Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.1

April 27, 2020 (Updated May 5, 2020)

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

What's New

Qualys API Server URL

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click here to identify your Qualys platform and get the API URL

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

Oracle Instance Discovery and System Record Creation

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

This release introduces instance discovery and auto record creation for Oracle authentication. This functionality is already available for other technologies like Apache Web Server, IBM WebSphere, JBoss and Tomcat. There are a few notable differences for Oracle though. When we auto discover Oracle instances, we'll discover the target configuration for each instance but not the login credentials. We've introduced a new configuration called "Oracle System Record Template" that you'll use to provide Oracle login credentials for system created records. You'll create the system record template and then select it in the option profile used for discovery scans. The template is linked automatically to the system created records created as a result of the scan.

Benefits

- We'll auto discover Oracle instances on each scanned host and create authentication records for those instances. We support auto discovery and system record creation for Oracle instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running Oracle.

- When we create Oracle authentication records for discovered instances, we'll insert the credentials from the Oracle system record template you selected in the option profile.

- You can easily rotate Oracle passwords. Simply edit the credentials in the Oracle system record template and all Oracle records linked to the template will be updated to use the new credentials with no additional scan or action by you.

- You can edit individual Oracle system created records and save them as user created. This allows you to change the credentials for individual records without changing the credentials for all records associated with a template.

How it works

Here's the basic flow for Oracle instance discovery and auto record creation.

1) Create an Oracle system record template and enter the login credentials you want to use for system created records.

2) Select the Oracle system record template in the compliance option profile you want to use for discovery scans.

3) Launch your discovery scan. Your scan results will list the auto discovered instances. You'll also see the template associated with each instance.

4) List your Oracle authentication records. For each system created record, you'll see the template associated with the record.

API changes

We made the following API changes to support this new functionality:

- When creating Oracle authentication records, you can specify the new input parameter "is_template" to indicate whether the new record is an Oracle system record template. Note that once you save a record as a template it cannot be converted to a regular Oracle record. Also, a regular Oracle record cannot be saved as a template. We also added the ability to specify whether an Oracle record is active or inactive using "status". During an update request you can specify the new input parameter "save_as_user_auth" to save a system created record as a user record.

- When listing Oracle authentication records, we added new input parameters to filter the output. For example, you can filter the list to only show Oracle system record templates, or list all records associated with a certain template ID or name. You can also filter the list by the status (active or inactive) and method of record creation (user created or system created). The XML output identifies whether each record is system created, is active, and is a template. We updated the Oracle Auth Record List Output DTD.

- When creating/updating option profiles you can now enable instance discovery and system record creation for the Oracle technology and specify the Oracle template by the template ID or name.

- When listing option profiles, the XML output identifies whether Oracle instance discovery and system record creation is enabled and the Oracle system record template ID and name selected in the profile. We updated the Option Profile Info DTD.

Create/Update Oracle Records

The following table shows new input parameters for creating/updating Oracle records.

Parameter	Description
is_template={0|1}	(Optional for create request, not valid for update request) By default, a new record is a regular Oracle record. Specify 1 to create an Oracle system record template. You must also specify login credentials, which are described below.
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. (This parameter applies to system created and user created Oracle records. It cannot be specified for Oracle system record templates.)

Parameter	Description
save_as_user_auth={0|1}	(Optional for update request, not valid for create request) Specify 1 to update a system created record and save it as a user created record. If another Oracle record already exists with the same IP address and target configuration then an error will be returned. (This parameter applies only to system created Oracle records. It cannot be specified for user created Oracle records and it cannot be specified for Oracle system record templates.)
Login credentials	
login_type={basic|vault}	(Optional) The login type is basic by default. You can choose vault (for vault based authentication).
username={value}	(Required to create record, optional to update record) The username to be used for authentication to Oracle server.
password={value}	(Required to create record, optional to update record) The password to be used for authentication to Oracle server.
vault_type={value}	(Required to create record when login_type=vault) The vault type to be used for authentication.
vault_id={value}	(Required to create record when login_type=vault) The vault ID from where you want to retrieve the password. Certain vaults support this capability.
{vault parameters}	(Required to create record when login_type=vault) Vault specific parameters required depend on the vault type you've selected. See the Qualys API (VM, PC) User Guide for vault parameters.

Sample create Oracle record

This sample creates an Oracle system record template by using is_template=1.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&is_template=1&title=OracleRecordTemplate&username=OracleUs
er&password=Password"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T18:43:59Z</DATETIME>
```

```
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2237956</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample create Oracle record with vault

In this sample we're creating an Oracle system record template record using a vault.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&is_template=1&title=Oracle_template_vault&username=usernam
e&login_type=vault&vault_id=1775541&vault_type=HashiCorp&secret_kv_name=T
est&secret_kv_key=1234"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T18:43:59Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>2238287</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample update Oracle record

This sample updates an Oracle system record template to change the username.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=2237956&username=updatedUser"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-22T23:23:53Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>2237956</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample update Oracle record to save as user record

This sample updates a system created Oracle record to save it as a user record.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=2238696&title=title&save_as_user_auth=1&username=usern
ame&password=Password&sid=sid"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-27T00:26:26Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
```

```
          <ID_SET>
            <ID>2238696</ID>
          </ID_SET>
        </BATCH>
      </BATCH_LIST>
    </RESPONSE>
  </BATCH_RETURN>
```

List Oracle Authentication Records

The following table shows new input parameters when listing Oracle records.

Parameter	Description
template_auth_id={value}	(Optional) Specify the template ID for an Oracle system record template to only show Oracle records associated with the specified template.
template_auth_name={value}	(Optional) Specify the template name for an Oracle system record template to only show Oracle records associated with the specified template.
is_template={0|1}	(Optional) By default, template records and regular Oracle records are listed. Set to 0 to list only regular Oracle records or set to 1 to list only Oracle system record templates.
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 Oracle record

This sample shows details for a single Oracle record specified by ID. The XML output identifies whether the record is system created, is active and is a template. In this example, the record listed is not system created. It is active and it is a template record.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&ids=2237956"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/auth_oracle_list_out
put.dtd">
```

```
<AUTH_ORACLE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-23T18:44:27Z</DATETIME>
    <AUTH_ORACLE_LIST>
      <AUTH_ORACLE>
        <ID>2237956</ID>
        <TITLE><![CDATA[OracleRecordTemplate]]></TITLE>
        <USERNAME><![CDATA[OracleUser]]></USERNAME>
        <CREATED>
          <DATETIME>2020-04-23T18:43:59Z</DATETIME>
          <BY>rey_pt11</BY>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-04-23T18:43:59Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>1</IS_TEMPLATE>
        <COMMENTS><![CDATA[my comments]]></COMMENTS>
      </AUTH_ORACLE>
    </AUTH_ORACLE_LIST>
  </RESPONSE>
</AUTH_ORACLE_LIST_OUTPUT>
```

Sample list Oracle system record templates

This sample lists only Oracle system record templates by using the filter is_template=1.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&is_template=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/auth_oracle_list_out
put.dtd">
<AUTH_ORACLE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-23T18:53:18Z</DATETIME>
    <AUTH_ORACLE_LIST>
      <AUTH_ORACLE>
        <ID>2237956</ID>
        <TITLE><![CDATA[OracleRecordTemplate]]></TITLE>
        <USERNAME><![CDATA[OracleUser]]></USERNAME>
        <WINDOWS_OS_CHECKS>0</WINDOWS_OS_CHECKS>
```

