Qualys Enterprise TruRisk™ Platform

Limited Customer Release Notes

Version 10.36

December 24, 2025

Qualys Vulnerability Management (VM)

Support to Display Ultra Low Risk QIDs under Private Vulnerability Provider

Contents

Support to Display Private Vulnerability Provider

UI Enhancements

Introduction

The Ultra Low Risk includes QIDs for which the risk is pretty low, and vendors have not yet released a patch or recommended mitigations. The Ultra Low Risk is currently supported for Red Hat, Debian, and Ubuntu packaged-based vulnerabilities for which a patch has not been released by the vendors

Until a vendor officially provides a patch or guidance, or we observe a higher threat impact on these vulnerabilities, these vulnerabilities will remain classified as **Ultra Low Risk,** and the associated risk will be considered **low**. As a result, the **QVS/QDS scores** for these detections will either be **unavailable** or marked as **low/medium**.

Once a vendor releases a patch or mitigation for any such QID, or if we observe a higher threat impact associated with these vulnerabilities, the existing QIDs are deprecated, and new QIDs are released. The new QID is added to the standard vulnerability management pipeline and included in the broader list of QIDs for active vulnerability tracking. At that point, if the vulnerability is contributing to a significant risk, the related QVS/QDS score are updated accordingly, considering the potential threats as High or Critical severity.

With this feature, you can now filter Ultra Low Risk QIDs in the scan report. To enable this, we have added a new field, **Private Vuln Provider**, and an **Ultra Low Risk** checkbox under Private Vuln Provider in the scan report template and Option Profile. To enhance the user experience, we have renamed the Unfixed QID to **Ultra Low Risk** in both the Dynamic Vulnerability Search Lists, including the Report and Knowledge Base **Search Lists**.

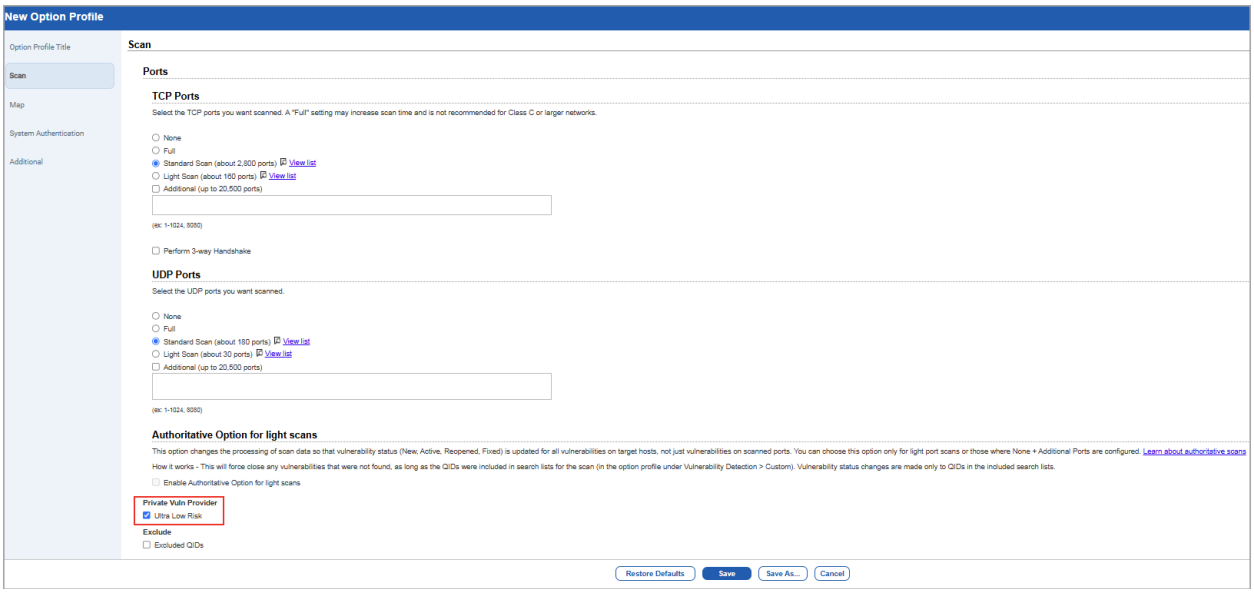
Benefits

The following are the benefits of displaying ultra low risk QIDs in the scan report:

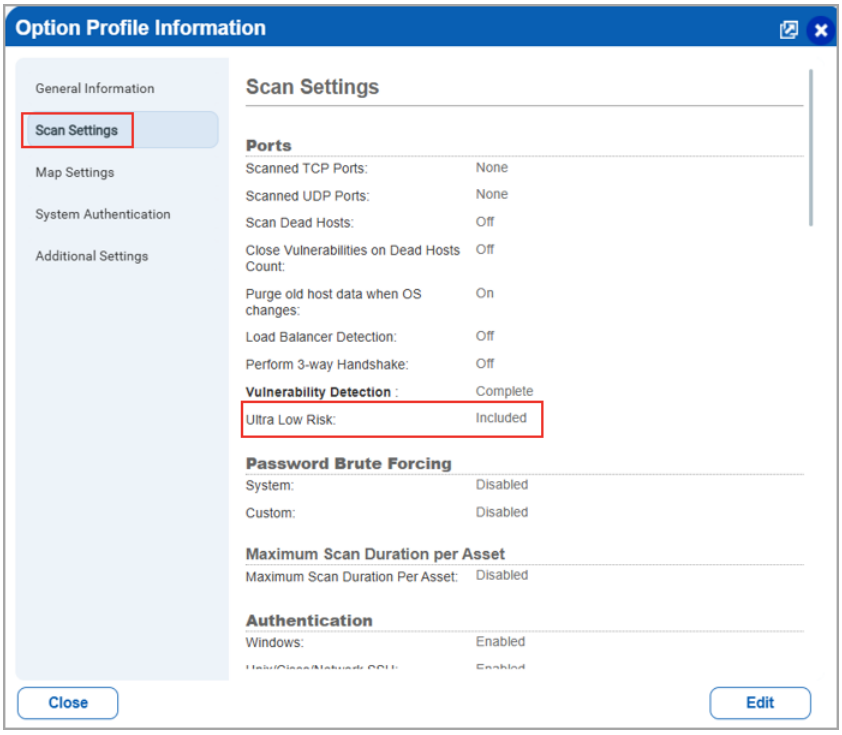
- **Clear Visibility:** Displaying the ultra low risk vulnerabilities highlights the remediation action required for the vulnerabilities to be fixed.
- **Supports prioritization:** This helps you to keep track of the ultra low risk vulnerabilities and prioritize the remediation based on the criticality.

