Qualys Certificate View v2.11.0

API Release Notes

Version 2.11.0

December 04, 2022

Qualys Certificate View API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

New API List Server Instances to Fetch Grade Summary of Instance

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. Please replace this URL with the appropriate server URL for your account if you're on another platform.

List Server Instances

APIs affected	/certview/v2/instances
Method	Post
New or Updated APIs	New

Use this API to fetch the grade summary of instances of the certificate identified by the requested parameters. You can use various filters to search the required result. You can use multiple filters and parameters. You can specify starting page number and page size. The response shows grading details of the instances of the certificate.

Input Parameters

filter (String)	(Optional) Filter the events list by providing a query using Qualys syntax. Refer to the list of tokens you can use to build the query: Tokens, Operators and Date Formats Compatibility
pageNumber (Integer)	(Optional) The page to be returned. The default value is zero.
pageSize (Integer)	(Optional) Provide the number of records per page to be included in single page of the response. Default: 10. Maximum: 200 For example, the total result set is 50 assets. If the page size is specified as 10, then the result is divided in 5 pages with 10 records each page.
Authorization (String)	(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with "Bearer" and one space. For example - Bearer authToken

Sample with a Single Filter

The following sample request specifies filter as `instance.id` and `pageSize` as 10 in the request. The request fetches grade summary of the certificate instance related to this query. The response has certificate details like instance summary and grade summary.

API request:

```
curl -X 'POST'
"https://gateway.gg1.apps.qualys.com/certview/v2/instances" -H 'Accept:
application/json'-H "Content-Type: application/json" -d "filterRequest":
{ "filters": [ { "field": "instance.id","value": "3247","operator":
"EQUALS" }]},"pageNumber": 0,"pageSize": 10}' -H  "Authorization: Bearer
<JWT Token>"
```

Response:


```
[
  {
    "id": 3247,
    "port": 443,
    "scannedDate": "2022-11-03T02:46:31.000+00:00",
    "protocol": "tcp",
    "service": "http",
    "grade": "C",
    "asset": {
      "id": 18166463,
      "uuid": "844e33a8-53e2-4c69-8bca-88b9a0aba4ab",
      "name": "joe.dough.example.com",
      "primaryIp": "10.10.10.10"
    },
    "certificate": {
      "id": 13024,
      "certhash":
"88be9dcfba0e89ae97c58ac6f1030c4a3a05e9e4b26f03daf3c260ec8e0daf71",
      "name": "joe.dough.example.com",
      "lastFound": 1667445018000
    },
    "gradeSummary": {
      "grade": "C",
      "gradeWithTrustIgnored": "C",
      "certificateScore": 100,
      "protocolSupportScore": 90,
      "keyExchangeScore": 65,
      "cipherStrengthScore": 65,
      "warnings": [
        "TLS 1.0 Supported. Grade capped to B.",
        "TLS 1.1 Supported. Grade capped to B.",
       "The server does not support Forward Secrecy. Grade capped to B.",
      "The server does not support AEAD (Authenticated encryption) cipher
suites. Grade capped to B."
```

```
      ],
      "errors": [
        "This server uses RC4 with TLS 1.1+. Grade capped to C.",
        "The server supports RC4. Grade capped to B."
      ],
      "notices": [],
      "infos": [],
      "highlights": [
        "SSLv3 is not Supported.",
        "This server supports TLS_FALLBACK_SCSV to prevent protocol
downgrade attacks."
      ],
      "protocolSupportInfo": {
        "SSLv2": false,
        "SSLv3": false,
        "TLSv1": true,
        "TLSv1.3": false,
        "TLSv1.2": true,
        "TLSv1.1": true
      },
      "protocolSupportWeightage": 27,
      "cipherStrengthInfo": {
        "< 128 bits (e.g., 40, 56)": false,
        "0 bits (no encryption)": false,
        ">= 256 bits (e.g., 256)": true,
        "< 256 bits (e.g., 128, 168)": true
      },
      "cipherStrengthWeightage": 26,
      "keyExchangeInfo": {
        "Key or DH parameter strength < 2048 bits (e.g., 1024)": false,
        "Key or DH parameter strength < 512 bits": false,
        "Weak key (Debian OpenSSL flaw)": false,
        "Key or DH parameter strength < 4096 bits (e.g., 2048)": true,
        "Key or DH parameter strength >= 4096 bits (e.g., 4096)": false,
        "Exportable key exchange": false,
        "Anonymous key exchange (no authentication)": false,
        "Key or DH parameter strength < 1024 bits (e.g., 512)": false
      },
      "keyExchangeWeightage": 19.5,
      "cipherSuites": {
        "TLSv1": [
          {
            "name": "RC4-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 4128,
            "category": "INSECURE"
          },
          {
            "name": "AES128-SHA",
```

```
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
      "name": "AES256-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 256,
      "category": "INSECURE"
    }
  ],
  "TLSv1.2": [
    {
      "name": "RC4-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 4128,
      "category": "INSECURE"
    },
    {
      "name": "AES128-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
      "name": "AES256-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 256,
      "category": "INSECURE"
    }
  ],
  "TLSv1.1": [
    {
      "name": "RC4-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 4128,
      "category": "INSECURE"
    },
    {
      "name": "AES128-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
      "name": "AES256-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 256,
      "category": "INSECURE"
```

```
                }
            ]
        }
    }
}
]
```