```
          <UNIX_OPATCH_CHECKS>0</UNIX_OPATCH_CHECKS>
          <UNIX_OS_CHECKS>0</UNIX_OS_CHECKS>
          <CREATED>
            <DATETIME>2020-04-23T18:43:59Z</DATETIME>
            <BY>rey_pt11</BY>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2020-04-23T18:43:59Z</DATETIME>
          </LAST_MODIFIED>
          <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
          <IS_ACTIVE>1</IS_ACTIVE>
          <IS_TEMPLATE>1</IS_TEMPLATE>
          <COMMENTS><![CDATA[my comments]]></COMMENTS
        </AUTH_ORACLE>
      </AUTH_ORACLE_LIST>
    </RESPONSE>
</AUTH_ORACLE_LIST_OUTPUT>
```

Sample list Oracle records with certain template ID

This sample lists active, system created Oracle records associated with the template ID 2237327.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&is_system_created=1&template_auth_id=2237327&status=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/auth_oracle_list_out
put.dtd">
<AUTH_ORACLE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-23T19:26:38Z</DATETIME>
    <AUTH_ORACLE_LIST>
      <AUTH_ORACLE>
        <ID>2237334</ID>
        <TITLE><![CDATA[Oracle [System Created] - 72019]]></TITLE>
        <USERNAME><![CDATA[QUALYS_SCAN]]></USERNAME>
        <SID><![CDATA[ora11107]]></SID>
        <PORT>1521</PORT>
        <IP_SET>
          <IP>10.10.30.173</IP>
        </IP_SET>
        <WINDOWS_OS_CHECKS>0</WINDOWS_OS_CHECKS>
```

```
        <UNIX_OPATCH_CHECKS>0</UNIX_OPATCH_CHECKS>
        <UNIX_OS_CHECKS>1</UNIX_OS_CHECKS>
        <UNIX_OS_OPTIONS>

<UNIX_ORA_HOME_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1]]></UNIX
_ORA_HOME_PATH>
          <UNIX_INIT_ORA_PATH><![CDATA[[IGNORED]]]></UNIX_INIT_ORA_PATH>

<UNIX_SPFILE_ORA_PATH><![CDATA[[IGNORED]]]></UNIX_SPFILE_ORA_PATH>

<UNIX_LISTENER_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/netw
ork/admin/listener.ora]]></UNIX_LISTENER_ORA_PATH>

<UNIX_SQLNET_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/networ
k/admin/sqlnet.ora]]></UNIX_SQLNET_ORA_PATH>

<UNIX_TNSNAMES_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/netw
ork/admin/tnsnames.ora]]></UNIX_TNSNAMES_ORA_PATH>
          <UNIX_INVPTRLOC_PATH><![CDATA[]]></UNIX_INVPTRLOC_PATH>
        </UNIX_OS_OPTIONS>
        <CREATED>
          <DATETIME>2020-04-22T20:57:00Z</DATETIME>
        </CREATED>
        <LAST_MODIFIED>
          <DATETIME>2020-04-22T20:57:00Z</DATETIME>
        </LAST_MODIFIED>
        <IS_SYSTEM_CREATED>1</IS_SYSTEM_CREATED>
        <IS_ACTIVE>1</IS_ACTIVE>
        <IS_TEMPLATE>0</IS_TEMPLATE>
        <TEMPLATE>
          <ID>2237327</ID>
          <TITLE>OracleTemplate_QUALYS_SCAN</TITLE>
        </TEMPLATE>
        <COMMENTS><![CDATA[System created Oracle auth record using scan
data with history ID 10898215.]]></COMMENTS>
      </AUTH_ORACLE>
    </AUTH_ORACLE_LIST>
  </RESPONSE>
</AUTH_ORACLE_LIST_OUTPUT>
```

Sample list Oracle records with certain template name

This sample lists active, system created Oracle records associated with the template name "OracleTemplate".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=list&is_system_created=1&template_auth_name=OracleTemplate_123&st
atus=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_ORACLE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/oracle/auth_oracle_list_out
put.dtd">
<AUTH_ORACLE_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-23T19:26:38Z</DATETIME>
    <AUTH_ORACLE_LIST>
      <AUTH_ORACLE>
        <ID>2237334</ID>
        <TITLE><![CDATA[Oracle [System Created] - 72019]]></TITLE>
        <USERNAME><![CDATA[QUALYS_SCAN]]></USERNAME>
        <SID><![CDATA[ora11107]]></SID>
        <PORT>1521</PORT>
        <IP_SET>
          <IP>10.10.30.173</IP>
        </IP_SET>
        <WINDOWS_OS_CHECKS>0</WINDOWS_OS_CHECKS>
        <UNIX_OPATCH_CHECKS>0</UNIX_OPATCH_CHECKS>
        <UNIX_OS_CHECKS>1</UNIX_OS_CHECKS>
        <UNIX_OS_OPTIONS>

<UNIX_ORA_HOME_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1]]></UNIX
_ORA_HOME_PATH>
          <UNIX_INIT_ORA_PATH><![CDATA[[IGNORED]]]></UNIX_INIT_ORA_PATH>

<UNIX_SPFILE_ORA_PATH><![CDATA[[IGNORED]]]></UNIX_SPFILE_ORA_PATH>

<UNIX_LISTENER_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/netw
ork/admin/listener.ora]]></UNIX_LISTENER_ORA_PATH>

<UNIX_SQLNET_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/networ
k/admin/sqlnet.ora]]></UNIX_SQLNET_ORA_PATH>

<UNIX_TNSNAMES_ORA_PATH><![CDATA[/u01/app/oracle/product/11.1.0/db_1/netw
ork/admin/tnsnames.ora]]></UNIX_TNSNAMES_ORA_PATH>
```

```
            <UNIX_INVPTRLOC_PATH><![CDATA[]]></UNIX_INVPTRLOC_PATH>
          </UNIX_OS_OPTIONS>
          <CREATED>
            <DATETIME>2020-04-22T20:57:00Z</DATETIME>
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2020-04-22T20:57:00Z</DATETIME>
          </LAST_MODIFIED>
          <IS_SYSTEM_CREATED>1</IS_SYSTEM_CREATED>
          <IS_ACTIVE>1</IS_ACTIVE>
          <IS_TEMPLATE>0</IS_TEMPLATE>
          <TEMPLATE>
            <ID>2237327</ID>
            <TITLE>OracleTemplate_123</TITLE>
          </TEMPLATE>
          <COMMENTS><![CDATA[System created Oracle auth record using scan
data with history ID 10898215.]]></COMMENTS>
        </AUTH_ORACLE>
      </AUTH_ORACLE_LIST>
    </RESPONSE>
</AUTH_ORACLE_LIST_OUTPUT>
```

DTD update:

The following elements were added to the Oracle Authentication Record List Output DTD: IS_SYSTEM_CREATED, IS_ACTIVE, IS_TEMPLATE and TEMPLATE.

DTD: <platform>/api/2.0/fo/auth/oracle/auth_oracle_list_output.dtd

```
<!-- QUALYS AUTH_ORACLE_LIST_OUTPUT DTD -->
<!-- $Revision$ -->
<!ELEMENT AUTH_ORACLE_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_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_ORACLE_LIST (AUTH_ORACLE+)>
```

```
<!ELEMENT AUTH_ORACLE (ID, TITLE, USERNAME, (SID|SERVICENAME)?, PORT?,
IP_SET?, PC_ONLY?, WINDOWS_OS_CHECKS, WINDOWS_OS_OPTIONS?,
UNIX_OPATCH_CHECKS, UNIX_OS_CHECKS, UNIX_OS_OPTIONS?, NETWORK_ID?,
CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED?, IS_ACTIVE?, IS_TEMPLATE?,
TEMPLATE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT SID (#PCDATA)>
<!ELEMENT SERVICENAME (#PCDATA)>
<!ELEMENT PORT (#PCDATA)>
<!ELEMENT PC_ONLY (#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 IS_TEMPLATE (#PCDATA)>
<!ELEMENT TEMPLATE (ID, TITLE)>
<!ELEMENT COMMENTS (#PCDATA)>
...
```

Create/Update Option Profiles

The following table shows new and updated input parameters for option profiles. See the Qualys API (VM, PC) User Guide for details on other input parameters.

Parameter	Description
auto_auth_types={value}	(Optional to create or update option profile record) Specify the technologies for which you want to enable auto discover instances and system record creation. The valid values are: Apache Web Server, IBM WebSphere App Server, Jboss Server, Tomcat Server and Oracle. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.
oracle_template_id={value}	(Optional) The Template ID for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.

Parameter	Description
oracle_template_name={value}	(Optional) The Template Name for the Oracle system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=Oracle is specified, then oracle_template_id or oracle_template_name must also be specified.

Sample create option profile using template ID

In this sample we are creating an option profile with instance discovery and system record creation enabled for Oracle and we're using template ID 2237327.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=Profile-Auth-Ins-
Oracle&enable_auth_instance_discovery=1&auto_auth_types=Oracle&scan_ports
=targeted&oracle_template_id=2237327"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T19:12:10Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3305478</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample create option profile using template name

In this sample we are creating an option profile with instance discovery and system record creation enabled for Oracle and we're using template name "OracleTemplate".

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=Profile-Auth-Ins-
Oracle_1&enable_auth_instance_discovery=1&auto_auth_types=Oracle&scan_por
ts=targeted&oracle_template_name=OracleTemplate"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-23T19:19:09Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3305527</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample update option profile

In this sample we are updating an option profile to enable instance discovery and system record creation for Oracle.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=update&id=3307590&enable_auth_instance_discovery=1&auto_auth_type
s=Oracle&oracle_template_id=2247418"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-05-05T19:38:15Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>3307590</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

List Option Profiles

When you list option profiles, you'll see authentication type Oracle in the XML output when Oracle is selected in the option profile. You'll also see the Oracle system record template ID and name selected in the profile.

Sample list option profiles

In this sample we are listing a single option profile specified by ID. The XML output shows authentication type Oracle with the Oracle system record template ID and name.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&id=3305478"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>3305478</ID>
      <GROUP_NAME><![CDATA[Profile-Auth-Ins-Oracle]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Joe User (joe_user)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1449438</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2020-04-23T19:12:10Z</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_DISCOVER
Y>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>
          <HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
      </DISSOLVABLE_AGENT>
      <SYSTEM_AUTH_RECORD>
```

```
            <ALLOW_AUTH_CREATION>
              <AUTHENTICATION_TYPE_LIST>
                <AUTHENTICATION_TYPE>Oracle</AUTHENTICATION_TYPE>
              </AUTHENTICATION_TYPE_LIST>
              <ORACLE_AUTHENTICATION_TEMPLATE>
                <ID>2237327</ID>
                <TITLE>OracleTemplate123</TITLE>
              </ORACLE_AUTHENTICATION_TEMPLATE>
            </ALLOW_AUTH_CREATION>
          </SYSTEM_AUTH_RECORD>
        ...
      </OPTION_PROFILE>
    </OPTION_PROFILES>
```

