Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.21.2

Dec 29, 2022 (Updated on Jan 9, 2023)

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

What's New

MongoDB authentication Instance Discovery and System Record Creation

PC API: Find Hosts Based on Last Scan Date

PC API: Set Truncation Limit for Evidence Data

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.

MongoDB authentication Instance Discovery and System Record Creation

APIs affected	/api/2.0/fo/auth/mongodb
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 MongoDB authentication record. When we auto discover MongoDB instances, we'll discover the target configuration for each instance but not the login credentials. We've introduced a new configuration called "MongoDB authentication record template" that you'll use to provide MongoDB 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 MongoDB instances on each scanned host and create authentication records for those instances. We support auto discovery and system record creation for MongoDB instances running on Unix platforms. Make sure you have Unix authentication records in your account for hosts running MongoDB.

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

- You can easily rotate MongoDB passwords. Simply edit the credentials in the MongoDB system record template and all MongoDB 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 MongoDB 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

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

2) Select the MongoDB 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 MongoDB 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 MongoDB authentication records, you can specify the new input parameter"is_template." It indicates whether the new record is an MongoDB system record template.

Note: Once you save a record as a template it cannot be converted to a regular MongoDB record. Also, a regular MongoDB record cannot be saved as a template.

- When listing MongoDB authentication records, we added new input parameters to filter the output. For example, you can filter the list only to show MongoDB system record templates,or list all records associated with a certain template ID or name. You can also filter the list by 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 MongoDB Auth Record List Output DTD.

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

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

Create/Update MongoDB Record Template

List MongoDB Authentication Records

Create/Update Option Profiles

Create/Update MongoDB Record Template

Use the following input parameter for creating/updating MongoDB record template. Refer to the Qualys API (VM,PC) User Guide for details on all input parameters.

Parameter	Description
is_template={**0**|1}	(Optional for create request, not valid for update request) By default, a new record is a regular MongoDB record. Specify 1 to create a MongoDB system record template.You must also specify login credentials, which are described below..
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 MongoDB record already exists with the same IP address and target configuration then an error will be returned. (This parameter applies only to system created MongoDB records. It cannot be specified for user created MongoDB records and it cannot be specified for MongoDB system record templates.)

Sample: Create MongoDB record template

This sample creates an MongoDB 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=MongoDBRecordTemplate&username=MongoDB
User&password=Password"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

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>2022-12-19T06:21:15Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6769303</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Create MongoDB record template with vault

