Qualys Cloud Platform (VM, SCA, PC) v8.x

API Release Notes

Version 8.15.2

September 25, 2018

This new version of the Qualys Cloud Platform (VM, SCA, 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

Apache Authentication - Multiple Improvements - Instance Discovery, Auto Record Creation and More

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

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

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

Compliance Scan Results - updated XML/DTD

URL to the Qualys API Server

Qualys maintains multiple Qualys platforms. The Qualys API server URL that you should use for API requests depends on the platform where your account is located.

Account Location	API Server URL
Qualys US Platform 1	https://qualysapi.qualys.com
Qualys US Platform 2	https://qualysapi.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysapi.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysapi.qualys.eu
Qualys EU Platform 2	https://qualysapi.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysapi.qg1.apps.qualys.in
Qualys Private Cloud Platform	https://qualysapi.<customer_base_url>

The Qualys API documentation and sample code use the API server URL for the Qualys US Platform 1. If your account is located on another platform, please replace this URL with the appropriate server URL for your account.

Apache Authentication - Multiple Improvements - Instance Discovery, Auto Record Creation and More

Instance discovery and auto record creation is now supported using Apache authentication records (UI and API). As before a single Apache record may be used when the same record configuration (Apache configuration file, Apache control command) is replicated across hosts in the record.

We've made several related API enhancements as described in these release notes.

Modules supported - SCA and PC

Permissions - Same as permissions for Apache records as before.

Summary

These capabilities are now available.

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

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

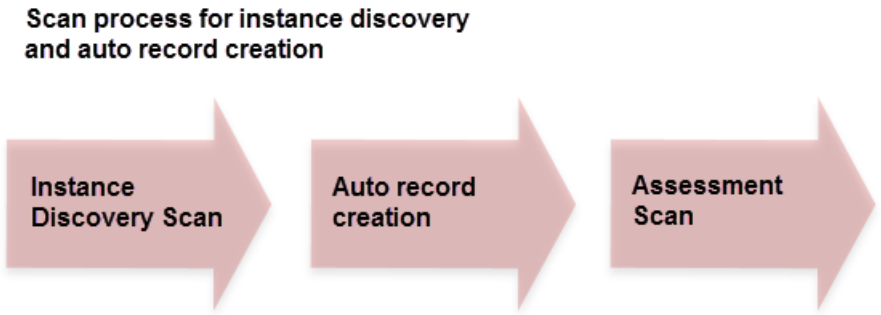
- New option profile settings allow you to 1) enable instance discovery and auto record creation, 2) include system-created records for scans, and 3) determine whether to send system records or user records when there are 2 records for the same instance configuration.

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

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

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

Scan process overview



Steps to get started

Step 1 - Option profile setup	You'll need to create 2 option profiles. Option profile 1: Enable option to allow auto discovery and system record creation Option profile 2: Enable option to include system-created authentication records for scans. If you have a system record and user record for the same instance configuration, choose which one to include for scans
Step 2 - Launch discovery scan for auto record creation	Launch compliance scan (using PC or SCA). Be sure to choose the option profile you've configured for instance discovery and record creation. (option profile 1) - Looking for instances discovered? Review the scan results appendix ***Auto record creation process*** - Instance scan data consolidation occurs based on authenticated scan data from the scan. - Auth records are created based on consolidated scan data. Record creation starts when the scan is Finished, during scan processing. Records may be created or updated (new IPs added, existing IPs removed)
Step 3 - Launch assessment scan for control evaluations	Launch compliance scan (using PC or SCA). Be sure to choose the option profile you've configured for including system-created records for scans. (option profile 2)

How it works - auto record creation

During scan processing instance scan data is consolidated, mapping Apache record configuration to hosts:

- Single host with single instance configuration

- Single host with multiple instance configurations

- Multiple hosts with single instance configuration

- Multiple hosts with multiple instance configurations

Let's consider a sample scan with instance discovery and auto record creation enabled. Sample scan data collected from the discovery scan is represented below.

