Qualys Cloud Platform (VM, PC) v8.x

API Release Notes

Version 8.21.2

September 19, 2019

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

What's New

IBM WebSphere App Server and Jboss Server: Instance Discovery, Auto Record Creation and more

Compliance Posture API: Parameters added to show fail/pass dates for controls

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 US Platform 4	https://qualysapi.qg4.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 Canada Platform 1	https://qualysapi.qg1.apps.qualys.ca
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.

IBM WebSphere App Server and Jboss Server: Instance Discovery, Auto Record Creation and more

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

Instance discovery and auto record creation is now supported for IBM WebSphere App Server/Jboss Server (UI and API). As before a single IBM WebSphere/Jboss record may be used when the same record configuration is replicated across hosts in the record.

Two IBM WebSphere instance records on same/different hosts are different if the value in "unix_websphere_home_dir" for WebSphere instances are different.

Two Jboss instance records on same/different hosts are considered different if values in any of these parameters for Jboss instances are different: jboss_domain_mode, jboss_home_path, jboss_base_path, jboss_conf_dir_path, jboss_conf_file_path, jboss_conf_host_file_path.

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

Modules supported - PC

Permissions - Same as permissions for IBM WebSphere/Jboss records as before. We support instance scanning for Jboss server that is installed on hosts running on Windows or Unix platforms for both EAP and WildFly, while for IBM WebSphere, we support scanning for hosts running on Unix platform. You need permission to create Unix and/or Windows authentication records to scan the hosts running on Windows and Unix platforms for IBM WebSphere and Jboss instances.

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 IBM WebSphere/Jboss 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.

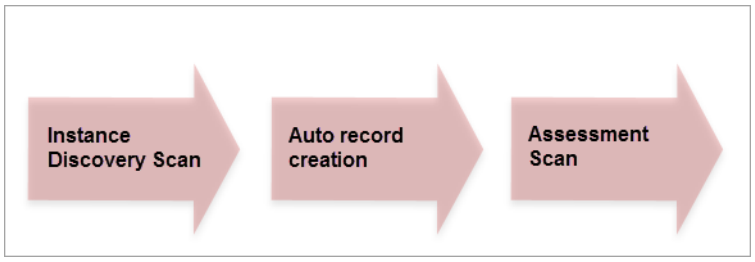
- New option profile settings allow you to 1) enable instance discovery and auto record creation, 2) include system-created records for scans, and 3) determine whether to send system records or user records when there are 2 records for the same instance configuration.

- 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 IBM WebSphere/Jboss 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). 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. IBM WebSphere/Jboss instance IPs with the same configuration are added to a single authentication record while a new authentication record is created if an instance has a home directory different from the existing instances. 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). 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 IBM WebSphere/Jboss 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 IBM WebSphere authentication records are auto created:

IBM WebSphere Installation directory	Hosts
home1	host1, host2
home2	host1
home3	host2

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

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

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

Use these optional parameters when creating or updating a compliance profile for IBM WebSphere/Jboss:

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

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

Sample - Create new pc option profile record to enable IBM WebSphere and Jboss auth instance discovery and system record creation

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

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

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

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

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

Sample - Update pc option profile record to enable IBM WAS and Jboss auth instance discovery and system record creation

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=update&enable_auth_instance_discovery=1&auto_auth_types=IB
M+WebSphere+App+Server,Jboss+Server"
"http://qualysapi.qualys.com/api/2.0/fo/subscription/option_profil
e/pc/"
```

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

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

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

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

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

API request:

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