Sample with Multiple Filters

The following sample request specifies two filters as `asset.name`, `instance.port` and `pageSize` as 10 in the request. The request fetches the grade summary of the certificate instances related to this query. The response has certificate details (like instance summary and grade summary) associated with the asset name and instance port given in the query.

API request:

```
curl -X 'POST'
  'https://gateway.gg1.apps.qualys.com/certview/v2/instances' \
  -H 'Accept: application/json'-H "Content-Type: application/json" -d
 "{"filterRequest": {"filters": [{"field": "asset.name","value":
"joe.dough.example.com","operator": "NOT_EQUALS"},{"field":
"instance.port","value": "400","operator":
"GREATER_THAN_EQUAL"}],"operation": "OR"},"pageNumber": 0,"pageSize":
10}" -H  "Authorization: Bearer <JWT Token>"
```

Response:

```
[
  {
    "id": 3247,
    "port": 443,
    "scannedDate": "2022-11-03T02:46:31.000+00:00",
    "protocol": "tcp",
    "service": "http",
    "grade": "C",
    "asset": {
      "id": 18166463,
      "uuid": "844e33a8-53e2-4c69-8bca-88b9a0aba4ab",
      "name": "joe.dough.example.com",
      "primaryIp": "10.10.10.10"
    },
    "certificate": {
      "id": 13024,
      "certhash":
"88be9dcfba0e89ae97c58ac6f1030c4a3a05e9e4b26f03daf3c260ec8e0daf71",
      "name": "joe.dough.example.com",
      "lastFound": 1667445018000
    },
    "gradeSummary": {
      "grade": "C",
      "gradeWithTrustIgnored": "C",
      "certificateScore": 100,
      "protocolSupportScore": 90,
      "keyExchangeScore": 65,
      "cipherStrengthScore": 65,
      "warnings": [
        "TLS 1.0 Supported. Grade capped to B.",
```

```
        "TLS 1.1 Supported. Grade capped to B.",
        "The server does not support Forward Secrecy. Grade capped to B.",
       "The server does not support AEAD (Authenticated encryption) cipher
suites. Grade capped to B."
      ],
      "errors": [
        "This server uses RC4 with TLS 1.1+. Grade capped to C.",
        "The server supports RC4. Grade capped to B."
      ],
      "notices": [],
      "infos": [],
      "highlights": [
        "SSLv3 is not Supported.",
        "This server supports TLS_FALLBACK_SCSV to prevent protocol
downgrade attacks."
      ],
      "protocolSupportInfo": {
        "SSLv2": false,
        "SSLv3": false,
        "TLSv1": true,
        "TLSv1.3": false,
        "TLSv1.2": true,
        "TLSv1.1": true
      },
      "protocolSupportWeightage": 27,
      "cipherStrengthInfo": {
        "< 128 bits (e.g., 40, 56)": false,
        "0 bits (no encryption)": false,
        ">= 256 bits (e.g., 256)": true,
        "< 256 bits (e.g., 128, 168)": true
      },
      "cipherStrengthWeightage": 26,
      "keyExchangeInfo": {
        "Key or DH parameter strength < 2048 bits (e.g., 1024)": false,
        "Key or DH parameter strength < 512 bits": false,
        "Weak key (Debian OpenSSL flaw)": false,
        "Key or DH parameter strength < 4096 bits (e.g., 2048)": true,
        "Key or DH parameter strength >= 4096 bits (e.g., 4096)": false,
        "Exportable key exchange": false,
        "Anonymous key exchange (no authentication)": false,
        "Key or DH parameter strength < 1024 bits (e.g., 512)": false
      },
      "keyExchangeWeightage": 19.5,
      "cipherSuites": {
        "TLSv1": [
          {
            "name": "RC4-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 4128,
```

```
      "category": "INSECURE"
    },
    {
      "name": "AES128-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
      "name": "AES256-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 256,
      "category": "INSECURE"
    }
  ],
  "TLSv1.2": [
    {
      "name": "RC4-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 4128,
      "category": "INSECURE"
    },
    {
      "name": "AES128-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
      "name": "AES256-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 256,
      "category": "INSECURE"
    }
  ],
  "TLSv1.1": [
    {
      "name": "RC4-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 4128,
      "category": "INSECURE"
    },
    {
      "name": "AES128-SHA",
