Qualys Cloud Platform (VM, PC) v8.x

API Release Notes

Version 8.21.6

November 11, 2019

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.

New Oracle HTTP Server Authentication API

APIs affected	/api/2.0/fo/auth/
New or Updated API	No
DTD or XSD changes	Yes
APIs affected	/api/2.0/fo/auth/oracle_http_server/
New or Updated API	New
DTD or XSD changes	Yes

Oracle HTTP Server authentication is now supported for compliance scans on Unix and Windows. The new Oracle HTTP Server Authentication API (api/2.0/fo/auth/oracle_http_server/) lets you list, create, update and delete Oracle HTTP Server authentication records. User permissions for this API are the same as other authentication record APIs. Note that the API supports authentication record creation only for Oracle Server installed on respective OS - Unix or Windows.

List all record types

Use the Authentication Record List API (/api/2.0/fo/auth/?action=list) to list records. You'll see <AUTH_ORACLE_HTTP_SERVER_IDS> in the output when you have Oracle HTTP Server records.

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -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>2019-10-04T09:24:19Z</DATETIME>
    <AUTH_RECORDS>
      <AUTH_UNIX_IDS>
        <ID_SET>
          <ID>206814</ID>
          <ID>353344</ID>
          <ID>936404</ID>
          <ID>1029116</ID>
          <ID>1296290</ID>
          <ID_RANGE>1375563-1375564</ID_RANGE>
          <ID>1505926</ID>
```

```
    </ID_SET>
  </AUTH_UNIX_IDS>
  <AUTH_WINDOWS_IDS>
    <ID_SET>
      <ID>201126</ID>
      <ID>217839</ID>
      <ID>218380</ID>
      <ID>259637</ID>
      <ID>277036</ID>
      <ID>286279</ID>
      <ID>306712</ID>
      <ID>835880</ID>
      <ID>936378</ID>
      <ID>947905</ID>
      <ID>986499</ID>
      <ID>1172435</ID>
      <ID>1505928</ID>
    </ID_SET>
  </AUTH_WINDOWS_IDS>
  <AUTH_MS_SQL_IDS>
    <ID_SET>
      <ID>997503</ID>
    </ID_SET>
  </AUTH_MS_SQL_IDS>
  <AUTH_VMWARE_IDS>
    <ID_SET>
      <ID>1350949</ID>
    </ID_SET>
  </AUTH_VMWARE_IDS>
  <AUTH_APACHE_IDS>
    <ID_SET>
      <ID>353346</ID>
      <ID_RANGE>353966-353967</ID_RANGE>
    </ID_SET>
  </AUTH_APACHE_IDS>
  <AUTH_POSTGRESQL_IDS>
    <ID_SET>
      <ID>1029117</ID>
      <ID>1296291</ID>
    </ID_SET>
  </AUTH_POSTGRESQL_IDS>
  <AUTH_PALO_ALTO_FIREWALL_IDS>
    <ID_SET>
      <ID>237951</ID>
      <ID>1446355</ID>
    </ID_SET>
  </AUTH_PALO_ALTO_FIREWALL_IDS>
  <AUTH_VCENTER_IDS>
    <ID_SET>
```

```
            <ID_RANGE>1351032-1351033</ID_RANGE>
          </ID_SET>
        </AUTH_VCENTER_IDS>
        <AUTH_JBOSS_IDS>
          <ID_SET>
            <ID>302585</ID>
          </ID_SET>
        </AUTH_JBOSS_IDS>
        <AUTH_ORACLE_HTTP_SERVER_IDS>
          <ID_SET>
            <ID>1505929</ID>
          </ID_SET>
        </AUTH_ORACLE_HTTP_SERVER_IDS>
      </AUTH_RECORDS>
    </RESPONSE>
</AUTH_RECORDS_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

Updated DTD

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

The element AUTH_ORACLE_HTTP_SERVER_IDS is added to identify Oracle HTTP Server 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?)>
<!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?)>
...
<!ELEMENT AUTH_INFORMIXDB_IDS (ID_SET)>
<!ELEMENT AUTH_MS_EXCHANGE_IDS (ID_SET)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_IDS (ID_SET)>
 ...
```

List Oracle HTTP Sever records

Use these parameters to list Oracle HTTP Server Authentication records.

Parameter	Description
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).
details={value}	(Optional) Default value is Basic. You can choose from None, Basic, and All.

Sample - List Oracle HTTP Server Records with Basic Details

API request:

```
curl -S -H 'X-Requested-With:curl demo2' -u "USERNAME:PASSWORD" -d
"action=list&details=Basic&ids=1505927"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/auth_ora
cle_http_server_list_output.dtd">
<AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-10-04T07:28:22Z</DATETIME>
```

```
    <AUTH_ORACLE_HTTP_SERVER_LIST>
      <AUTH_ORACLE_HTTP_SERVER>
        <ID>1505927</ID>
        <TITLE><![CDATA[Oracle_HTTP_Unix server]]></TITLE>
        <IP_SET>
          <IP>10.11.70.24</IP>
        </IP_SET>

        <UNIX>

<HOME_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1]]></HOME_PATH>
          <DOMAIN_PATH><![CDATA[]]></DOMAIN_PATH>

<INST_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1/instances/instance1
]]></INST_PATH>
          <INST_NAME><![CDATA[ohs1]]></INST_NAME>
        </UNIX>
        <CREATED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
          <BY> john_doe</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_ORACLE_HTTP_SERVER>
    </AUTH_ORACLE_HTTP_SERVER_LIST>
  </RESPONSE>
</AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

Sample - List Oracle HTTP Server Records with All Details

API request:

```
curl -S -H 'X-Requested-With:curl demo2' -u "USERNAME:PASSWORD" -d
"action=list&details=All&ids=1505927"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/auth_ora
cle_http_server_list_output.dtd">
<AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
  <RESPONSE>
```

```
    <DATETIME>2019-10-04T07:29:33Z</DATETIME>
    <AUTH_ORACLE_HTTP_SERVER_LIST>
      <AUTH_ORACLE_HTTP_SERVER>
        <ID>1505927</ID>
        <TITLE><![CDATA[Oracle_HTTP_Unix server]]></TITLE>
        <IP_SET>
          <IP>10.11.70.24</IP>
        </IP_SET>

        <UNIX>

<HOME_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1]]></HOME_PATH>
          <DOMAIN_PATH><![CDATA[]]></DOMAIN_PATH>

<INST_PATH><![CDATA[/opt/Oracle/Middleware/Oracle_WT1/instances/instance1
]]></INST_PATH>
          <INST_NAME><![CDATA[ohs1]]></INST_NAME>
        </UNIX>
        <CREATED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
          <BY> john_doe</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-03T12:24:04Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_ORACLE_HTTP_SERVER>
    </AUTH_ORACLE_HTTP_SERVER_LIST>
    <GLOSSARY>
      <USER_LIST>
        <USER>
          <USER_LOGIN> john_doe</USER_LOGIN>
          <FIRST_NAME>John</FIRST_NAME>
          <LAST_NAME>Doe</LAST_NAME>
        </USER>
      </USER_LIST>
    </GLOSSARY>
  </RESPONSE>
</AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

New DTD

<base_url>/api/2.0/fo/auth/oracle_http_server/auth_oracle_http_server_list_output.dtd

```
<!-- QUALYS AUTH_ORACLE_HTTP_SERVER_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_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_ORACLE_HTTP_SERVER_LIST|ID_SET)?,
WARNING_LIST?, GLOSSARY?)>
<!ELEMENT AUTH_ORACLE_HTTP_SERVER_LIST (AUTH_ORACLE_HTTP_SERVER+)>

