Qualys CloudView v1.x

API Release Notes

Version 1.17.0

July 19, 2021

The Qualys CloudView API provides automation and integration capabilities for your Qualys subscription. 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

Fetch Control Metadata API

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://qualysguard.qualys.com
Qualys US Platform 2	https://qualysguard.qg2.apps.qualys.com
Qualys US Platform 3	https://qualysguard.qg3.apps.qualys.com
Qualys EU Platform 1	https://qualysguard.qualys.eu
Qualys EU Platform 2	https://qualysguard.qg2.apps.qualys.eu
Qualys India Platform 1	https://qualysguard.qg1.apps.qualys.in
Qualys Canada Platform	https://qualysguard.qg1.apps.qualys.ca
Qualys AE Platform	https://qualysguard.qg1.apps.qualys.ae
Qualys Private Cloud Platform	https://qualysguard.<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.

Fetch Control Metadata API

New API	/rest/v1/controls/metadata/list GET
New or Updated APIs	New
Operator	GET

We have introduced a new API to fetch control metadata information. You can use the filters we support to narrow down the controls to be fetched in the response. We support two method: XML and JSON for the response. You can choose the required method and fetch the data in XML and JSON.

Input Parameters

Parameter	Description
filter	(query) Filter the controls list by providing a query using Qualys syntax. You can use the following tokens: - control.name - resource.type - service.type - cid - provider - control.criticality - control.type - policy.name - createdDate - modifiedDate - isCustomizable
pageNo	(integer) The page to be returned.
pageSize	(integer) The number of records per page to be included in the response.

Fetch Control Metadata (AWS)

Fetch Control Metadata (Azure)

Fetch Control Metadata (GCP)

Metadata DTD

Fetch Control Metadata (AWS)

API request:

```
curl -X GET -u <username>:<password>
```

```
'https:/<QualysURL>//cloudview-
api/rest/v1/controls/metadata/list?filter=provider%3AAWS&pageNo=0&pageSiz
e=100" -H "accept: application/xml'
```

Response (XML):

```
<?xml version='1.0' encoding='UTF-8'?>
  <CONTROL_LIST_OUTPUT>
    <DATETIME>2021-07-06T12:50:34.526+00:00</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <CID>1</CID>
        <CONTROL_NAME>Ensure multi-factor authentication (MFA) is enabled
for all IAM users that have a console password</CONTROL_NAME>
        <CREATED>2020-05-07T12:56:56+0000</CREATED>
        <MODIFIED>2021-05-06T11:31:00+0000</MODIFIED>
        <CONTROL_TYPE>System Defined</CONTROL_TYPE>
        <PROVIDER>AWS</PROVIDER>
        <IS_CUSTOMIZABLE>false</IS_CUSTOMIZABLE>
        <SERVICE_TYPE><![CDATA[IAM]]></SERVICE_TYPE>
        <CRITICALITY>HIGH</CRITICALITY>
        <EVALUATION>
          <EVALUATION_DESCRIPTION>
           <![CDATA[<p>Check IAM Users having console password enabled has
MFA Set to True.</p>
            /n
           <p>Changes in account credentials may take upto 4 hours to get
reflected in the AWS IAM evaluations. The time taken depends on when the
last credential report was fetched by the Cloud View service and the time
when changes were made in AWS IAM</p>
            ]]>
          </EVALUATION_DESCRIPTION>
          <PASS_MESSAGE>IAM user is configured with MFA.</PASS_MESSAGE>
         <FAIL_MESSAGE>IAM user is not configured with MFA.</FAIL_MESSAGE>
          <EVALUATION_CRITERIA_LIST/>
        </EVALUATION>
        <SPECIFICATION>
         <![CDATA[<p>Multi-Factor Authentication (MFA) adds an extra layer
of protection on top of a user name and password. With MFA enabled,
           when a user signs in to an AWS website, they will be prompted
for their user name and password as well as for an
            authentication code from their AWS MFA device. It is
recommended that MFA be enabled for all accounts that have a
            console password.</p>
          /n
          ...
        </REFERENCES>
        <RESOURCE_TYPE>IAM User</RESOURCE_TYPE>
        <REMEDIATION_ENABLED>false</REMEDIATION_ENABLED>
```

```
        <POLICY_NAME_LIST>
          <POLICY_NAME>CIS Amazon Web Services Foundations
Benchmark</POLICY_NAME>
        </POLICY_NAME_LIST>
        </CONTROL>
      </CONTROL_LIST>
    </CONTROL_LIST_OUTPUT>
```