```
"action=list&id=107091"
```

XML output:

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

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

API request:

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

XML output:

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

List IBM WebSphere Authentication Records API - new filter options, DTD updated

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

New input parameters allow you to filter the IBM WebSphere 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/ibm_websphere -d
"action=list&details=Basic"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_IBM_WEBSPHERE_LIST_OUTPUT SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere/auth_i
bm_websphere_list_output.dtd">
<AUTH_IBM_WEBSPHERE_LIST_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-08-07T03:29:58Z</DATETIME>
        <AUTH_IBM_WEBSPHERE_LIST>
            <AUTH_IBM_WEBSPHERE>
                <ID>67001</ID>
                <TITLE>
```

```
                    <![CDATA[IBM WebSphere - 10.10.34.52]]>
                </TITLE>
                <IP_SET>
                    <IP>10.10.34.52</IP>
                </IP_SET>
                <UNIX_INSTLLATION_DIRECTORY>
                    <![CDATA[/opt/IBM/WebSphere/AppServer]]>
                </UNIX_INSTLLATION_DIRECTORY>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2018-12-17T19:49:19Z</DATETIME>
                    <BY>quays_as2</BY>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2018-12-17T19:49:19Z</DATETIME>
                </LAST_MODIFIED>
                <IS_SYSTEM_CREATED>0</IS_SYSTEM_CREATED>
              <IS_ACTIVE>1</IS_ACTIVE>
            </AUTH_IBM_WEBSPHERE>
    ...
```

Sample - List active records only

API request:

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

Sample - List system created records only

API request:

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

Updated DTD

New tags appear in bold.

<base_url>/api/2.0/fo/auth/ibm_websphere/auth_ibm_websphere_list_output.dtd

```
...

<!ELEMENT AUTH_IBM_WEBSPHERE (ID, TITLE, IP_SET,
UNIX_INSTLLATION_DIRECTORY, NETWORK_ID?, CREATED, LAST_MODIFIED,
IS_SYSTEM_CREATED?, IS_ACTIVE?, COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT UNIX_INSTLLATION_DIRECTORY (#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)>
<!-- 8.21.2.0 new elements start -->
<!ELEMENT IS_SYSTEM_CREATED (#PCDATA)>
<!ELEMENT IS_ACTIVE (#PCDATA)>
<!-- new elements end -->
<!ELEMENT COMMENTS (#PCDATA)>
...
```

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

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

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

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

Use this parameter:

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

Sample - Create new active record

API request:

```
curl -u username:password -H "X-Requested-With: curl"
https://qualysapi.qualys.com/api/2.0/fo/auth/ibm_websphere -d
"action=create&status=1&title=create-new-sys-auth
&ips=10.10.31.112&unix_installation_dir=/root/IBM/WebSphere/AppSer
ver7"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-08-08T07:51:48Z</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/ibm_websphere -d
"action=update&ids=30004,48007&status=1"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-08-08T01:43:39Z</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>
```

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

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

New input parameters allow you to filter the Jboss 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.

Parameter	Description
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 in bold.

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE AUTH_JBOSS_LIST_OUTPUT SYSTEM
"https://qualysapi.p27.eng.sjc01.qualys.com/api/2.0/fo/auth/jboss/
auth_jboss_list_output.dtd">
<AUTH_JBOSS_LIST_OUTPUT>
...
                </WINDOWS>
                <NETWORK_ID>0</NETWORK_ID>
                <CREATED>
                    <DATETIME>2019-08-02T17:13:21Z</DATETIME>
                </CREATED>
                <LAST_MODIFIED>
                    <DATETIME>2019-08-02T17:13:21Z</DATETIME>
                </LAST_MODIFIED>
                <IS_SYSTEM_CREATED>1</IS_SYSTEM_CREATED>
              <IS_ACTIVE>1</IS_ACTIVE>
                <COMMENTS>
                  <![CDATA[System created Jboss Server auth record
using scan data with history ID 170976.]]>
                </COMMENTS>
            </AUTH_JBOSS>
...
```

Sample - List active records only

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

Sample - List system created records only

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

Updated DTD

New tags appear in bold.

<base_url>/api/2.0/fo/auth/jboss/auth_jboss_list_output.dtd

```
...