<!ELEMENT AUTH_ORACLE_HTTP_SERVER (ID, TITLE, IP_SET, WINDOWS?, UNIX?,
NETWORK_ID?, CREATED, LAST_MODIFIED, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
...
```

Create/Update Oracle HTTP Server Authentication Records

Use these parameters to create or update Oracle HTTP Server Authentication record.

Parameter	Description
title={value}	(Required to create record) A title for the record. The title must be unique. Maximum 255 characters (ascii).
network_id={value}	(Optional and valid when the networks feature is enabled) The network ID for the record.
add_ips={value}	(Optional to update record) Add IPs to the IPs list for this record. Multiple IPs/ranges are comma separated.
comments={value}	(Optional to create or update record) User defined comments. Maximum of 1999 characters.
action={action}	(Required) Specify create, update, delete (using POST) or list (using GET or POST).

Parameter	Description
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.
ids={value}	(Required to update record) Record Oracle HTTP type auth record IDs to update. Specify record IDs and/or ID ranges (for example, 1359-1407). Multiple entries are comma separated.
Unix Configuration	
unix_home_path={value}	(Required to create or update record if Unix working mode is selected) The root directory path for Oracle HTTP Server. Maximum of 255 characters.
unix_domain_path={value}	(Required to create or update record if Unix working mode is selected for Oracle HTTP Server 12c and higher) Absolute path to the top level directory where domains are configured. Maximum of 255 characters.
unix_inst_path={value}	(Required to create or update record if Unix working mode is selected for Oracle HTTP Server 11g) Absolute path to the top level directory where instances are configured. Maximum of 255 characters.
unix_inst_name={value}	(Optional) The Oracle HTTP server instance name. Maximum of 4000 characters.
Windows Configuration	
windows_home_path={value}	(Required to create or update record if Windows working mode is selected) The home directory path. Maximum of 255 characters.
windows_domain_path={value}	(Required to create or update record if Windows working mode is selected for Oracle HTTP Server 12c and higher) Absolute path to the top level directory where domains are configured. Maximum of 255 characters.
windows_inst_path={value}	(Required to create or update record if Windows working mode is selected for Oracle HTTP Server 11g) Absolute path to the top level directory where instances are configured. Maximum of 255 characters.
windows_inst_name={value}	(Optional) The Oracle HTTP server instance name. Maximum of 4000 characters.

Sample - Create Oracle HTTP Server 11g Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Unix
server_11&unix_home_path=/opt/Oracle/Middleware/Oracle_WT1&unix_inst_path
=/opt/Oracle/Middleware/Oracle_WT1/instances/instance1&unix_inst_name=ohs
1&ips=10.11.70.24"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T05:51:21Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530246</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 11g Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Windows_server_11&windows_home_path=C:\M
iddleware\Oracle_WT1&windows_inst_path=C:\Middleware\Oracle_WT1\instances
\instance1&windows_inst_name=ohs1&ips=10.11.70.193"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T05:50:01Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
```

```
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530243</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 12c Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Unix
server_12&unix_home_path=/opt/Oracle/Middleware/Oracle_Home&unix_domain_p
ath=/opt/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain&
windows_inst_name=ohs1&ips=10.11.70.68"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T05:45:50Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530234</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Create Oracle HTTP Server 12c Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=create&title=Oracle_HTTP_Windows
server_12&windows_home_path=C:\Oracle\Middleware\Oracle_Home&windows_doma
in_path=C:\Oracle\Middleware\Oracle_Home\user_projects\domains\base_domai
n&windows_inst_path=C:\Oracle\Middleware\Oracle_Home\instances\instance1&
windows_inst_name=ohs1&ips=10.11.70.84"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T05:48:55Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>1530241</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 11g Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530246&unix_home_path=/opt/Oracle/Middleware/Oracle_W
T1&unix_inst_path=/opt/Oracle/Middleware/Oracle_WT1/instances/instance1&u
nix_inst_name=ohs1&ips=10.11.70.24&comments=ohs unix auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T06:01:38Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
```

```
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530246</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 11g Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530243&windows_home_path=C:\Middleware\Oracle_WT1&win
dows_inst_path=C:\Middleware\Oracle_WT1\instances\instance1&windows_inst_
name=ohs1&ips=10.11.70.193&comments=ohs wind auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T06:05:43Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530243</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 12c Record(s) on Unix

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530234&unix_home_path=/opt/Oracle/Middleware/Oracle_H
ome&unix_domain_path=/opt/Oracle/Middleware/Oracle_Home/user_projects/dom
ains/base_domain&windows_inst_name=ohs1&ips=10.11.70.68&comments=ohs unix
auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T06:14:31Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530234</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update Oracle HTTP Server 12c Record(s) on Windows

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=update&ids=1530241&windows_home_path=C:\Oracle\Middleware\Oracle_
Home&windows_domain_path=C:\Oracle\Middleware\Oracle_Home\user_projects\d
omains\base_domain&windows_inst_path=C:\Oracle\Middleware\Oracle_Home\ins
tances\instance1&windows_inst_name=ohs1&ips=10.11.70.84&comments=ohs wind
auth record updated"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-15T06:11:46Z</DATETIME>
```

```
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>1530241</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Delete Oracle HTTP Server Records

Use following parameter to delete Oracle HTTP Server Authentication record(s).

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

Sample - Delete Oracle HTTP Server Record(s)

API request:

```
curl -u "USERNAME:PASSWORD" -S -H 'X-Requested-With:curl demo2' -d
"action=delete&ids=1507609"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle_http_server/"
```

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>2019-10-04T09:19:50Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Deleted</TEXT>
        <ID_SET>
          <ID>1507609</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Support for File Content Check on Windows

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
New or Updated API	Updated
DTD or XSD changes	Yes

With this release you can now configure a File Content Check control to check the contents of a Windows file. Tell us which file you want to evaluate and what you're looking for. We'll return all lines in the file that match. You can specify your file location using any of the path types: Registry Key, File Search, File Path

Sample - Control API

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=list&echo_request=1&ids=100006,100000,100026&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/">
control_list.xml
```

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>
  <REQUEST>
    <DATETIME>2019-10-14T21:17:21Z</DATETIME>
    <USER_LOGIN>username</USER_LOGIN>
<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/control/</RE
SOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>list</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>ids</KEY>
        <VALUE>100006,100000,100026</VALUE>
      </PARAM>
```

```
<PARAM>
        <KEY>details</KEY>
        <VALUE>All</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2019-10-14T21:17:21Z</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <ID>100000</ID>
        <UPDATE_DATE>2019-10-10T21:54:35Z</UPDATE_DATE>
        <CREATED_DATE>2019-10-08T19:16:02Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[preFCCUDC]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[min]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows File Content Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>
            <PATH_TYPE><![CDATA[Use file search]]></PATH_TYPE>
            <FILE_QUERY><![CDATA[QWEB*]]></FILE_QUERY>
            <BASE_DIR><![CDATA[c:\]]></BASE_DIR>
            <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>
            <FILE_NAME_MATCH><![CDATA[preTest2.txt]]></FILE_NAME_MATCH>
            <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
            <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
            <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
            <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
            <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>
            <DATA_TYPE>String List</DATA_TYPE>
            <DESCRIPTION><![CDATA[FileContentChech]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>53</ID>
            <NAME>Windows 2012 Server</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
```

```
            </DEFAULT_VALUES>
          </DATAPOINT>
        </TECHNOLOGY>
        <TECHNOLOGY>
          <ID>75</ID>
          <NAME>Windows Server 2012 R2</NAME>
          <RATIONALE><![CDATA[rationale]]></RATIONALE>
          <DATAPOINT>
              <CARDINALITY>contains</CARDINALITY>
              <OPERATOR>xre</OPERATOR>
              <DEFAULT_VALUES total="1">
                  <DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
              </DEFAULT_VALUES>
          </DATAPOINT>
        </TECHNOLOGY>
    </TECHNOLOGY_LIST>
</CONTROL>
<CONTROL>
    <ID>100006</ID>
    <UPDATE_DATE>2019-10-14T19:06:55Z</UPDATE_DATE>
    <CREATED_DATE>2019-10-09T22:00:50Z</CREATED_DATE>
    <CATEGORY>Database Settings</CATEGORY>
    <SUB_CATEGORY><![CDATA[DB Access Controls]]></SUB_CATEGORY>
    <STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
    <CRITICALITY>
      <LABEL><![CDATA[min]]></LABEL>
      <VALUE>1</VALUE>
    </CRITICALITY>
    <CHECK_TYPE><![CDATA[Windows File Content Check]]></CHECK_TYPE>
    <COMMENT><![CDATA[]]></COMMENT>
    <IGNORE_ERROR>0</IGNORE_ERROR>
    <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
    <SCAN_PARAMETERS>
        <PATH_TYPE><![CDATA[Use Registry key]]></PATH_TYPE>
        <REG_HIVE><![CDATA[HKEY_CLASSES_ROOT (HKCR)]]></REG_HIVE>
        <REG_KEY><![CDATA[TestKey\user]]></REG_KEY>
        <REG_VALUE_NAME><![CDATA[preName]]></REG_VALUE_NAME>
        <FILE_PATH><![CDATA[]]></FILE_PATH>
        <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
        <DATA_TYPE>String List</DATA_TYPE>
        <DESCRIPTION><![CDATA[reg key]]></DESCRIPTION>
    </SCAN_PARAMETERS>
    <TECHNOLOGY_LIST>
      <TECHNOLOGY>
        <ID>53</ID>
        <NAME>Windows 2012 Server</NAME>
        <RATIONALE><![CDATA[rationale]]></RATIONALE>
        <DATAPOINT>
            <CARDINALITY>contains</CARDINALITY>
```