DTD update:

The Option Profile Info DTD was updated to include the element ORACLE_AUTHENTICATION_TEMPLATE with the template ID and title.

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

```
...
<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
ORACLE_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT INCLUDE_SYSTEM_AUTH
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>

<!ELEMENT AUTHENTICATION_TYPE_LIST  (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>
...
```

Import/Export Option Profiles

When you export option profiles, you'll see authentication type Oracle in the XML output when Oracle is selected in the option profile. You'll also see the Oracle system record template ID and name selected in the profile.

Sample export option profile

In this sample we are exporting a single option profile specified by ID. The XML output shows authentication type Oracle with the Oracle system record template ID and name.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X GET
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/?act
ion=export&option_profile_id=3308884">OracleAutoAuthDiscovery/OptionProfi
leExport.xml
```

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>3308884</ID>
      <GROUP_NAME><![CDATA[OracleAutoDiscovery_qualys_scan]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Joe User (joe_user)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1449438</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2020-05-05T17:49:42Z</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_DISCOVER
Y>
      </PERFORMANCE>
      <DISSOLVABLE_AGENT>
        <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
        <PASSWORD_AUDITING_ENABLE>
          <HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
```

```
        </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
      </DISSOLVABLE_AGENT>
      <SYSTEM_AUTH_RECORD>
        <ALLOW_AUTH_CREATION>
          <AUTHENTICATION_TYPE_LIST>
            <AUTHENTICATION_TYPE>Oracle</AUTHENTICATION_TYPE>
          </AUTHENTICATION_TYPE_LIST>
          <ORACLE_AUTHENTICATION_TEMPLATE>
            <ID>2247418</ID>
            <TITLE>preOracle_Template_qualys_scan_new</TITLE>
          </ORACLE_AUTHENTICATION_TEMPLATE>
        </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_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

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

Sample import option profile

In this sample we are importing an option profile.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-05-05T18:32:01Z</DATETIME>
    <TEXT>Successfully imported Option profile for the subscription Id
1449438</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>3308891</KEY>
        <VALUE>OracleAutoDiscovery_qualys_scan_API</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Schema update:

The option_profiles.xsd schema is used to validate a proper format and required elements of the option profile XML file.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="OPTION_PROFILES" type="OPTION_PROFILESType"/>
...
    <xs:complexType name="ALLOW_AUTH_CREATIONType">
        <xs:sequence>
            <xs:element name="AUTHENTICATION_TYPE_LIST"
type="AUTHENTICATION_TYPE_LISTType"/>
            <xs:element name="ORACLE_AUTHENTICATION_TEMPLATE"
type="ORACLE_AUTHENTICATION_TEMPLATEType" />
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="INCLUDE_SYSTEM_AUTHType">
        <xs:choice>
```

```
            <xs:element name="ON_DUPLICATE_USE_USER_AUTH"
type="xs:boolean" fixed="1"/>
            <xs:element name="ON_DUPLICATE_USE_SYSTEM_AUTH"
type="xs:boolean" fixed="1"/>
        </xs:choice>
    </xs:complexType>
    <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"/>
                        <xs:enumeration value="Tomcat Server"/>
                        <xs:enumeration value="Oracle"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ORACLE_AUTHENTICATION_TEMPLATEType">
        <xs:sequence>
            <xs:element name="ID" type="xs:string"/>
            <xs:element name="TITLE" type="xs:string"/>
        </xs:sequence>
    </xs:complexType>
...
```

Asset Search Report - Change to Asset Group Value in Output for DNS hosts

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

Now when you run the Asset Search Report for DNS hosts, you'll see a comma separated list of asset groups the host belongs to. In previous releases you'd only see the All group listed for DNS hosts. The report output will show the associated groups only if the DNS host is found in the asset group specified in the API request.

Sample report in XML format

In this sample we are creating an Asset Search Report with DNS hosts in XML format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"action=search&output_format=xml&asset_groups=AG1&echo_request=1&
display_ag_titles=1&dns_name=10-10&dns_modifier=beginning+with"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE ASSET_SEARCH_REPORT SYSTEM
"https://qualysapi.qualys.com/asset_search_report_v2.dtd">

<ASSET_SEARCH_REPORT>
<HEADER>
  <COMPANY><![CDATA[Qualys]]></COMPANY>
  <USERNAME>John Doe</USERNAME>
  <GENERATION_DATETIME>2020-04-24T09:15:25Z</GENERATION_DATETIME>
  <TOTAL>1</TOTAL>
  <FILTERS>
    <ASSET_GROUPS>
      <ASSET_GROUP_TITLE><![CDATA[AG1]]></ASSET_GROUP_TITLE>
    </ASSET_GROUPS>
    <FILTER_DNS><![CDATA[Beginning With 10-10]]></FILTER_DNS>
    <FILTER_DISPLAY_AG_TITLES><![CDATA[1]]></FILTER_DISPLAY_AG_TITLES>
  </FILTERS>
</HEADER>

<HOST_LIST>
  <HOST>
    <IP><![CDATA[10.10.10.3]]></IP>
    <TRACKING_METHOD>IP address</TRACKING_METHOD>
```

```
      <DNS><![CDATA[10-10-10-3.qualys.com]]></DNS>
      <NETBIOS><![CDATA[SYS_10_10_10_3]]></NETBIOS>
      <ASSET_GROUPS>
        <ASSET_GROUP_TITLE><![CDATA[AG1]]></ASSET_GROUP_TITLE>
        <ASSET_GROUP_TITLE><![CDATA[AG2]]></ASSET_GROUP_TITLE>
        <ASSET_GROUP_TITLE><![CDATA[AG3]]></ASSET_GROUP_TITLE>
        <ASSET_GROUP_TITLE><![CDATA[All]]></ASSET_GROUP_TITLE>
      </ASSET_GROUPS>
      <LAST_SCAN_DATE>2015-10-20T10:35:58Z</LAST_SCAN_DATE>
      <FIRST_FOUND_DATE>2019-07-10T06:55:22Z</FIRST_FOUND_DATE>
    </HOST>
  </HOST_LIST>
  </ASSET_SEARCH_REPORT>
```

Sample report in CSV format

In this sample we are creating an Asset Search Report with DNS hosts in CSV format.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"action=search&output_format=csv&asset_groups=10.10.10.3&echo_request=1&
display_ag_titles=1&&dns_name=10-10&dns_modifier=beginning+with"
"https://qualysapi.qualys.com/api/2.0/fo/report/asset/
```

CSV output:

Create your own report to see all the columns in the CSV output.

