:13Z</POSTURE_MODIFIED_DATE>
        <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>N/A</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>N/A</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>2020-11-11T19:32:13Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2020-11-11T19:32:13Z</LAST_PASS_DATE>
      </INFO>
...
```

Addition of Host ID to Compliance Reports

APIs affected	/api/2.0/fo/report/"
New or Updated API	Updated
DTD or XSD changes	Yes

Now the Host ID information will be added to the Authentication Report, Policy Report, and Scorecard Reports in these formats (HTML, HTML New, PDF, XML, CSV). The Host ID only appears in the Authentication Report when it's selected by the user.

Refer to More Details in Authentication Reports: Host ID and All Asset Tags

API Sample - Authentication Report in CSV

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3239483&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:

```
...
SUMMARY
Asset Groups,Passed Authentications,Insufficient Authentications,Failed
Authentications,Not Attempted Authentications,Not Installed
Authentication,Total Authentications,Passed Percentage,Failed
Percentage,Not Attempted Percentage
"CRM AG","0",,"0","0",,"0","0","0","0"
"AG","1","0","0","0","0","1","100","0","0"
"CRM AG -1","1","0","0","0","0","1","100","0","0"
"JBOSS AG","1","0","0","0","0","1","100","0","0"
"IP_RANGE","1","0","0","0","0","1","100","0","0"
"MAC15-AG2","0",,"0","0",,"0","0","0","0"
"MAC 14-AG","2","0","0","0","0","2","100","0","0"
"Amol WIN AG","0","0","2","0","0","2","0","100","0"
"ARR","0","0","2","0","0","2","0","100","0"
RESULTS
Asset Groups,Technology,Host Technology,Instance,Host IP,DNS
Hostname,NetBIOS Hostname,Tracking Method,Network,Status,Failure
Reason,Host Id
"AG","Fabric","Brocade Fabric
8.x",,"10.10.99.99","fab","FABNETB","OCA","Global Default
Network","Passed","'-","2505976"
"CRM AG -1","Unix/Cisco/Checkpoint Firewall","CentOS
6.x",,"10.10.32.14",,,"IP","Global Default Network","Passed","'-
","2788183"
```