```
<OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>75</ID>
            <NAME>Windows Server 2012 R2</NAME>
            <RATIONALE><![CDATA[rationale]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
        </TECHNOLOGY_LIST>
      </CONTROL>
      <CONTROL>
        <ID>100026</ID>
        <UPDATE_DATE>2019-10-11T20:12:48Z</UPDATE_DATE>
        <CREATED_DATE>2019-10-11T20:12:48Z</CREATED_DATE>
        <CATEGORY>Access Control Requirements</CATEGORY>
        <SUB_CATEGORY><![CDATA[Account Creation/User
Management]]></SUB_CATEGORY>
        <STATEMENT><![CDATA[pre_fcc_file_path_regexwith$]]></STATEMENT>
        <CRITICALITY>
          <LABEL><![CDATA[min]]></LABEL>
          <VALUE>1</VALUE>
        </CRITICALITY>
        <CHECK_TYPE><![CDATA[Windows File Content Check]]></CHECK_TYPE>
        <COMMENT><![CDATA[]]></COMMENT>
        <IGNORE_ERROR>0</IGNORE_ERROR>
        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
        <SCAN_PARAMETERS>
            <PATH_TYPE><![CDATA[Use file path]]></PATH_TYPE>
<FILE_PATH><![CDATA[C:\user\PreTest\pretestfile1.txt]]></FILE_PATH>
            <FILE_QUERY><![CDATA[pre\$]]></FILE_QUERY>
            <DATA_TYPE>String List</DATA_TYPE>
            <DESCRIPTION><![CDATA[pre\$]]></DESCRIPTION>
        </SCAN_PARAMETERS>
        <TECHNOLOGY_LIST>
          <TECHNOLOGY>
            <ID>1</ID>
            <NAME>Windows XP desktop</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
```

```
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>2</ID>
    <NAME>Windows 2003 Server</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>12</ID>
    <NAME>Windows 2000</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>18</ID>
    <NAME>Windows Vista</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>21</ID>
    <NAME>Windows 2008 Server</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
```

```
<OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>37</ID>
            <NAME>Windows 7</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>53</ID>
            <NAME>Windows 2012 Server</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>54</ID>
            <NAME>Windows 8</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
                <DEFAULT_VALUES total="1">
                    <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
            </DATAPOINT>
          </TECHNOLOGY>
          <TECHNOLOGY>
            <ID>72</ID>
            <NAME>Windows 8.1</NAME>
            <RATIONALE><![CDATA[ration]]></RATIONALE>
            <DATAPOINT>
                <CARDINALITY>contains</CARDINALITY>
                <OPERATOR>xre</OPERATOR>
```

```
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>75</ID>
    <NAME>Windows Server 2012 R2</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>91</ID>
    <NAME>Windows 10</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>106</ID>
    <NAME>Windows 2016 Server</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
            <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
        </DEFAULT_VALUES>
    </DATAPOINT>
</TECHNOLOGY>
<TECHNOLOGY>
    <ID>144</ID>
    <NAME>Windows Embedded 7</NAME>
    <RATIONALE><![CDATA[ration]]></RATIONALE>
    <DATAPOINT>
        <CARDINALITY>contains</CARDINALITY>
        <OPERATOR>xre</OPERATOR>
        <DEFAULT_VALUES total="1">
```

```
<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>145</ID>
              <NAME>Windows Embedded 8</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>146</ID>
              <NAME>Windows Embedded 8.1</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
            <TECHNOLOGY>
              <ID>180</ID>
              <NAME>Windows 2019 Server</NAME>
              <RATIONALE><![CDATA[ration]]></RATIONALE>
              <DATAPOINT>
                  <CARDINALITY>contains</CARDINALITY>
                  <OPERATOR>xre</OPERATOR>
                  <DEFAULT_VALUES total="1">
                      <DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                  </DEFAULT_VALUES>
              </DATAPOINT>
            </TECHNOLOGY>
          </TECHNOLOGY_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

DTD update:

DTD: <platform>/api/2.0/fo/compliance/control/control_list_output.dtd

```
<!-- QUALYS CONTROL_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT CONTROL_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, (CONTROL_LIST|ID_SET)?, WARNING?)>
<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, UPDATE_DATE, CREATED_DATE, CATEGORY, SUB_CATEGORY,
STATEMENT, CRITICALITY?, DEPRECATED?, DEPRECATED_DATE?,
        CHECK_TYPE?, COMMENT?, USE_AGENT_ONLY?, AUTO_UPDATE?,
IGNORE_ERROR?, (IGNORE_ITEM_NOT_FOUND|ERROR_SET_STATUS)?,
SCAN_PARAMETERS?, TECHNOLOGY_LIST, FRAMEWORK_LIST?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)>
<!ELEMENT CREATED_DATE (#PCDATA)>
<!ELEMENT CATEGORY (#PCDATA)>
<!ELEMENT SUB_CATEGORY (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT DEPRECATED (#PCDATA)>
<!ELEMENT DEPRECATED_DATE (#PCDATA)>
<!ELEMENT CHECK_TYPE (#PCDATA)>
<!ELEMENT COMMENT (#PCDATA)>
<!ELEMENT USE_AGENT_ONLY (#PCDATA)>
<!ELEMENT AUTO_UPDATE (#PCDATA)>
<!ELEMENT IGNORE_ERROR (#PCDATA)>
<!ELEMENT IGNORE_ITEM_NOT_FOUND (#PCDATA)>
<!ELEMENT ERROR_SET_STATUS (#PCDATA)>
<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?, PATH_USER?, GROUP_NAME?, GROUP_NAME_LIMIT?,
BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?, INTEGRITY_CHECK_DEPTH_LIMIT?,
FOLLOW_SYMLINK?, FILE_NAME_MATCH?, FILE_NAME_SKIP?, DIR_NAME_MATCH?,
```

```
DIR_NAME_SKIP?, WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, PERMISSIONS?, PERM_COND?,
TYPE_MATCH?, USER_OWNER?, GROUP_OWNER?,
        TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE, DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_NAME_LIMIT (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>

...
```