Company	UserName	ReportDate	AssetGroups	IPAddress	DNSHostname	EC2InstanceID	NetBIOSHostname	TargetTra	EC2Instan	TargetOperatingSystem
Qualys	user name	2020-04-24T09:1	AG1		Beginning With 10-10					
IP	DNSHostname	NetBIOSHostnar	OperatingSystem	OSCPE	Port/Service/Default S	TrackingMethod	LastScanDate	LastComp	First Foun	AssetGroups
10.10.10.3	10-10-10-3.bogus.tld	SYS_10_10_10_3				IP address	2015-10-20T10:35:5		2019-07-1	AG1, AG2, AG3, All

Host-Based Scan Reports to Show Associated Asset Groups Information for Hosts

APIs affected	/api/2.0/fo/report/
New or Updated API	Updated
DTD or XSD changes	No
APIs affected	/api/2.0/fo/report/template/scan/
New or Updated API	Updated
DTD or XSD changes	No

You will now see the list of asset groups associated with each host in the Host-based Scan Report output generated in these formats: CSV, MHT, PDF, HTML, and DOCX. The report in XML format already shows this information.

We added a new Info Key "host_ag_details" in the Scan Template API. When creating or updating the template for host based findings, set this key to 1 to include asset groups information associated with the hosts in the host-based scan report.

Sample - Create Scan Template with the" host_ag_details" Key Enabled

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -H
"Content-type: text/xml" --data-binary @scan_export.xml
"https://qualysapi.qualys.com/api/2.0/fo/report/template/scan/?act
ion=create&report_format=xml"
```

scan_export.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
 <SCANTEMPLATE>
  <TITLE>
   <INFO key="owner"><![CDATA[quays_dp1]]></INFO>
 </TITLE>
 <TARGET>
  <INFO key="scan_selection"><![CDATA[HostBased]]></INFO>
  <INFO key="ips"><![CDATA[10.200.200.200]]></INFO>
 </TARGET>
 <DISPLAY>
  <INFO key="display_text_summary"><![CDATA[1]]></INFO>
  <INFO key="sort_by"><![CDATA[host]]></INFO>
  <INFO key="cvss"><![CDATA[all]]></INFO>
  <INFO key="host_details"><![CDATA[1]]></INFO>
  <INFO key="host_ag_details"><![CDATA[1]]></INFO>
</DISPLAY>
....
```

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>2029-04-28T05:41:32Z</DATETIME>
 <CODE>Scan Report Template(s) Created Successfully[89876]</CODE>
 <TEXT></TEXT>
 </RESPONSE>
</SIMPLE_RETURN>
```

Sample report

Here's a sample scan report in CSV format.

API request:

```
curl -H "X-Requested-With: Curl Sample"-d
"action=launch&report_type=Scan&output_format=csv&template_id=89876
&report_title=APILaunchReport_SCAN"
"https://qualysapi.qualys.com/api/2.0/fo/report/"
```

CSV output:

14												
15	IP	Network	DNS	NetBIOS	QG Host ID	IP Interfac	Tracking M	OS	IP Status	Port	Protocol	Associated AGs
16	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
17	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
18	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
19	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
20	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
21	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
22	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
23	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
24	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
25	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
26	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
27	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
28	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	22	tcp	AG1, AG2, AG3
29	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
30	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	443	tcp	AG1, AG2, AG3
31	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	443	tcp	AG1, AG2, AG3
32	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
33	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
34	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	443	tcp	AG1, AG2, AG3
35	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	443	tcp	AG1, AG2, AG3
36	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanr	443	tcp	AG1, AG2, AG3
37	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
38	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
39	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3
40	10.200.200.200	Global Default	10-200-200-200.bogus.tld				IP	VMware E	host scanned, found vuln			AG1, AG2, AG3

Remediation Information Available in Policy Import and Export of UDCs

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

You can now import or export remediation information of your UDC policies using an xml file.

Sample - Export policy with UDCs into XML file showing remediation information

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=export&id=1801961&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
  <RESPONSE>
    <DATETIME>2020-04-22T16:47:24Z</DATETIME>
<POLICY>
    <TITLE><![CDATA[RHEL_8]]></TITLE>
    <EXPORTED><![CDATA[2020-04-22T16:47:24Z]]></EXPORTED>
    <COVER_PAGE><![CDATA[]]></COVER_PAGE>
    <STATUS><![CDATA[active]]></STATUS>
    <TECHNOLOGIES total="1">
        <TECHNOLOGY>
            <ID>217</ID>
            <NAME>Red Hat Enterprise Linux 8.x</NAME>
        </TECHNOLOGY>
    </TECHNOLOGIES>
    <SECTIONS total="2">
       ...
        <SECTION>
            <NUMBER>2</NUMBER>
            <HEADING><![CDATA[UDC]]></HEADING>
            <CONTROLS total="6">
                <USER_DEFINED_CONTROL>
                    <ID>100028</ID>
                    <UDC_ID>c50922a1-1482-df3f-83e2-bb96c99ffc48</UDC_ID>
```

```
                    <CHECK_TYPE>Unix File/Directory Permission</CHECK_TYPE>
                      <CATEGORY>
                          <ID>3</ID>
                        <NAME><![CDATA[Access Control Requirements]]></NAME>
                      </CATEGORY>
                      <SUB_CATEGORY>
                          <ID>1007</ID>
                          <NAME><![CDATA[Authentication/Passwords]]></NAME>
                      </SUB_CATEGORY>
                      <STATEMENT><![CDATA[Basic File/Directory Permission-
UNIX-RHEL_8]]></STATEMENT>
                      <CRITICALITY>
                          <LABEL><![CDATA[SERIOUS]]></LABEL>
                          <VALUE>3</VALUE>
                      </CRITICALITY>
                      <COMMENT><![CDATA[Basic File/Directory
Permission]]></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>
                          <FILE_PATH><![CDATA[/etc/profile]]></FILE_PATH>
                          <DATA_TYPE>String</DATA_TYPE>
                          <DESCRIPTION><![CDATA[File/Directory
Permission]]></DESCRIPTION>
                      </SCAN_PARAMETERS>
                      <TECHNOLOGIES total="1">
                          <TECHNOLOGY>
                              <ID>217</ID>
                              <NAME>Red Hat Enterprise Linux 8.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_permission.1007079</K><OP>re</OP><V><!
[CDATA[.*]]></V></DP></CTRL></EVALUATE>
                              <RATIONALE><![CDATA[Basic File/Directory
Permission-UNIX]]></RATIONALE>
                              <REMEDIATION><![CDATA[]]></REMEDIATION>
                              <DATAPOINT>
                                  <CARDINALITY>no cd</CARDINALITY>
                                  <OPERATOR>re</OPERATOR>
                                  <DEFAULT_VALUES total="1">

<DEFAULT_VALUE><![CDATA[.*]]></DEFAULT_VALUE>
                                  </DEFAULT_VALUES>
                              </DATAPOINT>
                          </TECHNOLOGY>
                      </TECHNOLOGIES>
                      <REFERENCE_LIST/>
                  </USER_DEFINED_CONTROL>
```

```
                <USER_DEFINED_CONTROL>
                    <ID>100029</ID>
                    <UDC_ID>9da2c628-fb7d-50cf-8230-6f3ff59172a8</UDC_ID>
                   <CHECK_TYPE>Unix File/Directory Existence</CHECK_TYPE>
                    <CATEGORY>
                        <ID>3</ID>
                      <NAME><![CDATA[Access Control Requirements]]></NAME>
                    </CATEGORY>
                    <SUB_CATEGORY>
                        <ID>1007</ID>
                        <NAME><![CDATA[Authentication/Passwords]]></NAME>
                    </SUB_CATEGORY>
                    <STATEMENT><![CDATA[Basic File/Directory Existence-
UNIX-RHEL_8]]></STATEMENT>
                    <CRITICALITY>
                        <LABEL><![CDATA[SERIOUS]]></LABEL>
                        <VALUE>3</VALUE>
                    </CRITICALITY>
                    <COMMENT><![CDATA[File/Directory Existence - this is
in comment section]]></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>
                        <FILE_PATH><![CDATA[/etc/profile]]></FILE_PATH>
                        <DATA_TYPE>Boolean</DATA_TYPE>
                        <DESCRIPTION><![CDATA[test]]></DESCRIPTION>
                    </SCAN_PARAMETERS>
                    <TECHNOLOGIES total="1">
                        <TECHNOLOGY>
                            <ID>217</ID>
                            <NAME>Red Hat Enterprise Linux 8.x</NAME>

<EVALUATE><CTRL><DP><K>custom.file_dir_exist.1007080</K><L>2</L><V>false<
/V></DP></CTRL></EVALUATE>
                            <RATIONALE><![CDATA[File/Directory Existence-
this is in rationale section under default value]]></RATIONALE>
                            <REMEDIATION><![CDATA[]]></REMEDIATION>
                            <DATAPOINT>
                                <CARDINALITY>no cd</CARDINALITY>
                                <OPERATOR>no op</OPERATOR>
                                <DEFAULT_VALUES total="1">
                                    <DEFAULT_VALUE>true</DEFAULT_VALUE>
                                </DEFAULT_VALUES>
                            </DATAPOINT>
                        </TECHNOLOGY>
                    </TECHNOLOGIES>
                    <REFERENCE_LIST/>
```

```
                </USER_DEFINED_CONTROL>
            ...
          </SECTION>
      </SECTIONS>
</POLICY>
  </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Sample - Import policy with UDCs having remediation information using xml file

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -H Content-
Type:text/xml --data-binary "@UDC_with_Remedy_20200422.xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/?action=import
&title=Policy1&create_user_controls=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-22T22:51:16Z</DATETIME>
    <TEXT>Successfully imported compliance policy</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1867541</VALUE>
      </ITEM>
      <ITEM>
        <KEY>TITLE</KEY>
        <VALUE>Policy1</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

DTD update:

DTD: <platform API server>/api/2/fo/compliance/policy/policy_export_output.dtd

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

...

<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT IS_CONTROL_DISABLE (#PCDATA)>
<!ELEMENT REFERENCE_TEXT (#PCDATA)>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY*)>
<!ATTLIST TECHNOLOGIES total CDATA #IMPLIED>
<!ELEMENT TECHNOLOGY (ID, NAME?, EVALUATE?, RATIONALE?, REMEDIATION?,
DATAPOINT?, USE_SCAN_VALUE?, DB_QUERY?, DESCRIPTION?)>
<!ELEMENT NAME (#PCDATA)>
<!ELEMENT EVALUATE (CTRL*)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT CTRL (AND|OR|NOT|DP)+>
<!ELEMENT AND (AND|OR|NOT|DP)+>
<!ELEMENT OR (AND|OR|NOT|DP)+>
<!ELEMENT NOT (AND|OR|NOT|DP)+>
<!ELEMENT DP (K|OP|CD|L|V|FV|DBCOL|DT)+>
<!ELEMENT K (#PCDATA)>
<!ELEMENT OP (#PCDATA)>
<!ELEMENT CD (#PCDATA)>
<!ELEMENT L (#PCDATA)>
<!ELEMENT V (#PCDATA)>
<!ELEMENT FV (#PCDATA)>
<!ATTLIST FV set CDATA #IMPLIED>
<!ELEMENT DBCOL (#PCDATA)>
<!ELEMENT DT (#PCDATA)>

...
<!ELEMENT APPENDIX (OP_ACRONYMS, DATA_POINT_ACRONYMS+)>
<!ELEMENT OP_ACRONYMS (OP+)>
<!ATTLIST OP id CDATA #IMPLIED>
<!ELEMENT DATA_POINT_ACRONYMS (DP+)>
<!ATTLIST K id CDATA #IMPLIED>
<!ATTLIST FV id CDATA #IMPLIED>

<!-- EOF -->
```