<!ELEMENT AUTH_JBOSS (ID, TITLE, IP_SET, WINDOWS?, UNIX?,
NETWORK_ID?, CREATED, LAST_MODIFIED, IS_SYSTEM_CREATED?, IS_ACTIVE?,
COMMENTS?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT TITLE (#PCDATA)>
<!ELEMENT WINDOWS (HOME_PATH?, DOMAIN_MODE?, BASE_PATH?,
CONF_DIR_PATH?, CONF_FILE_PATH?, CONF_HOST_FILE_PATH?)>
<!ELEMENT HOME_PATH (#PCDATA)>
<!ELEMENT DOMAIN_MODE (#PCDATA)>
<!ELEMENT BASE_PATH (#PCDATA)>
<!ELEMENT CONF_DIR_PATH (#PCDATA)>
<!ELEMENT CONF_FILE_PATH (#PCDATA)>
<!ELEMENT CONF_HOST_FILE_PATH (#PCDATA)>
<!ELEMENT UNIX (HOME_PATH?, DOMAIN_MODE?, BASE_PATH?,
CONF_DIR_PATH?, CONF_FILE_PATH?, CONF_HOST_FILE_PATH?)>
<!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)>
<!-- 8.21.2.0 new elements start -->
<!ELEMENT IS_SYSTEM_CREATED (#PCDATA)>
<!ELEMENT IS_ACTIVE (#PCDATA)>
...
```

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

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

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

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

Use this parameter:

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

Sample - Create new active record

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST
"action=create&title=jbos_rec&windows_working_mode=standalone_mode
&windows_base_path=c:\&windows_home_path=c:\&windows_conf_file_pat
h=c:\&windows_conf_dir_path=c:\&comment=record
creation&ips=10.10.10.224&status=1"
"https://qualysapi.qualys.com/api/2.0/fo/auth/jboss/"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
  <RESPONSE>
    <DATETIME>2019-08-08T07:51:48Z</DATETIME>
    <BATCH_LIST>
      <BATCH>
        <TEXT>Successfully Created</TEXT>
```

```
        <ID_SET>
          <ID>55848</ID>
        </ID_SET>
      </BATCH>
    </BATCH_LIST>
  </RESPONSE>
</BATCH_RETURN>
```

Sample - Update system created record to make the status active

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE BATCH_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/batch_return.dtd">
<BATCH_RETURN>
    <RESPONSE>
        <DATETIME>2019-08-08T01:43:39Z</DATETIME>
        <BATCH_LIST>
            <BATCH>
                <TEXT>Successfully updated</TEXT>
                <ID_SET>
                    <ID>90004</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 Jboss and/or IBM WebSphere instance discovery and auto record creation

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

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

XSD update (option_profiles.xsd)

New enum values "IBM WebSphere App Server" and "Jboss Server" in bold added under AUTHENTICATION_TYPE element.

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

Sample - Export option profile for Jboss and IBM WebSphere instance discovery and record creation

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

API request:

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

XML output:

