Table of Contents

Preface........................................................................................................................................ 4
   About Qualys ............................................................................................................................. 4
   Contact Qualys Support........................................................................................................... 4

Chapter 1 - Welcome ............................................................................................................ 5
   Qualys API Framework .......................................................................................................... 5
   Introduction to Certificate View API Paradigm .................................................................... 7

Chapter 2 - Certificate API ................................................................................................. 9
   List Certview Certificates..................................................................................................... 9

Chapter 3 - Analyze Certificate API .................................................................................. 22
   Analyze Certificate Information.......................................................................................... 22

Chapter 4 - Endpoint API .................................................................................................... 24
   List Endpoints ........................................................................................................................ 24

Appendix A - Error Messages .............................................................................................. 31
Preface

This user guide is intended for application developers who will use the Qualys Certificate View API.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Contact Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/.
Chapter 1 - Welcome

Welcome to Certificate View API.

Get Started

Qualys API Framework - Learn the basics about making API requests. The base URL depends on the platform where your Qualys account is located.

Introduction to Certificate View API Paradigm - Get tips on using the Curl command-line tool to make API requests. Every API request must authenticate using a JSON Web Token (JWT) obtained from the Qualys Authentication API.

Get API Notifications

Subscribe to our API Notifications RSS Feeds for announcements and latest news.

From our Community

Join our Community
API Notifications RSS Feeds

Qualys API Framework

The Qualys Certificate View API uses the following framework.

Request URL

The URL for making API requests respects the following structure:

https://<baseurl>/<module>/<object>/<object_id>/<operation>

where the components are described below.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;baseurl&gt;</td>
<td>The Qualys API server URL that you should use for API requests depends on the platform where your account is located. The base URL for Qualys US Platform 1 is: <a href="https://gateway.qg1.apps.qualys.com">https://gateway.qg1.apps.qualys.com</a></td>
</tr>
<tr>
<td>&lt;module&gt;</td>
<td>The API module. For the Certificate View API, the module is: “certview”.</td>
</tr>
<tr>
<td>&lt;object&gt;</td>
<td>The module specific object.</td>
</tr>
<tr>
<td>&lt;object_id&gt;</td>
<td>(Optional) The module specific object ID, if appropriate.</td>
</tr>
<tr>
<td>&lt;operation&gt;</td>
<td>The request operation, such as count.</td>
</tr>
</tbody>
</table>
## Base URL to the Qualys API Server

The Qualys API documentation and sample code within it use the API server URL for Qualys US Platform 1: gateway.qg1.apps.qualys.com.

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

<table>
<thead>
<tr>
<th>Account Login</th>
<th>API Server URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qualys US Platform 1</td>
<td><a href="https://gateway.qg1.apps.qualys.com">https://gateway.qg1.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 2</td>
<td><a href="https://gateway.qg2.apps.qualys.com">https://gateway.qg2.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys US Platform 3</td>
<td><a href="https://gateway.qg3.apps.qualys.com">https://gateway.qg3.apps.qualys.com</a></td>
</tr>
<tr>
<td>Qualys EU Platform 1</td>
<td><a href="https://gateway.qg1.apps.qualys.eu">https://gateway.qg1.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys EU Platform 2</td>
<td><a href="https://gateway.qg2.apps.qualys.eu">https://gateway.qg2.apps.qualys.eu</a></td>
</tr>
<tr>
<td>Qualys India Platform 1</td>
<td><a href="https://gateway.qg1.apps.qualys.in">https://gateway.qg1.apps.qualys.in</a></td>
</tr>
<tr>
<td>Qualys Canada Platform 1</td>
<td><a href="https://qualysapi.qg1.apps.qualys.ca/">https://qualysapi.qg1.apps.qualys.ca/</a></td>
</tr>
<tr>
<td>Qualys Private Cloud Platform</td>
<td><a href="https://gateway">https://gateway</a>.&lt;customer_base_url&gt;</td>
</tr>
</tbody>
</table>
Introduction to Certificate View API Paradigm

Authentication

You must authenticate to the Qualys Cloud Platform using Qualys account credentials (user name and password) and get the JSON Web Token (JWT) before you can start using the Certificate View APIs. Use the Qualys Authentication API to get the JWT.