```
"JBOSS AG","Juniper","Juniper IVE
8.x",,"10.10.10.12","host_name","NB","OCA","Global Default
Network","Passed","'-","3076407"
"IP_RANGE","Juniper","Juniper IVE
8.x",,"10.10.10.12","host_name","NB","OCA","Global Default
Network","Passed","'-","3076407"
"MAC 14-AG","Unix/Cisco/Checkpoint Firewall","Mac OS X
10.15",,"10.11.75.219",,,"IP","Global Default Network","Passed","'-
","3515919"
"MAC 14-AG","Unix/Cisco/Checkpoint Firewall","Mac OS X
10.14",,"10.11.75.222",,,"IP","Global Default Network","Passed","'-
","3515902"
...
```

API Sample - Authentication Report in XML

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3240477&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_AUTHENTICATION_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_authentication_report.dtd">
<!-- This report was generated with an evaluation version of Qualys //-->
<COMPLIANCE_AUTHENTICATION_REPORT>
  <HEADER>
    <NAME><![CDATA[Authentication Report XML]]></NAME>
    ...
        <ASSET_GROUP>
          <NAME><![CDATA[ARR]]></NAME>
        </ASSET_GROUP>
      </ASSET_GROUP_LIST>
    </FILTERS>
  </HEADER>
  <ASSET_GROUP_LIST>
    <ASSET_GROUP>
      <NAME><![CDATA[CRM AG]]></NAME>
      <AUTH_PASSED>0</AUTH_PASSED>
      <AUTH_INSUFFICIENT></AUTH_INSUFFICIENT>
      <AUTH_FAILED>0</AUTH_FAILED>
      <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
      <AUTH_NOT_INSTALLED></AUTH_NOT_INSTALLED>
      <AUTH_TOTAL>0</AUTH_TOTAL>
      <PASSED_PERCENTAGE>0</PASSED_PERCENTAGE>
      <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
```

```
        <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
        <TECHNOLOGY_LIST />
      </ASSET_GROUP>
      <ASSET_GROUP>
        <NAME><![CDATA[AG]]></NAME>
        <AUTH_PASSED>1</AUTH_PASSED>
        <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
        <AUTH_FAILED>0</AUTH_FAILED>
        <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
        <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
        <AUTH_TOTAL>1</AUTH_TOTAL>
        <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
        <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
        <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <NAME><![CDATA[Fabric]]></NAME>
            <HOST_LIST>
              <HOST>
                <TRACKING_METHOD><![CDATA[OCA]]></TRACKING_METHOD>
                <IP><![CDATA[10.10.99.99]]></IP>
                <DNS><![CDATA[fab]]></DNS>
                <NETBIOS><![CDATA[FABNETB]]></NETBIOS>
                <HOST_TECHNOLOGY><![CDATA[Brocade Fabric
8.x]]></HOST_TECHNOLOGY>
                <STATUS><![CDATA[Passed]]></STATUS>
                <NETWORK><![CDATA[Global Default Network]]></NETWORK>
                <HOST_ID><![CDATA[2505976]]></HOST_ID>
              </HOST>
            </HOST_LIST>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </ASSET_GROUP>
      <ASSET_GROUP>
        <NAME><![CDATA[CRM AG -1]]></NAME>
        <AUTH_PASSED>1</AUTH_PASSED>
        <AUTH_INSUFFICIENT>0</AUTH_INSUFFICIENT>
        <AUTH_FAILED>0</AUTH_FAILED>
        <AUTH_NOT_ATTEMPTED>0</AUTH_NOT_ATTEMPTED>
        <AUTH_NOT_INSTALLED>0</AUTH_NOT_INSTALLED>
        <AUTH_TOTAL>1</AUTH_TOTAL>
        <PASSED_PERCENTAGE>100</PASSED_PERCENTAGE>
        <FAILED_PERCENTAGE>0</FAILED_PERCENTAGE>
        <NOT_ATTEMPTED_PERCENTAGE>0</NOT_ATTEMPTED_PERCENTAGE>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <NAME><![CDATA[Unix/Cisco/Checkpoint Firewall]]></NAME>
            <HOST_LIST>
              <HOST>
```

```
                <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
                <IP><![CDATA[10.10.32.14]]></IP>
                <DNS><![CDATA[]]></DNS>
                <NETBIOS><![CDATA[]]></NETBIOS>
                <HOST_TECHNOLOGY><![CDATA[CentOS 6.x]]></HOST_TECHNOLOGY>
                <STATUS><![CDATA[Passed]]></STATUS>
                <NETWORK><![CDATA[Global Default Network]]></NETWORK>
                <HOST_ID><![CDATA[2788183]]></HOST_ID>
              </HOST>
            </HOST_LIST>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </ASSET_GROUP>
      ...
  </COMPLIANCE_AUTHENTICATION_REPORT>
  <!-- This report was generated with an evaluation version of Qualys //-->
  <!-- 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 2020, Qualys, Inc. //-->
```

DTD Update: Authentication Report

<base_url>/compliance_authentication_report.dtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE AUTHENTICATION REPORT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_AUTHENTICATION_REPORT (ERROR | (HEADER,
(BUSINESS_UNIT_LIST | ASSET_GROUP_LIST | ASSET_TAG_LIST | IPS_LIST),
APPENDIX?))>
...
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, IP, DNS?, NETBIOS?, HOST_TECHNOLOGY?,
INSTANCE?, STATUS, CAUSE?, NETWORK?, OS?, LAST_AUTH?, LAST_SUCCESS?,
HOST_ID?,ALL_ASSET_TAGS?)>