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

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&is_template=1&title=mongo_template_vault&username=mongo-
admin&login_type=vault&vault_id=2557183&vault_type=CyberArk
AIM&file=test&folder=test123"
https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/
```

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>2022-12-28T10:21:09Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6810538</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Create MongoDB record template for LDAP Authentication

In this sample we're creating an MongoDB system record template for LDAP authentication using a vault.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&is_template=1&title=mongo_template_vault_ldap&username=mon
goadmin&credential_type=external&login_type=vault&vault_id=2557183&vault_
type=CyberArk AIM&file=test&folder=test123"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

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>2022-12-28T10:21:09Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6818053</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Create MongoDB record template using privatekey/certbased template

In this sample we're creating an MongoDB system record template using privatekey/certbased template.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=create&title=preTestpkcertapi_1&passphrase=abc123&login_type=pkce
rt&is_template=1&login_type=pkcert&private_key=-----
BEGIN+RSA+PRIVATE+KEY-----%0D%0AProc-Type%3A+4%2CENCRYPTED%0D%0ADEK-
Info%3A+AES-192-
CBC%2C5CB8FB86562920D0340BF086D03C3C67%0D%0A%0D%0AugpPaTFCveC8MYJDci%2F6E
N%2Bywrq8kM0DogcXg9bOV7cSMdMm7Vh0gdzhdL0wTnwY%0D%0A4xfMvITnR5au48iCixqPBA
OGEma7W2MaPwmhPEafYGZ3ubAr8ZV2BdrnSTUloFx%2B%0D%0A91yCQZrGDwWzl3YSAiRBThy
l2MZefuqj6PwfHXttmc7Heg%2FdhvBZdXAIR4Q9biXp%0D%0A2PO%2BINq5jzPBvcf%2BsxUI
WZ1R97Z1H%2BNalekxzjn5ydZDix1UHGZZWh8QhJMts%2BhR%0D%0AGJEUb3OodzaoI%2FdkW
8F9WA62t7UMBRwzzmhhw4tqaQ%2BPmqOyU8qJuyjGewClgGec%0D%0Az75ZaNDPzuLknyADfX
p85kM00wTJ3kF28ZFiMajaAmyVkTb3kjRpM5diKbkfMdzu%0D%0AqCnjoc6ygdYpEN0rJ9hKi
yN08w5AJNDwhCjTr4gmq81UHjkd5vkbRFzWGrASPxwp%0D%0A1AtbD27APYYAqHbQop1klz4l
YVuZsWoQw%2F6sPGGWFaesGUcdhBcmv%2BQGbesw%2Ff0s%0D%0AFK0tuYle8avJqCQtSp0tf
CBQqqRyYtBOVQOa527HvynO2erRV5GXLP6eA33%2Blg4W%0D%0A2bfjXxqTHxdDNpSqZjvvr3
PXW%2B6538%2FwRS0l1h3PzLwtyeCJ%2FiCcu4jYIsw4kqkH%0D%0ABsxf%2B7Y7Y4%2Fp3%2
FsW9WvuNF0ZusBoVViqciEW%2BQujH%2BMTA6tJgtdwLwFinXT8G4jU%0D%0AKxOYi%2B9SQf
P27GxBEOIybnozqz8vv0cTabWl8YWz589Rm7%2BnrNzHPYlXS1sk3AdA%0D%0A8hfYaM4tD3S
AzVFMLTPPqj2CaDjjX%2B9PR8LVjv7mGjozmAmnRvniOHUaKHAd7JwZ%0D%0AyW7wWOSTrqfK
JU9DufXcqv9Ed0LZHfPux57M3HqGO4jjopUeUAgX%2FAg1x8ScMEx2%0D%0AB18Z%2Fix7%2F
u9K59E7pYOgyTLc0hxptoc8UIGHGrK5w7rJvivGyCIUG9LD20iCG4uS%0D%0AkxFjECDgR3pa
jNEToLhc7W4iK1Zk5wkWLr49PGIhfGpadjMXmNwNIULqpUrWdi1Q%0D%0AzBOD1wmeO0XMo04
YUz827fSrVoKuYrbVNw6ncjKSfpbtOWq%2BoOgOOhexKZpmyToJ%0D%0Acm62sSy3klVomVLq
3APLLs5cCRMyGfHVxws2qkTr6%2Ff5%2BbVQXBKDmM6fsKmwhk9y%0D%0AOdKfJzYLdqQK6UI
12zIlhfG70HVg242O9pK72gaXKX8Be0T%2BJQXmLq1ysoSr7Ggn%0D%0AUV%2FzdBnNDutNgd
85HTibV2U%2BUAZrazcL4Pg%2BhmEgJxJwSpXALgPOpWTcWNuZgyQm%0D%0AS6gdEIG7IWByC
z%2BNkZHJMU5CXeYuwmag8kaGFYnwlpvZdWQDjJJp7emQeMJS9o%2Ft%0D%0ALfOKPFsza5E%
2FpyiB9EfboSVPw4rZwRwahGqVnNtmGyhQuwyLTOKAZV1dB9%2BRYzEo%0D%0AUmbg7h3WyTF
gFRKoPL7UWTfP0BRRyDK6ZlMyaHmNKOHma4I202iaObumfkU8gbTn%0D%0AhuWzunDc%2FQr9
```

```
SclFcdLegBphJlgEBtE2RPXosIY2VnQLGCCLG8qVp6%2BQ%2BgT%2FXWLm%0D%0AF8P9vo24w
148DeuQ%2Bj2t5pQUrdeTabgkQymMWRM4BoLk%2BS0sYhxiba8C%2FHb30UVk%0D%0A-----
END+RSA+PRIVATE+KEY-----&certificate=-----BEGIN+CERTIFICATE-----
%0D%0AMIIC%2FDCCAmUCCQCmk0zsovAvhzANBgkqhkiG9w0BAQUFADBsMQswCQYDVQQGEwJV%
0D%0AUzELMAkGA1UECAwCQ0ExFTATBgNVBAcMDFJlZHdvb2QgQ2l0eTEPMA0GA1UECgwG%0D%
0AUXVhbHlzMRQwEgYDVQQLDAtFbmdpbmVlcmluZzESMBAGA1UEAwwJc2VydmVyLWNh%0D%0AM
B4XDTE3MDQyNzIyMTY0NFoXDTMxMDEwNDIyMTY0NFowgZQxCzAJBgNVBAYTAlVT%0D%0AMQsw
CQYDVQQIDAJDQTEVMBMGA1UEBwwMUmVkd29vZCBDaXR5MQ8wDQYDVQQKDAZR%0D%0AdWFseXM
xGzAZBgNVBAsMEkVuZ2luZWVyaW5nX2NsaWVudDEzMDEGA1UEAwwqbWxt%0D%0Ab25nb2RiMz
RlLnMyMDEycjIubWxxYS5yZGxhYi5xdWFseXMuY29tMIIBIjANBgkq%0D%0AhkiG9w0BAQEFA
AOCAQ8AMIIBCgKCAQEAzYIzvdqaViRHFFOb1veMIUVaeTXtZm70%0D%0AuyS66f01KgUkZbp%
2FgTUuipMCp%2FKRTtDICGHgp%2B%2F4LHZb1U2LYRK%2B6MggnWOl7AzF%0D%0AyG0U8rlY1
%2F6XORZgmlgrtQdW%2FCABzKvEvWwhauSGv3aE9zpazwsoFFZtTit8TT87%0D%0Azxu%2FgQ
4zrCzJszunWD%2FHbXpt0%2FdN7jwWMEgYIIbJA2ehwUQFoaVMdGPdb0%2FJGHda%0D%0AlKW
lwSyE%2FySVCLRegGR7SW%2BJsWV15Nj2%2BzYq5ik5Pkrv7uWLUrg5q8be%2Bwo48vEm%0D%
0Aa88VnXqfGbS3eYbQaSRldqI1Q6Tb4mUOVerEW6%2Flx1Cs7Be8TFC2ewIDAQABMA0G%0D%0
ACSqGSIb3DQEBBQUAA4GBAA8WcYVFNsWfULL%2F2TM6PHHHi41Jeosu9duFhnJoKUv1%0D%0A
7JNR2qgT5Dt5sm403tTZFpv7j59GocaS2lOBOjv8RhsNyIRnCH43ByyM%2BBXkR4G0%0D%0Av
Uy7GE%2BphCdDSPnS%2Fm7ANhkXRmEjEylXzI6JJwNwcUiemOc7S4TC69PBy4OOtLwQ%0D%0A
-----END+CERTIFICATE-----"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

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>2022-12-28T10:21:09Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>6860030</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Update MongoDB record template

This sample updates an existing MongoDB record template.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=6841415&title=MongoDbrecord_template_basic_update_api"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/""
```