More Regions Supported for VM, Compliance and Cloud Perimeter Scans

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

It's now possible to launch a vulnerability scan, compliance scan for EC2 instances or cloud perimeter scan in three new regions: Stockholm, Hong Kong and Bahrain. You need to set the input parameter to the respective region and include it in the scan request.

Input Parameters

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

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

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

Sample - Launch On-demand VM Scan on EC2 instances in Stockholm region

Sample - Launch On-demand Compliance Scan on EC2 instances in Stockholm region

Sample - Launch On-demand Cloud Perimeter Scan in Hong Kong region for VM

Sample - Launch On-demand Cloud Perimeter Scan in Bahrain region for PC

Sample - Launch Scheduled VM Scan on EC2 instances in Hong Kong region

Sample - Launch Scheduled Cloud Perimeter Scan in Bahrain region for VM

Sample - Launch Scheduled Cloud Perimeter Scan in Bahrain region for PC

Sample - Launch On-demand VM Scan on EC2 instances in Stockholm region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/scan/?action=launch&scan_title=A
PI_OnDemand_EC2&target_from=tags&tag_set_by=name&tag_include_selector=any
&tag_set_include=StockHolm&connector_name=AWS_Connector&ec2_endpoint=eu-
north-1&option_title=Initial Options&iscanner_name=StockHolm_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-20T04:59:43Z</DATETIME>
    <TEXT>New vm scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6755964</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>scan/1587358782.55964</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch On-demand Compliance Scan on EC2 instances in Stockholm region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/?action=launch&s
can_title=API_OnDemand_EC2_PC&target_from=tags&tag_set_by=name&tag_includ
e_selector=any&tag_set_include=StockHolm&connector_name=AWS_Connector&ec2
_endpoint=eu-north-1&option_title=Initial PC
Options&iscanner_name=StockHolm_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-20T05:01:38Z</DATETIME>
    <TEXT>New compliance scan launched</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6755969</VALUE>
      </ITEM>
      <ITEM>
        <KEY>REFERENCE</KEY>
        <VALUE>compliance/1587358897.55969</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch On-demand Cloud Perimeter Scan in Hong Kong region for VM

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?" -d
"action=create&module=vm&active=1&schedule=now&tag_set_include=Hong
Kong&tag_set_by=name&platform_type=vpc_peered&option_id=646656&connector_
name=AWS_Connector&region_code=ap-east-1&iscanner_id=HongKong_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
```

```
  <RESPONSE>
    <DATETIME>2020-04-20T05:06:12Z</DATETIME>
    <TEXT>Scan has been created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2427409</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch On-demand Cloud Perimeter Scan in Bahrain region for PC

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?" -d
action=create&module=pc&active=1&schedule=now&tag_set_include=Bahrain
&tag_set_by=name&platform_type=vpc_peered&option_id=646660&connector_name
=AWS_Connector&region_code=me-south-1&iscanner_id=Bahrain_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-20T05:03:15Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2427408</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch Scheduled VM Scan on EC2 instances in Hong Kong region

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"https://qualysapi.qualys.com/api/2.0/fo/schedule/scan/?action=create&sca
n_title=API_Schedule_EC2_Hong
Kong&target_from=tags&tag_set_by=name&tag_include_selector=any&tag_set_in
clude=Hong Kong&connector_name=AWS_Connector&ec2_endpoint=ap-east-
1&active=1&occurrence=daily&start_date=04/20/2020&start_hour=11&start_min
ute=00&time_zone_code=IN&option_title=Initial
Options&frequency_days=364&end_after=1&observe_dst=no&iscanner_name=HongK
ong_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-20T05:03:15Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2427408</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch Scheduled Cloud Perimeter Scan in Bahrain region for VM

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?" -d
action=create&module=pc&active=1&schedule=now&tag_set_include=Bahrain
&tag_set_by=name&platform_type=vpc_peered&option_id=646660&connector_name
=AWS_Connector&region_code=me-south-1&iscanner_id=Bahrain_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
```

```
    <DATETIME>2020-04-20T05:03:15Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2427408</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Launch Scheduled Cloud Perimeter Scan in Bahrain region for PC

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl"
"https://qualysapi.qualys.com/api/2.0/fo/scan/cloud/perimeter/job/index.p
hp?" -d
action=create&module=pc&active=1&schedule=now&tag_set_include=Bahrain
&tag_set_by=name&platform_type=vpc_peered&option_id=646660&connector_name
=AWS_Connector&region_code=me-south-1&iscanner_id=Bahrain_Scanner"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2020-04-20T05:03:15Z</DATETIME>
    <TEXT>New scan scheduled successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>2427408</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Azure Key Vault Support for Palo Alto Network Firewall Authentication Records

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

With this release you can create and update authentication records for Palo Alto Network Firewall, using the Azure Key vault. Before creating the authentication record, you need to create the Azure Key vault record using Vaults API. See "Manage Vaults section in Chapter 6 - Vault Support" in the Qualys VM/PC API Guide for the list of parameters for creating Azure Key Vault record.

Input Parameters

Use these vault parameters to retrieve password from the Azure Key vault.

Parameter	Description
login_type={basic|vault}	Specify vault as login type.
vault_id={value}	(Required to create and update record when login_type=vault) Specify the ID of the Azure Key vault record.
vault_type={value}	(Required to create record when login_type=vault). Specify Azure Key as vault type.
ak_secret_name={value}	(Required to create record) The secret name assigned to the secret stored in the vault.