For this scan, 3 Apache authentication records are auto created:

Apache config file	Apache control command	Hosts
conf1	bin1	host1, host2
conf2	bin2	host1
conf3	bin3	host2

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

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

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

Use these optional parameters:

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

Sample - List all records, show basic settings

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

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_APACHE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/apache/auth_apache_list_out
put.dtd">
<AUTH_APACHE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-08-01T19:27:13Z</DATETIME>
        <AUTH_APACHE_LIST>
            <AUTH_APACHE>
                <ID>30004</ID>
                <TITLE>
                    <![CDATA[Apache 2.2]]>
                </TITLE>
```

```
                    <IP_SET>
                        <IP>10.10.31.129</IP>
                    </IP_SET>
                    <UNIX_CONFIGURATION_FILE>
                        <![CDATA[/etc/httpd/conf/httpd.conf]]>
                    </UNIX_CONFIGURATION_FILE>
                    <UNIX_CONTROL_COMMAND>
                        <![CDATA[/usr/sbin/apachectl]]>
                    </UNIX_CONTROL_COMMAND>
                    <NETWORK_ID>0</NETWORK_ID>
                    <CREATED>
                        <DATETIME>2018-05-09T18:33:21Z</DATETIME>
                        <BY>acme_as2</BY>
                    </CREATED>
                    <LAST_MODIFIED>
                        <DATETIME>2018-08-01T19:11:25Z</DATETIME>
                    </LAST_MODIFIED>
                    <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
                    <IS_ACTIVE>0</IS_ACTIVE>
                </AUTH_APACHE>
                <AUTH_APACHE>
                    <ID>47136</ID>
                    <TITLE>
                        <![CDATA[Apache Web Server [System Created]]]>
                    </TITLE>
                    <IP_SET>
                        <IP>10.10.26.46</IP>
                        <IP>10.10.31.129</IP>
                        <IP>10.10.35.249</IP>
                    </IP_SET>
                    <UNIX_CONFIGURATION_FILE>
...
```

Sample - List active records only

API request:

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

Sample - List system created records only

API request:

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

Updated DTD

New tags appear in bold.

<base_url>/api/2.0/fo/auth/apache/auth_apache_list_output.dtd

```
...

<!ELEMENT AUTH_APACHE (ID, TITLE, IP_SET, UNIX_CONFIGURATION_FILE,
UNIX_CONTROL_COMMAND, NETWORK_ID?, CREATED, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX_CONFIGURATION_FILE (#PCDATA)>
<!ELEMENT UNIX_CONTROL_COMMAND (#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)>
<!-- new elements start -->
<!ELEMENT IS_SYSTEM_CREATED (#PCDATA)>
<!ELEMENT IS_ACTIVE (#PCDATA)>
<!-- new elements end -->
<!ELEMENT COMMENTS (#PCDATA)>
...
```

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

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

We added a new input parameter to support creation of Apache auth records with a certain status (active or inactive). This parameter can also be set when updating user-created Apache records. Note that system-created records cannot be updated.

Use this parameter:

Parameter	Description
status={0|1}	(Optional) The record status, active or inactive. By default a new record is set to active (1). Set to 0 for inactive record, or 1 for active record. For Update action, this parameter is valid only when user-created records are specified in the request.

Sample - Create new active record

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/apache -d
"action=create&status=1&title=create-new-sys-auth
&ips=10.10.31.112&unix_apache_config_file=/user/apache/httpd.conf&unix_ap
ache_control_command=/etc/local/apachectl"
```

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>2018-08-03T07:51:48Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
        <ID_SET>
          <ID>55838</ID>
        </ID_SET>
      </BATCH>
```

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

Sample - Update user created record, make status active

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2018-08-02T01:43:39Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully updated</TEXT>
                <ID_SET>
                    <ID>30004</ID>
                </ID_SET>
            </BATCH>
            <BATCH>
                <TEXT>Successfully updated</TEXT>
                <ID_SET>
                    <ID>48007</ID>
                </ID_SET>
            </BATCH>
        </BATCH_LIST>
    </RESPONSE>
</BATCH_RETURN>
```

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

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

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

DTD update (option_profile_info.dtd)

Added new tag <SYSTEM_AUTH_RECORD>.