Added Private Vuln Provider in the Option Profile

We have introduced a new option, Private Vuln Provider: Ultra Low Risk, which allows you to exclude or launch Ultra Low QIDs from the scan. When you enable this option (**Scans** > **Option Profiles** > **New** > **Option Profile** > **Scan** > **Private Vuln Provider**) and perform a scan operation, all the ultra low risk QIDs are visible in your scan. With this feature, you can exclude all the ultra low risk QIDs from being scanned.



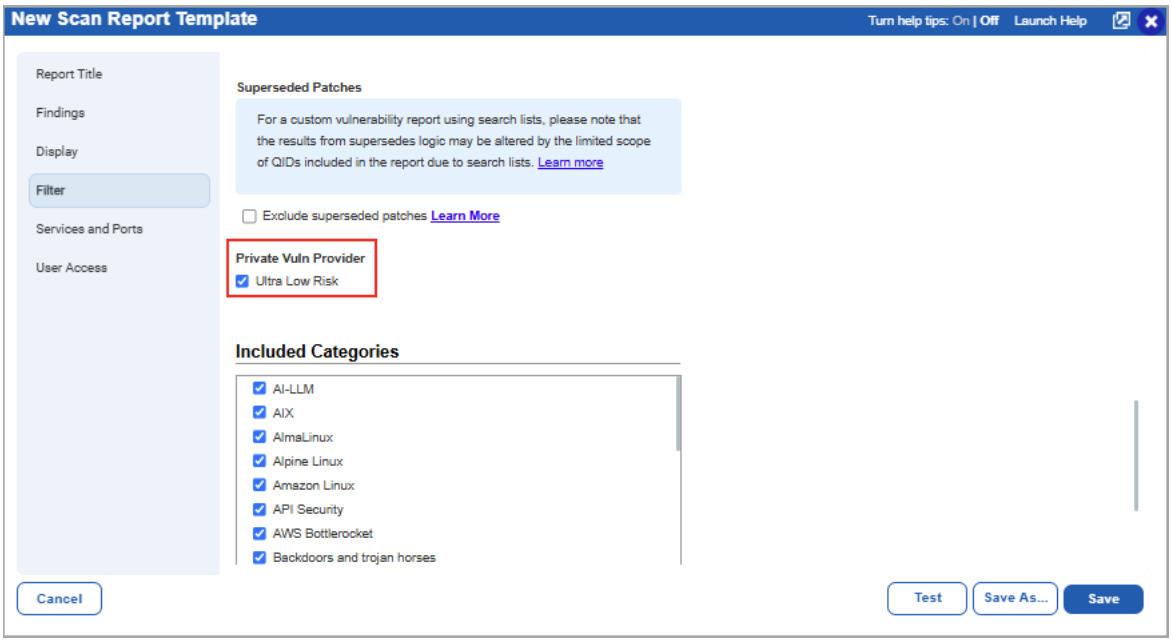
You can view the Ultra Low Risk included in the Scan Settings under Option Profile Information (Select any of the Option Profiles > select Info from **Quick Actions** menu). You can focus on higher risk vulnerabilities by excluding the ultra low risk QIDs, which saves your scan time.



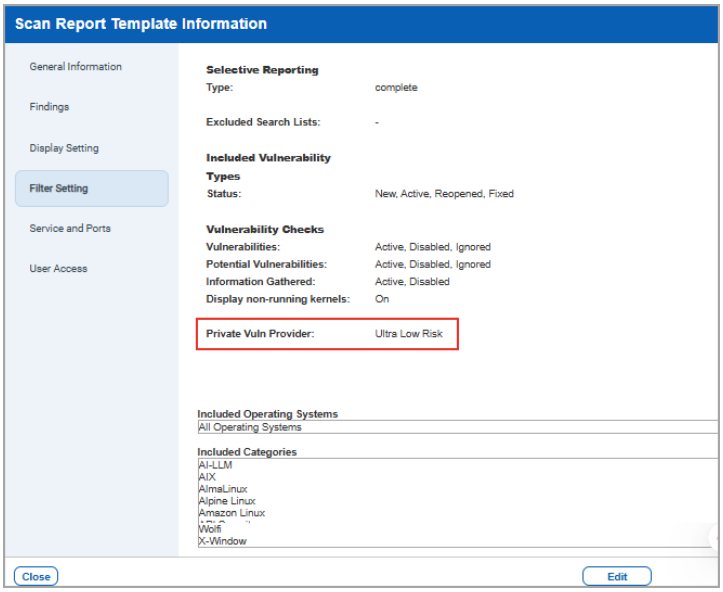
Note: In the consequent scans, when this option is disabled, the existing ultra low risk QIDs are ignored, and no further processing is performed on those QIDs. The status of the QIDs remains the same as earlier, for example, if the earlier status is open, it remains the same now also.

Added Private Vuln Provider in the Scan Report Template

We have provided a new option, **Private Vuln Provider: Ultra Low Risk**, to support the detection of vulnerabilities in VMDR. You can view this option by navigating to **Report** > **Templates** > **New** > **Scan Templates** > **QID Based Template** > **Filter** > **Private Vuln Provider** > **Ultra Low Risk.**



When you enable this option, you can view all the ultra low risk QIDs in the report. You can view the private vulnerability provider in the scan report template information under **Filter Setting** (**Report** > **Templates** > Select a template > Select **Info** from **Quick Actions** > **Filter Setting**).