...
<!ELEMENT LAST_SUCCESS (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
...
```

API Sample - Policy Report in CSV

<u>API request:</u>

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3240496&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

<u>Response:</u>


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_policy_report.dtd">
<COMPLIANCE_POLICY_REPORT>
  <HEADER>
    <NAME><![CDATA[Policy Report XML]]></NAME>
    ...
    <FILTERS>
      <POLICY><![CDATA[Policy AR - 1]]></POLICY>
      <POLICY_LOCKING><![CDATA[Unlocked]]></POLICY_LOCKING>
      <IPS>
        <IP_LIST>
          <IP><![CDATA[10.10.36.111]]></IP>
          <IP><![CDATA[10.10.36.122]]></IP>
        </IP_LIST>
        <NEWWORK><![CDATA[All]]></NEWWORK>
      </IPS>
      <PC_AGENT_IPS><![CDATA[No]]></PC_AGENT_IPS>
      <POLICY_LAST_EVALUATED><![CDATA[11/10/2020 at 16:15:46
(GMT+0530)]]></POLICY_LAST_EVALUATED>
    </FILTERS>
  </HEADER>
  <SUMMARY>
    <TOTAL_ASSETS>2</TOTAL_ASSETS>
    <TOTAL_CONTROLS>10</TOTAL_CONTROLS>
    <CONTROL_INSTANCES>
      <TOTAL>11</TOTAL>
      <TOTAL_PASSED>10</TOTAL_PASSED>
      <TOTAL_FAILED>1</TOTAL_FAILED>
      <TOTAL_ERROR>0</TOTAL_ERROR>
      <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
    </CONTROL_INSTANCES>
    <HOST_STATISTICS>
      <HOST_INFO>
        <IP><![CDATA[10.10.36.111]]></IP>
        <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
        <DNS><![CDATA[-]]></DNS>
        <NETBIOS><![CDATA[DB2V105WIN2K8R2]]></NETBIOS>
        <OPERATING_SYSTEM><![CDATA[Windows Server 2008 R2 Enterprise 64
bit Edition]]></OPERATING_SYSTEM>
```

```
        <LAST_SCAN_DATE><![CDATA[2020-06-17T15:30:05Z]]></LAST_SCAN_DATE>
        <PERCENTAGE>83.33% (5 of 6)</PERCENTAGE>
        <NETWORK>Global Default Network</NETWORK>
        <Host ID><![CDATA[2788189]]></Host ID>
      </HOST_INFO>
      <HOST_INFO>
        <IP><![CDATA[10.10.36.122]]></IP>
        <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
        <DNS><![CDATA[-]]></DNS>
        <NETBIOS><![CDATA[-]]></NETBIOS>
        <OPERATING_SYSTEM><![CDATA[Oracle Enterprise Linux
7.0]]></OPERATING_SYSTEM>
        <LAST_SCAN_DATE><![CDATA[2020-06-17T09:43:24Z]]></LAST_SCAN_DATE>
        <PERCENTAGE>100% (5 of 5)</PERCENTAGE>
        <NETWORK>Global Default Network</NETWORK>
        <Host ID><![CDATA[2431364]]></Host ID>
      </HOST_INFO>
    </HOST_STATISTICS>
  </SUMMARY>
  ...
</COMPLIANCE_POLICY_REPORT>
```


API Sample - Policy Report in XML

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3241486&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:


```
<!DOCTYPE COMPLIANCE_POLICY_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_policy_report.dtd">
<COMPLIANCE_POLICY_REPORT>
  <HEADER>
    <NAME><![CDATA[Policy Report XML - SI]]></NAME>
    <GENERATION_DATETIME>2020-11-11T07:44:16Z</GENERATION_DATETIME>
      ...
     <INSTANCE><![CDATA[os]]></INSTANCE>
      </HOST_INSTANCE>
      <PC_AGENT_IPS><![CDATA[No]]></PC_AGENT_IPS>
      <POLICY_LAST_EVALUATED><![CDATA[11/10/2020 at 16:15:46
(GMT+0530)]]></POLICY_LAST_EVALUATED>
    </FILTERS>
  </HEADER>
  <SUMMARY>
    <TOTAL_ASSETS>1</TOTAL_ASSETS>
    <TOTAL_CONTROLS>10</TOTAL_CONTROLS>
```

```
      <CONTROL_INSTANCES>
        <TOTAL>7</TOTAL>
        <TOTAL_PASSED>7</TOTAL_PASSED>
        <TOTAL_FAILED>0</TOTAL_FAILED>
        <TOTAL_ERROR>0</TOTAL_ERROR>
        <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
      </CONTROL_INSTANCES>
      <HOST_STATISTICS>
        <HOST_INFO>
          <IP><![CDATA[10.10.32.14]]></IP>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <DNS><![CDATA[-]]></DNS>
          <NETBIOS><![CDATA[-]]></NETBIOS>
          <OPERATING_SYSTEM><![CDATA[CentOS Linux 6.0]]></OPERATING_SYSTEM>
          <LAST_SCAN_DATE><![CDATA[2020-06-23T05:52:16Z]]></LAST_SCAN_DATE>
          <PERCENTAGE>100% (7 of 7)</PERCENTAGE>
          <NETWORK>Global Default Network</NETWORK>
          <Host ID><![CDATA[2788183]]></Host ID>
        </HOST_INFO>
      </HOST_STATISTICS>
    </SUMMARY>
   ...
```