Sample - Policy API

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=export&id=1758961&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/">
FCCWin_Policy_Export.xml
```

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>2019-10-14T21:21:45Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[SamplePolicyWithFileContentSearchUDCs]]></TITLE>
    <EXPORTED><![CDATA[2019-10-14T21:21:45Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
```

```
            <TECHNOLOGY>
                <ID>75</ID>
                <NAME>Windows Server 2012 R2</NAME>
            </TECHNOLOGY>
        </TECHNOLOGIES>
        <SECTIONS total="1">
            <SECTION>
                <NUMBER>1</NUMBER>
                <HEADING><![CDATA[Untitled]]></HEADING>
                <CONTROLS total="3">
                    <USER_DEFINED_CONTROL>
                        <ID>100006</ID>
                        <UDC_ID>98e7dde1-412d-4a95-8262-b7bd168ebad8</UDC_ID>
                        <CHECK_TYPE>Windows File Content Check</CHECK_TYPE>
                        <CATEGORY>
                            <ID>8</ID>
                            <NAME><![CDATA[Database Settings]]></NAME>
                        </CATEGORY>
                        <SUB_CATEGORY>
                            <ID>1044</ID>
                            <NAME><![CDATA[DB Access Controls]]></NAME>
                        </SUB_CATEGORY>
                       <STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
                        <CRITICALITY>
                            <LABEL><![CDATA[min]]></LABEL>
                            <VALUE>1</VALUE>
                        </CRITICALITY>
                        <COMMENT><![CDATA[]]></COMMENT>
                        <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                        <AUTO_UPDATE>0</AUTO_UPDATE>
                        <IGNORE_ERROR>0</IGNORE_ERROR>
                        <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                        <SCAN_PARAMETERS>
                          <PATH_TYPE><![CDATA[Use Registry key]]></PATH_TYPE>
                            <REG_HIVE><![CDATA[HKEY_CLASSES_ROOT
(HKCR)]]></REG_HIVE>
                            <REG_KEY><![CDATA[TestKey\user]]></REG_KEY>

<REG_VALUE_NAME><![CDATA[preName]]></REG_VALUE_NAME>
                            <FILE_PATH><![CDATA[]]></FILE_PATH>
                            <FILE_QUERY><![CDATA[.*]]></FILE_QUERY>
                            <DATA_TYPE>String List</DATA_TYPE>
                            <DESCRIPTION><![CDATA[reg key]]></DESCRIPTION>
                        </SCAN_PARAMETERS>
                        <TECHNOLOGIES total="1">
                            <TECHNOLOGY>
                                <ID>75</ID>
                                <NAME>Windows Server 2012 R2</NAME>
```

```
<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1007110</K><L>0</L><
CD>contains</CD><OP>xre</OP><V><![CDATA[.*]]></V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[rationale]]></RATIONALE>
                            <DATAPOINT>
                                <CARDINALITY>contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
                <USER_DEFINED_CONTROL>
                    <ID>100000</ID>
                    <UDC_ID>b24df689-0714-7045-833a-987f04cdab15</UDC_ID>
                    <CHECK_TYPE>Windows File Content Check</CHECK_TYPE>
                    <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[preFCCUDC]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[min]]></LABEL>
                        <VALUE>1</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
                    <IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>
                       <PATH_TYPE><![CDATA[Use file search]]></PATH_TYPE>
                        <FILE_QUERY><![CDATA[QWEB*]]></FILE_QUERY>
                        <BASE_DIR><![CDATA[c:\]]></BASE_DIR>
                        <DEPTH_LIMIT><![CDATA[3]]></DEPTH_LIMIT>

<FILE_NAME_MATCH><![CDATA[preTest2.txt]]></FILE_NAME_MATCH>
                        <FILE_NAME_SKIP><![CDATA[]]></FILE_NAME_SKIP>
                        <DIR_NAME_MATCH><![CDATA[*]]></DIR_NAME_MATCH>
                        <DIR_NAME_SKIP><![CDATA[]]></DIR_NAME_SKIP>
                        <TIME_LIMIT><![CDATA[300]]></TIME_LIMIT>
```

```
                        <MATCH_LIMIT><![CDATA[50]]></MATCH_LIMIT>
                        <DATA_TYPE>String List</DATA_TYPE>

<DESCRIPTION><![CDATA[FileContentChech]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>75</ID>
                            <NAME>Windows Server 2012 R2</NAME>

<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1007020</K><L>0</L><
CD>contains</CD><OP>xre</OP><V><![CDATA[true]]></V></DP></CTRL></EVALUATE
>
                            <RATIONALE><![CDATA[rationale]]></RATIONALE>
                            <DATAPOINT>
                                <CARDINALITY>contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[true]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
                <USER_DEFINED_CONTROL>
                    <ID>100026</ID>
                    <UDC_ID>d908b3f9-59f9-fb70-801c-29d04fb12511</UDC_ID>
                    <CHECK_TYPE>Windows File Content Check</CHECK_TYPE>
                    <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[pre_fcc_file_path_regexwith$]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[min]]></LABEL>
                        <VALUE>1</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[]]></COMMENT>
                    <USE_AGENT_ONLY>0</USE_AGENT_ONLY>
                    <AUTO_UPDATE>0</AUTO_UPDATE>
                    <IGNORE_ERROR>0</IGNORE_ERROR>
```

```
<IGNORE_ITEM_NOT_FOUND>0</IGNORE_ITEM_NOT_FOUND>
                    <SCAN_PARAMETERS>
                        <PATH_TYPE><![CDATA[Use file path]]></PATH_TYPE>

<FILE_PATH><![CDATA[C:\user\PreTest\pretestfile1.txt]]></FILE_PATH>
                        <FILE_QUERY><![CDATA[pre\$]]></FILE_QUERY>
                        <DATA_TYPE>String List</DATA_TYPE>
                        <DESCRIPTION><![CDATA[pre\$]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>75</ID>
                            <NAME>Windows Server 2012 R2</NAME>

<EVALUATE><CTRL><DP><K>custom.win_file_content_check.1008003</K><L>0</L><
CD>contains</CD><OP>xre</OP><V><![CDATA[.*]]></V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[ration]]></RATIONALE>
                            <DATAPOINT>
                                <CARDINALITY>contains</CARDINALITY>
                                <OPERATOR>xre</OPERATOR>
                                <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
                </USER_DEFINED_CONTROL>
            </CONTROLS>
        </SECTION>
    </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

DTD update:

DTD: <platform>/api/2.0/fo/compliance/policy/policy_export_output

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

```
...
<!ELEMENT REF_DESCRIPTION (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ERROR_SET_STATUS (#PCDATA)>

<!ELEMENT SCAN_PARAMETERS (PATH_TYPE?, REG_HIVE?, REG_KEY?,
REG_VALUE_NAME?, FILE_PATH?, FILE_QUERY?, HASH_TYPE?, WMI_NS?,
WMI_QUERY?, SHARE_USER?,
PATH_USER?, BASE_DIR?, SHOULD_DESCEND?, DEPTH_LIMIT?,
INTEGRITY_CHECK_DEPTH_LIMIT?, FOLLOW_SYMLINK?, FILE_NAME_MATCH?,
FILE_NAME_SKIP?, DIR_NAME_MATCH?,
DIR_NAME_SKIP?, PERMISSIONS?, PERM_COND?, TYPE_MATCH?, USER_OWNER?,
GROUP_OWNER?, TIME_LIMIT?, MATCH_LIMIT?, INTEGRITY_CHECK_TIME_LIMIT?,
INTEGRITY_CHECK_MATCH_LIMIT?, INTEGRITY_CHECK_OBJECT_TYPES?,
WIN_FILE_SYS_OBJECT_TYPES?,
MATCH_WELL_KNOWN_USERS_FOR_ANY_DOMAIN?, WIN_PERMISSION_USERS?,
WIN_PERMISSION_MATCH?, WIN_PERMISSIONS?, GROUP_NAME?,
GROUP_NAME_LIMIT?, DIGEST_HASH?, PERMISSION_MONITOR?, DATA_TYPE,
DESCRIPTION)>
<!ELEMENT PATH_TYPE (#PCDATA)>
<!ELEMENT REG_HIVE (#PCDATA)>
<!ELEMENT REG_KEY (#PCDATA)>
<!ELEMENT REG_VALUE_NAME (#PCDATA)>
<!ELEMENT FILE_PATH (#PCDATA)>
<!ELEMENT FILE_QUERY (#PCDATA)>
<!ELEMENT HASH_TYPE (#PCDATA)>
<!ELEMENT WMI_NS (#PCDATA)>
<!ELEMENT WMI_QUERY (#PCDATA)>
<!ELEMENT SHARE_USER (#PCDATA)>
<!ELEMENT PATH_USER (#PCDATA)>
<!ELEMENT BASE_DIR (#PCDATA)>
<!ELEMENT SHOULD_DESCEND (#PCDATA)>
<!ELEMENT DEPTH_LIMIT (#PCDATA)>
...
```

Sample - Posture API

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST" -d
"action=list&echo_request=1&policy_id=1758961&details=All&include_dp_name
=1" "https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/">
posture_info_result.xml
```

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>
  <REQUEST>
    <DATETIME>2019-10-14T21:19:57Z</DATETIME>
    <USER_LOGIN>rey_pt11</USER_LOGIN>

<RESOURCE>https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info
/</RESOURCE>
    <PARAM_LIST>
      <PARAM>
        <KEY>action</KEY>
        <VALUE>list</VALUE>
      </PARAM>
      <PARAM>
        <KEY>echo_request</KEY>
        <VALUE>1</VALUE>
      </PARAM>
      <PARAM>
        <KEY>policy_id</KEY>
        <VALUE>1758961</VALUE>
      </PARAM>
      <PARAM>
        <KEY>details</KEY>
        <VALUE>All</VALUE>
      </PARAM>
      <PARAM>
        <KEY>include_dp_name</KEY>
        <VALUE>1</VALUE>
      </PARAM>
    </PARAM_LIST>
  </REQUEST>
  <RESPONSE>
    <DATETIME>2019-10-14T21:19:57Z</DATETIME>
    <INFO_LIST>
      <INFO>
        <ID>34544283</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100006</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</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>2019-10-14T21:15:46Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2019-10-14T21:15:46Z</LAST_PASS_DATE>
        <EVIDENCE>
```

```
<BOOLEAN_EXPR><![CDATA[:dp_2 contains $tp_2]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_2</LABEL>
              <V fileName="c:\Agent\user\test2.txt"><![CDATA[QWEB]]></V>
              <TM_REF>@tm_1</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>34544284</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100000</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Failed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</POSTURE_MODIFIED_DATE>
        <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
        <FIRST_FAIL_DATE>2019-10-14T21:15:46Z</FIRST_FAIL_DATE>
        <LAST_FAIL_DATE>2019-10-14T21:15:46Z</LAST_FAIL_DATE>
        <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
        <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_1 contains $tp_1]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_1</LABEL>
              <V fileName="C:\preTest2.txt"><![CDATA[QWEB]]></V>
              <TM_REF>@tm_2</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
      <INFO>
        <ID>34544285</ID>
        <HOST_ID>7368441</HOST_ID>
        <CONTROL_ID>100026</CONTROL_ID>
        <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
        <INSTANCE></INSTANCE>
        <STATUS>Passed</STATUS>
        <POSTURE_MODIFIED_DATE>2019-10-
14T21:15:46Z</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>2019-10-14T21:15:46Z</FIRST_PASS_DATE>
        <LAST_PASS_DATE>2019-10-14T21:15:46Z</LAST_PASS_DATE>
```