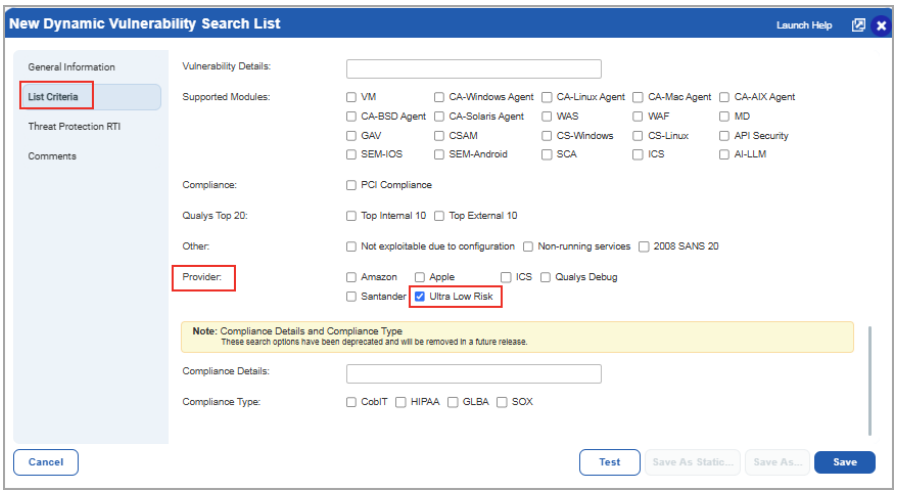
Notes:

- This is applicable to both Host based and Scan Based Scan reports
- Ultra Low Severity QIDs are visible in all the report formats, such as PDF, CSV, HTML, DOCX, and XML.

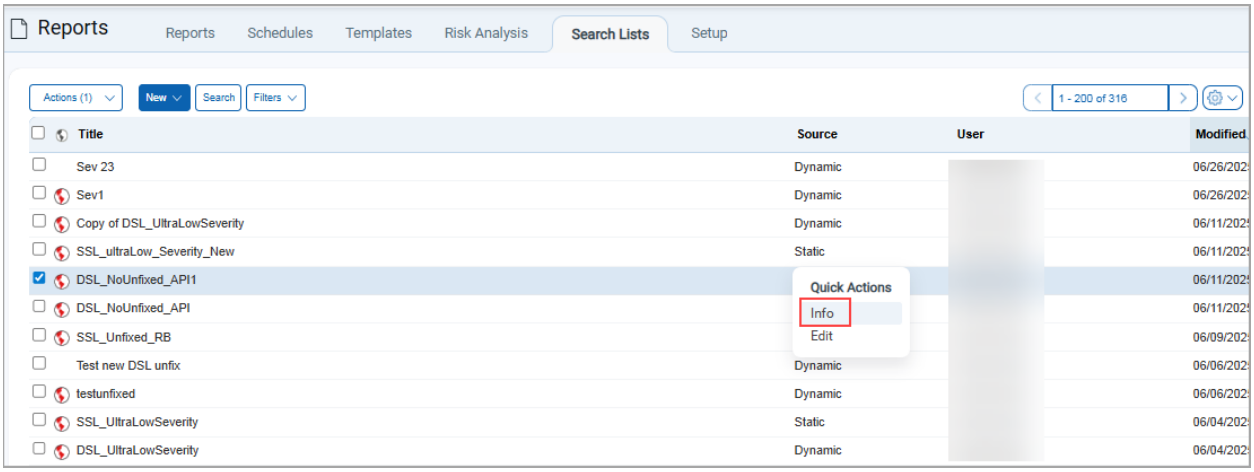
- Delay might be observed while generating the reports when this feature is activated for your subscription.

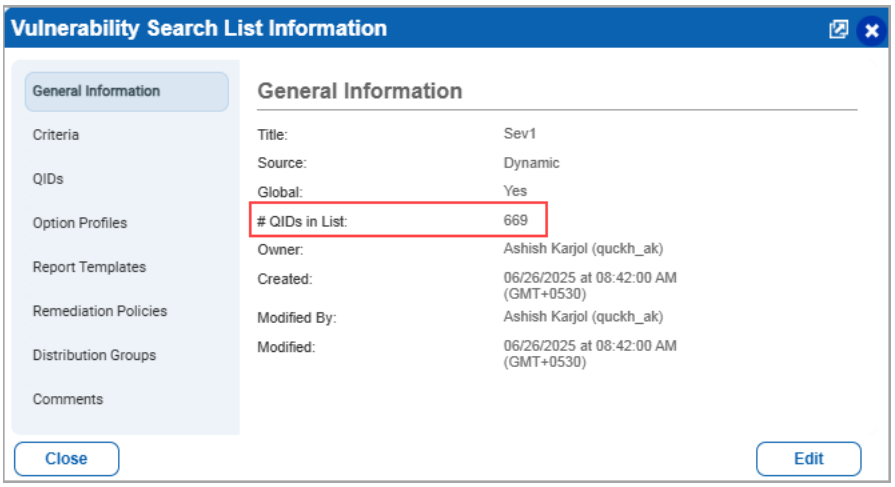
Renamed the Provider name in Dynamic Vulnerability Search Lists

To enhance the user experience, we have renamed the Unfixed QID name to **Ultra Low Risk** in the **New Dynamic Vulnerability Search List** in **Reports and KnowledgeBase Search list** (**Reports/KnowledgeBase** > **Search Lists** > **New** > **Dynamic List** > **List Criteria** > **Provider** > **Ultra Low Risk**).

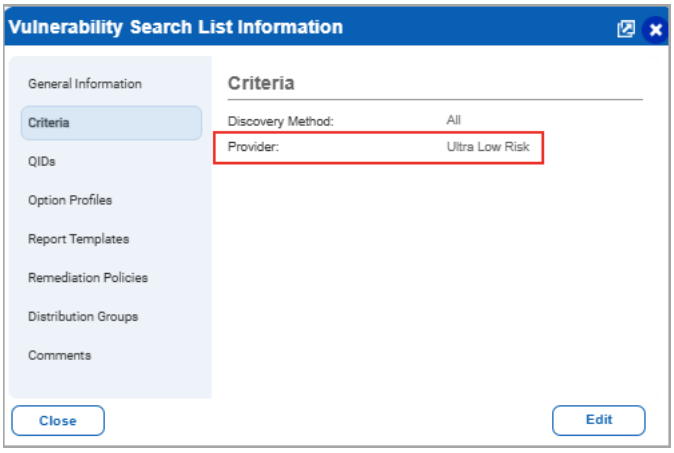


If a dynamic search list is created with **Ultra Low Risk** enabled in either report search lists or KnowledgeBase search lists, the Ultra Low Severity QIDs are visible in the **Vulnerability Search List Information** page (Click any one of the Titles > **Info** from the **Quick Actions** menu).





You can view the provider as **Ultra Low Risk** under **Criteria** when you select the **Ultra Low Risk** checkbox under the **List Criteria** of Dynamic Search.