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>2023-01-06T09:30:45Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>6841415</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample: Update MongoDB record to save as user record

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

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With: curl" -d
"action=update&ids=6834518&title=title&save_as_user_auth=1&username=usern
ame&password=Password"
"http://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

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>2023-01-06T09:30:45Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Updated</TEXT>
        <ID_SET>
          <ID>6834518</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

List MongoDB Authentication Records

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

Parameter	Description
is_template={**0**|1}	(Optional for create request, not valid for update request) By default, a new record is a regular MongoDB record. Specify 1 to create a MongoDB system record template.You must also specify login credentials, which are described below..
template_auth_id={value}	(Optional) Specify the template ID for an MongoDB system record template to only show MongoDB records associated with the specified template.
template_auth_name={value}	(Optional) Specify the template name for an MongoDB system record template to only show MongoDB records associated with the specified template.
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 MongoDB Record Template

This sample is filtered by template ID. Note that the XML output shows new values for each template record indicating if the record is system created, is active and is a template.

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/mongodb"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb_list_o
utput.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-01-06T09:42:10Z</DATETIME>
    <AUTH_MONGODB_LIST>
      <AUTH_MONGODB>
        <ID>6818052</ID>
        <TITLE><![CDATA[Sample1]]></TITLE>
        <USERNAME><![CDATA[mlqa]]></USERNAME>
```

```
    <CREDENTIAL_TYPE><![CDATA[external]]></CREDENTIAL_TYPE>
    <CLEARTEXT><![CDATA[No]]></CLEARTEXT>
    <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
    <REQUIRE_CERT><![CDATA[0]]></REQUIRE_CERT>
    <CREATED>
      <DATETIME>2022-12-29T09:19:14Z</DATETIME>
      <BY>newpc_da</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2022-12-29T09:19:14Z</DATETIME>
    </LAST_MODIFIED>
    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
    <IS_ACTIVE>1</IS_ACTIVE>
    <IS_TEMPLATE>1</IS_TEMPLATE>
  </AUTH_MONGODB>
  <AUTH_MONGODB>
    <ID>6834412</ID>
    <TITLE><![CDATA[update_mongo_db_api]]></TITLE>
    <USERNAME><![CDATA[update]]></USERNAME>
    <CREDENTIAL_TYPE><![CDATA[local]]></CREDENTIAL_TYPE>
    <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
    <REQUIRE_CERT><![CDATA[0]]></REQUIRE_CERT>
    <CREATED>
      <DATETIME>2023-01-03T07:20:42Z</DATETIME>
      <BY>newpc_da</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2023-01-04T15:16:52Z</DATETIME>
    </LAST_MODIFIED>
    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
    <IS_ACTIVE>1</IS_ACTIVE>
    <IS_TEMPLATE>1</IS_TEMPLATE>
  </AUTH_MONGODB>
  <AUTH_MONGODB>
    <ID>6834413</ID>
    <TITLE><![CDATA[MongoDbrecord_templateAPI2]]></TITLE>
    <USERNAME><![CDATA[qualys_scan]]></USERNAME>
    <CREDENTIAL_TYPE><![CDATA[local]]></CREDENTIAL_TYPE>
    <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
    <REQUIRE_CERT><![CDATA[0]]></REQUIRE_CERT>
    <CREATED>
      <DATETIME>2023-01-03T07:21:23Z</DATETIME>
      <BY>newpc_da</BY>
    </CREATED>
    <LAST_MODIFIED>
      <DATETIME>2023-01-03T09:53:18Z</DATETIME>
    </LAST_MODIFIED>
    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
    <IS_ACTIVE>1</IS_ACTIVE>
```

```
        <IS_TEMPLATE>1</IS_TEMPLATE>
      </AUTH_MONGODB>
    </AUTH_MONGODB_LIST>
  </RESPONSE>
</AUTH_MONGODB_LIST_OUTPUT>
```

Sample: List Mongodb record

This sample lists system created MongoDB record template associated with the template ID 6847704

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&ids=6847704"
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb_list_o
utput.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
     <RESPONSE>
          <DATETIME>2023-01-05T12:47:03Z</DATETIME>
          <AUTH_MONGODB_LIST>
               <AUTH_MONGODB>
                    <ID>6847704</ID>
                    <TITLE>
                         <![CDATA[MongoDB system record template]]>
                    </TITLE>
                    <USERNAME>
                         <![CDATA[root]]>
                    </USERNAME>
                    <CREDENTIAL_TYPE>
                         <![CDATA[local]]>
                    </CREDENTIAL_TYPE>
                    <LOGIN_TYPE>
                         <![CDATA[basic]]>
                    </LOGIN_TYPE>
                    <REQUIRE_CERT>
                         <![CDATA[0]]>
                    </REQUIRE_CERT>
                    <CREATED>
                         <DATETIME>2023-01-05T07:16:46Z</DATETIME>
                         <BY>vt_sm1</BY>
                    </CREATED>
                    <LAST_MODIFIED>
```

```
                        <DATETIME>2023-01-05T07:16:46Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>1</IS_ACTIVE>
                    <IS_TEMPLATE>1</IS_TEMPLATE>
                </AUTH_MONGODB>
            </AUTH_MONGODB_LIST>
        </RESPONSE>
</AUTH_MONGODB_LIST_OUTPUT>
```