```
        <EVIDENCE>
          <BOOLEAN_EXPR><![CDATA[:dp_3 contains $tp_2]]></BOOLEAN_EXPR>
          <DPV_LIST>
            <DPV lastUpdated="2019-10-14T19:53:41Z">
              <LABEL>:dp_3</LABEL>
              <V
fileName="C:\user\PreTest\pretestfile1.txt"><![CDATA[pre$]]></V>
              <TM_REF>@tm_3</TM_REF>
            </DPV>
          </DPV_LIST>
        </EVIDENCE>
      </INFO>
    </INFO_LIST>
    <SUMMARY>
      <TOTAL_ASSETS>1</TOTAL_ASSETS>
      <TOTAL_CONTROLS>3</TOTAL_CONTROLS>
      <CONTROL_INSTANCES>
        <TOTAL>3</TOTAL>
        <TOTAL_PASSED>2</TOTAL_PASSED>
        <TOTAL_FAILED>1</TOTAL_FAILED>
        <TOTAL_ERROR>0</TOTAL_ERROR>
        <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
      </CONTROL_INSTANCES>
    </SUMMARY>
    <GLOSSARY>
      <HOST_LIST>
        <HOST>
          <ID>7368441</ID>
          <IP>10.115.74.93</IP>
          <TRACKING_METHOD>AGENT</TRACKING_METHOD>
          <DNS><![CDATA[win-890blrmesc6]]></DNS>
          <NETBIOS><![CDATA[WIN-890BLRMESC6]]></NETBIOS>
          <OS><![CDATA[Windows Server 2012 R2 Standard 64 bit
Edition]]></OS>
          <QG_HOSTID>3031a534-6b78-4c4c-aacd-db56257c155f</QG_HOSTID>
          <LAST_VULN_SCAN_DATETIME>2019-10-
14T19:18:12Z</LAST_VULN_SCAN_DATETIME>
          <LAST_COMPLIANCE_SCAN_DATETIME>2019-10-
14T20:21:07Z</LAST_COMPLIANCE_SCAN_DATETIME>
          <PERCENTAGE><![CDATA[66.67% (2 of 3)]]></PERCENTAGE>
        </HOST>
      </HOST_LIST>
      <CONTROL_LIST>
        <CONTROL>
          <ID>100006</ID>
          <STATEMENT><![CDATA[Windows_FCC_Use_Reg]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[min]]></LABEL>
            <VALUE>1</VALUE>
```

```
      </CRITICALITY>
      <RATIONALE_LIST>
        <RATIONALE>
          <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
          <TEXT><![CDATA[rationale]]></TEXT>
        </RATIONALE>
      </RATIONALE_LIST>
    </CONTROL>
    <CONTROL>
      <ID>100000</ID>
      <STATEMENT><![CDATA[preFCCUDC]]></STATEMENT>
      <CRITICALITY>
        <LABEL><![CDATA[min]]></LABEL>
        <VALUE>1</VALUE>
      </CRITICALITY>
      <RATIONALE_LIST>
        <RATIONALE>
          <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
          <TEXT><![CDATA[rationale]]></TEXT>
        </RATIONALE>
      </RATIONALE_LIST>
    </CONTROL>
    <CONTROL>
      <ID>100026</ID>
      <STATEMENT><![CDATA[pre_fcc_file_path_regexwith$]]></STATEMENT>
      <CRITICALITY>
        <LABEL><![CDATA[min]]></LABEL>
        <VALUE>1</VALUE>
      </CRITICALITY>
      <RATIONALE_LIST>
        <RATIONALE>
          <TECHNOLOGY_ID>75</TECHNOLOGY_ID>
          <TEXT><![CDATA[ration]]></TEXT>
        </RATIONALE>
      </RATIONALE_LIST>
    </CONTROL>
  </CONTROL_LIST>
  <TECHNOLOGY_LIST>
    <TECHNOLOGY>
      <ID>75</ID>
      <NAME><![CDATA[Windows Server 2012 R2]]></NAME>
    </TECHNOLOGY>
  </TECHNOLOGY_LIST>
  <DPD_LIST>
    <DPD>
      <LABEL>:dp_1</LABEL>
      <ID>1007020</ID>
      <NAME><![CDATA[custom.win_file_content_check.1007020]]></NAME>
      <DESC><![CDATA[FileContentChech]]></DESC>
```

```
</DPD>
        <DPD>
          <LABEL>:dp_2</LABEL>
          <ID>1007110</ID>
          <NAME><![CDATA[custom.win_file_content_check.1007110]]></NAME>
          <DESC><![CDATA[reg key]]></DESC>
        </DPD>
        <DPD>
          <LABEL>:dp_3</LABEL>
          <ID>1008003</ID>
          <NAME><![CDATA[custom.win_file_content_check.1008003]]></NAME>
          <DESC><![CDATA[pre\$]]></DESC>
        </DPD>
      </DPD_LIST>
      <TP_LIST>
        <TP>
          <LABEL>$tp_1</LABEL>
          <V><![CDATA[true]]></V>
        </TP>
        <TP>
          <LABEL>$tp_2</LABEL>
          <V><![CDATA[.*]]></V>
        </TP>
      </TP_LIST>
      <TM_LIST>
        <TM>
          <LABEL>@tm_1</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
        </TM>
        <TM>
          <LABEL>@tm_2</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
        </TM>
        <TM>
          <LABEL>@tm_3</LABEL>
          <PAIR>
            <K><![CDATA[item not found:2]]></K>
            <V><![CDATA[Set status Passed for â€œitem not foundâ€?
error]]></V>
          </PAIR>
        </TM>
```

```
      </TM_LIST>
    </GLOSSARY>
  </RESPONSE>
</POSTURE_INFO_LIST_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the
QualysGuard Service "As Is," without any warranty of any kind. Qualys
makes no warranty that the information contained in this report is
complete or error-free. Copyright 2019, Qualys, Inc. //-->
```

DTD update:

DTD: <platform>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd

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

<!ELEMENT REQUEST (DATETIME, USER_LOGIN, RESOURCE, PARAM_LIST?,
POST_DATA?)>
...
<!ELEMENT PREVIOUS_STATUS (#PCDATA)>
<!ELEMENT FIRST_FAIL_DATE (#PCDATA)>
<!ELEMENT LAST_FAIL_DATE (#PCDATA)>
<!ELEMENT FIRST_PASS_DATE (#PCDATA)>
<!ELEMENT LAST_PASS_DATE (#PCDATA)>
<!ELEMENT EXCEPTION (ASSIGNEE, STATUS, END_DATETIME?, CREATED?,
LAST_MODIFIED?, COMMENT_LIST?)>
<!ELEMENT ASSIGNEE (#PCDATA)>
<!ELEMENT END_DATETIME (#PCDATA)>
<!ELEMENT CREATED (BY, DATETIME)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (BY, DATETIME)>
<!ELEMENT COMMENT_LIST (COMMENT+)>
<!ELEMENT COMMENT (DATETIME, BY, TEXT)>
<!ELEMENT TEXT (#PCDATA)>

<!ELEMENT EVIDENCE (BOOLEAN_EXPR, DPV_LIST?)>
<!ELEMENT BOOLEAN_EXPR (#PCDATA)>
<!ELEMENT DPV_LIST (DPV+)>
<!ELEMENT DPV (LABEL, (ERROR|V)+, TM_REF?)>
<!ATTLIST DPV lastUpdated CDATA #IMPLIED>
<!ELEMENT V (#PCDATA|H|R)*>
<!ATTLIST V fileName CDATA #IMPLIED>
<!ELEMENT H (C+)>
<!ELEMENT R (C+)>
...
```

Schema update:

The ImportableControl.xsd schema is used when importing and exporting controls.

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

...
   <xs:element name="SCAN_PARAMETERS">
<xs:complexType>
<xs:sequence>
<xs:element ref="PATH_TYPE" minOccurs="0" maxOccurs="1" />
<xs:element ref="REG_HIVE" minOccurs="0" maxOccurs="1" />
<xs:element ref="REG_KEY" minOccurs="0" maxOccurs="1" />
<xs:element ref="REG_VALUE_NAME" minOccurs="0" maxOccurs="1" />

....