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

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

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
        </PACKET_OPTIONS>
      </ADDITIONAL>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export option profile 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_profi
le/?action=export&option_profile_id=2788517"
```

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788517</ID>
      <GROUP_NAME><![CDATA[apache_UCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>0</IS_GLOBAL>
      <UPDATE_DATE>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_D
ISCOVERY>
      </PERFORMANCE>
      <SYSTEM_AUTH_RECORD>
        <INCLUDE_SYSTEM_AUTH>
          <ON_DUPLICATE_USE_USER_AUTH>1</ON_DUPLICATE_USE_USER_AUTH>
        </INCLUDE_SYSTEM_AUTH>
      </SYSTEM_AUTH_RECORD>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>
<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample - Export option profile with Include system created auth records and use System created record on duplicate

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

API request:

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

XML output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profi
le/option_profile_info.dtd">
<OPTION_PROFILES>
  <OPTION_PROFILE>
    <BASIC_INFO>
      <ID>2788518</ID>
      <GROUP_NAME><![CDATA[apache_SCR_INIOP]]></GROUP_NAME>
      <GROUP_TYPE>compliance</GROUP_TYPE>
      <USER_ID><![CDATA[Patrick Slimmer (qualys_ps)]]></USER_ID>
      <UNIT_ID>0</UNIT_ID>
      <SUBSCRIPTION_ID>1249050</SUBSCRIPTION_ID>
      <IS_GLOBAL>1</IS_GLOBAL>
      <UPDATE_DATE>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_D
ISCOVERY>
      </PERFORMANCE>
      <SYSTEM_AUTH_RECORD>
        <INCLUDE_SYSTEM_AUTH>
          <ON_DUPLICATE_USE_SYSTEM_AUTH>1</ON_DUPLICATE_USE_SYSTEM_AUTH>
        </INCLUDE_SYSTEM_AUTH>
      </SYSTEM_AUTH_RECORD>
      <FILE_INTEGRITY_MONITORING>
        <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
      </FILE_INTEGRITY_MONITORING>
      <CONTROL_TYPES>
        <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
        <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
      </CONTROL_TYPES>
    </SCAN>
    <ADDITIONAL>
      <HOST_DISCOVERY>
        <TCP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </TCP_PORTS>
        <UDP_PORTS>
          <STANDARD_SCAN>1</STANDARD_SCAN>
        </UDP_PORTS>
        <ICMP>1</ICMP>
      </HOST_DISCOVERY>
      <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TC
P_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATE
D_TCP_SYN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP
_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>
      </PACKET_OPTIONS>
    </ADDITIONAL>
```

```
  </OPTION_PROFILE>
</OPTION_PROFILES>
```

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

We'll now show you in the XML output the auth types for which no authentication record instance is found on any scanned assets under <AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED> when instance discovery and system record creation is enabled in the option profile used for the scan. <AUTH_TYPE_LIST> will list the auth types in the <AUTH_TYPE> tags for which no instances are found.

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/complianc
e_scan_result_output.dtd">
<COMPLIANCE_SCAN_RESULT_OUTPUT>
    <RESPONSE>
        <DATETIME>2019-08-07T04:21:07Z</DATETIME>
        <COMPLIANCE_SCAN>
...
                <AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST>
                    <AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                        <AUTH_TYPE>IBM WebSphere App
                         Server</AUTH_TYPE>
                        <IP>10.10.26.134</IP>
```

```
                    </AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                    <AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                        <AUTH_TYPE>Jboss Server</AUTH_TYPE>
                        <IP>10.10.26.134</IP>
                    </AUTH_DISCOVERY_INSTANCE_NOT_FOUND>
                </AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST>
                <AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED>
                    <AUTH_TYPE_LIST>
                        <AUTH_TYPE>Apache Web Server</AUTH_TYPE>
                    </AUTH_TYPE_LIST>
                </AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED>
                <OS_AUTH_BASED_TECHNOLOGY_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

Two new elements in bold: <AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED> and <AUTH_TYPE_LIST> are added in the DTD.

```
 ...
<!ELEMENT APPENDIX (TARGET_HOSTS?, TARGET_DISTRIBUTION?,
AUTHENTICATION?, AUTH_DISCOVERY_INSTANCE_LIST?,
AUTH_DISCOVERY_INSTANCE_NOT_FOUND_LIST?,
AUTH_DISCOVERY_INSTANCE_NOT_COLLECTED?,
OS_AUTH_BASED_TECHNOLOGY_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 HOSTS_NOT_ALIVE (#PCDATA)>
<!ELEMENT HOSTS_SCAN_ABORTED (#PCDATA)>
<!ELEMENT PAUSE_CANCEL_ACTION (HOSTS, ACTION, BY)>
<!ELEMENT ACTION (#PCDATA)>
<!ELEMENT BY (#PCDATA)>

<!ELEMENT TARGET_DISTRIBUTION (SCANNER+)>
<!ELEMENT SCANNER (NAME, HOSTS)>
```

```
<!ELEMENT HOSTS (#PCDATA)>

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

<!ELEMENT OS_AUTH_BASED_TECHNOLOGY_LIST
(OS_AUTH_BASED_TECHNOLOGY*)>
<!ELEMENT OS_AUTH_BASED_TECHNOLOGY (TECHNOLOGY_FAMILY,
TECHNOLOGY_INSTANCE_LIST*)>
<!ELEMENT TECHNOLOGY_FAMILY (#PCDATA)>
<!ELEMENT TECHNOLOGY_INSTANCE_LIST (TECHNOLOGY_INSTANCE+)>
<!ELEMENT TECHNOLOGY_INSTANCE (TECHNOLOGY, INSTANCE_INFO_LIST*,
IP)>
<!ELEMENT INSTANCE_INFO_LIST (INSTANCE_INFO*)>
<!ELEMENT TECHNOLOGY (#PCDATA)>
<!ELEMENT INSTANCE_INFO (#PCDATA)>
<!ATTLIST INSTANCE_INFO key CDATA #IMPLIED>

<!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_DISCOVERY_INSTANCE_NOT_COLLECTED (AUTH_TYPE_LIST*)>
<!ELEMENT AUTH_TYPE_LIST (AUTH_TYPE*)>

<!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 -->
```