If you need to view only particular ultra low risk QIDs, then a static search list can be used within the report. Accordingly, you can filter only the particular ultra low risk QIDs in the report.

API Enhancement

Option Profile API: New Tag Added in the Option Profile

New or Updated API	Updated
API Endpoint (deprecation Timeline - December 2025)	/api/3.0/fo/subscription/option_profile/vm/
API Endpoint (New Version)	/api/4.0/fo/subscription/option_profile/vm/
Method	GET, POST
DTD or XSD changes	No

You can now create, update, list, import, and export an option profile. We have implemented versioning to perform create, update, and list actions. When you perform a scan to list all the ultra low risk QIDs with the input parameter set to 1, you can view the input parameter tag in the response. Simultaneously, you can observe the tag being added automatically when you perform an export action on the option profile.

Note: If you make any changes to the list action in the export or import action, the export or import action also has an impact, which is reflected in the tag displayed in the response.

Input Parameter

Parameter	Required/Optional	Data Type	Description
Include_ultra_low_risk_vulns={0|1}	Optional	Integer	Specify 1 to view all ultra-low-risk QIDs when performing the scan. This is supported for create and update option profile.

Sample: To create an option profile

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?%20action=create&scan_tcp_ports=none&scan_udp_ports=none&vulnerability_detection=complete&basic_information_gathering=none%20&include_ultra_low_risk_vulns=1&title=newv3366' \
--header 'Content-Type: test/xml' \
--header 'X-Requested-With: test' \
--header 'Accept-Encoding: *' \
--header 'Authorization: Bearer  <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
  <SIMPLE_RETURN>
    <RESPONSE>
      <DATETIME>2025-09-29T07:00:16Z</DATETIME>
      <TEXT>Option profile successfully added.</TEXT>
      <ITEM_LIST>
        <ITEM>
          <KEY>ID</KEY>
          <VALUE>7807370</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
  </SIMPLE_RETURN>
```

Sample: To update an option profile

API Request:

```
curl --location --request POST '
```

```
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?%20action=update&scan_tcp_port
s=none&scan_udp_ports=none&vulnerability_detection=complete&basic_information_gathering
=none%20&include_ultra_low_risk_vulns=0&id=7807370' \
--header 'Content-Type: test/xml' \
--header 'X-Requested-With: test' \
--header 'Accept-Encoding: *' \
--header 'Authorization: Bearer
   <JWT Token>'
```

API Response:

```
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
   <SIMPLE_RETURN>
      <RESPONSE>
         <DATETIME>2025-09-29T08:01:13Z</DATETIME>
         <TEXT>Option profile successfully updated.</TEXT>
         <ITEM_LIST>
            <ITEM>
               <KEY>ID</KEY>
               <VALUE>7807370</VALUE>
            </ITEM>
         </ITEM_LIST>
      </RESPONSE>
   </SIMPLE_RETURN>
```

Sample: To list an option profile

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/4.0/fo/subscription/option_profile/vm/?%20action=list&title=newv3366' \
--header 'Content-Type: test/xml' \
--header 'X-Requested-With: test' \
--header 'Accept-Encoding: *' \
--header 'Authorization: Bearer  <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd">
   <OPTION_PROFILES>
      <OPTION_PROFILE>
         <BASIC_INFO>
            <ID>7807370</ID>
            <GROUP_NAME>
               <![CDATA[newv3366]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
               <![CDATA[t b (vmspxtb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
```

```
        <IS_DEFAULT>0</IS_DEFAULT>
        <IS_GLOBAL>0</IS_GLOBAL>
        <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
        <UPDATE_DATE>2025-09-29T08:11:53Z</UPDATE_DATE>
      </BASIC_INFO>
      <SCAN>
        <PORTS>
          <TCP_PORTS>
            <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
            <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
          </TCP_PORTS>
          <UDP_PORTS>
            <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
          </UDP_PORTS>
          <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
        </PORTS>
        <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
        <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
        <PERFORMANCE>
          <PARALLEL_SCALING>1</PARALLEL_SCALING>
          <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
          <HOSTS_TO_SCAN>
            <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
            <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
          </HOSTS_TO_SCAN>
          <PROCESSES_TO_RUN>
            <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
            <HTTP_PROCESSES>20</HTTP_PROCESSES>
          </PROCESSES_TO_RUN>
          <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVE
RY>
          <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
          <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>
          <CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
          <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
        </PERFORMANCE>
        <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
        <VULNERABILITY_DETECTION>
          <COMPLETE>
            <![CDATA[complete]]>
          </COMPLETE>
          <DETECTION_INCLUDE>
            <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
            <OVAL_CHECKS>0</OVAL_CHECKS>
            <QRDI_CHECKS>0</QRDI_CHECKS>
            <ULTRA_LOW_RISK_VULNS>1</ULTRA_LOW_RISK_VULNS>
          </DETECTION_INCLUDE>
        </VULNERABILITY_DETECTION>
        <AUTHENTICATION>
          <![CDATA[Windows,Unix]]>
        </AUTHENTICATION>
```

```
          <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
          <DISSOLVABLE_AGENT>
            <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
          </DISSOLVABLE_AGENT>
        </SCAN>
        <MAP>
          <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
          <MAP_OPTIONS>
            <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
          </MAP_OPTIONS>
          <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
              <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
              <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Minimum</PACKET_DELAY>
          </MAP_PERFORMANCE>
          <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
          <HOST_DISCOVERY>
            <TCP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </TCP_PORTS>
            <UDP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </UDP_PORTS>
            <ICMP>0</ICMP>
          </HOST_DISCOVERY>
          <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
            <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SY
N_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: To export an option profile

API Request:

```
curl --location '
```

```
<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action=export&option_profile_title=ne
wv3366' \
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd">
   <OPTION_PROFILES>
      <OPTION_PROFILE>
         <BASIC_INFO>
            <ID>7807370</ID>
            <GROUP_NAME>
               <![CDATA[newv3366]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
               <![CDATA[t b (vmspxtb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2025-09-29T08:11:53Z</UPDATE_DATE>
         </BASIC_INFO>
         <SCAN>
            <PORTS>
               <TCP_PORTS>
                  <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                  <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
               </TCP_PORTS>
               <UDP_PORTS>
                  <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
               </UDP_PORTS>
               <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
            </PORTS>
            <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
            <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
            <PERFORMANCE>
               <PARALLEL_SCALING>1</PARALLEL_SCALING>
               <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
               <HOSTS_TO_SCAN>
                  <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
                  <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
               </HOSTS_TO_SCAN>
               <PROCESSES_TO_RUN>
                  <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
                  <HTTP_PROCESSES>20</HTTP_PROCESSES>
               </PROCESSES_TO_RUN>
               <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVE
RY>
```