Response (JSON):


```
{
    "dateTime":"2021-07-06T12:52:15.637+00:00",
    "control":[
        {
            "cid":1,
            "controlName":"Ensure multi-factor authentication (MFA) is
enabled for all IAM users that have a console password",
            "created":"2020-05-07T12:56:56+0000",
            "modified":"2021-05-06T11:31:00+0000",
            "controlType":"System Defined",
            "provider":"AWS",
            "isCustomizable":false,
            "serviceType":"IAM",
            "criticality":"HIGH",
            "evaluation":{
               "evaluationDescription":"<p>Check IAM Users having console
password enabled has MFA Set to True.</p>/n<p>Changes in account
credentials may take upto 4 hours to get reflected in the AWS IAM
evaluations. The time taken depends on when the last credential report was
fetched by the Cloud View service and the time when changes were made in
AWS IAM</p>",
                "passMessage":"IAM user is configured with MFA.",
                "failMessage":"IAM user is not configured with MFA.",
                "evaluationCriteria":[

                ]
            },
           "specification":"<p>Multi-Factor Authentication (MFA) adds an
extra layer of protection on top of a user name and password. With MFA
enabled,\n           when a user signs in to an AWS website, they will be
prompted for their user name and password as well as for an\n
authentication code from their AWS MFA device. It is recommended that MFA
be enabled for all accounts that have a\n           console
password.</p>/n<p>\n        CIS reference: CIS Amazon Web Services
Foundations Benchmark v1.3.0 - 08-07-2020: Recommendation #1.10\n
</p>",
            ...
                "CIS Amazon Web Services Foundations Benchmark"
            ]
```

```
        }
    ]
}
```

Fetch Control Metadata (Azure)

API request:

```
curl -k -X GET -u <username>:<password>
'https://<QualysURL>/cloudview-
api/rest/v1/azure/connectors?pageNo=0&pageSize=50'
```

Response (XML):

```
?xml version='1.0' encoding='UTF-8'?>
  <CONTROL_LIST_OUTPUT>
    <DATETIME>2021-07-06T12:55:48.065+00:00</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <CID>50001</CID>
        <CONTROL_NAME>Ensure that Data encryption is set to ON for a SQL
database</CONTROL_NAME>
        <CREATED>2020-05-07T01:27:53+0000</CREATED>
        <MODIFIED>2021-04-22T06:41:05+0000</MODIFIED>
        <CONTROL_TYPE>System Defined</CONTROL_TYPE>
        <PROVIDER>AZURE</PROVIDER>
        <IS_CUSTOMIZABLE>false</IS_CUSTOMIZABLE>
        <SERVICE_TYPE><![CDATA[Azure SQL]]></SERVICE_TYPE>
        <CRITICALITY>HIGH</CRITICALITY>
        <EVALUATION>
          <EVALUATION_DESCRIPTION>
            <![CDATA[<p>
       This control ensures that `Transparent Data Encryption' is enabled
for a threat detection policy on a SQL server.
      </p>
...
    <POLICY_NAME_LIST>
          <POLICY_NAME>CIS Microsoft Azure Foundations
Benchmark</POLICY_NAME>
        </POLICY_NAME_LIST>
      </CONTROL>
    </CONTROL_LIST>
  </CONTROL_LIST_OUTPUT>
```