Sample - Create Palo Alto Network Firewall record, using Azure Key vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=create&title=palo4&ips=10.10.10.11&login_type=vault&username=root
&vault_type=Azure Key&vault_id=16034&ak_secret_name=root-secret"
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-04-15T01:02:32Z</DATETIME>
```

```
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>2444494</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Update Palo Alto Network Firewall record, using Azure Key vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=update&title=palo_alto&ips=10.10.10.11&login_type=vault&username=
root&vault_type=Azure Key&ids=2444494&vault_id=16034&ak_secret_name=root-
secret"
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.p04.eng.sjc01.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-04-15T01:08:29Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Updated</TEXT>
                <ID_SET>
                    <ID>2444494</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Palo Alto Network Firewall records with Azure Key vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl Sample" -d
"action=list&ids=2440695
"https://qualysapi.qualys.com/api/2.0/fo/auth/palo_alto_firewall/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_PALO_ALTO_FIREWALL_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.p04.eng.sjc01.qualys.com/api/2.0/fo/auth/palo_alto_fir
ewall/auth_palo_alto_firewall_list_output.dtd">
<AUTH_PALO_ALTO_FIREWALL_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-04-15T01:02:40Z</DATETIME>
        <AUTH_PALO_ALTO_FIREWALL_LIST>
            <AUTH_PALO_ALTO_FIREWALL>
                <ID>2444494</ID>
                ...
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[1865182]]>
                    </DIGITAL_VAULT_ID>
                    <DIGITAL_VAULT_TYPE>
                        <![CDATA[Azure Key]]>
                    </DIGITAL_VAULT_TYPE>
                    <DIGITAL_VAULT_TITLE>
                        <![CDATA[azure_key_ui]]>
                    </DIGITAL_VAULT_TITLE>
                    <VAULT_SECRET_NAME>
                        <![CDATA[root-secret]]>
                    </VAULT_SECRET_NAME>
                </DIGITAL_VAULT>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2020-04-15T01:02:32Z</DATETIME>
                    <BY>rey_pt10</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2020-04-15T01:02:32Z</DATETIME>
                </LAST_MODIFIED>
            </AUTH_PALO_ALTO_FIREWALL>
        </AUTH_PALO_ALTO_FIREWALL_LIST>
    </RESPONSE>
</AUTH_PALO_ALTO_FIREWALL_LIST_OUTPUT>
```

Network Element Added to Compliance Scan Result Output DTD

APIs affected	/api/2.0/fo/scan/compliance/?action=fetch
New or Updated API	Updated (DTD change only)
DTD or XSD changes	Yes

We updated the compliance_scan_result_output.dtd to include the Network element in Host Info. You will see this element in the API output when the Network Support feature is enabled.

Updated DTD

<base_url>/api/2.0/fo/scan/compliance/compliance_scan_result_output.dtd

```
...
<AUTH_SCAN_ISSUES>
        <AUTH_SCAN_FAILED>
          <HOST_INFO>
            <DNS><![CDATA[com-sql-24-67]]></DNS>
            <IP><![CDATA[10.10.24.67]]></IP>
            <NETBIOS><![CDATA[COM-SQL-24-67]]></NETBIOS>
            <INSTANCE><![CDATA[os]]></INSTANCE>
            <CAUSE><![CDATA[Unable to complete Windows login for
host=10.10.24.67, user=administrator, domain=, ntstatus=22220016]]>
            </CAUSE>
            <NETWORK><![CDATA[Global Default Network]]></NETWORK>
          </HOST_INFO>
        </AUTH_SCAN_FAILED>
 </AUTH_SCAN_ISSUES>
...
```

New Support for ARCON PAM (Privilege Access Management) Vault

APIs affected	/api/2.0/fo/vault/index.php/
New or Updated API	Updated
DTD or XSD changes	No
APIs affected	/api/2.0/fo/auth/windows/ /api/2.0/fo/auth/unix/ /api/2.0/fo/auth/greenplum/ /api/2.0/fo/auth/ms_sql/ /api/2.0/fo/auth/mysql/ /api/2.0/fo/auth/mariadb/ /api/2.0/fo/auth/mongodb/ /api/2.0/fo/auth/oracle/ /api/2.0/fo/auth/postgresql/ /api/2.0/fo/auth/sybase/ /api/2.0/fo/auth/ibm_db2/
New or Updated API	Updated (DTD change only)
DTD or XSD changes	Yes

This new vault type can be used to retrieve authentication credentials from an ARCON PAM vault. We updated the authentication vault API (create, update, list, view) and the authentication record API (create, update, list) to support the new vault type.

Authentication Vault API

You can now create, update, list and view authentication records for ARCON PAM vaults.

Create/Update ARCON PAM Authentication Vault

Use the parameter “action=create” or “action=update” to create/update a new ARCON PAM vault in your account.

Parameter	Description
action=create|update	(Required)
id={value}	(Required to update) A vault ID
title={value}	(Required to create and optional to update vault) The vault title
type={value}	(Required to create and optional to update vault) Specify type=Arcon PAM
comments={value}	(Optional) User defined comments.

Parameter	Description
url={value}	(Required to create and optional to update vault) The HTTP or HTTPS URL to access the ARCON PAM Vault API. The HTTPS URL is required if the ssl_verify parameter is set 1.
ssl_verify={0|**1**}	(Required to create and optional to update vault) When set to 1 (the default), our service will verify the SSL certificate of the web server to make sure the certificate is valid and trusted. When set to 0, our service will not verify the certificate of the web server.
username	(Required to create and optional to update vault) A username required to access the vault.
password	(Required to create and optional to update vault) A password required to access the vault.

Sample - Create ARCON PAM Vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&type=Arcon PAM&title=My ARCON PAM key
Vault&url=https://arcon.com&ssl_verify=1&username=root&password=pass1&com
ments=creating ARCON PAM vault from api"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2020-04-22T00:51:28Z</DATETIME>
        <TEXT>Success</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>45006</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Update ARCON PAM Vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
```

```
"action=update&id=45006&type=Arcon PAM&title=My ARCON PAM key
Vault&url=https://arcon.com&ssl_verify=1&username=root&password=pass2&com
ments=creating ARCON PAM vault from api"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2020-04-21T00:51:28Z</DATETIME>
        <TEXT>Success</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>45006</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

Sample - View details of an ARCON PAM Vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=view&id=45006"
"https://qualysapi.qualys.com/api/2.0/fo/vault/index.php/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE VAULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/vault/vault_view.dtd">
<VAULT_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-04-19T00:51:37Z</DATETIME>
        <VAULT_QUEST>
            <TITLE>
                <![CDATA[arcon-api1]]>
            </TITLE>
            <COMMENTS>
                <![CDATA[]]>
            </COMMENTS>
            <VAULT_TYPE>
                <![CDATA[Arcon PAM]]>
            </VAULT_TYPE>
            <CREATED_ON>2020-04-19T00:51:28Z</CREATED_ON>
```

```
                <OWNER>quays_rs23</OWNER>
                <LAST_MODIFIED>
                    <DATETIME>2020-04-19T00:51:28Z</DATETIME>
                    <BY>quays_rs23</BY>
                </LAST_MODIFIED>
                <USERNAME>
                    <![CDATA[root]]>
                </USERNAME>
                <URL>
                    <![CDATA[https://host1.domain]]>
                </URL>
                <SSL_VERIFY>
                    <![CDATA[1]]>
                </SSL_VERIFY>
                <ID>45006</ID>
            </VAULT_QUEST>
        </RESPONSE>
    </VAULT_OUTPUT>
```

Authentication Record API

Create, update, list authentication records with Arcon PAM vaults. You can use Arcon PAM vaults with Windows, Unix, Cisco, Check Point, Greenplum, MS SQL, MySQL, MariaDB, Oracle, MongoDB, PostgreSQL, Sybase and IBM DB2.

Note that Password retrieval is supported for all the authentication records. Retrieval of Private key is only supported for Unix authentication records. Retrieval of Passphrase and Root delegation in Unix is NOT supported.

Create/Update Authentication Record

Choose the Arcon PAM vault in your authentication record and provide the vault service type that you have assigned to the vault..

Parameter	Description
action=create|update	(Required)
login_type={value}	(Required to create/update vault information) Specify login_type=vault to add vault information. By default, the parameter is set to basic.
vault_id={value}	(Required when action=create and login_type=vault) A vault ID.
vault_type={value}	(Required when action=create and login_type=vault) Specify type=Arcon PAM

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.
vault_service_type	(Required) Specify a vault service type. This value is validated against the predefined list of service types.