```
            <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
            <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>
            <CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
            <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
          </PERFORMANCE>
          <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
          <VULNERABILITY_DETECTION>
            <COMPLETE>
              <![CDATA[complete]]>
            </COMPLETE>
            <DETECTION_INCLUDE>
              <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
              <OVAL_CHECKS>0</OVAL_CHECKS>
              <QRDI_CHECKS>0</QRDI_CHECKS>
              <ULTRA_LOW_RISK_VULNS>1</ULTRA_LOW_RISK_VULNS>
            </DETECTION_INCLUDE>
          </VULNERABILITY_DETECTION>
          <AUTHENTICATION>
            <![CDATA[Windows,Unix]]>
          </AUTHENTICATION>
          <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
          <DISSOLVABLE_AGENT>
            <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
          </DISSOLVABLE_AGENT>
        </SCAN>
        <MAP>
          <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
          <MAP_OPTIONS>
            <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
          </MAP_OPTIONS>
          <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
              <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
              <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Minimum</PACKET_DELAY>
          </MAP_PERFORMANCE>
          <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
          <HOST_DISCOVERY>
            <TCP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </TCP_PORTS>
            <UDP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </UDP_PORTS>
            <ICMP>0</ICMP>
```

```
            </HOST_DISCOVERY>
            <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
               <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SY
N_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: To import an option profile

API Request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/subscription/option_profile/?action=import' \
--header 'X-Requested-With: curl' \
--header 'Content-Type: application/xml' \
--header 'Authorization: Bearer
   <JWT Token>' \
--data ' <?xml version="1.0" encoding="UTF-8" ?>
```

API Response:

```
<!DOCTYPE OPTION_PROFILES SYSTEM "
<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd">
   <OPTION_PROFILES>
      <OPTION_PROFILE>
         <BASIC_INFO>
            <ID>7807373</ID>
            <GROUP_NAME>
               <![CDATA[newv33636]]>
            </GROUP_NAME>
            <GROUP_TYPE>user</GROUP_TYPE>
            <USER_ID>
               <![CDATA[t b (vmspxtb)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>4428525</SUBSCRIPTION_ID>
            <IS_DEFAULT>0</IS_DEFAULT>
            <IS_GLOBAL>0</IS_GLOBAL>
            <IS_OFFLINE_SYNCABLE>0</IS_OFFLINE_SYNCABLE>
            <UPDATE_DATE>2025-09-29T08:11:53Z</UPDATE_DATE>
         </BASIC_INFO>
         <SCAN>
            <PORTS>
               <TCP_PORTS>
                  <TCP_PORTS_TYPE>none</TCP_PORTS_TYPE>
                  <THREE_WAY_HANDSHAKE>0</THREE_WAY_HANDSHAKE>
```

```
            </TCP_PORTS>
            <UDP_PORTS>
              <UDP_PORTS_TYPE>none</UDP_PORTS_TYPE>
            </UDP_PORTS>
            <AUTHORITATIVE_OPTION>0</AUTHORITATIVE_OPTION>
          </PORTS>
          <SCAN_DEAD_HOSTS>0</SCAN_DEAD_HOSTS>
          <PURGE_OLD_HOST_OS_CHANGED>1</PURGE_OLD_HOST_OS_CHANGED>
          <PERFORMANCE>
            <PARALLEL_SCALING>1</PARALLEL_SCALING>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <HOSTS_TO_SCAN>
              <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>50</SCANNER_APPLIANCES>
            </HOSTS_TO_SCAN>
            <PROCESSES_TO_RUN>
              <TOTAL_PROCESSES>20</TOTAL_PROCESSES>
              <HTTP_PROCESSES>20</HTTP_PROCESSES>
            </PROCESSES_TO_RUN>
            <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVE
RY>
            <HOST_CGI_CHECKS>0</HOST_CGI_CHECKS>
            <MAX_TARGETS_PER_SLICE>0</MAX_TARGETS_PER_SLICE>
            <CONF_SCAN_LIMITED_CONNECTIVITY>0</CONF_SCAN_LIMITED_CONNECTIVITY>
            <SKIP_PRE_SCANNING>0</SKIP_PRE_SCANNING>

<SCAN_MULTIPLE_SLICES_PER_SCANNER>0</SCAN_MULTIPLE_SLICES_PER_SCANNER>
          </PERFORMANCE>
          <LOAD_BALANCER_DETECTION>0</LOAD_BALANCER_DETECTION>
          <VULNERABILITY_DETECTION>
            <COMPLETE>
              <![CDATA[complete]]>
            </COMPLETE>
            <DETECTION_INCLUDE>
              <BASIC_HOST_INFO_CHECKS>0</BASIC_HOST_INFO_CHECKS>
              <OVAL_CHECKS>0</OVAL_CHECKS>
              <QRDI_CHECKS>0</QRDI_CHECKS>
              <ULTRA_LOW_RISK_VULNS>1</ULTRA_LOW_RISK_VULNS>
            </DETECTION_INCLUDE>
          </VULNERABILITY_DETECTION>
          <AUTHENTICATION>
            <![CDATA[Windows,Unix]]>
          </AUTHENTICATION>
          <ADDL_CERT_DETECTION>0</ADDL_CERT_DETECTION>
          <DISSOLVABLE_AGENT>
            <DISSOLVABLE_AGENT_ENABLE>1</DISSOLVABLE_AGENT_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>
          </DISSOLVABLE_AGENT>
        </SCAN>
        <MAP>
          <BASIC_INFO_GATHERING_ON>none</BASIC_INFO_GATHERING_ON>
          <MAP_OPTIONS>
```