For example,

```
curl -X POST https://gateway.qg1.apps.qualys.com/auth -d "username=value1&password=passwordValue&token=true&permissions=true" -H "ContentType: application/x-www-form-urlencoded"
```

where gateway.qg1.apps.qualys.com is the base URL to the Qualys API server where your account is located.

- **username** and **password** are the credentials of the user account for which you want to fetch Certificate View data
- **token** should be true
- **permissions** should be true
- **Content-Type** should be "application/x-www-form-urlencoded"

The Authentication API returns a JSON Web Token (JWT) which you can use for authentication during Certificate View API calls. The token expires in 2 to 3 hours. You must regenerate the token to continue using the Certificate View API.

Using Curl

**Curl** is a multi-platform command-line tool used to transfer data using multiple protocols. This tool is supported on many systems, including Windows, Unix, Linux and Mac. In this document Curl is used in the examples to build Qualys API requests using the HTTP over SSL (https) protocol, which is required.

Want to learn more? Visit [https://curl.haxx.se/](https://curl.haxx.se/)

The following Curl options are used according to different situations:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-X &quot;POST&quot;</code></td>
<td>The POST method is required for all Certificate View API requests.</td>
</tr>
<tr>
<td><code>-H &quot;Authorization: Bearer &lt;token&gt;&quot;</code></td>
<td>This option is used to provide a custom HTTP request header parameter for authentication. Provide the JSON Web Token (JWT) received from Qualys authentication API in the following format: <strong>Authorization: Bearer &lt;token&gt;</strong>&lt;br&gt;For information about Qualys authentication API, see <strong>Authentication</strong>.</td>
</tr>
</tbody>
</table>
The sample below shows a typical Curl request using options mentioned above and how they interact with each other.

Chapter 2 - Certificate API

Use these API functions to retrieve a list of certificates based on an input filter query. The response contains certificate details including associated host information and SSL/TLS related vulnerabilities and grades.

List Certview Certificates

/certview/v1/certificates

[POST]

**Input Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter (String)</td>
<td>Filter the events list by providing a query using Qualys syntax. Refer to the “How to Search” topic in the online help for assistance with creating your query. For example - expiryGroup: Expired Refer to the list of tokens you can use to build the query: Search tokens</td>
</tr>
<tr>
<td>pageNumber (Integer)</td>
<td>The page to be returned. Starts from zero.</td>
</tr>
<tr>
<td>pageSize (Integer)</td>
<td>The number of records per page to be included in the response. Default is 10.</td>
</tr>
<tr>
<td>sort (String)</td>
<td>Sort the results using a Qualys token. For example - [&quot;lastFound&quot;:&quot;desc&quot;]</td>
</tr>
<tr>
<td>Authorization (String)</td>
<td>(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with “Bearer” and one space. For example - Bearer authToken</td>
</tr>
</tbody>
</table>
List Certview Certificates

**Certificate Details (String)**

(Optional) Define the level of certificate attributes you want to list. Default value `basic` is used to fetch commonly used attributes. Use value `extended` to fetch these additional attributes:
- Serial number
- Auth Key Identifier
- Subject Key Identifier
- Key Usage
- Base64 certificate
- Enhanced Key Usage

The `enhancedKeyUsage` attribute returns a list of OIDs in the EKU attribute of the certificate.
Some of the most commonly used OIDs are:

1.3.6.1.5.5.7.3.1—Server Authentication
1.3.6.1.5.5.7.3.2—Client Authentication
1.3.6.1.5.5.7.3.3—Code Signing
1.3.6.1.5.5.7.3.4—Email Protection
1.3.6.1.5.5.7.3.8—Time Stamping
1.3.6.1.5.5.7.3.9—OCSP Signing

For more information refer to [http://www.oid-info.com/](http://www.oid-info.com/)

**Permissions**

- User must be a Super User or must have the `CERTVIEW.API.ACCESS` permission.

