Qualys Cloud Platform (VM, PC) v10.x

API Release Notes

Version 10.9

February 25, 2021

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

Control References Added to Compliance Posture Information API Output

Support for database technology data collection by using underlying OS authentication records

Qualys API Server URL

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

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

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

Control References Added to Compliance Posture Information API Output

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

We updated the Compliance Posture Information API output to include control references. You'll see CIS references in CIS policies, STIG references in STIG policies, and user-defined references in custom policies. This feature allows you to easily parse data based on the reference value.

Control references will appear in XML output when the API request includes details=All or details=Basic. When a control has no reference, then the reference value is empty.

The References column always appears in CSV output. When a control has no reference, then N/A appears in the References column.

Sample Stig policy in CSV Format

You'll see the new column header "Reference". In this sample, the reference value for control ID 8249 is SV-51752r1_rule.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&policy_id=597463&details=All&output_format=csv"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

CSV output:

```
----BEGIN_RESPONSE_BODY_CSV
"POLICY ID","DATETIME"
"597463","02/24/2021 09:27:22"

"ID","IP","OS","DNS Name","NetBios","Tracking Method","Control
ID","Control Statement","Criticality Label","Criticality
Value","Technology ID","Technology Name","Posture","Previous
Status","First Fail Date","Last Fail Date","First Pass Date","Last Pass
Date","Evaluation Date","Qualys Host ID","Posture Evidence","Reference"
"7258550","10.10.10.10","Windows Server 2012 Standard 64 bit
Edition","2k12std.sample.qualys.com","2K12STD-SAMPLE","IP","8249","Status
of the 'Allow Basic authentication' setting (WinRM
client)","SERIOUS","3","53","Windows 2012
Server","Failed","Failed","02/24/2021 07:34:26","02/24/2021
07:34:26","N/A","N/A","02/24/2021 07:11:21",,"This integer value <B>X</B>
indicates the status of the setting <B>Allow Basic authentication</B>
```

```
using the registry key path
<B>HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WinRM\Client\Al
lowBasic</B>. A value of <B>0</B> indicates the setting is
<B>Disabled</B>, A value of <B>1</B> indicates the setting is
<B>Enabled</B>.

======Expected Value(s)======

Disabled (0)

======Current Value(s) - Last updated: 02/24/2021 at 07:11:21 AM
(GMT+0000)======
Key not Found","SV-51752r1_rule"
...
```

Sample CIS Policy in XML Format

You'll see that REFERENCE appears under CONTROL_LIST in the GLOSSARY section of the XML. In this sample, the reference value for control ID 9705 is 1.1.1.1.a.

API request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -d
"action=list&policy_id=7256700&details=All&output_format=xml"
"https://qualysapi.qualys.com/api/2.0/fo/compliance/posture/info/"
```

XML output:

```
...
    <GLOSSARY>
      <HOST_LIST>
        <HOST>
          <ID>1574730</ID>
          <IP>10.10.10.10</IP>
          <TRACKING_METHOD>IP</TRACKING_METHOD>
          <DNS><![CDATA[centos.sample.qualys.com]]></DNS>
          <DNS_DATA>
            <HOSTNAME><![CDATA[centos]]></HOSTNAME>
            <DOMAIN><![CDATA[sample.qualys.com]]></DOMAIN>
            <FQDN><![CDATA[centos.sample.qualys.com]]></FQDN>
          </DNS_DATA>
          <OS><![CDATA[CentOS Linux 6.0]]></OS>
          <LAST_COMPLIANCE_SCAN_DATETIME>2021-02-
24T05:37:44Z</LAST_COMPLIANCE_SCAN_DATETIME>
          <PERCENTAGE><![CDATA[62.50% (280 of 448)]]></PERCENTAGE>
        </HOST>
      </HOST_LIST>
      <CONTROL_LIST>
```