Sample - Create Unix record with ARCON PAM Vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=create&title=Unix-Arcon-
API&username=root&username=Qualys&ips=10.10.10.2&port=5857&login_type=vau
lt&vault_id=45001&vault_type=Arcon PAM&vault_service_type=SSH UNIX"
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/"--data-binary
@create-arcon-pam-pk.xml
```

create-arcon-pam-pk.xml

```
<?xml version="1.0" encoding="UTF-8" ?>
<UNIX_AUTH_PARAMS>
 <PRIVATE_KEY_CERTIFICATES>
 <PRIVATE_KEY_CERTIFICATE>
 <PRIVATE_KEY_INFO type="vault">
 <DIGITAL_VAULT>
 <VAULT_TYPE>Arcon PAM</VAULT_TYPE>
 <VAULT_ID>45006</VAULT_ID>
<VAULT_SERVICE_TYPE><![CDATA[App UNIX GUI]]></VAULT_SERVICE_TYPE>
 </DIGITAL_VAULT>
 </PRIVATE_KEY_INFO>
 <PASSPHRASE_INFO type="basic">
 <PASSPHRASE><![CDATA[secret]]></PASSPHRASE>
 </PASSPHRASE_INFO>
 </PRIVATE_KEY_CERTIFICATE>
 </PRIVATE_KEY_CERTIFICATES>
</UNIX_AUTH_PARAMS>
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2020-04-22T01:12:43Z</DATETIME>
```

```
            <BATCH_LIST>
                <BATCH>
                    <TEXT>Successfully Created</TEXT>
                    <ID_SET>
                        <ID>139015</ID>
                    </ID_SET>
                </BATCH>
            </BATCH_LIST>
        </RESPONSE>
    </BATCH_RETURN>
```

Sample - Create MySQL record with ARCON PAM Vault

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
action=create&title=Mysql_Arcon_api&username=root&ips=10.10.10.3&login_ty
pe=vault&vault_id=45001&vault_type=Arcon PAM&port=3306&database=mysql
&unix_config_file=/etc/mysql&vault_service_type=MySQL QA
"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>2020-04-22T01:24:12Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully Created</TEXT>
                <ID_SET>
                    <ID>139016</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

Sample - List Unix authentication records

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: Curl" -d
"action=list&ids=139015"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_UNIX_LIST_OUTPUT SYSTEM
```

```
"https://qualysapi.qualys.com/api/2.0/fo/auth/unix/auth_unix_list_output.
dtd">
<AUTH_UNIX_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-04-22T01:13:49Z</DATETIME>
        <AUTH_UNIX_LIST>
            <AUTH_UNIX>
                <ID>139015</ID>
                <TITLE>
                    <![CDATA[Unix-Arcon-API]]>
                </TITLE>
                <USERNAME>
                    <![CDATA[Qualys]]>
                </USERNAME>
                <SKIP_PASSWORD>0</SKIP_PASSWORD>
                <CLEARTEXT_PASSWORD>0</CLEARTEXT_PASSWORD>
                <PRIVATE_KEY_CERTIFICATE_LIST>
                    <PRIVATE_KEY_CERTIFICATE>
                        <ID>22002</ID>
                        <PRIVATE_KEY_INFO type="vault">
                            <DIGITAL_VAULT>
                                <DIGITAL_VAULT_ID>
                                    <![CDATA[45006]]>
                                </DIGITAL_VAULT_ID>
                                <DIGITAL_VAULT_TYPE>
                                    <![CDATA[Arcon PAM]]>
                                </DIGITAL_VAULT_TYPE>
                                <DIGITAL_VAULT_TITLE>
                                    <![CDATA[arcon-api1]]>
                                </DIGITAL_VAULT_TITLE>
                                <VAULT_SERVICE_TYPE>
                                    <![CDATA[App UNIX GUI]]>
                                </VAULT_SERVICE_TYPE>
                            </DIGITAL_VAULT>
                        </PRIVATE_KEY_INFO>
                        <PASSPHRASE_INFO type="basic" />
                    </PRIVATE_KEY_CERTIFICATE>
                </PRIVATE_KEY_CERTIFICATE_LIST>
                <PORT>5857</PORT>
                <IP_SET>
                    <IP>10.10.10.2</IP>
                </IP_SET>
                <LOGIN_TYPE>
                    <![CDATA[vault]]>
                </LOGIN_TYPE>
                <DIGITAL_VAULT>
                    <DIGITAL_VAULT_ID>
                        <![CDATA[45001]]>
                    </DIGITAL_VAULT_ID>
```

```
                        <DIGITAL_VAULT_TYPE>
                            <![CDATA[Arcon PAM]]>
                        </DIGITAL_VAULT_TYPE>
                        <DIGITAL_VAULT_TITLE>
                            <![CDATA[arcon1]]>
                        </DIGITAL_VAULT_TITLE>
                        <VAULT_SERVICE_TYPE>
                            <![CDATA[SSH UNIX]]>
                        </VAULT_SERVICE_TYPE>
                    </DIGITAL_VAULT>
                    <CREATED>
                        <DATETIME>2020-04-22T01:12:43Z</DATETIME>
                        <BY>quays_rs23</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2020-04-22T01:12:43Z</DATETIME>
                    </LAST_MODIFIED>
                </AUTH_UNIX>
            </AUTH_UNIX_LIST>
        </RESPONSE>
    </AUTH_UNIX_LIST_OUTPUT>
```

Updated DTD

<base_url>/api/2.0/fo/auth/<type>/auth_<type>_list_output.dtd

Here type is an authentication type that supports the ARCON PAM vault: Windows, Unix, Cisco, Check Point, Greenplum, MS SQL, MySQL, MariaDB, Oracle, MongoDB, PostgreSQL, Sybase, and IBM DB2.

The element “VAULT_SERVICE_TYPE” has been added to the DTDs of the authentication types that support the ARCON PAM vault.

New Database UDCs for Sybase

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

With this release you can create, update, list and export Option Profiles for Sybase Database UDCs. We've added new elements to the XML output and DTDs for Control List Output, Policy Export Output, Posture Info List Output, Option Profiles, and the ImportableControl.xsd schema.

You'll see these changes:

- We have added parameters sybase_db_udc_restriction and sybase_db_udc_limit to the Options Profile API to help you set limit on number of rows returned per scan for the Sybase UDC. Default value is 256 and maximum allowed limit for Sybase is 2500 rows.

- We have added new CHECK_TYPE element to the XML output for Control List API: Sybase Database Check.

- We've added support for Sybase technologies (Sybase ASE 15 and SAP ASE 16) Database UDC for Posture API and Policy Export API.

- We updated the ImportableControl.xsd schema to include new enumeration values for

the CHECK_TYPE element: Sybase Database Check.

Sample - Options Profile API: Create

You'll create an option profile using new parameters for Sybase: sybase_db_udc_restriction and sybase_db_udc_limit.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=create&title=API-PC-OP-
Sybase&scan_ports=targeted&sybase_db_udc_restriction=1&sybase_db_udc_limi
t=50"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
```

```
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T19:16:41Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1710286</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Options Profile API: Update

You'll update an option profile using new parameters for Sybase: sybase_db_udc_restriction and sybase_db_udc_limit

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=update&id=1709710&title=API-PC-OP-Sybase-custom-
limit&scan_ports=targeted&sybase_db_udc_restriction=1&sybase_db_udc_limit
=50"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2019-05-20T06:45:00Z</DATETIME>
    <TEXT>Compliance Option profile successfully updated.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>1709710</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample - Options Profile API: List

You'll list the option profiles for Sybase with database preference keys and their corresponding values.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X -d
"action=list&id=1710150"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>1710150</ID>
      ...
        </SCAN_BY_POLICY>
      </SCAN_RESTRICTION
     ...
        <SYBASE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
        </SYBASE>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    </SCAN>
    ...
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Options Profile API: Export

You'll export the Option Profile for Sybase with database preference keys and their corresponding values.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X -d
"action=export&option_profile_id=1710150"
"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>
...
        <SYBASE>
          <DB_UDC_RESTRICTION>1</DB_UDC_RESTRICTION>
          <DB_UDC_LIMIT>60</DB_UDC_LIMIT>
        </SYBASE>
      </DATABASE_PREFERENCE_KEY>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
    ...
</OPTION_PROFILES>
```

DTD update:

option_profile_info.dtd DTD is updated to include Sybase in Database Preference Key and corresponding elements for Sybase.

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

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>
 <!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
...
<!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?, CLOSE_VULNERABILITIES?,
PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?, LOAD_BALANCER_DETECTION?,
PASSWORD_BRUTE_FORCING?, VULNERABILITY_DETECTION?, AUTHENTICATION?,
        ADDL_CERT_DETECTION?, DISSOLVABLE_AGENT?, LITE_OS_SCAN?,
ETHERNET_IP_PROBING?, CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?,
SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?, SYSTEM_AUTH_RECORD?,
FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?,
TEST_AUTHENTICATION?)>
 ...

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

Schema update:

The option_profiles.xsd schema is used to validate a proper format and required elements of the option profile XML file.

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