Compliance Posture API: Parameters added to show fail/pass dates for controls

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

We have added 5 new elements to the Compliance posture info list output DTD to show you the following information in the compliance posture information output: 1) for failed controls, the first and last failed dates. 2) for passed controls, the first and last passed dates and 3) previous posture status (failed/passed) for a control.

Each compliance posture info record in the output now includes this information:

Output	Description
First Fail Date	The first scan date when the control was reported as Fail. If the previous status was Pass then this is the date the status changed from Pass to Fail.
Last Fail Date	The most recent scan date when the control was reported as Fail.
First Pass Date	The first scan date when the control was reported as Pass. If the previous status was Fail then this is the date the status changed from Fail to Pass.
Last Pass Date	The most recent scan date when the control was reported as Pass.
Previous Status	The compliance status (Pass or Fail) for each control before the most recent compliance scan.

Sample - Compliance posture info list output with the new information

API request:

```
curl -u "username:password" -H "Content-type: text/xml" -X "POST"
-d "action=list&policy_id=21481&details=All"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/">
PostureInfo.xml
```

XML output:

```
...
<INFO_LIST>
            <INFO>
                <ID>41769</ID>
                <HOST_ID>686176</HOST_ID>
```

```
                    <CONTROL_ID>1045</CONTROL_ID>
                    <TECHNOLOGY_ID>12</TECHNOLOGY_ID>
                    <INSTANCE></INSTANCE>
                    <STATUS>Failed</STATUS>
                    <POSTURE_MODIFIED_DATE>2019-07-
10T08:20:59Z</POSTURE_MODIFIED_DATE>
                  <PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
                   <FIRST_FAIL_DATE>2019-07-09T08:20:59Z</FIRST_FAIL_DATE>
                   <LAST_FAIL_DATE>2019-07-23T05:24:38Z</LAST_FAIL_DATE>
                    <EVIDENCE>
                        <BOOLEAN_EXPR>
                            <![CDATA[(:dp_1 in #fv_1 )]]>
                        </BOOLEAN_EXPR>
                        <DPV_LIST>
                            <DPV lastUpdated="2019-06-21T07:13:37Z">
                                <LABEL>:dp_1</LABEL>
                                <V>
                                    <![CDATA[3]]>
                                </V>
                            </DPV>
                        </DPV_LIST>
                    </EVIDENCE>
                </INFO>
                <INFO>
                    <ID>42283</ID>
                    <HOST_ID>686176</HOST_ID>
                    <CONTROL_ID>1048</CONTROL_ID>
                    <TECHNOLOGY_ID>12</TECHNOLOGY_ID>
                    <INSTANCE></INSTANCE>
                    <STATUS>Passed</STATUS>
                    <POSTURE_MODIFIED_DATE>2019-07-
23T05:23:50Z</POSTURE_MODIFIED_DATE>
                   <PREVIOUS_STATUS>Passed</PREVIOUS_STATUS>
                   <FIRST_PASS_DATE>2019-07-23T05:23:50Z</FIRST_PASS_DATE>
                   <LAST_PASS_DATE>2019-07-23T05:24:38Z</LAST_PASS_DATE>
....
```