Sample: List Mongodb auth record using certain Template Id

This sample lists active, system created MongoDB records associated with the template ID 6834412

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&is_system_created=1&template_auth_id=6834412&status=1""https
://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_MONGODB_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/mongodb/auth_mongodb_list_o
utput.dtd">
<AUTH_MONGODB_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2023-01-06T09:46:48Z</DATETIME>
    <AUTH_MONGODB_LIST>
      <AUTH_MONGODB>
        <ID>6834517</ID>
        <TITLE><![CDATA[MongoDB [System Created] - 261003]]></TITLE>
        <USERNAME><![CDATA[update]]></USERNAME>
        <CREDENTIAL_TYPE><![CDATA[local]]></CREDENTIAL_TYPE>
        <DATABASE><![CDATA[admin]]></DATABASE>
        <PORT>27409</PORT>
        <UNIX_CONFIGURATION_FILE><![CDATA[/etc/mongod-
pc9.conf]]></UNIX_CONFIGURATION_FILE>
        <SSL_VERIFY><![CDATA[0]]></SSL_VERIFY>
        <IP_SET>
          <IP>10.20.30.40</IP>
        </IP_SET>
        <LOGIN_TYPE><![CDATA[basic]]></LOGIN_TYPE>
        <REQUIRE_CERT><![CDATA[0]]></REQUIRE_CERT>
        <NETWORK_ID>0</NETWORK_ID>
        <CREATED>
          <DATETIME>2023-01-03T10:00:41Z</DATETIME>
```

```
          </CREATED>
          <LAST_MODIFIED>
            <DATETIME>2023-01-03T10:00:41Z</DATETIME>
          </LAST_MODIFIED>
          <IS_SYSTEM_CREATED>1</IS_SYSTEM_CREATED>
          <IS_ACTIVE>1</IS_ACTIVE>
          <IS_TEMPLATE>0</IS_TEMPLATE>
          <TEMPLATE>
            <ID>6834412</ID>
            <TITLE>update_mongo_db_api</TITLE>
          </TEMPLATE>
          <COMMENTS><![CDATA[System created MongoDB auth record using scan
data with history ID 14409195.]]></COMMENTS>
        </AUTH_MONGODB>
      </AUTH_MONGODB_LIST>
    </RESPONSE>
</AUTH_MONGODB_LIST_OUTPUT>
```

DTD update:

The following tags were added to the MongoDB Authentication Record List Output DTD: IS_SYSTEM_CREATED, IS_ACTIVE and IS_TEMPLATE.

DTD: <platform>/api/2.0/fo/auth/mongodb/auth_mongodb_list_output.dtd

```
<!-- QUALYS AUTH_MONGODB_LIST_OUTPUT DTD -->
<!ELEMENT AUTH_MONGODB_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)>
<!ELEMENT POST_DATA (#PCDATA)>
<!ELEMENT RESPONSE (DATETIME, (AUTH_MONGODB_LIST|ID_SET)?, WARNING_LIST?,
GLOSSARY?)>
<!ELEMENT AUTH_MONGODB_LIST (AUTH_MONGODB+)>
<!ELEMENT AUTH_MONGODB (ID, TITLE, USERNAME?, CREDENTIAL_TYPE?,
CLEARTEXT?, DATABASE?, PORT?, UNIX_CONFIGURATION_FILE?, SSL_VERIFY?,
HOSTS?, IP_SET?, LOGIN_TYPE?, DIGITAL_VAULT?, REQUIRE_CERT?,
PRIVATE_KEY_CERTIFICATE_LIST?, NETWORK_ID?, CREATED, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, IS_TEMPLATE?, TEMPLATE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT USERNAME (#PCDATA)>
<!ELEMENT CREDENTIAL_TYPE (#PCDATA)>
<!ELEMENT CLEARTEXT (#PCDATA)>
```

```
<!ELEMENT REQUIRE_CERT (#PCDATA)>
<!ELEMENT PRIVATE_KEY_CERTIFICATE_LIST (PRIVATE_KEY_CERTIFICATE)*>

<!ELEMENT PRIVATE_KEY_CERTIFICATE (ID, PRIVATE_KEY_INFO, PASSPHRASE_INFO,
CERTIFICATE?)+>
<!ELEMENT PRIVATE_KEY_INFO (PRIVATE_KEY|DIGITAL_VAULT)>
<!ATTLIST PRIVATE_KEY_INFO type (basic|vault) "basic">

<!-- Private key contents will never be rendered -->
<!ELEMENT PRIVATE_KEY EMPTY>
<!ELEMENT PASSPHRASE_INFO (DIGITAL_VAULT?)>
<!ATTLIST PASSPHRASE_INFO type (basic|vault) "basic">
<!-- Certificate contents will never be rendered -->
<!ELEMENT CERTIFICATE EMPTY>