```
        <CONTROL>
          <ID>9705</ID>
          <STATEMENT><![CDATA[Status of the cramfs Filesystems
(modprobe)]]></STATEMENT>
          <CRITICALITY>
            <LABEL><![CDATA[MEDIUM]]></LABEL>
            <VALUE>2</VALUE>
          </CRITICALITY>
          <REFERENCE><![CDATA[1.1.1.1.a]]></REFERENCE>
          <RATIONALE_LIST>
            <RATIONALE>
              <TECHNOLOGY_ID>43</TECHNOLOGY_ID>
              <TEXT><![CDATA[The cramfs filesystem type is a compressed
read-only Linux filesystem embedded in small footprint systems. A cramfs
image can be used without having to first decompress the image. Disable
mount utility for unneeded filesystem types reduces the local attack
surface of the server. If this filesystem type is not needed, disable
it.]]></TEXT>
            </RATIONALE>
          </RATIONALE_LIST>
        </CONTROL>
...
```

Updated DTD

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

The element REFERENCE was added to the CONTROL definition in the Posture Info List Output DTD.

```
...
<!ELEMENT CONTROL_LIST (CONTROL+)>
<!ELEMENT CONTROL (ID, STATEMENT, CRITICALITY?, REFERENCE?, DEPRECATED?,
RATIONALE_LIST?)>
<!ELEMENT STATEMENT (#PCDATA)>
<!ELEMENT CRITICALITY (LABEL, VALUE)>
<!ELEMENT REFERENCE (#PCDATA)>
<!ELEMENT DEPRECATED (#PCDATA)>
<!ELEMENT RATIONALE_LIST (RATIONALE*)>
<!ELEMENT RATIONALE (TECHNOLOGY_ID, TEXT)>
...
```

Support for database technology data collection by using underlying OS authentication records

APIs affected	/api/2.0/fo/subscription/option_profile/pc/?action=update|create /api/2.0/fo/subscription/option_profile/pc/?action=list api/2.0/fo/subscription/option_profile/?action=export api/2.0/fo/subscription/option_profile/?action=import
New or Updated API	Updated
DTD or XSD changes	Yes

Now you have an option to enable database instance data collection by using the underlying OS authentication records without creating an authentication record for the database technology. We are supporting the following database versions in this enhancement:

Database	Supported Versions
MongoDB	MongoDB 3.x MongoDB 4.x
Oracle	Oracle 12c Oracle 18c Oracle 19c
MySQL	MySQL 5.x MySQL 8.x
MSSQL	MSSQL 2012 MSSQL 2014 MSSQL 2016 MSSQL 2017 MSSQL 2019

Note: If you are using database authentication records for compliance scans, we recommend that you do not enable this option. Because if you enable it, you will see duplicate results in your compliance reports, one by using database authentication records and the other by using OS-based authentication records. This functionality is useful in a scenario where you have a team responsible for compliance assessment of host operating systems, which does not have access to database authentication records. In this case, if they want to scan database instances running on host assets, they can go ahead by using OS-based authentication records.

We have updated the Option Profile APIs with new input parameters to incorporate this change. We have also added the following definitions to the Option Profile Info DTD (option_profile_info.dtd).

```
<!ELEMENT INSTANCE_DATA_COLLECTION (DATABASES?)>
<!ELEMENT DATABASES (AUTHENTICATION_TYPES_LIST)>
<!ELEMENT AUTHENTICATION_TYPES_LIST (AUTHENTICATION_TYPE+)>
```

Create/Update Compliance Option Profile

The following table contains new input parameters that we've introduced in the Option Profile APIs. You need these parameters while creating or updating an option profile. See the Qualys API (VM, PC) User Guide for details on all the supported input parameters.

Input Parameters

Parameter	Description
enable_instance_data_collection={0|1}	(Required) Specify 1 to enable database instance data collection by using underlying OS authentication record. By default, this option is disabled.
instance_data_collection_auth_types	(Required) Specify the database technologies for which you want to enable OS authentication-based data collection. The valid values are: MongoDB, Oracle, MySQL, MSSQL. You can use this parameter only if you set the value of the enable_instance_data_collection parameter to 1.

Sample create compliance option profile

In this sample, we are creating an option profile with the enable_instance_data_collection option enabled for Oracle, MS SQL, MongoDB and MySQL.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=create&title=API_Option_profile_all&scan_ports=standard&enable_in
stance_data_collection=1&instance_data_collection_auth_types=Oracle,MS
SQL,MongoDB,MySQL"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-02-01T09:15:43Z</DATETIME>
        <TEXT>Compliance Option profile successfully added.</TEXT>
```

```
            <ITEM_LIST>
                <ITEM>
                    <KEY>ID</KEY>
                    <VALUE>108430</VALUE>
                </ITEM>
            </ITEM_LIST>
        </RESPONSE>
    </SIMPLE_RETURN>
```