```
            <PERFORM_LIVE_HOST_SWEEP>0</PERFORM_LIVE_HOST_SWEEP>
            <DISABLE_DNS_TRAFFIC>0</DISABLE_DNS_TRAFFIC>
          </MAP_OPTIONS>
          <MAP_PERFORMANCE>
            <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
            <MAP_PARALLEL>
              <EXTERNAL_SCANNERS>6</EXTERNAL_SCANNERS>
              <SCANNER_APPLIANCES>8</SCANNER_APPLIANCES>
              <NETBLOCK_SIZE>16384 IPs</NETBLOCK_SIZE>
            </MAP_PARALLEL>
            <PACKET_DELAY>Minimum</PACKET_DELAY>
          </MAP_PERFORMANCE>
          <MAP_AUTHENTICATION>none</MAP_AUTHENTICATION>
        </MAP>
        <ADDITIONAL>
          <HOST_DISCOVERY>
            <TCP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </TCP_PORTS>
            <UDP_PORTS>
              <STANDARD_SCAN>1</STANDARD_SCAN>
            </UDP_PORTS>
            <ICMP>0</ICMP>
          </HOST_DISCOVERY>
          <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>1</IGNORE_FIREWALL_GENERATED_TCP_RST>
            <IGNORE_ALL_TCP_RST>0</IGNORE_ALL_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>1</IGNORE_FIREWALL_GENERATED_TCP_SY
N_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>
```

DTD Output

```
curl --location '<qualys_base_url>/api/4.0/fo/subscription/option_profile/option_profile_info.dtd'
<!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?, DEAD_HOST_PROCESSING?,
DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?, MAX_SCAN_DURATION_PER_ASSET?,
PERFORM_PARTIAL_SSL_TLS_AUDITING?)>
<!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?,**ULTRA_LOW_RISK_VULNS?**)>
<!ELEMENT BASIC_HOST_INFO_CHECKS (#PCDATA)>
<!ELEMENT OVAL_CHECKS (#PCDATA)>
<!ELEMENT QRDI_CHECKS (#PCDATA)>
<!ELEMENT ULTRA_LOW_RISK_VULNS (#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?, MYSQL_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 MYSQL_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)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>
<!ELEMENT LITE_OS_SCAN (#PCDATA)>
<!ELEMENT CUSTOM_HTTP_HEADER (VALUE?, DEFINITION_KEY?, DEFINITION_VALUE?)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT DEFINITION_KEY (#PCDATA)>
<!ELEMENT DEFINITION_VALUE (#PCDATA)>
<!ELEMENT HOST_ALIVE_TESTING (#PCDATA)>
<!ELEMENT ETHERNET_IP_PROBING (#PCDATA)>
<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
<!ELEMENT AUTO_UPDATE_EXPECTED_VALUE (#PCDATA)>
<!ELEMENT CONTROL_TYPES (FIM_CONTROLS_ENABLED?, CUSTOM_WMI_QUERY_CHECKS?)>
<!ELEMENT FIM_CONTROLS_ENABLED (#PCDATA)>
<!ELEMENT CUSTOM_WMI_QUERY_CHECKS (#PCDATA)>
<!ELEMENT DO_NOT_OVERWRITE_OS (#PCDATA)>
<!ELEMENT TEST_AUTHENTICATION (#PCDATA)>
<!ELEMENT PERFORM_PARTIAL_SSL_TLS_AUDITING (#PCDATA)>
<!ELEMENT MAP (BASIC_INFO_GATHERING_ON, TCP_PORTS?, UDP_PORTS?, MAP_OPTIONS?,
MAP_PERFORMANCE?, MAP_AUTHENTICATION?, DISCONNECTED_ESXI?)>
<!ELEMENT BASIC_INFO_GATHERING_ON (#PCDATA)>
<!ELEMENT TCP_PORTS_STANDARD_SCAN (#PCDATA)>
<!ELEMENT UDP_PORTS_STANDARD_SCAN (#PCDATA)>
<!ELEMENT MAP_OPTIONS (PERFORM_LIVE_HOST_SWEEP?, DISABLE_DNS_TRAFFIC?)>
<!ELEMENT PERFORM_LIVE_HOST_SWEEP (#PCDATA)>
<!ELEMENT DISABLE_DNS_TRAFFIC (#PCDATA)>
<!ELEMENT MAP_PERFORMANCE (OVERALL_PERFORMANCE, MAP_PARALLEL?, PACKET_DELAY)>
<!ELEMENT MAP_PARALLEL (EXTERNAL_SCANNERS, SCANNER_APPLIANCES, NETBLOCK_SIZE)>
<!ELEMENT NETBLOCK_SIZE (#PCDATA)>
<!ELEMENT MAP_AUTHENTICATION (#PCDATA)>
<!ELEMENT DISCONNECTED_ESXI (#PCDATA)>
<!ELEMENT ADDITIONAL (HOST_DISCOVERY, BLOCK_RESOURCES?, PACKET_OPTIONS?)>
<!ELEMENT HOST_DISCOVERY (TCP_PORTS?, UDP_PORTS?, ICMP?)>
<!ELEMENT TCP_ADDITIONAL (HAS_ADDITIONAL?, ADDITIONAL_PORTS?)>
<!ELEMENT CUSTOM_PORT (#PCDATA)>
<!ELEMENT ICMP (#PCDATA)>
<!ELEMENT BLOCK_RESOURCES
((WATCHGUARD_DEFAULT_BLOCKED_PORTS|CUSTOM_PORT_LIST),
(ALL_REGISTERED_IPS|CUSTOM_IP_LIST))>
<!ELEMENT WATCHGUARD_DEFAULT_BLOCKED_PORTS (#PCDATA)>
<!ELEMENT CUSTOM_PORT_LIST (#PCDATA)>
<!ELEMENT ALL_REGISTERED_IPS (#PCDATA)>
<!ELEMENT CUSTOM_IP_LIST (#PCDATA)>
<!ELEMENT PACKET_OPTIONS (IGNORE_FIREWALL_GENERATED_TCP_RST?,
IGNORE_ALL_TCP_RST?, IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK?,
NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY?)>
<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_RST (#PCDATA)>
<!ELEMENT IGNORE_ALL_TCP_RST (#PCDATA)>