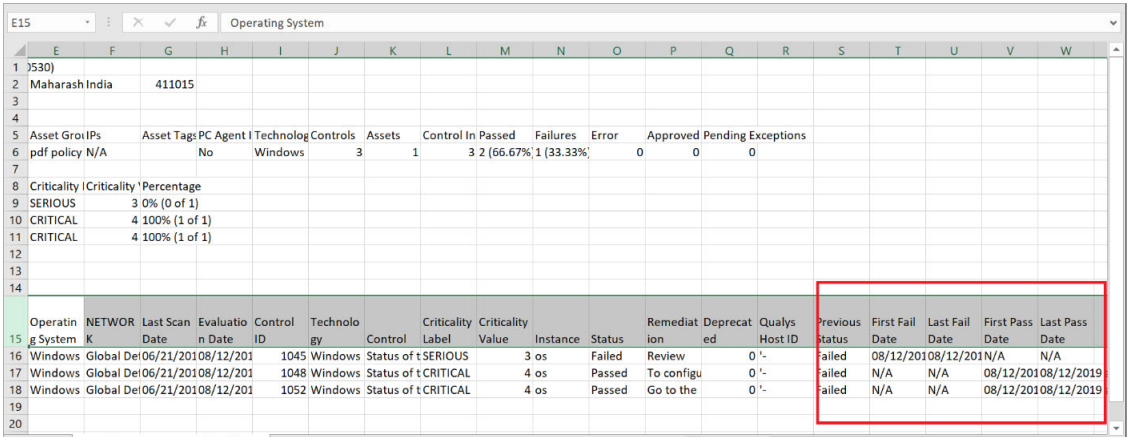
Updated DTD

New tags appear in bold.

<base_url>/api/2.0/fo/compliance/posture/info/posture_info_list_output.dtd"

```
...
<!ELEMENT INFO (ID, HOST_ID, CONTROL_ID, TECHNOLOGY_ID, INSTANCE?,
STATUS, REMEDIATION?, POSTURE_MODIFIED_DATE?, PREVIOUS_STATUS?,
FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?, LAST_PASS_DATE?,
EXCEPTION?, EVIDENCE?, CAUSE_OF_FAILURE?)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT HOST_ID (#PCDATA)>
<!ELEMENT CONTROL_ID (#PCDATA)>
<!ELEMENT TECHNOLOGY_ID (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT POSTURE_MODIFIED_DATE (#PCDATA)>
<!ELEMENT PREVIOUS_STATUS (#PCDATA)>
<!ELEMENT FIRST_FAIL_DATE (#PCDATA)>
<!ELEMENT LAST_FAIL_DATE (#PCDATA)>
<!ELEMENT FIRST_PASS_DATE (#PCDATA)>
<!ELEMENT LAST_PASS_DATE (#PCDATA)>
...
```

Sample compliance posture report in CSV format with the new information



Operating System	NETWORK	Last Scan Date	Evaluation Date	Control ID	Technology	Control	Criticality Label	Criticality Value	Instance	Status	Remediation	Deprecated	Qualys Host ID	Previous Status	First Fail Date	Last Fail Date	First Pass Date	Last Pass Date
Windows	Global Def	06/21/201	08/12/201	1045	Windows	Status of t	SERIOUS	3	os	Failed	Review	0	'-	Failed	08/12/201	08/12/201	N/A	N/A
Windows	Global Def	06/21/201	08/12/201	1048	Windows	Status of t	CRITICAL	4	os	Passed	To configu	0	'-	Failed	N/A	N/A	08/12/201	08/12/2019
Windows	Global Def	06/21/201	08/12/201	1052	Windows	Status of t	CRITICAL	4	os	Passed	Go to the	0	'-	Failed	N/A	N/A	08/12/201	08/12/2019

Compliance Policy Report - updated XML/DTD

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

We have updated the compliance_policy_report.dtd to show the new information that is added to the the compliance posture info output in the compliance report. New elements added in the compliance_policy_report.dtd are: <PREVIOUS_STATUS>, <FIRST_FAIL_DATE>, <LAST_FAIL_DATE>, <FIRST_PASS_DATE>, <LAST_PASS_DATE>.