Sample update compliance option profile

In this sample, we are updating an existing option profile to enable database instance data collection by using the underlying OS authentication record. We are enabling data collection for MongoDB and Oracle database instances.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=update&id=108440&enable_instance_data_collection=1&instance_data_
collection_auth_types=MongoDB,Oracle"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE SIMPLE_RETURN SYSTEM
"https://qualysapi.qualys.com/api/2.0/simple_return.dtd">
<SIMPLE_RETURN>
    <RESPONSE>
        <DATETIME>2021-02-01T09:17:00Z</DATETIME>
        <TEXT>Compliance Option profile successfully updated.</TEXT>
        <ITEM_LIST>
            <ITEM>
                <KEY>ID</KEY>
                <VALUE>108440</VALUE>
            </ITEM>
        </ITEM_LIST>
    </RESPONSE>
</SIMPLE_RETURN>
```

List Compliance Option Profile

In this sample, we are listing a single option profile specified by profile ID. In the XML output, you see the database technology names as the authentication types listed inside the <INSTANCE_DATA_COLLECTION> parent tag.

API Request:

```
curl -u "USERNAME:PASSWORD" -H "X-Requested-With:curl" -X POST -d
"action=list&id=108430"
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/pc/"
```

XML Output:

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE OPTION_PROFILES SYSTEM
"https://qualysapi.qualys.com/api/2.0/fo/subscription/option_profile/opti
on_profile_info.dtd">
<OPTION_PROFILES>
    <OPTION_PROFILE>
        <BASIC_INFO>
            <ID>108430</ID>
            <GROUP_NAME>
               <![CDATA[Profile-Instance-Data-Collection-OS-based-Auth]]>
            </GROUP_NAME>
            <GROUP_TYPE>compliance</GROUP_TYPE>
            <USER_ID>
                <![CDATA[Joe User (joe_user)]]>
            </USER_ID>
            <UNIT_ID>0</UNIT_ID>
            <SUBSCRIPTION_ID>218748</SUBSCRIPTION_ID>
            <IS_GLOBAL>0</IS_GLOBAL>
            <UPDATE_DATE>2021-02-01T09:16:52Z</UPDATE_DATE>
        </BASIC_INFO>
        <SCAN>
            <PORTS>
                <STANDARD_SCAN>1</STANDARD_SCAN>
            </PORTS>
            <PERFORMANCE>
                <PARALLEL_SCALING>0</PARALLEL_SCALING>
                <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                <HOSTS_TO_SCAN>
                    <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                    <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
                </HOSTS_TO_SCAN>
                <PROCESSES_TO_RUN>
                    <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
                    <HTTP_PROCESSES>15</HTTP_PROCESSES>
                </PROCESSES_TO_RUN>
                <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
            </PERFORMANCE>
            <DISSOLVABLE_AGENT>
                <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
                <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
                </PASSWORD_AUDITING_ENABLE>
```

```
<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
            </DISSOLVABLE_AGENT>
            <FILE_INTEGRITY_MONITORING>
                <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
            </FILE_INTEGRITY_MONITORING>
            <CONTROL_TYPES>
                <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
                <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
            </CONTROL_TYPES>
        </SCAN>
        <ADDITIONAL>
            <HOST_DISCOVERY>
                <TCP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </TCP_PORTS>
                <UDP_PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </UDP_PORTS>
                <ICMP>1</ICMP>
            </HOST_DISCOVERY>
            <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
            </PACKET_OPTIONS>
        </ADDITIONAL>
        <INSTANCE_DATA_COLLECTION>
            <DATABASES>
                <AUTHENTICATION_TYPES_LIST>
                    <AUTHENTICATION_TYPE>MongoDB</AUTHENTICATION_TYPE>
                    <AUTHENTICATION_TYPE>Oracle</AUTHENTICATION_TYPE>
                    <AUTHENTICATION_TYPE>MySQL</AUTHENTICATION_TYPE>
                </AUTHENTICATION_TYPES_LIST>
            </DATABASES>
        </INSTANCE_DATA_COLLECTION>
    </OPTION_PROFILE>
</OPTION_PROFILES>
```