<baseURL>/api/2.0/fo/subscription/option_profile/option_profile_info.dtd

```
...

<!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?,
CUSTOM_HTTP_HEADER?, HOST_ALIVE_TESTING?, SCAN_RESTRICTION?,
SYSTEM_AUTH_RECORD?, FILE_INTEGRITY_MONITORING?, CONTROL_TYPES?,
DO_NOT_OVERWRITE_OS?, TEST_AUTHENTICATION?)>

...
<!ELEMENT SYSTEM_AUTH_RECORD (ALLOW_AUTH_CREATION|INCLUDE_SYSTEM_AUTH)>
<!ELEMENT ALLOW_AUTH_CREATION (AUTHENTICATION_TYPE_LIST)>
<!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 ON_DUPLICATE_USE_USER_AUTH (#PCDATA)>
<!ELEMENT ON_DUPLICATE_USE_SYSTEM_AUTH (#PCDATA)>

<!ELEMENT FILE_INTEGRITY_MONITORING (AUTO_UPDATE_EXPECTED_VALUE?)>
<!ELEMENT AUTO_UPDATE_EXPECTED_VALUE (#PCDATA)>
...
```

XSD update (option_profiles.xsd)

New type added is SYSTEM_AUTH_RECORDType.

```
...
            <xs:element type="SCAN_RESTRICTIONType"
name="SCAN_RESTRICTION" minOccurs="0"/>
            <xs:element type="SYSTEM_AUTH_RECORDType"
name="SYSTEM_AUTH_RECORD" minOccurs="0"/>
            <xs:element type="FILE_INTEGRITY_MONITORINGType"
name="FILE_INTEGRITY_MONITORING" minOccurs="0"/>

...

    <xs:complexType name="SCAN_RESTRICTIONType">
        <xs:sequence>
            <xs:element type="SCAN_BY_POLICYType" name="SCAN_BY_POLICY"/>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="SYSTEM_AUTH_RECORDType">
        <xs:choice>
            <xs:element name="ALLOW_AUTH_CREATION"
type="ALLOW_AUTH_CREATIONType"/>
            <xs:element name="INCLUDE_SYSTEM_AUTH"
type="INCLUDE_SYSTEM_AUTHType"/>
        </xs:choice>
    </xs:complexType>
    <xs:complexType name="ALLOW_AUTH_CREATIONType">
        <xs:sequence>
            <xs:element name="AUTHENTICATION_TYPE_LIST"
type="AUTHENTICATION_TYPE_LISTType"/>
        </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:restriction>
                </xs:simpleType>
```

```
            </xs:element>
        </xs:sequence>
    </xs:complexType>

    <xs:complexType name="HOST_DISCOVERYType">
        <xs:sequence>
            <xs:element type="TCP_PORTSType" name="TCP_PORTS"
minOccurs="0"/>
            <xs:element type="UDP_PORTSType" name="UDP_PORTS"
minOccurs="0"/>
...
```

Sample - Export option profile for instance discovery and record creation

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

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788516</ID>
      <GROUP_NAME><![CDATA[Apache_Discovery_OP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2018-09-18T06:37:50Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
```

```
            <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
          </HOSTS_TO_SCAN>
          <PROCESSES_TO_RUN>
            <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
            <HTTP_PROCESSES>10</HTTP_PROCESSES>
          </PROCESSES_TO_RUN>
          <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
      </PERFORMANCE>
      <SYSTEM_AUTH_RECORD>
        <ALLOW_AUTH_CREATION>
          <AUTHENTICATION_TYPE_LIST>
            <AUTHENTICATION_TYPE>Apache Web Server</AUTHENTICATION_TYPE>
          </AUTHENTICATION_TYPE_LIST>
        </ALLOW_AUTH_CREATION>
      </SYSTEM_AUTH_RECORD>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_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 - Export option profile with Include system created auth records and use User created record on duplicate