      "keyExchange": "RSA",
      "encryptionKeyStrength": 128,
      "category": "INSECURE"
    },
    {
```

```
            "name": "AES256-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 256,
            "category": "INSECURE"
          }
        ]
      }
    }
  },
  {
    "id": 3177,
    "port": 443,
    "scannedDate": "2022-10-18T10:07:02.000+00:00",
    "protocol": "tcp",
    "service": "http",
    "grade": "C",
    "asset": {
      "id": 17729052,
      "uuid": "4e354c6b-78f2-45a8-b8e2-bfc54e76ef30",
      "name": "joe.dough.example.com",
      "primaryIp": "10.10.10.10"
    },
    "certificate": {
      "id": 13024,
      "certhash":
"88be9dcfba0e89ae97c58ac6f1030c4a3a05e9e4b26f03daf3c260ec8e0daf71",
      "name": "joe.dough.example.com",
      "lastFound": 1667445018000
    },
    "gradeSummary": {
      "grade": "C",
      "gradeWithTrustIgnored": "C",
      "certificateScore": 100,
      "protocolSupportScore": 90,
      "keyExchangeScore": 65,
      "cipherStrengthScore": 65,
      "warnings": [
        "TLS 1.0 Supported. Grade capped to B.",
        "TLS 1.1 Supported. Grade capped to B.",
       "The server does not support Forward Secrecy. Grade capped to B.",
      "The server does not support AEAD (Authenticated encryption) cipher
suites. Grade capped to B."
      ],
      "errors": [
        "This server uses RC4 with TLS 1.1+. Grade capped to C.",
        "The server supports RC4. Grade capped to B."
      ],
      "notices": [],
      "infos": [],
```

```
      "highlights": [
        "SSLv3 is not Supported.",
        "This server supports TLS_FALLBACK_SCSV to prevent protocol
downgrade attacks."
      ],
      "protocolSupportInfo": {
        "SSLv2": false,
        "SSLv3": false,
        "TLSv1": true,
        "TLSv1.3": false,
        "TLSv1.2": true,
        "TLSv1.1": true
      },
      "protocolSupportWeightage": 27,
      "cipherStrengthInfo": {
        "< 128 bits (e.g., 40, 56)": false,
        "0 bits (no encryption)": false,
        ">= 256 bits (e.g., 256)": true,
        "< 256 bits (e.g., 128, 168)": true
      },
      "cipherStrengthWeightage": 26,
      "keyExchangeInfo": {
        "Key or DH parameter strength < 2048 bits (e.g., 1024)": false,
        "Key or DH parameter strength < 512 bits": false,
        "Weak key (Debian OpenSSL flaw)": false,
        "Key or DH parameter strength < 4096 bits (e.g., 2048)": true,
        "Key or DH parameter strength >= 4096 bits (e.g., 4096)": false,
        "Exportable key exchange": false,
        "Anonymous key exchange (no authentication)": false,
        "Key or DH parameter strength < 1024 bits (e.g., 512)": false
      },
      "keyExchangeWeightage": 19.5,
      "cipherSuites": {
        "TLSv1": [
          {
            "name": "RC4-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 4128,
            "category": "INSECURE"
          },
          {
            "name": "AES128-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 128,
            "category": "INSECURE"
          },
          {
            "name": "AES256-SHA",
            "keyExchange": "RSA",
```

```
            "encryptionKeyStrength": 256,
            "category": "INSECURE"
          }
        ],
        "TLSv1.2": [
          {
            "name": "RC4-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 4128,
            "category": "INSECURE"
          },
          {
            "name": "AES128-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 128,
            "category": "INSECURE"
          },
          {
            "name": "AES256-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 256,
            "category": "INSECURE"
          }
        ],
        "TLSv1.1": [
          {
            "name": "RC4-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 4128,
            "category": "INSECURE"
          },
          {
            "name": "AES128-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 128,
            "category": "INSECURE"
          },
          {
            "name": "AES256-SHA",
            "keyExchange": "RSA",
            "encryptionKeyStrength": 256,
            "category": "INSECURE"
          }
        ]
      }
    }
  }
]
```