<!ELEMENT IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK (#PCDATA)>
<!ELEMENT NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY (#PCDATA)>
<!ELEMENT INSTANCE_DATA_COLLECTION (DATABASES?)>
<!ELEMENT DATABASES (AUTHENTICATION_TYPES_LIST)>
<!ELEMENT AUTHENTICATION_TYPES_LIST (AUTHENTICATION_TYPE+)>
<!ELEMENT OS_BASED_INSTANCE_DISC_COLLECTION (TECHNOLOGIES?)>
<!ELEMENT TECHNOLOGIES (TECHNOLOGY+)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT DEAD_HOST_PROCESSING (PROCESS_DEAD_HOST_ENABLED?,
DEAD_HOST_TIMES_NOT_FOUND?)>
<!ELEMENT PROCESS_DEAD_HOST_ENABLED (#PCDATA)>
<!ELEMENT DEAD_HOST_TIMES_NOT_FOUND (#PCDATA)>

Scan Template API: Enhanced Report Efficiency with QID Based Template

New or Updated API	Updated
API Endpoint (deprecation Timeline - December 2025)	api/3.0/fo/report/template/scan/
API Endpoint (New Version)	api/4.0/fo/report/template/scan/
Method	GET, POST
DTD or XSD changes	No

With this feature, you can now create, update, delete, and export the QID based scan report template. This helps you improve risk visibility and response efficiency, ensuring reports highlight vulnerabilities.

Sample: To create a report scan template

API Request:

```
curl --location
'<qualys_base_url>/api/4.0/fo/report/template/scan/?action=create&report_format=xml' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
--data '<SCANTEMPLATE>
```

API Response

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
  <SIMPLE_RETURN>
    <RESPONSE>
      <DATETIME>2025-06-30T12:10:57Z</DATETIME>
      <TEXT>Scan Report Template(s) Successfully Created.</TEXT>
      <ITEM_LIST>
        <ITEM>
          <KEY>ID</KEY>
          <VALUE>8829399</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
  </SIMPLE_RETURN>
```

Sample: To update a report scan template

API Request:

```
curl --location
'<qualys_base>/api/4.0/fo/report/template/scan/?action=update&report_format=xml&template_
id=8829399' \
--header 'Accept: */*' \
--header 'X-Requested-With: curl' \
--header 'content-type: text/xml' \
--header 'Authorization: Bearer <JWT Token>' \
--data '<?xml version="1.0" encoding="UTF-8" ?>
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url>/api/4.0/simple_return.dtd">
  <SIMPLE_RETURN>
    <RESPONSE>
      <DATETIME>2025-06-30T12:23:06Z</DATETIME>
      <TEXT>Scan Report Template Successfully Updated.</TEXT>
      <ITEM_LIST>
        <ITEM>
          <KEY>ID</KEY>
          <VALUE>8829399</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
  </SIMPLE_RETURN>
```

Sample: To export a report scan template

API Request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/report/template/scan/?action=export&report_format=xml&templa
te_id=8829399' \
```

```
--header 'X-Requested-With: curl' \
--header 'Authorization: Bearer <JWT Token>'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE REPORTTEMPLATE SYSTEM "
<qualys_base_url>/api/4.0/fo/report/template/scan/scanreporttemplate_info.dtd">
   <REPORTTEMPLATE>
      <SCANTEMPLATE>
         <TITLE>
            <INFO key="template_id">
               <![CDATA[8829399]]>
            </INFO>
            <INFO key="title">
               <![CDATA[update_ultraLowSeverityAPI1]]>
            </INFO>
            <INFO key="owner">
               <![CDATA[221146]]>
            </INFO>
         </TITLE>
         <TARGET>
            <INFO key="scan_selection">
               <![CDATA[HostBased]]>
            </INFO>
            <INFO key="include_trending">
               <![CDATA[1]]>
            </INFO>
            <INFO key="selection_type">
               <![CDATA[days]]>
            </INFO>
            <INFO key="selection_range">
               <![CDATA[15]]>
            </INFO>
            <INFO key="limit_timeframe">
               <![CDATA[0]]>
            </INFO>
            <INFO key="asset_groups">
               <![CDATA[]]>
            </INFO>
            <INFO key="network">
               <![CDATA[-100]]>
            </INFO>
            <INFO key="ips">
               <![CDATA[]]>
            </INFO>
            <INFO key="host_with_cloud_agents">
               <![CDATA[all]]>
            </INFO>
         </TARGET>
         <DISPLAY>
            <INFO key="graph_business_risk">
               <![CDATA[0]]>
            </INFO>
            <INFO key="graph_vuln_over_time">
```

```
    <![CDATA[0]]>
</INFO>
<INFO key="display_text_summary">
    <![CDATA[1]]>
</INFO>
<INFO key="graph_status">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_potential_status">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_potential_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_ig_severity">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_categories">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_vulns">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_os">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_services">
    <![CDATA[0]]>
</INFO>
<INFO key="graph_top_ports">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer">
    <![CDATA[0]]>
</INFO>
<INFO key="display_custom_footer_text">
    <![CDATA[]]>
</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>
<INFO key="qualys_system_ids">
    <![CDATA[1]]>
```

```
    </INFO>
    <INFO key="include_text_summary">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_threat">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_impact">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_solution">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_vpatch">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_compliance">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_exploit">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_malware">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_results">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_appendix">
      <![CDATA[0]]>
    </INFO>
    <INFO key="exclude_account_id">
      <![CDATA[0]]>
    </INFO>
    <INFO key="include_vuln_details_reopened">
      <![CDATA[1]]>
    </INFO>
    <INFO key="metadata_ec2_instances">
      <![CDATA[1]]>
    </INFO>
    <INFO key="cloud_provider_metadata">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_vuln_details_detection_logic">
      <![CDATA[1]]>
    </INFO>
    <INFO key="include_trurisk_details">
      <![CDATA[1]]>
    </INFO>
  </DISPLAY>
  <FILTER>
    <INFO key="selective_vulns">
```

```
    <![CDATA[complete]]>
  </INFO>
  <INFO key="search_list_ids">
    <![CDATA[]]>
  </INFO>
  <INFO key="exclude_qid_option">
    <![CDATA[0]]>
  </INFO>
  <INFO key="exclude_search_list_ids">
    <![CDATA[]]>
  </INFO>
  <INFO key="included_os">
    <![CDATA[ALL]]>
  </INFO>
  <INFO key="status_new">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_reopen">
    <![CDATA[1]]>
  </INFO>
  <INFO key="status_fixed">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="vuln_ignored">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="potential_ignored">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_active">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_disabled">
    <![CDATA[1]]>
  </INFO>
  <INFO key="ig_ignored">
    <![CDATA[0]]>
  </INFO>
  <INFO key="display_non_running_kernels">
    <![CDATA[1]]>
```

```
        </INFO>
        <INFO key="exclude_non_running_kernel">
          <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_non_running_services">
          <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_superceded_patches">
          <![CDATA[0]]>
        </INFO>
        <INFO key="exclude_qids_not_exploitable_due_to_configuration">
          <![CDATA[0]]>
        </INFO>
        <INFO key="categories_list">
          <![CDATA[ALL]]>
        </INFO>
        <INFO key="qds_score_min">
          <![CDATA[]]>
        </INFO>
        <INFO key="qds_score_max">
          <![CDATA[]]>
        </INFO>
        <INFO key="ultra_low_risk">
          <![CDATA[1]]>
        </INFO>
      </FILTER>
      <SERVICESPORTS>
        <INFO key="required_services">
          <![CDATA[]]>
        </INFO>
        <INFO key="unauthorized_services">
          <![CDATA[]]>
        </INFO>
        <INFO key="services_info">
          <![CDATA[]]>
        </INFO>
        <INFO key="required_ports">
          <![CDATA[]]>
        </INFO>
        <INFO key="unauthorized_ports">
          <![CDATA[]]>
        </INFO>
      </SERVICESPORTS>
      <USERACCESS>
        <INFO key="global">
          <![CDATA[1]]>
        </INFO>
        <INFO key="report_access_users">
          <![CDATA[]]>
        </INFO>
      </USERACCESS>
    </SCANTEMPLATE>
  </REPORTTEMPLATE>
```