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

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788517</ID>
      <GROUP_NAME><![CDATA[apache_UCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>2018-09-18T06:41:37Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
```

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

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

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

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788518</ID>
      <GROUP_NAME><![CDATA[apache_SCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>2018-09-18T06:43:44Z</UPDATE_DATE>
    </BASIC_INFO>
    <SCAN>
      <PORTS>
        <TARGETED_SCAN>1</TARGETED_SCAN>
      </PORTS>
      <PERFORMANCE>
        <PARALLEL_SCALING>0</PARALLEL_SCALING>
        <OVERALL_PERFORMANCE>Normal</OVERALL_PERFORMANCE>
        <HOSTS_TO_SCAN>
          <EXTERNAL_SCANNERS>15</EXTERNAL_SCANNERS>
          <SCANNER_APPLIANCES>30</SCANNER_APPLIANCES>
        </HOSTS_TO_SCAN>
        <PROCESSES_TO_RUN>
          <TOTAL_PROCESSES>10</TOTAL_PROCESSES>
          <HTTP_PROCESSES>10</HTTP_PROCESSES>
        </PROCESSES_TO_RUN>
        <PACKET_DELAY>Medium</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
```

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

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_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>
```

Compliance Scan Results - updated XML/DTD

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

You'll now see instances discovered under <AUTH_DISCOVERY_INSTANCE_LIST> in the XML output when instance discovery and system record creation is enabled in the option profile used for the scan. Scanned hosts with no instances discovered will be listed under <AUTH_DISCOERY_INSTANCE_NOT_FOUND_LIST>.

Compliance Scan Results XML

Compliance scan results XML can be downloaded from your account using the Fetch Compliance Scan API (below) or the Qualys UI.

Sample - Fetch Compliance Scan Results XML

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/scan/compliance -d
"action=fetch&scan_ref=compliance/1531783925.07893"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE COMPLIANCE_SCAN_RESULT_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/scan/compliance/compliance_scan_
result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
    <RESPONSE>
        <DATETIME>2018-09-13T23:41:49Z</DATETIME>
        <COMPLIANCE_SCAN>
            <HEADER>
                <NAME>
                    <![CDATA[Compliance Scan Results]]>
                </NAME>
                <GENERATION_DATETIME>2018-09-
13T23:41:49Z</GENERATION_DATETIME>
                <COMPANY_INFO>
                    <NAME>
                        <![CDATA[Qualys]]>
                    </NAME>
                    <ADDRESS>
                        <![CDATA[919 E Hillsdale Blvd, 4th Floor]]>
                    </ADDRESS>
```

```
                        <CITY>
                            <![CDATA[Foster City]]>
                        </CITY>
                        <STATE>
                            <![CDATA[California]]>
                        </STATE>
                        <COUNTRY>
                            <![CDATA[United States of America]]>
                        </COUNTRY>
                        <ZIP_CODE>
                            <![CDATA[94404]]>
                        </ZIP_CODE>
                    </COMPANY_INFO>
                    <USER_INFO>
                        <NAME>
                            <![CDATA[Irina Starsky]]>
                        </NAME>
                        <USERNAME>compq_is3</USERNAME>
                        <ROLE>Manager</ROLE>
                    </USER_INFO>
                    <KEY value="USERNAME">compq_is3</KEY>
                    <KEY value="COMPANY">
                        <![CDATA[Qualys]]>
                    </KEY>
                    <KEY value="DATE">2018-09-13T23:02:11Z</KEY>
                    <KEY value="TITLE">
                        <![CDATA[Auto Discovery multiple instances]]>
                    </KEY>
                    <KEY value="TARGET">10.10.31.129, 10.10.35.249</KEY>
                    <KEY value="EXCLUDED_TARGET">
                        <![CDATA[N/A]]>
                    </KEY>
                    <KEY value="NETWORK_ID">
                        <![CDATA[0]]>
                    </KEY>
                    <KEY value="NETWORK_TITLE">
                        <![CDATA[Global Default Network]]>
                    </KEY>
                    <KEY value="DURATION">00:01:31</KEY>
                    <KEY value="SCAN_HOST">qvsa_host22 (Scanner 10.4.39-1,
Vulnerability Signatures 2.1.2048-1)</KEY>
                    <KEY value="NBHOST_ALIVE">2</KEY>
                    <KEY value="NBHOST_TOTAL">2</KEY>
                    <KEY value="REPORT_TYPE">On-demand</KEY>
                    <KEY value="OPTIONS">Scanned Ports: Targeted Scan, Hosts
to Scan in Parallel - External Scanners: 15, Hosts to Scan in Parallel -
Scanner Appliances: 30, Total Processes to Run in Parallel: 10, HTTP