<!ELEMENT PORT (#PCDATA)>
<!ELEMENT DATABASE (#PCDATA)>
<!ELEMENT SSL_VERIFY (#PCDATA)>
<!ELEMENT HOSTS (HOST+)>
<!ELEMENT HOST (#PCDATA)>
<!ELEMENT IP_SET (IP|IP_RANGE)+>
<!ELEMENT IP (#PCDATA)>
<!ELEMENT IP_RANGE (#PCDATA)>
<!ELEMENT LOGIN_TYPE (#PCDATA)>
<!ELEMENT UNIX_CONFIGURATION_FILE (#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)>
<!ELEMENT WARNING_LIST (WARNING+)>
<!ELEMENT WARNING (CODE?, TEXT, URL?, ID_SET?)>
<!ELEMENT CODE (#PCDATA)>
<!ELEMENT TEXT (#PCDATA)>
<!ELEMENT URL (#PCDATA)>
<!ELEMENT ID_SET (ID|ID_RANGE)+>
<!ELEMENT ID_RANGE (#PCDATA)>
<!ELEMENT GLOSSARY (USER_LIST?)>
<!ELEMENT USER_LIST (USER+)>
<!ELEMENT USER (USER_LOGIN, FIRST_NAME, LAST_NAME)>
<!ELEMENT FIRST_NAME (#PCDATA)>
<!ELEMENT LAST_NAME (#PCDATA)>
<!ELEMENT DIGITAL_VAULT (DIGITAL_VAULT_ID, DIGITAL_VAULT_TYPE,
DIGITAL_VAULT_TITLE, VAULT_FOLDER?, VAULT_FILE?, VAULT_SECRET_NAME?,
VAULT_SYSTEM_NAME?, VAULT_EP_NAME?, VAULT_EP_TYPE?, VAULT_EP_CONT?,
```