**Sample with all parameters defined**

**Request:**

```bash
curl -X POST "https://gateway.qg1.apps.qualys.com/certview/v1/certificates" -H "Accept: application/json" -H "Content-Type: application/json" -d "\{ "filter": {\"certhash\":9d576081850549e5b05449b22054620586d2ce28f00576ee43a4ccb59c19c017\", "pageNumber":0, "pageSize":1}\}" -H "Authorization: Bearer <jwt token>"
```

**Response:**

```json
[
{
    "keySize": 2048,
    "subject": {
        "organization": "Qualys, Inc.",
        "locality": "Foster City",
        "name": ".p01.eng.sjc01.qualys.com",
        "state": "California"
    }
}
```
"country": "US",
"organizationUnit": [
   "Production"
]
},
"validFrom": 1542842460000,
"signatureAlgorithm": "SHA256withRSA",
"issuer": {
   "organization": "Qualys, Inc.",
   "organizationUnit": [
      "Operations"
   ],
   "name": "Qualys Ops T2v1",
   "country": "US",
   "state": "California",
   "certhash": "8c127ee4dda53afe064d6c11723968820610ada22df4a549283f07e83dfbf31"
   "locality": "Redwood City"
},
"rootissuer": {
   "organization": "Qualys, Inc.",
   "organizationUnit": [
      "Operations"
   ],
   "name": "Qualys Ops T2v1",
   "country": "US",
   "state": "California",
   "certhash": "11b3989aa1f515a9c76c2079d64ef6f4b0e3a0d5f0360837c7a29c5dcf71a555"
   "locality": "Redwood City"
},
"instanceCount": 1,
"dn": "CN=*.p01.eng.sjc01.qualys.com, OU=Production, O=\"Qualys, Inc.\", L=Foster City, ST=California, C=US",
"certhash": "9d576081850549e5b05449b220546205862ce28f00576ee43a4cc59c19c017"
"assets": [
   {"netbiosName": ",
   "assetId": "495dfba4-f943-4d66-b88c-6b118262f4eb",
   "name": "qualysguard.p01.eng.sjc01.qualys.com",
   "operatingSystem": "NetScaler",
   "tags": [}
{  
  "name": "Test",  
  "uuid": "cadd8477-ce01-4d81-a86c-dc909304ed24"  
},  
"hostInstances": [  
  {  
    "protocol": "tcp",  
    "sslProtocols": [  
      "TLSv1.2",  
      "TLSv1.1"  
    ],  
    "port": 443,  
    "grade": "T",  
    "service": "http",  
    "fqdn": "",  
    "vulnerabilities": [  
      {  
        "title": "SSL Certificate - Information",  
        "severity": 1,  
        "qid": 86002  
      },  
      {  
        "title": "SSL Server Information Retrieval",  
        "severity": 1,  
        "qid": 38116  
      },  
      {  
        "title": "SSL/TLS use of weak RC4(Arcfour) cipher",  
        "severity": 3,  
        "qid": 38601  
      },  
      {  
        "title": "SSL Certificate - Self-Signed Certificate",  
        "severity": 2,  
        "qid": 38169  
      },  
      {  
        "title": "HTTP Strict Transport Security (HSTS) Support Detected",  
        "severity": 1,  
        "qid": 86137  
      },  
      {  
        "title": "SSL Certificate - Signature Verification"  
      }  
  ]
}
Failed Vulnerability",
   "severity": 2,
   "qid": 38173
 },
[{"title": "TLS Secure Renegotiation Extension Support Information",
   "severity": 1,
   "qid": 42350
 ]},
"vulnCount": 7
],
"created": 1568092607000,
"updated": 1569844893000,
"assetInterfaces": [
  {
    "hostname": "qualysguard.p01.eng.sjc01.qualys.com",
    "address": "10.44.1.66"
  }
],
"certificateCount": 0
]
},
"selfSigned": false,
"validTo": 1606000860000,
"issuerCategory": "unapproved",
"subjectAlternativeNames": {},
"lastFound": 1569844893000,
"extendedValidation": false,
"orderStatus": ""}]}
Sample with certificateDetails parameter set to Basic

Request:

curl -X POST
"https://gateway.qgl.apps.qualys.com/certview/v1/certificates" -H
'Accept: application/json' -H "Content-Type: application/json" -d
"{ "filter": {"certhash":9d576081850549e5b05449b22054620586d2ce28f00576ee43a4ccb59c19c017", "pageNumber": 0, "pageSize": 1, "certificateDetails": "basic"}, "Authorization": Bearer <jwt token>"