DTD Update: Policy Report

<base_url>/compliance_policy_report.dtd

```
...
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE POLICY REPORT DTD -->
<!-- $Revision$ -->
<!ELEMENT COMPLIANCE_POLICY_REPORT (ERROR | (HEADER, (SUMMARY),
(RESULTS)))>
...
<!ELEMENT RESULTS ( HOST_LIST, CHECKS?, DP_DESCRIPTIONS?) >
<!ELEMENT HOST_LIST (HOST*)>
<!ELEMENT HOST (TRACKING_METHOD, QG_HOSTID?, IP, DNS?, NETBIOS?,
OPERATING_SYSTEM?, OS_CPE?, LAST_SCAN_DATE?,TOTAL_PASSED, TOTAL_FAILED,
TOTAL_ERROR, TOTAL_EXCEPTIONS, ASSET_TAGS?, CONTROL_LIST, NETWORK?,
HOST_ID?)>
...
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
...
```

API Sample - Scorecard Report in CSV

<u>API request:</u>

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3216464&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

<u>Response:</u>

```
"SCR Tags - CSV","11/10/2020 at 18:38:19
(GMT+0530)","DATETIME_RPTDATECSV_GMT2USER"
ABOUT REPORT
Report Type,Created,User Name,Login Name,User
Role,Company,Address1,Address2,City,State,Zip,Country
"Compliance Scorecard Report","11/10/2020 at 18:38:19
...
REPORT DISCOVERIES
Overall Compliance,Unique Policies,Passed,%,Failed,%,Error,%
"95%","2","142","95","8","5","0","0"
Total Controls Detected,Changed Controls,Passed,%,Failed,%,Error,%
"150","36","34","94","2","6","0","0"
Total Hosts in Policies,Scanned Hosts,Unique Hosts Changed,%
"3","0","3","0"
Total Technologies,Technologies with Hosts Change
"6","3"
Technology,Count,%
"Oracle Enterprise Linux 7.x","1","33"
"CentOS 6.x","1","33"
"Windows 2008 Server","1","33"
Compliance by Policy
By Policy
Policy,Control Instances,Hosts Total,Hosts Scanned,Hosts Changed,Passed
Total,Passed Changed,Failed Total,Failed Changed,Error Total,Error
Changed,Compliance
"Policy REG","114","1","0","0","108","0","6","0","0","0","94.74%"
"Policy AR - 1","36","3","0","3","34","34","2","2","0","0","94.44%"
...
IP Address,Traking,NetBios,DNS,Network,Asset Tag,Technology,# of
Policies,Pass Total,Pass Changed,Compliance,Host ID
"10.20.32.200","IP",,,"Global Default Network","UNIX_NAG","Oracle
Enterprise Linux 7.x","1","5","5","100%","2704645"
"10.20.32.200","IP",,,"Global Default Network","UNIXREG","Oracle
Enterprise Linux 7.x","1","5","5","100%","2704645"
"10.10.32.14","IP",,,"Global Default Network","UNIXREG","CentOS
6.x","1","7","7","100%","2788183"
...
```

API Sample - Scorecard Report in XML

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=fetch&id=3215493&echo_request=1"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