DTD update:

The newly added definitions in the Option Profile Info DTD (option_profile_info.dtd) are highlighted in bold for your reference.

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

```
<!ELEMENT OPTION_PROFILES (OPTION_PROFILE)*>

<!ELEMENT OPTION_PROFILE (BASIC_INFO, SCAN, MAP?, ADDITIONAL)>
<!ELEMENT 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 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+)>
```

Export Compliance Option Profile:

In this sample, we are exporting a single option profile specified by ID. In the XML output, you see the database technology names as the authentication types listed under inside the <INSTANCE_DATA_COLLECTION> parent tag.

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&output_format=xml&option_profile_type=compliance&option_profil
e_id=108430"
```

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>108430</ID>
            <GROUP_NAME>
               <![CDATA[Profile-Instance-Data-Collection-OS-based-Auth]]>
```

```
                </GROUP_NAME>
                <GROUP_TYPE>compliance</GROUP_TYPE>
                <USER_ID>
                    <!CDATA[Joe User (joe_user)]]>
                </USER_ID>
                <UNIT_ID>0</UNIT_ID>
                <SUBSCRIPTION_ID>218748</SUBSCRIPTION_ID>
                <IS_GLOBAL>0</IS_GLOBAL>
                <UPDATE_DATE>2021-02-01T09:16:52Z</UPDATE_DATE>
            </BASIC_INFO>
            <SCAN>
                <PORTS>
                    <STANDARD_SCAN>1</STANDARD_SCAN>
                </PORTS>
                <PERFORMANCE>
                    <PARALLEL_SCALING>0</PARALLEL_SCALING>
                    <OVERALL_PERFORMANCE>High</OVERALL_PERFORMANCE>
                    <HOSTS_TO_SCAN>
                        <EXTERNAL_SCANNERS>20</EXTERNAL_SCANNERS>
                        <SCANNER_APPLIANCES>40</SCANNER_APPLIANCES>
                    </HOSTS_TO_SCAN>
                    <PROCESSES_TO_RUN>
                        <TOTAL_PROCESSES>15</TOTAL_PROCESSES>
                        <HTTP_PROCESSES>15</HTTP_PROCESSES>
                    </PROCESSES_TO_RUN>
                    <PACKET_DELAY>Short</PACKET_DELAY>

<PORT_SCANNING_AND_HOST_DISCOVERY>Normal</PORT_SCANNING_AND_HOST_DISCOVER
Y>
                </PERFORMANCE>
                <DISSOLVABLE_AGENT>
                    <DISSOLVABLE_AGENT_ENABLE>0</DISSOLVABLE_AGENT_ENABLE>
                    <PASSWORD_AUDITING_ENABLE>

<HAS_PASSWORD_AUDITING_ENABLE>0</HAS_PASSWORD_AUDITING_ENABLE>
                    </PASSWORD_AUDITING_ENABLE>

<WINDOWS_SHARE_ENUMERATION_ENABLE>0</WINDOWS_SHARE_ENUMERATION_ENABLE>

<WINDOWS_DIRECTORY_SEARCH_ENABLE>0</WINDOWS_DIRECTORY_SEARCH_ENABLE>
                </DISSOLVABLE_AGENT>
                <FILE_INTEGRITY_MONITORING>
                    <AUTO_UPDATE_EXPECTED_VALUE>0</AUTO_UPDATE_EXPECTED_VALUE>
                </FILE_INTEGRITY_MONITORING>
                <CONTROL_TYPES>
                    <FIM_CONTROLS_ENABLED>0</FIM_CONTROLS_ENABLED>
                    <CUSTOM_WMI_QUERY_CHECKS>0</CUSTOM_WMI_QUERY_CHECKS>
                </CONTROL_TYPES>
            </SCAN>
```

```
            <ADDITIONAL>
                <HOST_DISCOVERY>
                    <TCP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </TCP_PORTS>
                    <UDP_PORTS>
                        <STANDARD_SCAN>1</STANDARD_SCAN>
                    </UDP_PORTS>
                    <ICMP>1</ICMP>
                </HOST_DISCOVERY>
                <PACKET_OPTIONS>

<IGNORE_FIREWALL_GENERATED_TCP_RST>0</IGNORE_FIREWALL_GENERATED_TCP_RST>

<IGNORE_FIREWALL_GENERATED_TCP_SYN_ACK>0</IGNORE_FIREWALL_GENERATED_TCP_S
YN_ACK>

<NOT_SEND_TCP_ACK_OR_SYN_ACK_DURING_HOST_DISCOVERY>0</NOT_SEND_TCP_ACK_OR
_SYN_ACK_DURING_HOST_DISCOVERY>
                </PACKET_OPTIONS>
            </ADDITIONAL>
            <INSTANCE_DATA_COLLECTION>
                <DATABASES>
                    <AUTHENTICATION_TYPES_LIST>
                        <AUTHENTICATION_TYPE>MongoDB</AUTHENTICATION_TYPE>
                        <AUTHENTICATION_TYPE>Oracle</AUTHENTICATION_TYPE>
                        <AUTHENTICATION_TYPE>MySQL</AUTHENTICATION_TYPE>
                    </AUTHENTICATION_TYPES_LIST>
                </DATABASES>
            </INSTANCE_DATA_COLLECTION>
        </OPTION_PROFILE>
</OPTION_PROFILES>
```