<xs:element name="PATH_TYPE">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="Use Registry key" />
<xs:enumeration value="Use file search" />
<xs:enumeration value="Use file path" />
</xs:restriction>
</xs:simpleType>
</xs:element>

<xs:element name="DATA_TYPE">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="Boolean" />
...
```

Support for HashiCorp vault in Database Authentication records

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

HashiCorp vault is now supported for the following database authentication records: MySQL, MariaDB, Sybase, PostgreSQL, MongoDB.

You can create, update, list, and view authentication credentials from a HashiCorp vault.

Sample - Create MySQL auth record using HashiCorp vault

API request:

```
curl -u "username:password" -H 'X-Requested-With:curl demo2' -d
"action=create&title=API_v2_netwr_ne_MySQL&username=mlqa&&login_type=vaul
t&ips=10.10.0.10&port=3306&database=mysql&vault_id=2005776&vault_type=Has
hiCorp&secret_kv_name=secret_name1&secret_kv_key=secret_key1&secret_kv_pa
th=default/path&unix_config_file=/etc/mysql/"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

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>2019-10-31T11:52:11Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2070077</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - List MySQL auth records with HashiCorp vault

API request:

```
curl -u "username:password" -H 'X-Requested-With:curl demo2' -d
"action=list&ids=2070077"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MYSQL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mysql/auth_mysql_list_output.dtd">
<AUTH_MYSQL_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2019-10-31T11:53:48Z</DATETIME>
    <AUTH_MYSQL_LIST>
      <AUTH_MYSQL>
        <ID>2070077</ID>
        <TITLE><![CDATA[API_v2_netwr_ne_MySQL]]></TITLE>
        <USERNAME><![CDATA[mlqa]]></USERNAME>
        <DATABASE><![CDATA[mysql]]></DATABASE>
        <PORT>3306</PORT>
        <IP_SET>
          <IP>10.10.0.10</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[vault]]></LOGIN_TYPE>
        <DIGITAL_VAULT>
          <DIGITAL_VAULT_ID><![CDATA[2005776]]></DIGITAL_VAULT_ID>
          <DIGITAL_VAULT_TYPE><![CDATA[HashiCorp]]></DIGITAL_VAULT_TYPE>
          <DIGITAL_VAULT_TITLE><![CDATA[Test-Hashi]]></DIGITAL_VAULT_TITLE>
          <VAULT_SECRET_KV_PATH><![CDATA[default/path]]></VAULT_SECRET_KV_PATH>
          <VAULT_SECRET_KV_NAME><![CDATA[secret_name1]]></VAULT_SECRET_KV_NAME>
          <VAULT_SECRET_KV_KEY><![CDATA[secret_key1]]></VAULT_SECRET_KV_KEY>
        </DIGITAL_VAULT>
        <SSL_VERIFY>false</SSL_VERIFY>
        <WINDOWS_CONF_FILE><![CDATA[]]></WINDOWS_CONF_FILE>
        <UNIX_CONF_FILE><![CDATA[/etc/mysql/]]></UNIX_CONF_FILE>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2019-10-31T11:52:11Z</DATETIME>
          <BY>amazn_ak</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2019-10-31T11:52:11Z</DATETIME>
        </LAST_MODIFIED>
      </AUTH_MYSQL>
    </AUTH_MYSQL_LIST>
  </RESPONSE>
</AUTH_MYSQL_LIST_OUTPUT>
<!-- CONFIDENTIAL AND PROPRIETARY INFORMATION. Qualys provides the QualysGuard
Service "As Is," without any warranty of any kind. Qualys makes no warranty that
the information contained in this report is complete or error-free. Copyright 2019,
Qualys, Inc. //-->
```

Updated DTDs

auth_mysql_list_output.dtd

New parameters (in Bold) are added.

```
<!-- QUALYS AUTH_MYSQL_LIST_OUTPUT DTD -->
<!-- $Revision: 68724 $ -->
<!ELEMENT AUTH_MYSQL_LIST_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?,
VAULT_NS_TYPE?, VAULT_NS_NAME?, VAULT_ACCOUNT_NAME?,
VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?, VAULT_SECRET_KV_KEY?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
...
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
...
<!ELEMENT LAST_NAME (#PCDATA)>
        <!-- EOF -->
```

auth_mariadb_list_output.dtd

New parameters (in Bold) are added.

```
<!-- QUALYS AUTH_MARIADB_LIST_OUTPUT DTD -->
<!-- $Revision: 68724 $ -->
<!ELEMENT AUTH_MARIADB_LIST_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?,
VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?)>
...
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
...
<!ELEMENT LAST_NAME (#PCDATA)>
        <!-- EOF -->
```

auth_sybase_list_output.dtd

New parameters (in Bold) are added.

```
<!-- QUALYS AUTH_SYBASE_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_SYBASE_LIST_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?,
VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?)>
...
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
...
<!ELEMENT LAST_NAME (#PCDATA)>
  <!-- EOF -->
```

auth_postgresql_list_output.dtd

New parameters (in Bold) are added.

```
<!-- QUALYS AUTH_POSTGRESQL_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_POSTGRESQL_LIST_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?,
VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?)>
...
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
...
<!ELEMENT LAST_NAME (#PCDATA)>
  <!-- EOF -->
```

auth_mongodb_list_output.dtd

New parameters (in Bold) are added.

```
<!-- QUALYS AUTH_MONGODB_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_MONGODB_LIST_OUTPUT (REQUEST?, RESPONSE)>
...
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?,
VAULT_SECRET_NAME?, VAULT_SYSTEM_NAME?, VAULT_EP_NAME?,
VAULT_EP_TYPE?, VAULT_EP_CONT?, VAULT_NS_TYPE?, VAULT_NS_NAME?,
VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?)>
...
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
...
<!ELEMENT LAST_NAME (#PCDATA)>
  <!-- EOF -->
```

Updates to Input Parameters for Cloud Perimeter Scan Jobs

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

It's now possible to launch a cloud perimeter scan job without specifying the platform, region code, vpc id or asset tags. Multiple input parameters changed from Required to Optional to provide this flexibility. Note - There are no changes to the XML output or DTD.

Create/Update Cloud Perimeter Scan

Now when you want to create a new cloud perimeter scan job, only the connector_name or connector_uuid is required in the API request. The following parameters are now optional: vpc_id, region_code, tag_set_include and platform_type.

If no assets are resolved from the connector (and/or other optional target input parameters) then the scan is launched only on the load balancer DNS names specified using the elb_dns parameter. If no load balancer DNS names are specified, then the scan will result in an error since there won't be any assets to scan.

Note - You'll see these changes in your account only when available on your platform. Please reach out to Qualys Support if you need more information.

Input parameters

Input parameters for specifying the cloud perimeter scan target are described below. For complete information on all input parameters for cloud perimeter scan jobs, please refer to the Qualys API (VM/PC) User Guide.

Parameter	Description
connector_name={value}	(Optional) The name of the connector to be used. One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.
connector_uuid={value}	(Optional) The ID of the connector to be used. One of these parameters must be specified in the request: conector_name or connector_uuid. These are mutually exclusive and cannot be specified in the same request.

Parameter	Description
region_code={value}	(Optional) The EC2 region code. Valid values are: ap-northeast-1, ap-southeast-1, ap-southeast-2, eu-west-1, sa-east-1, us-east-1, us-west-1 and us-west-2.
	These parameters are mutually exclusive and cannot be specified in the same request: region_code and vpc_id. When region_code is specified, you must specify platform_type and connector_name or connector_uuid in the same request.
vpc_id={value}	(Optional) The ID of the Virtual Private Cloud (VPC) zone. The ID value must start with vpc%
	These parameters are mutually exclusive and cannot be specified in the same request: region_code and vpc_id. When vpc_id is specified, you must specify platform_type and connector_name or connector_uuid in the same request.
platform_type={value}	(Optional) The platform type. Valid values are: classic, vpc_peered or selected_vpc.
	When platform_type is specified you must also specify: region_code or vpc_id and connector_name or connector_uuid.
tag_set_include={value}	(Optional) Specify a tag set to include. Hosts that match these tags will be included. You identify the tag set by providing tag name or IDs. Multiple entries are comma separated.
elb_dns={value}	(Optional) One or more load balancer DNS names to include in the scan job. Multiple values are comma-separated.

Sample 1

In this example, the scan will be launched on all assets from the connector, and on the load balancer DNS name specified in the request. If no assets are resolved from the connector then only the load balancer DNS name will be scanned.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=action=create&module=vm&active=0&schedule=now&option_title=Initia
l%20Options&connector_uuid=00b37f4f-30fa-46e7-9bce-
c1f0ac950b00&elb_dns=ec2-34-230-58-205.compute-1.amazonaws.com"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

Sample 2

In this example, only the connector is specified so the scan will be launched on all assets from the connector.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&module=vm&active=0&schedule=now&option_title=Initial%20Opt
ions&connector_uuid=00b37f4f-30fa-46e7-9bce-c1f0ac950b00"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

Sample 3

In this example, the scan will be launched on all assets from the connector that also match the specified VPC and asset tags.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&module=vm&active=0&schedule=now&tag_set_include=CloudPerim
eter&tag_set_by=name&connector_uuid=00b37f4f-30fa-46e7-9bce-
c1f0ac950b00&platform_type=selected_vpc&vpc_id=vpc-
1e37cd76&option_title=Initial%20Options"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