```
VAULT_ACCOUNT_NAME?, VAULT_SECRET_KV_PATH?, VAULT_SECRET_KV_NAME?,
VAULT_SECRET_KV_KEY?, VAULT_SERVICE_TYPE?)>
<!ELEMENT DIGITAL_VAULT_ID (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TYPE (#PCDATA)>
<!ELEMENT DIGITAL_VAULT_TITLE (#PCDATA)>
<!ELEMENT VAULT_USERNAME (#PCDATA)>
<!ELEMENT VAULT_FOLDER (#PCDATA)>
<!ELEMENT VAULT_FILE (#PCDATA)>
<!ELEMENT VAULT_SECRET_NAME (#PCDATA)>
<!ELEMENT VAULT_SYSTEM_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_NAME (#PCDATA)>
<!ELEMENT VAULT_EP_TYPE (#PCDATA)>
<!ELEMENT VAULT_EP_CONT (#PCDATA)>
<!ELEMENT VAULT_ACCOUNT_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_PATH (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_NAME (#PCDATA)>
<!ELEMENT VAULT_SECRET_KV_KEY (#PCDATA)>
<!ELEMENT VAULT_SERVICE_TYPE (#PCDATA)>
<!-- EOF -->
```

Create/Update Option Profiles

The following table shows the 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, Oracle and Mongodb. Multiple technologies are specified as comma separated values. This parameter can only be specified if enable_auth_instance_discovery=1.
mongodb_template_id={value}	(Optional) The Template ID for the MongoDB system record template you want to assign to the compliance profile for discovery scans. When auto_auth_types=MongoDB is specified, then mongodb_template_id or mongodb_template_name must also be specified.

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

Sample: Create Option Profile

In this sample we are creating an option profile with the option to enable instance discovery and system record creation for MongoDB and we're using template ID 6731346.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=Profile-Auth-
InsMongodtestapi2&enable_auth_instance_discovery=1&auto_auth_types=MongoD
B&scan_ports=targeted&mongodb_template_id=6731346"
"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>2022-12-19T07:48:27Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6863066</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample: Update Option Profile

In this sample we are updating an existing option profile with the option to enable instance discovery and we're using template ID 279035.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&title=Profile-Auth-
```

```
InsMongoDesttUpdate&enable_auth_instance_discovery=1&auto_auth_types=Mong
oDB&scan_ports=targeted&mongodb_template_id=279035&id=6861963"
"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>2022-12-19T07:46:21Z</DATETIME>
    <TEXT>Compliance Option profile successfully added.</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6863065</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Sample: List Option Profile

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=list&id=167075"
"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>2177419</ID>
      <GROUP_NAME><![CDATA[MongoDB_instance_discovery_OP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[root]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>306942</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2022-12-27T08:27:53Z</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>MongoDB</AUTHENTICATION_TYPE>
            </AUTHENTICATION_TYPE_LIST>
            <MONGODB_AUTHENTICATION_TEMPLATE>
              <ID>2345663</ID>
              <TITLE>Mongo_DB_Template</TITLE>
            </MONGODB_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>
    <INSTANCE_DATA_COLLECTION />
    <OS_BASED_INSTANCE_DISC_COLLECTION />
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

DTD update:

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*><!ELEMENT OPTION_PROFILE
(BASIC_INFO, SCAN, MAP?, ADDITIONAL,
INSTANCE_DATA_COLLECTION?,OS_BASED_INSTANCE_DISC_COLLECTION?)>
<!ELEMENT BASIC_INFO (ID, GROUP_NAME, GROUP_TYPE, USER_ID, UNIT_ID,
SUBSCRIPTION_ID, IS_DEFAULT?, IS_GLOBAL?, IS_OFFLINE_SYNCABLE?,
UPDATE_DATE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT GROUP_NAME (#PCDATA)>
<!ELEMENT GROUP_TYPE (#PCDATA)>
<!ELEMENT USER_ID (#PCDATA)>
<!ELEMENT UNIT_ID (#PCDATA)>
<!ELEMENT SUBSCRIPTION_ID (#PCDATA)>
<!ELEMENT IS_DEFAULT (#PCDATA)>
<!ELEMENT IS_GLOBAL (#PCDATA)>
<!ELEMENT IS_OFFLINE_SYNCABLE (#PCDATA)>
<!ELEMENT UPDATE_DATE (#PCDATA)><!ELEMENT SCAN (PORTS?, SCAN_DEAD_HOSTS?,
CLOSE_VULNERABILITIES?, PURGE_OLD_HOST_OS_CHANGED?, PERFORMANCE?,
LOAD_BALANCER_DETECTION?, PASSWORD_BRUTE_FORCING?,
VULNERABILITY_DETECTION?, AUTHENTICATION?,
AUTHENTICATION_LEAST_PRIVILEGE?, ADDL_CERT_DETECTION?,
DISSOLVABLE_AGENT?, SCAN_RESTRICTION?, DATABASE_PREFERENCE_KEY?,
SYSTEM_AUTH_RECORD?, LITE_OS_SCAN?, CUSTOM_HTTP_HEADER?,
HOST_ALIVE_TESTING?, ETHERNET_IP_PROBING?, FILE_INTEGRITY_MONITORING?,
```

```
CONTROL_TYPES?, DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?,
MAX_SCAN_DURATION_PER_ASSET?)><!ELEMENT PORTS (TCP_PORTS?, UDP_PORTS?,
AUTHORITATIVE_OPTION?, (STANDARD_SCAN|TARGETED_SCAN)?)>