Sample compliance policy report in XML format with the new information

Note that this new information is shown when you select the report type as compliance report in the request while launching a report.

API request:

```
curl -H "X-Requested-With: Curl Sample"
"http://qualysapi.qualys.com/api/2.0/fo/report/?action=fetch&id=60
726"
```

XML output:

```
...
<REMEDIATION>
Review and verify the startup type of the 'Clipbook' service is in
line with business needs and organization's security policies. #
To configure startup type of a service follow the steps below: 1.
Open 'services.msc' 2. Double click to open the properties of
```

```
service to be configured 3. Configure the 'Startup Type' of the
service from the drop down menu. # Example 1. Open 'services.msc'
2. Double click the 'Clipbook' to open the service properties 3.
Configure the 'Startup Type' of the service to 'Automatic'
</REMEDIATION>
<TECHNOLOGY>
<ID>
<![CDATA[ 12 ]]>
</ID>
<NAME>Windows 2000</NAME>
</TECHNOLOGY>
<EVALUATION_DATE>2019-08-12T05:57:52Z</EVALUATION_DATE>
<PREVIOUS_STATUS>Failed</PREVIOUS_STATUS>
<FIRST_FAIL_DATE>2019-08-12T05:57:52Z</FIRST_FAIL_DATE>
<LAST_FAIL_DATE>2019-08-12T05:57:52Z</LAST_FAIL_DATE>
</CONTROL>
<CONTROL>
<CID>1048</CID>
<STATEMENT>
<![CDATA[
Status of the 'Shutdown: Clear virtual memory pagefile' setting
]]>
...
```

Updated DTD

New tags appear in bold.

```
...
<!ELEMENT CONTROL_LIST (CONTROL*)>
<!ELEMENT CONTROL (CID, STATEMENT, CRITICALITY?,
CONTROL_REFERENCES?, DEPRECATED?, RATIONALE?, INSTANCE?, STATUS,
REMEDIATION?, CAUSE_OF_FAILURE?, TECHNOLOGY, EVALUATION_DATE?,
PREVIOUS_STATUS?, FIRST_FAIL_DATE?, LAST_FAIL_DATE?, FIRST_PASS_DATE?,
LAST_PASS_DATE?, EVIDENCE?, EXCEPTION?)>
<!ELEMENT CID (#PCDATA)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CONTROL_REFERENCES (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT STATUS (#PCDATA)>
<!ELEMENT REMEDIATION (#PCDATA)>
<!ELEMENT CAUSE_OF_FAILURE ((UNEXPECTED?, MISSING?)|(CRITERIA*))>
```

```
<!ELEMENT UNEXPECTED (V*)>
<!ELEMENT MISSING (V*)>
<!ATTLIST MISSING logic CDATA #FIXED "OR">
<!ELEMENT TECHNOLOGY (ID, NAME)>
<!ELEMENT ID (#PCDATA)>
<!ELEMENT EVALUATION_DATE (#PCDATA)>
<!ELEMENT PREVIOUS_STATUS (#PCDATA)>
<!ELEMENT FIRST_FAIL_DATE (#PCDATA)>
<!ELEMENT LAST_FAIL_DATE (#PCDATA)>
<!ELEMENT FIRST_PASS_DATE (#PCDATA)>
<!ELEMENT LAST_PASS_DATE (#PCDATA)>
<!ELEMENT INSTANCE (#PCDATA)>
<!ELEMENT EVIDENCE (#PCDATA)>
...
```