Response (JSON):

```
<?xml version='1.0' encoding='UTF-8'?>
  <CONTROL_LIST_OUTPUT>
    <DATETIME>2021-07-06T12:55:48.065+00:00</DATETIME>
```

```
    <CONTROL_LIST>
      <CONTROL>
        <CID>50001</CID>
        <CONTROL_NAME>Ensure that Data encryption is set to ON for a SQL
database</CONTROL_NAME>
        <CREATED>2020-05-07T01:27:53+0000</CREATED>
        <MODIFIED>2021-04-22T06:41:05+0000</MODIFIED>
        <CONTROL_TYPE>System Defined</CONTROL_TYPE>
        <PROVIDER>AZURE</PROVIDER>
        <IS_CUSTOMIZABLE>false</IS_CUSTOMIZABLE>
        <SERVICE_TYPE><![CDATA[Azure SQL]]></SERVICE_TYPE>
        <CRITICALITY>HIGH</CRITICALITY>
        <EVALUATION>
          <EVALUATION_DESCRIPTION>
            <![CDATA[<p>
       This control ensures that `Transparent Data Encryption' is enabled
for a threat detection policy on a SQL server.
      </p>
            ]]>
          </EVALUATION_DESCRIPTION>
          <PASS_MESSAGE>Transparent Encryption is Enabled for a SQL
Database</PASS_MESSAGE>
          <FAIL_MESSAGE>Transparent Encryption is not Enabled for a SQL
Database</FAIL_MESSAGE>
          <EVALUATION_CRITERIA_LIST/>
        </EVALUATION>
        <SPECIFICATION>
          <![CDATA[<p>
        Enable Transparent Data Encryption on every SQL database.
      </p>
         ...
                "CIS Microsoft Azure Foundations Benchmark"
            ]
        }
    ]
}
```

Fetch Control Metadata (GCP)

API request:

```
curl -k -X GET -u <username>:<password>
'https://<QualysURL>/cloudview-
api/rest/v1/gcp/connectors?pageNo=0&pageSize=50'
```

Response (XML):

```
<?xml version='1.0' encoding='UTF-8'?>
  <CONTROL_LIST_OUTPUT>
```

```
    <DATETIME>2021-07-06T12:57:27.547+00:00</DATETIME>
    <CONTROL_LIST>
      <CONTROL>
        <CID>52000</CID>
        <CONTROL_NAME>Ensure that corporate login credentials are used
instead of Gmail accounts</CONTROL_NAME>
        <CREATED>2020-05-07T01:24:08+0000</CREATED>
        <MODIFIED>2021-05-19T09:00:54+0000</MODIFIED>
        <CONTROL_TYPE>System Defined</CONTROL_TYPE>
        <PROVIDER>GCP</PROVIDER>
        <IS_CUSTOMIZABLE>false</IS_CUSTOMIZABLE>
        <SERVICE_TYPE><![CDATA[IAM & Admin]]></SERVICE_TYPE>
        <CRITICALITY>MEDIUM</CRITICALITY>
        <EVALUATION>
          <EVALUATION_DESCRIPTION>
            <![CDATA[<p>
        This control ensures that corporate login credentials are used
instead of Gmail accounts.
      </p>
...
 <POLICY_NAME_LIST>
          <POLICY_NAME>CIS Google Cloud Platform Foundation
Benchmark</POLICY_NAME>
        </POLICY_NAME_LIST>
      </CONTROL>
  </CONTROL_LIST_OUTPUT>
```