Sample 4

In this example, the scan will be launched on all assets from the connector that also match the specified asset tags.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl"
"action=create&module=vm&active=0&schedule=now&tag_set_include=CloudPerim
eter&tag_set_by=name&connector_uuid=00b37f4f-30fa-46e7-9bce-
c1f0ac950b00&option_title=Initial%20Options"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/"
```

Sybase Authentication is Now Supported in VM

APIs affected	/api/2.0/fo/auth/sybase/ /api/2.0/fo/subscription/option_profile/
New or Updated API	Updated
DTD or XSD changes	No

Sybase authentication was already supported for PC and now it's also supported in VM for vulnerability scanning. Each Sybase record identifies account login credentials, database information and target host IPs for authenticating to Sybase Adaptive Server Enterprise (ASE) instances. How you create and manage Sybase records is the same as previously documented for PC. You can find all the details in the Qualys API (VM/PC) User Guide.

We made updates to the VM option profile API to allow users to enable Sybase authentication for vulnerability scans. You'll also see Sybase in the XML output when you list/export option profiles with Sybase enabled. Note that there are no DTD changes.

Create/Update Option Profile

Now you can specify "authentication=sybase" when creating/updating VM option profiles using the API. This works in the same way as other authentication types supported in VM.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=MyOptionProfile&global=1&scan_tcp_ports=full&scan_ud
p_ports=standard&scan_overall_performance=normal&vulnerability_detection=
complete&basic_information_gathering=all&authentication=sybase"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

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>2019-10-31T06:40:03Z</DATETIME>
    <TEXT>Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>32112</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

List Option Profile

When you list option profiles you'll see "Sybase" in the <AUTHENTICATION> tag in the XML output for each option profile where Sybase is selected. This tag lists all the authentication types selected in the option profile as a comma-separated list.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=list"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/vm/"
```

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>51451401</ID>
...
            </VULNERABILITY_DETECTION>
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,Sybase]]></AUTHENTICATION>
...
          </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Export Option Profile

When you export option profiles you'll see "Sybase" in the <AUTHENTICATION> tag in the XML output for each option profile where Sybase is selected. This tag lists all the authentication types selected in the option profile as a comma-separated list.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"action=export"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/"
```

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>111186</ID>
...
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,Sybase]]></AUTHENTICATION>
 ...
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Import Option Profile

When you import option profiles you can specify "Sybase" as a value in the <AUTHENTICATION> tag to enable Sybase in the option profile, along with any other authentication types you want to enable in the option profile as a comma-separated list.

API request:

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

Note: "Export_OP.xml" contains the request POST data.

Request POST data:

```
<?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>11123</ID>
      ...
      </VULNERABILITY_DETECTION>
      <AUTHENTICATION><![CDATA[Windows,Unix,Oracle,Oracle
Listener,SNMP,VMware,DB2,HTTP,MySQL,Sybase]]></AUTHENTICATION>
 ...
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

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>2019-10-31T11:17:43Z</DATETIME>
   <TEXT>Successfully imported Option profile for the subscription Id
76084</TEXT>
   <ITEM_LIST>
     <ITEM>
       <KEY>111234</KEY>
       <VALUE>PCI-John</VALUE>
     </ITEM>
   </ITEM_LIST>
 </RESPONSE>
</SIMPLE_RETURN>
```

Support for Instance Discovery, Auto Record Creation for Apache Tomcat Server

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

Instance discovery and auto record creation is now supported for Apache Tomcat Server (UI and API). We've made several related API enhancements as described in the release notes.

Modules supported - PC

Permissions - Same as permissions for creating Tomcat records as before. We support this feature for Tomcat server instances that are installed on hosts running on the Unix platform. So be sure you have Unix authentication records in your account.

Summary

These capabilities are now available.

- Support for scanning multiple instances running on the same host, and when hosts have varying configurations

- 2 phased scanning process. First, a discovery scan finds Tomcat instances, consolidates instance data, and creates/updates auth records in the user's account. Then an assessment scan uses the records saved in the user's account for control evaluations.

- New option profile settings allow you to 1) enable instance discovery and auto record creation, 2) include system-created records for scans, and 3) determine whether to send system records or user records when there are 2 records for the same instance configuration.

- Compliance scan results show a list of instances discovered by the scan when the instance discovery and auto record creation feature is enabled for the scan. Compliance assessment data is not collected during instance discovery scans.

- New System created auth records. Auto created authentication records have the owner "System". These records cannot be edited by users.

- You can enable Tomcat records for authenticated scanning, i.e. set as Active, or disable this, i.e. set as Inactive.

PC Option Profile API - parameters for instance discovery and record creation

APIs affected	api/2.0/fo/subscription/option_profile/pc/
New or Updated API	No
DTD or XSD changes	No

You'll need to create 2 option profiles. Option profile 1: Enable option to allow auto discovery and system record creation. Option profile 2: Enable option to include system-created authentication records for scans. If you have a system record and user record for the same instance configuration, choose which one to include for scans.

Use these optional parameters when creating or updating a compliance profile for Tomcat:

Parameter	Description
enable_auth_instance_discovery={**0**|1}	(Optional to create or update option profile record) Specify enable_auth_instance_discovery=1 to enable auto discover instances and system record creation for the chosen auth types. When unspecified (enable_auth_instance_discovery=0), we will not scan to auto discover instances. This parameter is mutually exclusive with "scan_by_policy" and "include_system_auth" and cannot be specified together in the same request. In UI, this parameter is a check box and is referred to as "Allow instance discovery..." in the System Authentication Records section in the Scan tab on the Scans > Option Profiles > New/Edit Compliance Profile screen.
auto_auth_types	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. Multiple technologies are specified as comma separated values. In addition to Tomcat Server, we also support Apache Web Server, IBM WebSphere App Server and Jboss Server. We have added Tomcat Server in the list of supported technologies. This parameter can only be specified if enable_auth_instance_discovery=1.

Parameter	Description
include_system_auth={**0**|1}	(Optional to create or update option profile record) Specify include_system_auth=1 if you have a system created auth record and user created auth record for the same instance configuration and choose which one to include for scans. When unspecified (include_system_auth=0), system record will be selected for scan by default. When include_system_auth=1, one of these parameters should be enabled: use_system_auth_on_duplicate or use_user_auth_on_duplicate. In UI, this parameter is a check box and referred as "Use System Authentication Records" in the System Authentication Records section in the Scan tab on the Scans > Option Profiles > New/Edit Compliance Profile screen.
use_system_auth_on_duplicate={**0**|1}	(Optional to create or update option profile record) Specify use_system_auth_on_duplicate=1 to include system created auth record if you have a system record and user record for the same instance configuration. This parameter is mutually exclusive with use_user_auth_on_duplicate and can only be specified if "include_system_auth=1".
use_user_auth_on_duplicate={0|**1**}	(Optional to create or update option profile record) Specify use_user_auth_on_duplicate=1 to include user created auth record if you have a system record and user record for the same instance configuration. This parameter is mutually exclusive with use_system_auth_on_duplicate and can only be specified if "include_system_auth=1".

Sample - Create new pc option profile record to enable Tomcat instance discovery and system record creation

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=Profile-Auth-Ins-Tomcat-
Server&enable_auth_instance_discovery=1&auto_auth_types=Tomcat+Ser
ver&scan_ports=targeted"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - Create pc option profile record to include system auth record on duplicate

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=use_sys_auth&include_system_auth=1&
use_system_auth_on_duplicate=1&scan_ports=targeted"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - Create pc option profile record to include user auth record on duplicate

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=use_user_auth&include_system_auth=1&
use_user_auth_on_duplicate=1&scan_ports=targeted"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - Update Tomcat instance discovery and system record creation

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=105624&enable_auth_instance_discovery=1&auto_aut
h_types=Tomcat+Server"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - Update pc option profile record to include system auth record on duplicate

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=105624&include_system_auth=1&
use_system_auth_on_duplicate=1"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - Update pc option profile record to include user auth record on duplicate

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&id=107091&include_system_auth=1&
use_user_auth_on_duplicate=1"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

Sample - List pc option profile record with auth-instance discovery options

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
"action=list&id=76709"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
...
            <SYSTEM_AUTH_RECORD>
               <ALLOW_AUTH_CREATION>
                   <AUTHENTICATION_TYPE_LIST>
                       <AUTHENTICATION_TYPE>Tomcat
                       Server</AUTHENTICATION_TYPE>
                   </AUTHENTICATION_TYPE_LIST>
               </ALLOW_AUTH_CREATION>
            </SYSTEM_AUTH_RECORD>
...
```