<!ELEMENT TCP_PORTS (TCP_PORTS_TYPE?, TCP_PORTS_STANDARD_SCAN?,
TCP_PORTS_ADDITIONAL?, THREE_WAY_HANDSHAKE?, STANDARD_SCAN?,
TCP_ADDITIONAL?)>
<!ELEMENT TCP_PORTS_TYPE (#PCDATA)>
<!ELEMENT TCP_PORTS_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT HAS_ADDITIONAL (#PCDATA)>
<!ELEMENT ADDITIONAL_PORTS (#PCDATA)>
<!ELEMENT THREE_WAY_HANDSHAKE (#PCDATA)><!ELEMENT UDP_PORTS
(UDP_PORTS_TYPE?, UDP_PORTS_STANDARD_SCAN?, UDP_PORTS_ADDITIONAL?,
(STANDARD_SCAN|CUSTOM_PORT)?)>
<!ELEMENT UDP_PORTS_TYPE (#PCDATA)>
<!ELEMENT UDP_PORTS_ADDITIONAL (HAS_ADDITIONAL?,
ADDITIONAL_PORTS?)><!ELEMENT AUTHORITATIVE_OPTION (#PCDATA)>
<!ELEMENT STANDARD_SCAN (#PCDATA)>
<!ELEMENT TARGETED_SCAN (#PCDATA)><!ELEMENT SCAN_DEAD_HOSTS
(#PCDATA)><!ELEMENT CLOSE_VULNERABILITIES (HAS_CLOSE_VULNERABILITIES?,
HOST_NOT_FOUND_ALIVE?)>
<!ELEMENT HAS_CLOSE_VULNERABILITIES (#PCDATA)>
<!ELEMENT HOST_NOT_FOUND_ALIVE (#PCDATA)><!ELEMENT
PURGE_OLD_HOST_OS_CHANGED (#PCDATA)><!ELEMENT PERFORMANCE
(PARALLEL_SCALING?, OVERALL_PERFORMANCE, HOSTS_TO_SCAN, PROCESSES_TO_RUN,
PACKET_DELAY, PORT_SCANNING_AND_HOST_DISCOVERY,
EXTERNAL_SCANNERS_TO_USE?, HOST_CGI_CHECKS?, MAX_CGI_CHECKS?,
MAX_TARGETS_PER_SLICE?, MAX_NUMBER_OF_TARGETS?,
CONF_SCAN_LIMITED_CONNECTIVITY?, SKIP_PRE_SCANNING?,
SCAN_MULTIPLE_SLICES_PER_SCANNER?)>
<!ELEMENT PARALLEL_SCALING (#PCDATA)>
<!ELEMENT OVERALL_PERFORMANCE (#PCDATA)>
<!ELEMENT HOSTS_TO_SCAN (EXTERNAL_SCANNERS, SCANNER_APPLIANCES)>
<!ELEMENT EXTERNAL_SCANNERS (#PCDATA)>
<!ELEMENT SCANNER_APPLIANCES (#PCDATA)>
<!ELEMENT PROCESSES_TO_RUN (TOTAL_PROCESSES, HTTP_PROCESSES)>
<!ELEMENT TOTAL_PROCESSES (#PCDATA)>
<!ELEMENT HTTP_PROCESSES (#PCDATA)>
<!ELEMENT PACKET_DELAY (#PCDATA)>
<!ELEMENT PORT_SCANNING_AND_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT EXTERNAL_SCANNERS_TO_USE (#PCDATA)>
<!ELEMENT HOST_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_CGI_CHECKS (#PCDATA)>
<!ELEMENT MAX_TARGETS_PER_SLICE (#PCDATA)>
<!ELEMENT MAX_NUMBER_OF_TARGETS (#PCDATA)>
<!ELEMENT CONF_SCAN_LIMITED_CONNECTIVITY (#PCDATA)>
<!ELEMENT SKIP_PRE_SCANNING (#PCDATA)>
<!ELEMENT SCAN_MULTIPLE_SLICES_PER_SCANNER (#PCDATA)>
<!ELEMENT LOAD_BALANCER_DETECTION (#PCDATA)><!ELEMENT
PASSWORD_BRUTE_FORCING (SYSTEM?, CUSTOM_LIST?)>
```

```
<!ELEMENT SYSTEM (HAS_SYSTEM?, SYSTEM_LEVEL?)>
<!ELEMENT HAS_SYSTEM (#PCDATA)>
<!ELEMENT SYSTEM_LEVEL (#PCDATA)><!ELEMENT CUSTOM_LIST (CUSTOM+)>
<!ELEMENT CUSTOM (ID, TITLE, TYPE?, LOGIN_PASSWORD?)+>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT TYPE (#PCDATA)>
<!ELEMENT LOGIN_PASSWORD (#PCDATA)><!ELEMENT MAX_SCAN_DURATION_PER_ASSET
(#PCDATA)><!ELEMENT VULNERABILITY_DETECTION
((COMPLETE|CUSTOM_LIST|RUNTIME), DETECTION_INCLUDE?, DETECTION_EXCLUDE?)>
<!ELEMENT COMPLETE (#PCDATA)>
<!ELEMENT RUNTIME (#PCDATA)><!ELEMENT DETECTION_INCLUDE
(BASIC_HOST_INFO_CHECKS, OVAL_CHECKS, QRDI_CHECKS?)>
<!ELEMENT BASIC_HOST_INFO_CHECKS (#PCDATA)>
<!ELEMENT OVAL_CHECKS (#PCDATA)>
<!ELEMENT QRDI_CHECKS (#PCDATA)>
<!ELEMENT DETECTION_EXCLUDE (CUSTOM_LIST+)><!ELEMENT AUTHENTICATION
(#PCDATA)>
<!ELEMENT AUTHENTICATION_LEAST_PRIVILEGE (#PCDATA)>
<!ELEMENT ADDL_CERT_DETECTION (#PCDATA)><!ELEMENT DISSOLVABLE_AGENT
(DISSOLVABLE_AGENT_ENABLE, PASSWORD_AUDITING_ENABLE?,
WINDOWS_SHARE_ENUMERATION_ENABLE, WINDOWS_DIRECTORY_SEARCH_ENABLE?)>
<!ELEMENT DISSOLVABLE_AGENT_ENABLE (#PCDATA)>
<!ELEMENT PASSWORD_AUDITING_ENABLE (HAS_PASSWORD_AUDITING_ENABLE?,
CUSTOM_PASSWORD_DICTIONARY?)>
<!ELEMENT HAS_PASSWORD_AUDITING_ENABLE (#PCDATA)>
<!ELEMENT CUSTOM_PASSWORD_DICTIONARY (#PCDATA)>
<!ELEMENT WINDOWS_SHARE_ENUMERATION_ENABLE (#PCDATA)>
<!ELEMENT WINDOWS_DIRECTORY_SEARCH_ENABLE (#PCDATA)><!ELEMENT
SCAN_RESTRICTION (SCAN_BY_POLICY?)>
<!ELEMENT SCAN_BY_POLICY  (POLICY+)>
<!ELEMENT POLICY (ID, TITLE)><!ELEMENT DATABASE_PREFERENCE_KEY (MSSQL?,
ORACLE?, SYBASE?, POSTGRESQL?, SAPIQ?, DB2?)>
<!ELEMENT MSSQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT ORACLE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SYBASE (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT POSTGRESQL (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT SAPIQ (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB2 (DB_UDC_RESTRICTION, DB_UDC_LIMIT)>
<!ELEMENT DB_UDC_RESTRICTION (#PCDATA)>
<!ELEMENT DB_UDC_LIMIT (#PCDATA)><!ELEMENT SYSTEM_AUTH_RECORD
(ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST,
IBM_WAS_DISCOVERY_MODE?, ORACLE_AUTHENTICATION_TEMPLATE?,
MONGODB_AUTHENTICATION_TEMPLATE?)>
<!ELEMENT AUTHENTICATION_TYPE_LIST  (AUTHENTICATION_TYPE+)>
<!ELEMENT AUTHENTICATION_TYPE (#PCDATA)>
<!ELEMENT IBM_WAS_DISCOVERY_MODE  (#PCDATA)>
<!ELEMENT ORACLE_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
<!ELEMENT MONGODB_AUTHENTICATION_TEMPLATE  (ID, TITLE)>
```

```
<!ELEMENT INCLUDE_SYSTEM_AUTH
(ON_DUPLICATE_USE_USER_AUTH|ON_DUPLICATE_USE_SYSTEM_AUTH)>
<!ELEMENT ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
```