Tokens, Operators and Date Formats Compatibility

You can refer to the following tokens and their supported data types and operator while forming each queries.

Token	Data Types	Operators Supported
asset.primaryIp	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS
certificate.certhash	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.keySize	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.serialNumber	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.signatureAlgorithem	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.name	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.country	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.state	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.locality	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.organization	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.organizationUnit	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.source	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.issuerCategory	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.orderStatus	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
asset.uuid	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
asset.name	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS

asset.netbiosName	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
asset.operatingSystem	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
asset.agentId	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.assetId	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.certificateId	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.port	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.fqdn	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.protocol	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.service	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
instance.grade	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.updateDate	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
certificate.createDate	string	IN, IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS
asset.createDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL
certificate.validToDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL
certificate.validFromDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL
asset.updateDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL

asset.scannedDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL
instance.scannedDate	long/date	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL
certificate.issuerId	long	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL, CONTAINS
certificate.rootissuerId	long	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL, CONTAINS
instance.id	long	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL, CONTAINS
certificate.id	long	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL, CONTAINS
asset.id	long	IN, LESSER, IS_EMPTY, GREATER, GREATER_THAN_EQUAL, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, LESS_THAN_EQUAL, CONTAINS
certificate.isEv	Boolean	IN, IS_EMPTY,IS_NOT_EMPTY, EQUALS, NOT_EQUALS
certificate.isImported	Boolean	IN, IS_EMPTY,IS_NOT_EMPTY, EQUALS, NOT_EQUALS
certificate.isSelfSigned	Boolean	IN, IS_EMPTY,IS_NOT_EMPTY, EQUALS, NOT_EQUALS
certificate.dn	String	IS_EMPTY, IS_NOT_EMPTY, EQUALS, NOT_EQUALS, CONTAINS

Tokens with Date Format Compatibility

Refer the following tokens which take dates in the queries and their supported date formats with example

Tokens	Format	Example
certificate.validToDate, certificate.validFromDate, certificate.createDate , certificate.updateDate, asset.createDate, asset.updateDate, asset.scannedDate, instance.scannedDate,	epoch date format	1863402251000
	yyyy-MM-dd'T'HH:mm:ss'Z	2029-01-18T09:14:11Z
	yyyy-MM-dd'T'HH:mm'Z'	2029-01-18T09:14Z
	yyyy-MM-dd'T'HH'Z'	2029-01-18T09Z
	yyyy-MM-dd'Z'	2029-01-18Z
	yyyy-MM-dd	2029-01-18
	yyyy-MM-dd HH:mm:ss	2029-01-18 09:14:11