Response:


```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCORECARD_REPORT SYSTEM
"https://qualysapi.qualys.com/compliance_scorecard_report.dtd">
<COMPLIANCE_SCORECARD_REPORT>
  <HEADER>
    <REPORT_TYPE><![CDATA[SCR Tags - XML]]></REPORT_TYPE>
    <GENERATION_DATETIME>2020-11-10T13:06:47Z</GENERATION_DATETIME>
  </HEADER>
  ...
  <TOP_HOST_WITH_CHANGES>
      <TOP><![CDATA[10]]></TOP>
      <CHANGED_TO_PASS>
        <HOST>
          <IP_ADDRESS><![CDATA[10.20.32.200]]></IP_ADDRESS>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <NETBIOS><![CDATA[ ]]></NETBIOS>
          <DNS><![CDATA[ ]]></DNS>
          <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          <ASSET_TAG_NAME><![CDATA[]]></ASSET_TAG_NAME>
          <TECHNOLOGY>Oracle Enterprise Linux 7.x</TECHNOLOGY>
          <NUMBER_OF_POLICIES>1</NUMBER_OF_POLICIES>
          <PASSED_TOTAL>5</PASSED_TOTAL>
          <PASSED_CHANGED>5</PASSED_CHANGED>
          <COMPLIANCE>100%</COMPLIANCE>
          <HOST_ID>2704645</HOST_ID>
        </HOST>
        <HOST>
          <IP_ADDRESS><![CDATA[10.20.32.200]]></IP_ADDRESS>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <NETBIOS><![CDATA[ ]]></NETBIOS>
          <DNS><![CDATA[ ]]></DNS>
          <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          <ASSET_TAG_NAME><![CDATA[]]></ASSET_TAG_NAME>
          <TECHNOLOGY>Oracle Enterprise Linux 7.x</TECHNOLOGY>
          <NUMBER_OF_POLICIES>1</NUMBER_OF_POLICIES>
          <PASSED_TOTAL>5</PASSED_TOTAL>
          <PASSED_CHANGED>5</PASSED_CHANGED>
          <COMPLIANCE>100%</COMPLIANCE>
          <HOST_ID>2704645</HOST_ID>
        </HOST>
```

```
        <HOST>
          <IP_ADDRESS><![CDATA[10.10.32.14]]></IP_ADDRESS>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <NETBIOS><![CDATA[ ]]></NETBIOS>
          <DNS><![CDATA[ ]]></DNS>
          <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          <ASSET_TAG_NAME><![CDATA[]]></ASSET_TAG_NAME>
          <TECHNOLOGY>CentOS 6.x</TECHNOLOGY>
          <NUMBER_OF_POLICIES>1</NUMBER_OF_POLICIES>
          <PASSED_TOTAL>7</PASSED_TOTAL>
          <PASSED_CHANGED>7</PASSED_CHANGED>
          <COMPLIANCE>100%</COMPLIANCE>
          <HOST_ID>2788183</HOST_ID>
        </HOST>
        <HOST>
          <IP_ADDRESS><![CDATA[10.10.32.14]]></IP_ADDRESS>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <NETBIOS><![CDATA[ ]]></NETBIOS>
          <DNS><![CDATA[ ]]></DNS>
          <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          <ASSET_TAG_NAME><![CDATA[]]></ASSET_TAG_NAME>
          <TECHNOLOGY>CentOS 6.x</TECHNOLOGY>
          <NUMBER_OF_POLICIES>1</NUMBER_OF_POLICIES>
          <PASSED_TOTAL>7</PASSED_TOTAL>
          <PASSED_CHANGED>7</PASSED_CHANGED>
          <COMPLIANCE>100%</COMPLIANCE>
          <HOST_ID>2788183</HOST_ID>
        </HOST>
        <HOST>
          <IP_ADDRESS><![CDATA[10.10.36.111]]></IP_ADDRESS>
          <TRACKING_METHOD><![CDATA[IP]]></TRACKING_METHOD>
          <NETBIOS><![CDATA[DB2V105WIN2K8R2]]></NETBIOS>
          <DNS><![CDATA[ ]]></DNS>
          <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          <ASSET_TAG_NAME><![CDATA[]]></ASSET_TAG_NAME>
          <TECHNOLOGY>Windows 2008 Server</TECHNOLOGY>
          <NUMBER_OF_POLICIES>2</NUMBER_OF_POLICIES>
          <PASSED_TOTAL>59</PASSED_TOTAL>
          <PASSED_CHANGED>5</PASSED_CHANGED>
          <COMPLIANCE>8.47%</COMPLIANCE>
          <HOST_ID>2788189</HOST_ID>
        </HOST>
        ...
</COMPLIANCE_SCORECARD_REPORT>
```

DTD Update: Scorecard Report

<base_url>/compliance_scorecard_report.dtd

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- QUALYS COMPLIANCE SCORECARD REPORT DTD -->
<!-- $Revision$ -->

<!ELEMENT COMPLIANCE_SCORECARD_REPORT (ERROR | (HEADER, (SUMMARY),
(DETAILS)))>
...
<!ELEMENT CHANGED_TO_ERROR (HOST*|CONTROL*|CRITICALITY*)>
<!ELEMENT HOST (IP_ADDRESS, TRACKING_METHOD, NETBIOS, DNS, NETWORK?,
ASSET_GROUP_NAME?, ASSET_TAG_NAME?, TECHNOLOGY, NUMBER_OF_POLICIES,
PASSED_TOTAL?, PASSED_CHANGED?, FAILED_TOTAL?, FAILED_CHANGED?,
ERROR_TOTAL?, ERROR_CHANGED?, COMPLIANCE, NETWORK?, HOST_ID?)>

...
<!ELEMENT NETWORK (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
...
```

Update to ImportableControl.xsd Schema

APIs affected	N/A (import/export from UI only)
New or Updated API	Updated (XSD change only)
DTD or XSD changes	Yes

The ImportableControl.xsd schema is used when you import and export user defined controls in XML format. In this schema, we increased the maximum length for database UDC SQL statements from 4000 to 32000 characters. This increase will allow for more complex queries in your database UDCs.

ImportableControl.xsd Schema Update

The maxLength value for database query string is now 32000 for DB_QUERY element.

```
...

<xs:element name="DB_QUERY">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="32000"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>

...
```