PC API: Find Hosts Based on Last Scan Date

API affected	/pcrs/1.0/posture/hostids
New or Updated API	Updated
DTD or XSD changes	No

The Resolve Host IDs API has been updated to include a new optional parameter that helps you filter hosts based on the date on which the host was last scanned.

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

Input Parameters

Parameter	Description
lastScanDate	(Optional) Get host IDs based on the specified date on which they were last scanned. The formats for date are: lastScanDate=YYYY-MM-DD For example: lastScanDate=2022-05-25 Or, lastScanDate=2022-05-25T18:48:16Z

API Sample

Sample - Get hosts based on the specified date

In this sample, only the hosts that were last scanned on the date and time that are specified are listed.

API request:

```
curl -X GET https://gateway.<assigned
URL>/pcrs/1.0/posture/hostids?policyId=4677689&lastScanDate=2022-05-
25
-H "accept: */*"
-H
"Authorization: <token>"
```

Response:

```
[
    {
        "policyId": "4677689",
        "subscriptionId": "<SUBSCRIPTION ID>",
        "hostIds": [
            "<HOST ID 1>",
            "<HOST ID 2>",
            "<HOST ID 3>",
            "<HOST ID 4>",
            "<HOST ID 5>",
        ]
    }
]
```

PC API: Set Truncation Limit for Evidence Data

API affected	/pcrs/1.0/posture/postureInfo
New or Updated API	Updated
DTD or XSD changes	No

The Get Posture API has been updated to include a new optional parameter that helps you set a limit for posture evidence data. The evidence data beyond the specified limit is truncated.

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

Input Parameter

Parameter	Description
evidenceTruncationLimit	(Optional) Set a limit on asset posture evidence data. You can use this parameter if you have set the value for **evidenceRequired** parameter to **1**.

API Sample

Sample - Set a limit of 5 lines for the posture evidence data

API request:

```
curl -X POST "https://gateway.<assigned
URL>/pcrs/1.0/posture/postureInfo?evidenceRequired=1&compressionRe
quired=0&evidenceTruncationLimit=5" -H "accept: /" -H
"Authorization: Bearer " -H "Content-Type: application/json" -d "[

{\"policyId\":\"\",\"subscriptionId\":\"\",\"hostIds\":[\"\",\"\"]
}
]"
```

Response:

```
[
    {
        "id": xxxx,
        "instance": "MSSQL 2019:1:1433:MSSQLSERVER:master",
        "policyId": 5291724,
        "policyTitle": "<POLICY NAME>",
        "netBios": "<NET BIOS>",
        "controlId": <CONTROL ID>,
```

```
            "controlStatement": "MS_SQL-100081",
            "rationale": "rational_test",
            "remediation": null,
            "controlReference": null,
            "technologyId": xxx,
            "status": "Failed",
            "previousStatus": "Failed",
            "firstFailDate": "2022-11-07T12:22:00Z",
            "lastFailDate": "2022-12-16T12:33:11Z",
            "firstPassDate": "2022-11-07T12:43:27Z",
            "lastPassDate": "2022-11-07T12:43:27Z",
            "postureModifiedDate": "2022-11-07T12:58:37Z",
            "lastEvaluatedDate": "2022-12-16T12:33:10Z",
            "created": "2023-01-03T10:37:08Z",
            "hostId": <HOST ID>,
            "cloudResourceId": null,
            "ip": "xx.xx.xx.xxx",
            "trackingMethod": "IP",
            "os": null,
            "osCpe": "cpe:/o:microsoft:windows_10:2009::x64:",
            "domainName": "<DOMAIN NAME>",
            "dns": "<DNS>",
            "qgHostid": null,
            "networkId": 0,
            "networkName": "<NETWORK NAME>",
            "complianceLastScanDate": "2022-11-07T12:09:38Z",
            "customerUuid": "<CUSTOMER UUID>",
            "customerId": "<CUSTOMER ID>",
            "assetId": <ASSET ID>,
            "technology": {
                "id": xxx,
                "name": "Microsoft SQL Server 2019"
            },
            "criticality": {
                "label": "MINIMAL",
                "value": 1
            },
            "evidence": {
                "expectedValues": "Set status to PASS if no data
found\n------------ OR ------------\nDB Column Name
:SQLLoginWithPwdNotSetToExpire\nis contained in regular expression
list\n(rdsa|dbadmin|db_.+_node.+_login|rdsadmin|VASCANWIN|ConfigMg
rEndpointLogin\\w{3}$)",
                "currentValues": [
                    "SQLLoginWithPwdNotSetToExpire",
                    "qcrm80003",
                    "qncrestricted",
```

```
                "sqllogin_nlastname"
            ],
            "actualValues": [],
            "directoryFimUdc": []
        },
        "causeOfFailure": {
            "missing": {
                "logic": null,
                "value": []
            },
            "unexpected": {
                "value": [
                    "sqllogin_nlastname",
                    "qcrm80003",
                    "qncrestricted"
                ]
            }
        },
        "currentDataSizeKB": "1.70",
        "totalDataSizeKB": "1.70",
        "currentBatch": 1,
        "totalBatches": 1
    }
    ]
```