Processes to Run in Parallel: 10, Packet (Burst) Delay: Medium, Intensity:
Normal, Overall Performance: Normal, ICMP Host Discovery, Ignore RST
```

```
packets: Off, Ignore firewall-generated SYN-ACK packets: Off, Do not send
ACK or SYN-ACK packets during host discovery: Off</KEY>
                <KEY value="STATUS">FINISHED</KEY>
                <OPTION_PROFILE>
                    <OPTION_PROFILE_TITLE option_profile_default="0">
                        <![CDATA[New Auto Discovery]]>
                    </OPTION_PROFILE_TITLE>
                </OPTION_PROFILE>
            </HEADER>
            <APPENDIX>
                <TARGET_HOSTS>
                    <HOSTS_SCANNED>10.10.31.129,
10.10.35.249</HOSTS_SCANNED>
                </TARGET_HOSTS>
                <TARGET_DISTRIBUTION>
                    <SCANNER>
                        <NAME>
                            <![CDATA[qvsa_host22]]>
                        </NAME>
                        <HOSTS>10.10.31.129, 10.10.35.249</HOSTS>
                    </SCANNER>
                </TARGET_DISTRIBUTION>
                <AUTHENTICATION>
                    <AUTH>
                        <TYPE>SSH</TYPE>
                        <SUCCESS>
                            <IP>10.10.31.129, 10.10.35.249</IP>
                        </SUCCESS>
                    </AUTH>
                </AUTHENTICATION>
                <AUTH_DISCOVERY_INSTANCE_LIST>
                    <AUTH_DISCOVERY_INSTANCE>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <AUTH_PARAM_LIST>
                            <AUTH_PARAM name="unix_apache_config_file">
                                <![CDATA[/etc/httpd-inst1-
qweb/conf/httpd.conf]]>
                            </AUTH_PARAM>
                          <AUTH_PARAM name="unix_apache_control_command">
                                <![CDATA[/usr/sbin/httpd]]>
                            </AUTH_PARAM>
                        </AUTH_PARAM_LIST>
                        <IP>10.10.31.129</IP>
                    </AUTH_DISCOVERY_INSTANCE>
                    <AUTH_DISCOVERY_INSTANCE>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <AUTH_PARAM_LIST>
                            <AUTH_PARAM name="unix_apache_config_file">
                                <![CDATA[/etc/httpd-inst5-
```

```
qweb/conf/httpd.conf]]>
                            </AUTH_PARAM>
                          <AUTH_PARAM name="unix_apache_control_command">
                              <![CDATA[/usr/sbin/httpd]]>
                            </AUTH_PARAM>
                        </AUTH_PARAM_LIST>
                        <IP>10.10.31.129</IP>
                    </AUTH_DISCOVERY_INSTANCE>
                    <AUTH_DISCOVERY_INSTANCE>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <AUTH_PARAM_LIST>
                            <AUTH_PARAM name="unix_apache_config_file">
                                <![CDATA[/etc/httpd-inst3-
qweb/conf/httpd.conf]]>
                            </AUTH_PARAM>
                          <AUTH_PARAM name="unix_apache_control_command">
                              <![CDATA[/usr/sbin/httpd]]>
                            </AUTH_PARAM>
                        </AUTH_PARAM_LIST>
                        <IP>10.10.31.129</IP>
                    </AUTH_DISCOVERY_INSTANCE>
                    <AUTH_DISCOVERY_INSTANCE>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <AUTH_PARAM_LIST>
                            <AUTH_PARAM name="unix_apache_config_file">
                                <![CDATA[/etc/httpd-inst4-
qweb/conf/httpd.conf]]>
                            </AUTH_PARAM>
                          <AUTH_PARAM name="unix_apache_control_command">
                              <![CDATA[/usr/sbin/httpd]]>
                            </AUTH_PARAM>
                        </AUTH_PARAM_LIST>
                        <IP>10.10.31.129</IP>
                    </AUTH_DISCOVERY_INSTANCE>
                    <AUTH_DISCOVERY_INSTANCE>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <AUTH_PARAM_LIST>
                            <AUTH_PARAM name="unix_apache_config_file">
                                <![CDATA[/etc/httpd-inst2-
qweb/conf/httpd.conf]]>
                            </AUTH_PARAM>
                          <AUTH_PARAM name="unix_apache_control_command">
                              <![CDATA[/usr/sbin/httpd]]>
                            </AUTH_PARAM>
                        </AUTH_PARAM_LIST>
                        <IP>10.10.31.129</IP>
                    </AUTH_DISCOVERY_INSTANCE>
                </AUTH_DISCOVERY_INSTANCE_LIST>
                <AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST>
```

```
                    <AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                        <IP>10.10.35.249</IP>
                    </AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                </AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST>
            </APPENDIX>
        </COMPLIANCE_SCAN>
    </RESPONSE>
</COMPLIANCE_SCAN_RESULT_OUTPUT>
```