```
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="OPTION_PROFILES" type="OPTION_PROFILESType"/>
...
    <xs:complexType name="DATABASE_PREFERENCE_KEYType">
        <xs:sequence>
            <xs:element type="MSSQLType" name="MSSQL" minOccurs="0"/>
            <xs:element type="ORACLEType" name="ORACLE" minOccurs="0"/>
            <xs:element type="SYBASEType" name="SYBASE" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
...
     <xs:complexType name="SYBASEType">
        <xs:sequence>
            <xs:element name="DB_UDC_RESTRICTION">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:enumeration value="1"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="DB_UDC_LIMIT">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:minInclusive value="1"/>
                        <xs:maxInclusive value="256"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
...
```

Sample - Control API for Sybase

We have added new CHECK_TYPE element to the XML output for Control List API: Sybase Database Check.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=list&details=All&ids=100947"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE CONTROL_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/control/control_list_
```

```
output.dtd">
<CONTROL_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2020-03-21T05:29:10Z</DATETIME>
        <CONTROL_LIST>
            <CONTROL>
              ...
                    <![CDATA[sybase db udc]]>
                </STATEMENT>
                <CRITICALITY>
                    <LABEL>
                        <![CDATA[UNDEFINED]]>
                    </LABEL>
                    <VALUE>0</VALUE>
                </CRITICALITY>
                <CHECK_TYPE>
                    <![CDATA[Sybase Database Check]]>
                </CHECK_TYPE>
                <COMMENT>
                    <![CDATA[]]>
                </COMMENT>
                <IGNORE_ERROR>0</IGNORE_ERROR>
                <ERROR_SET_STATUS></ERROR_SET_STATUS>
                <TECHNOLOGY_LIST>
                    <TECHNOLOGY>
                        <ID>69</ID>
                        <NAME>Sybase ASE 15</NAME>
                        <RATIONALE>
...
    </RESPONSE>
</CONTROL_LIST_OUTPUT>
```

Sample - Posture API

We've added support for Sybase technologies (Sybase ASE 15 and SAP ASE 16) Database UDC for Posture API.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=list&policy_id=1303776&details=All&include_dp_name=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

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

```
  <RESPONSE>
        <DATETIME>2020-03-21T05:21:14Z</DATETIME>
            <INFO>
                <ID>90290</ID>
                <HOST_ID>7916697</HOST_ID>
                <CONTROL_ID>100947</CONTROL_ID>
                <TECHNOLOGY_ID>116</TECHNOLOGY_ID>
                <INSTANCE>SAP ASE 16:5000:COMSYBASE16:master</INSTANCE>
                <STATUS>Failed</STATUS>
                <POSTURE_MODIFIED_DATE>2020-03-
21T04:39:47Z</POSTURE_MODIFIED_DATE>
                <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
                <FIRST_FAIL_DATE>2020-03-21T04:39:47Z</FIRST_FAIL_DATE>
                <LAST_FAIL_DATE>2020-03-21T05:09:53Z</LAST_FAIL_DATE>
                <FIRST_PASS_DATE>N/A</FIRST_PASS_DATE>
                <LAST_PASS_DATE>N/A</LAST_PASS_DATE>
            </INFO>
        ...
        <SUMMARY>
            <TOTAL_ASSETS>1</TOTAL_ASSETS>
            <TOTAL_CONTROLS>3</TOTAL_CONTROLS>
            <CONTROL_INSTANCES>
                <TOTAL>15</TOTAL>
                <TOTAL_PASSED>0</TOTAL_PASSED>
                <TOTAL_FAILED>15</TOTAL_FAILED>
                <TOTAL_ERROR>0</TOTAL_ERROR>
                <TOTAL_EXCEPTIONS>0</TOTAL_EXCEPTIONS>
            </CONTROL_INSTANCES>
        </SUMMARY>
        <GLOSSARY>
                 ...
                <CONTROL>
                    <ID>100947</ID>
                    <STATEMENT>
                        <![CDATA[sybase db udc]]>
                    </STATEMENT>
                    <CRITICALITY>
                        <LABEL>
                            <![CDATA[UNDEFINED]]>
                        </LABEL>
                        <VALUE>0</VALUE>
                    </CRITICALITY>
                </CONTROL>
            ...
        </GLOSSARY>
   </RESPONSE>
</POSTURE_INFO_LIST_OUTPUT>
```

Sample - Policy API

We have updated support for Sybase technologies (Sybase ASE 15 and SAP ASE 16) Database UDC for Policy Export API.

API request:

```
curl -u "USERNAME:PASSWORD" -H "Content-type: text/xml" -X "POST"
-d "action=export&id=1358790&show_user_controls=1"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE POLICY_EXPORT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/compliance/policy/policy_export_
output.dtd">
<POLICY_EXPORT_OUTPUT>
     <RESPONSE>
        <DATETIME>2020-03-21T05:35:07Z</DATETIME>
        <POLICY>
            <TITLE>
                <![CDATA[sybase db udc]]>
            </TITLE>
            <EXPORTED>
                <![CDATA[2020-03-21T05:35:07Z]]>
            </EXPORTED>
            <COVER_PAGE>
                <![CDATA[]]>
            </COVER_PAGE>
            <STATUS>
                <![CDATA[active]]>
            </STATUS>
            <TECHNOLOGIES total="4">
                <TECHNOLOGY>
                    <ID>69</ID>
                    <NAME>Sybase ASE 15</NAME>
                </TECHNOLOGY>
                <TECHNOLOGY>
                    <ID>116</ID>
                    <NAME>SAP ASE 16</NAME>
                </TECHNOLOGY>
            </TECHNOLOGIES>
           ...
                          <STATEMENT>
                              <![CDATA[sybase db udc]]>
                          </STATEMENT>
                          <CRITICALITY>
                              <LABEL>
                                  <![CDATA[UNDEFINED]]>
```

```
                                    </LABEL>
                                    <VALUE>0</VALUE>
                                </CRITICALITY>
                                <COMMENT>
                                    <![CDATA[]]>
                                </COMMENT>
                                <IGNORE_ERROR>0</IGNORE_ERROR>
                                <ERROR_SET_STATUS></ERROR_SET_STATUS>
                                <TECHNOLOGIES total="4">
                                    <TECHNOLOGY>
                                        <ID>69</ID>
                                        <NAME>Sybase ASE 15</NAME>
                                        <EVALUATE>
                                            <CTRL>
                                                <AND>
                                                    <OR>
                                                        <DP>

<K>custom.sybase_query.1027025</K>
...
    </RESPONSE>
</POLICY_EXPORT_OUTPUT>
```

Schema update: ImportableControl.xsd

The enumeration value Sybase Database Check is added in ImportableControl.xsd schema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
...
<xs:element name="CHECK_TYPE">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Registry Key Existence" />
                <xs:enumeration value="Registry Value Existence" />
                <xs:enumeration value="Registry Value Content Check" />
                <xs:enumeration value="Registry Permission" />
               <xs:enumeration value="Window File/Directory Existence" />
              <xs:enumeration value="Window File/Directory Permission" />
               <xs:enumeration value="Unix File/Directory Permission" />
               <xs:enumeration value="Unix File Content Check" />
               <xs:enumeration value="Unix File/Directory Existence" />
               <xs:enumeration value="Window File Integrity Check" />
               <xs:enumeration value="Unix File Integrity Check" />
               <xs:enumeration value="WMI Query Check" />
               <xs:enumeration value="Share Access Check" />
               <xs:enumeration value="Unix Directory Search Check" />
```

```
                <xs:enumeration value="Windows Directory Search Check" />
                <xs:enumeration value="Windows Group Membership Check" />
                <xs:enumeration value="Windows Directory Integrity Check"
/>
                <xs:enumeration value="Unix Directory Integrity Check" />
                <xs:enumeration value="MSSQL Database Check" />
                <xs:enumeration value="Oracle Database Check" />
                <xs:enumeration value="Sybase Database Check" />
                <xs:enumeration value="Windows File Content Check" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
...
```