Sample - List pc option profile record with include system auth-record options

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
"action=list&id=107091"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
...
            <SYSTEM_AUTH_RECORD>
               <INCLUDE_SYSTEM_AUTH>
              <ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
               </INCLUDE_SYSTEM_AUTH>
            </SYSTEM_AUTH_RECORD>
...
```

List Tomcat Authentication Records API - new filter options, DTD updated

APIs affected	/api/2.0/fo/auth/tomcat/?action=list
New or Updated API	Updated
DTD or XSD changes	Yes

New input parameters allow you to filter the Tomcat authentication record list by status (active or inactive) and creation type (user created or system created). Elements for these properties were added to the Tomcat auth record list output DTD.

Use these optional parameters:

Parameter	Description
status={0|1}	(Optional) By default, active and inactive auth records are listed. Set to 0 to list only inactive records or set to 1 to list only active records.
is_system_created={0|1}	(Optional) By default, user created records and system created auth records are listed. Set to 0 to list only user created records, or set to 1 to list only system created records.

Sample - List all records, show basic settings

The new tags <IS_SYSTEM_CREATED> and <IS_ACTIVE> appear in the XML output.

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat -d
"action=list&details=Basic"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_TOMCAT_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat/auth_tomcat_l
ist_output.dtd">
<AUTH_TOMCAT_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-11-05T03:29:58Z</DATETIME>
        <AUTH_TOMCAT_LIST>
            <AUTH_TOMCAT>
                <ID>67001</ID>
                <TITLE>
```

```
                    <![CDATA[Tomcat - 10.10.34.52]]>
                </TITLE>
                <IP_SET>
                    <IP>10.10.34.52</IP>
                </IP_SET>
                <UNIX_INSTLLATION_DIRECTORY>
                    <![CDATA[/opt/Tomcat/AppServer]]>
                </UNIX_INSTLLATION_DIRECTORY>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2019-11-05T19:49:19Z</DATETIME>
                    <BY>quays_as2</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2019-11-07T19:49:19Z</DATETIME>
                </LAST_MODIFIED>
                <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
              <IS_ACTIVE>1</IS_ACTIVE>
            </AUTH_TOMCAT>
    ...
```

Sample - List active records only

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat -d
"action=list&status=1"
```

Sample - List system created records only

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat -d
"action=list&is_system_created=1"
```

Updated DTD

New tags appear in bold.

<base_url>/api/2.0/fo/auth/tomcat/auth_tomcat_list_output.dtd

```
...

<!ELEMENT AUTH_TOMCAT (ID, TITLE, IP_SET, INSTALLATION_PATH?,
INSTANCE_PATH?, AUTO_DISCOVER_INSTANCES?,
INSTALLATION_PATH_WINDOWS?, INSTANCE_PATH_WINDOWS?,
SERVICE_NAME_WINDOWS?, NETWORK_ID?, CREATED, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT INSTALLATION_PATH (#PCDATA)>
<!ELEMENT INSTANCE_PATH (#PCDATA)>
<!ELEMENT AUTO_DISCOVER_INSTANCES (#PCDATA)>
<!ELEMENT INSTALLATION_PATH_WINDOWS (#PCDATA)>
<!ELEMENT INSTANCE_PATH_WINDOWS (#PCDATA)>
<!ELEMENT SERVICE_NAME_WINDOWS (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT NETWORK_ID (#PCDATA)>
<!ELEMENT CREATED (DATETIME, BY)>
<!ELEMENT BY (#PCDATA)>
<!ELEMENT LAST_MODIFIED (DATETIME)>
<!ELEMENT IS_SYSTEM_CREATED (#PCDATA)>
<!ELEMENT IS_ACTIVE (#PCDATA)>
<!ELEMENT COMMENTS (#PCDATA)>
...
```

Create/Update Tomcat Authentication Record API - set record to Active or Inactive

APIs affected	/api/2.0/fo/auth/tomcat/?action=create /api/2.0/fo/auth/tomcat/?action=update
New or Updated API	Updated
DTD or XSD changes	No

We added a new input parameter to support the creation of Tomcat auth records with a certain status (active or inactive). This parameter can also be set when updating user-created Tomcat records.

Note that for system-created authentication records you can update only the status of records to active or inactive.

Use this parameter:

Parameter	Description
status={0|1}	(Optional) The record status, active or inactive. By default, a new record is set to active (1). Set to 0 for inactive record, or 1 for active record.

Sample - Create new active record

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat -d
"action=create&status=1&title=create-new-sys-auth
&ips=10.10.31.112&unix_installation_dir=/root/tomcat/AppServer"
```

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>2019-11-05T07:51:48Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>55838</ID>
```

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

Sample - Update user created record, make status active

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/tomcat -d
"action=update&ids=30004,48007&status=1"
```

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>2019-11-07T01:43:39Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully updated</TEXT>
                <ID_SET>
                    <ID>30004</ID>
                </ID_SET>
            </BATCH>
            <BATCH>
                <TEXT>Successfully updated</TEXT>
                <ID_SET>
                    <ID>48007</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Scan Option Profile Import/Export API - enable Tomcat Server instance discovery and auto record creation

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

We've added new tags and definitions to the XSD used by the Scan Option Profile Import/Export API to support new capabilities. There were no changes to input parameters.

XSD update (option_profiles.xsd)

New enum value "Tomcat Server" in bold is added under AUTHENTICATION_TYPE element.

```
<xs:complexType name="AUTHENTICATION_TYPE_LISTType">
    <xs:sequence>
        <xs:element name="AUTHENTICATION_TYPE"
        maxOccurs="unbounded">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Apache Web Server"/>
                    <xs:enumeration value="IBM WebSphere App
                     Server"/>
                    <xs:enumeration value="Jboss Server"/>
                    <!-- added new enum Tomcat Server -->
                    <xs:enumeration value="Tomcat Server"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
    </xs:sequence>
</xs:complexType>
```

Sample - Export option profile for Tomcat instance discovery and record creation

In this sample, the option "Allow instance discovery and record creation" is enabled.

API request:

```
curl -u username:password -H "X-Requested-With: curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/?action=export&option_profile_id=2788516"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788516</ID>
      <GROUP_NAME><![CDATA[Apache_Discovery_OP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2019-11-04T06:37:50Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <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_D
ISCOVERY>
      </PERFORMANCE>
      <SYSTEM_AUTH_RECORD>
        <ALLOW_AUTH_CREATION>
          <AUTHENTICATION_TYPE_LIST>
            <AUTHENTICATION_TYPE>Tomcat Server
            </AUTHENTICATION_TYPE>
```

```
            </AUTHENTICATION_TYPE_LIST>
          </ALLOW_AUTH_CREATION>
        </SYSTEM_AUTH_RECORD>
        <FILE_INTEGRITY_MONITORING>
          <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
        </FILE_INTEGRITY_MONITORING>
        <CONTROL_TYPES>
          <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
          <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
        </CONTROL_TYPES>
      </SCAN>
      <ADDITIONAL>
        <HOST_DISCOVERY>
          <TCP_PORTS>
            <STANDARD_SCAN>1</STANDARD_SCAN>
          </TCP_PORTS>
          <UDP_PORTS>
            <STANDARD_SCAN>1</STANDARD_SCAN>
          </UDP_PORTS>
          <ICMP>1</ICMP>
        </HOST_DISCOVERY>
        <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_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 - Export option profile Include system created auth records and use User created record on duplicate option enabled

In this sample, the option “Include system created authentication records in scans” is enabled. Also, if there are 2 records with the same instance configuration, use the “User created record” is set. In the output, you’ll see ON_DUPLICATE_USE_USER_AUTH is set to 1.

API request:

```
curl -u username:password -H "X-Requested-With: curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/?action=export&option_profile_id=2788517"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788517</ID>
      <GROUP_NAME><![CDATA[apache_UCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2019-11-04T06:41:37Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <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_D
ISCOVERY>
      </PERFORMANCE>
```

```
        <SYSTEM_AUTH_RECORD>
          <INCLUDE_SYSTEM_AUTH>
            <ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
          </INCLUDE_SYSTEM_AUTH>
        </SYSTEM_AUTH_RECORD>
         <FILE_INTEGRITY_MONITORING>
           <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
         </FILE_INTEGRITY_MONITORING>
         <CONTROL_TYPES>
           <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
           <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
         </CONTROL_TYPES>
       </SCAN>
       <ADDITIONAL>
         <HOST_DISCOVERY>
           <TCP_PORTS>
             <STANDARD_SCAN>1</STANDARD_SCAN>
           </TCP_PORTS>
           <UDP_PORTS>
             <STANDARD_SCAN>1</STANDARD_SCAN>
           </UDP_PORTS>
           <ICMP>1</ICMP>
         </HOST_DISCOVERY>
         <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_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 - Export option profile with Include system created auth records and use System created record on duplicate

In this sample, the option “Include system created authentication records in scans” is enabled. Also, if there are 2 records with the same instance configuration, use the “System created record” is set. In the output, you’ll see ON_DUPLICATE_USE_SYSTEM_AUTH is set to 1.

API request:

```
curl -u username:password -H "X-Requested-With: curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/?action=export&option_profile_id=2788518"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788518</ID>
      <GROUP_NAME><![CDATA[apache_SCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2019-11-04T06:43:44Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <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_D
ISCOVERY>
```

```
      </PERFORMANCE>
      <SYSTEM_AUTH_RECORD>
        <INCLUDE_SYSTEM_AUTH>
          <ON_DUPLICATE_USE_SYSTEM_AUTH>1</ON_DUPLICATE_USE_SYSTEM_AUTH>
        </INCLUDE_SYSTEM_AUTH>
      </SYSTEM_AUTH_RECORD>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_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>
```