Response (JSON):

```
{
    "dateTime":"2021-07-06T12:58:24.633+00:00",
    "control":[
        {
            "cid":52000,
           "controlName":"Ensure that corporate login credentials are used
instead of Gmail accounts",
            "created":"2020-05-07T01:24:08+0000",
            "modified":"2021-05-19T09:00:54+0000",
            "controlType":"System Defined",
            "provider":"GCP",
            "isCustomizable":false,
            "serviceType":"IAM & Admin",
            "criticality":"MEDIUM",
            "evaluation":{
               "evaluationDescription":"<p>\n       This control ensures
that corporate login credentials are used instead of Gmail accounts.\n
</p>",
              "passMessage":"Corporate login credentials are used instead
of Gmail account",
```

```
                "failMessage":"Corporate login credentials are not used
instead of Gmail account",
                "evaluationCriteria":[

                ]
            },
            "specification":"<p>\n        Use corporate login credentials
instead of Gmail accounts.\n      </p>/n<p>\n\t    CIS reference: Google
Cloud Platform Foundation Benchmark v1.1.0 - 03-12-2020: Recommendation
#1.1\n\t  </p>",
            ...
      "policyNames":[
                "CIS Google Cloud Platform Foundation Benchmark"
            ]
        }
    ]
}
```

Metadata DTD

Below the metadata.dtd used in the new API that we introduced.

```
<!DOCTYPE CONTROL_LIST_OUTPUT [
        <!ELEMENT CONTROL_LIST_OUTPUT (DATETIME,WARNING?,CONTROL_LIST)*>
        <!ELEMENT DATETIME (#PCDATA)>
        <!ELEMENT WARNING (CODE,TEXT,URL)*>
        <!ELEMENT CODE (#PCDATA)>
        <!ELEMENT TEXT (#PCDATA)>
        <!ELEMENT URL (#PCDATA)>
        <!ELEMENT CONTROL_LIST (CONTROL)*>
        <!ELEMENT CONTROL
(CID,CONTROL_NAME,CREATED,MODIFIED,CONTROL_TYPE,PROVIDER,IS_CUSTOMIZABLE,
SERVICE_TYPE,CRITICALITY,EVALUATION,SPECIFICATION,RATIONALE,MANUAL_REMEDI
ATION,REFERENCES,RESOURCE_TYPE,REMEDIATION_ENABLED,POLICY_NAME_LIST)*>
        <!ELEMENT CID (#PCDATA)>
        <!ELEMENT CONTROL_NAME (#PCDATA)>
        <!ELEMENT CREATED (#PCDATA)>
        <!ELEMENT MODIFIED (#PCDATA)>
        <!ELEMENT CONTROL_TYPE (#PCDATA)>
        <!ELEMENT PROVIDER (#PCDATA)>
        <!ELEMENT IS_CUSTOMIZABLE (#PCDATA)>
        <!ELEMENT SERVICE_TYPE (#PCDATA)>
        <!ELEMENT CRITICALITY (#PCDATA)>
        <!ELEMENT EVALUATION
(EVALUATION_DESCRIPTION,PASS_MESSAGE,FAIL_MESSAGE,EVALUATION_CRITERIA_LIS
T)*>
        <!ELEMENT EVALUATION_DESCRIPTION (#PCDATA)>
        <!ELEMENT PASS_MESSAGE (#PCDATA)>
        <!ELEMENT FAIL_MESSAGE (#PCDATA)>
```

```
<!ELEMENT EVALUATION_CRITERIA_LIST (EVALUATION_CRITERIA)*>
<!ELEMENT EVALUATION_CRITERIA (LABEL,OPERATOR,VALUE)*>
<!ELEMENT LABEL (#PCDATA)>
<!ELEMENT OPERATOR (#PCDATA)>
<!ELEMENT VALUE (#PCDATA)>
<!ELEMENT SPECIFICATION (#PCDATA)>
<!ELEMENT RATIONALE (#PCDATA)>
<!ELEMENT MANUAL_REMEDIATION (#PCDATA)>
<!ELEMENT REFERENCES (#PCDATA)>
<!ELEMENT RESOURCE_TYPE (#PCDATA)>
<!ELEMENT REMEDIATION_ENABLED (#PCDATA)>
<!ELEMENT POLICY_NAME_LIST (POLICY_NAME)*>
<!ELEMENT POLICY_NAME (#PCDATA)>
]>
```