Sample Option Profile: Import

API Request:

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

XML Output:

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

```
    <DATETIME>2021-02-22T05:48:33Z</DATETIME>
    <TEXT>Successfully imported Option profile for the subscription Id
218748</TEXT>
    <ITEM_LIST>
      <ITEM>
        <KEY>108689</KEY>
        <VALUE>Database_Instance_Data_Collection_OS-Auth_API</VALUE>
      </ITEM>
    </ITEM_LIST>
  </RESPONSE>
</SIMPLE_RETURN>
```

Schema Update (option_profiles.xsd)

The option_profiles.xsd schema is used to validate a proper format and required elements of the option profile XML file when importing and exporting option profiles. To support database instance data collection by using OS-based authentication records, we have added the <xs:element type="INSTANCE_DATA_COLLECTIONType" name="INSTANCE_DATA_COLLECTION"/> tag to the XSD file.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <xs:element name="OPTION_PROFILES" type="OPTION_PROFILESType"/>
...
    <xs:complexType name="OPTION_PROFILEType">
        <xs:sequence>
            <xs:element type="BASIC_INFOType" name="BASIC_INFO"/>
            <xs:element type="SCANType" name="SCAN"/>
            <xs:element type="MAPType" name="MAP" minOccurs="0"/>
            <xs:element type="ADDITIONALType" name="ADDITIONAL"/>
            <xs:element type="INSTANCE_DATA_COLLECTIONType"
name="INSTANCE_DATA_COLLECTION"/>
        </xs:sequence>
...
    <xs:complexType name="INSTANCE_DATA_COLLECTIONType">
        <xs:sequence>
            <xs:element type="DATABASESType" name="DATABASES"
minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="DATABASESType">
        <xs:sequence>
            <xs:element name="AUTHENTICATION_TYPES_LIST"
type="AUTHENTICATION_TYPES_LISTType"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="AUTHENTICATION_TYPES_LISTType">
```

```
            <xs:sequence>
                <xs:element name="AUTHENTICATION_TYPE" maxOccurs="unbounded">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="MongoDB"/>
                            <xs:enumeration value="Oracle"/>
                            <xs:enumeration value="MySQL"/>
                            <xs:enumeration value="MSSQL"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:schema>
```