Sample: To delete a report scan template

API Request:

```
curl --location '
<qualys_base_url>/api/4.0/fo/report/template/scan/' \
--header 'X-Requested-With: curl' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Bearer <JWT Token>' \
--data-urlencode 'template_id=8829399' \
--data-urlencode 'action=delete'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "
<qualys_base_url./api/2.0/simple_return.dtd">
  <SIMPLE_RETURN>
    <RESPONSE>
      <DATETIME>2025-06-30T12:28:22Z</DATETIME>
      <TEXT>Scan Report Template(s) Successfully Deleted.</TEXT>
      <ITEM_LIST>
        <ITEM>
          <KEY>ID</KEY>
          <VALUE>8829399</VALUE>
        </ITEM>
      </ITEM_LIST>
    </RESPONSE>
  </SIMPLE_RETURN>
```

Dynamic search API: Enhance Search Efficiency using Dynamic Search

New or Updated API	Updated
API Endpoint (New Version)	/api/2.0/fo/qid/search_list/dynamic/
Method	POST
DTD or XSD changes	No

You can now create, update, and export a dynamic search list to ensure you always access the most current and relevant data, improving decision-making and operational efficiency. It also enables seamless integration across systems, reducing manual effort and enhancing scalability.

Sample - Create Dynamic Search List

API Request:

```
curl --location --request POST '
<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/?action=create&title=DSL_ULR_API_RB&gl
obal=1&comments=Dynamic%20SL%20Created%20for%20QID%20Service&vuln_provider=Ultra
%20Low%20Risk' \
--header 'Accept: */*' \
--header 'Accept-Encoding: gzip, deflate' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Connection: keep-alive' \
```

```
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'User-Agent: python-requests/2.19.1' \
--header 'X-Access-Token: automation' \
--header 'X-Requested-With: curl'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "<qualys-base_url./api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-10-17T04:49:23Z</DATETIME>
    <TEXT>New search list created successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6038506</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Update Dynamic Search List

API Request

```
curl --location --request POST 'https://<qualys-
base_url>/api/2.0/fo/qid/search_list/dynamic/?action=update&title=DSL_update_RB&global=1&c
omments=Dynamic%20SL%20Created%20for%20QID%20Service&vuln_provider=Ultra%20Low%
20Risk&id=5836610' \
--header 'Accept: */*' \
--header 'Accept-Encoding: gzip, deflate' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'User-Agent: python-requests/2.19.1' \
--header 'X-Access-Token: automation' \
--header 'X-Requested-With: curl'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM "<qualys_base_url>/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
  <RESPONSE>
    <DATETIME>2025-11-05T07:22:02Z</DATETIME>
    <TEXT>search list updated successfully</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>ID</KEY>
        <VALUE>6038506</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Export Search List API

API Request:

```
curl –location
'<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/?action=list&ids=5799554' \
--header 'Accept: */*' \
--header 'Accept-Encoding: gzip, deflate' \
--header 'Authorization: Bearer <JWT Token>' \
--header 'Connection: keep-alive' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'User-Agent: python-requests/2.19.1' \
--header 'X-Access-Token: automation' \
--header 'X-Requested-With: curl'
```

API Response:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE DYNAMIC_SEARCH_LIST_OUTPUT SYSTEM
"<qualys_base_url>/api/2.0/fo/qid/search_list/dynamic/dynamic_list_output.dtd">
<DYNAMIC_SEARCH_LIST_OUTPUT>
  <RESPONSE>
    <DATETIME>2025-10-16T12:58:26Z</DATETIME>
    <DYNAMIC_LISTS>
      <DYNAMIC_LIST>
        <ID>5799554</ID>
        <TITLE>
          <![CDATA[ULR_enabled]]>
        </TITLE>
        <GLOBAL>Yes</GLOBAL>
        <OWNER>
          <![CDATA[username]]>
        </OWNER>
        <CREATED>2025-09-15T04:51:16Z</CREATED>
        <MODIFIED_BY>
          <![CDATA[username]]>
        </MODIFIED_BY>
        <MODIFIED>2025-09-15T04:51:16Z</MODIFIED>
        <QIDS>
          <QID>200664</QID>
          <QID>200665</QID>
          <QID>200666</QID>
          <QID>200667</QID>
          <QID>200668</QID>
        </QIDS>
        <CRITERIA>
          <DISCOVERY_METHOD>
            <![CDATA[All]]>
          </DISCOVERY_METHOD>
          <PROVIDER>
            <![CDATA[Ultra Low Risk]]>
          </PROVIDER>
        </CRITERIA>
      </DYNAMIC_LIST>
    </DYNAMIC_LISTS>
  </RESPONSE>
</DYNAMIC_SEARCH_LIST_OUTPUT>
```