Compliance Scan Results DTD updated

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

DTD Updates: 1) The tag USERNAME is now optional, and 2) We added new optional tags AUTH_DISCOVERY_INSTANCE_LIST and AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST and sub tags.

```
 ...
<!-- made USERNAME optional since it is controlled by template setting -->
<!ELEMENT USER_INFO (NAME, USERNAME?, ROLE)>
<!ELEMENT USERNAME (#PCDATA)*>
<!ELEMENT ROLE (#PCDATA)*>

 ...

<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?, AUTHENTICATION?,
AUTH_DISCOVERY_INSTANCE_LIST?, AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?)>
<!ELEMENT TARGET_HOSTS (HOSTS_SCANNED?, EXCLUDED_HOSTS?,
HOSTS_NOT_ALIVE?, PAUSE_CANCEL_ACTION?, HOSTNAME_NOT_FOUND?,
HOSTS_SCAN_ABORTED?)>
<!ELEMENT HOSTS_SCANNED (#PCDATA)>
<!ELEMENT HOSTNAME_NOT_FOUND (#PCDATA)>
<!ELEMENT EXCLUDED_HOSTS (#PCDATA)>

...

<!ELEMENT AUTHENTICATION (AUTH+)>
<!ELEMENT AUTH (TYPE?, (FAILED | SUCCESS | INSUFFICIENT)+)>
<!ELEMENT TYPE (#PCDATA)>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_LIST (AUTH_DISCOVERY_INSTANCE*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE (AUTH_TYPE, AUTH_PARAM_LIST?, IP)>

<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST
(AUTH_DISCOVERY_INSTANCE_NOT_FOUND*)>
<!ELEMENT AUTH_DISCOVERY_INSTANCE_NOT_FOUND (AUTH_TYPE, IP)>
```

```
<!ELEMENT AUTH_PARAM_LIST (AUTH_PARAM+)>
<!ELEMENT AUTH_TYPE (#PCDATA)>
<!ELEMENT AUTH_PARAM (#PCDATA)>
<!ATTLIST AUTH_PARAM name CDATA #IMPLIED>

<!ELEMENT FAILED (IP,INSTANCE?)>
<!ELEMENT SUCCESS (IP,INSTANCE?)>
<!ELEMENT INSUFFICIENT (IP,INSTANCE?)>
<!-- EOF -->
```