Response:
[
{
"keySize": 2048,
"subject": {
"organization": "Qualys, Inc.",
"locality": "Foster City",
"name": "*.p01.eng.sjc01.qualys.com",
"state": "California",
"country": "US",
"organizationUnit": [
"Production"
]
},
"validFrom": 1542842460000,
"signatureAlgorithm": "SHA256withRSA",
"issuer": {
"organization": "Qualys, Inc.",
"organizationUnit": [
"Operations"
]
},
"name": "Qualys Ops T2v1",
"country": "US",
"state": "California",
"certhash": "8c127eec4dda53adf064d6c1172396b8d20610da22df4a549283f07e83dfbf31",
"locality": "Redwood City"
},
"rootissuer": {
"organization": "Qualys, Inc.",
"organizationUnit": [
"Operations"
]"}
"name": "Qualys Ops T2v1",
"country": "US",
"state": "California",
"certhash": "11b3989a1f515a9c76c2079d64ef6f4b0e3a0d5f0360837c7a29c5dcf71a555",
"locality": "Redwood City"
"instanceCount": 1,
"dn": "CN=*.p01.eng.sjc01.qualys.com, OU=Production, O="Qualys, Inc.", L=Foster City, ST=California, C=US",
"certhash": "9d576081850549e5b05449b22054620586d2ce28f00576ee43a4ccb59c19c017",
"assets": [
{
"netbiosName": "",
"assetId": "495dfba4-f943-4d66-b88c-6b118262f4eb",
"name": "qualysguard.p01.eng.sjc01.qualys.com",
"operatingSystem": "NetScaler",
"tags": [
{
"name": "Test",
"uuid": "cadd8477-ce01-4d81-a86c-dc909304ed24"
}
],
"hostInstances": [
{
"protocol": "tcp",
"sslProtocols": [
"TLSv1.2",
"TLSv1.1"
],
"port": 443,
"grade": "T",
"service": "http",
"fqdn": "",
"vulnerabilities": [
{
"title": "SSL Certificate - Information",
"severity": 1,
"qid": 86002
},
{
"title": "SSL Server Information Retrieval",
"severity": 1,
"qid": 38116
},
{
  "title": "SSL/TLS use of weak RC4(Arcfour) cipher",
  "severity": 3,
  "qid": 38601
},
{
  "title": "SSL Certificate - Self-Signed Certificate",
  "severity": 2,
  "qid": 38169
},
{
  "title": "HTTP Strict Transport Security (HSTS) Support Detected",
  "severity": 1,
  "qid": 86137
},
{
  "title": "SSL Certificate - Signature Verification Failed Vulnerability",
  "severity": 2,
  "qid": 38173
},
{
  "title": "TLS Secure Renegotiation Extension Support Information",
  "severity": 1,
  "qid": 42350
}
],
"vulnCount": 7
},
{
"created": 1568092607000,
"updated": 156984893000,
"assetInterfaces": [
{
  "hostname": "qualysguard.p01.eng.sjc01.qualys.com",
  "address": "10.44.1.66"
}
],
"certificateCount": 0
}
"selfSigned": false,
"validTo": 1606000860000,
"issuerCategory": "unapproved",
"subjectAlternativeNames": {},
"lastFound": 1569848930000,
"extendedValidation": false,
"orderStatus": ""
}
]

Sample with certificateDetails parameter set to Extended

Request:

curl -X POST 
"https://gateway.qgl.apps.qualys.com/certview/v1/certificates" -H 
"Accept: application/json" -H "Content-Type: application/json" -d 
"{"filter": \"expiryGroup:Expired\", \"pageNumber\": 0, \n\"pageSize\": 1, \"certificateDetails\": \"extended\"}" -H 
"Authorization: Bearer <jwt token>"

Response:

[ 
  
  "keySize": 2048,
  "subject": {
    "organization": "Qualys, Inc.",
    "locality": "Foster City",
    "name": "user",
    "state": "California",
    "country": "US",
    "organizationUnit": [
      "Production"
    ],
  },
  "validFrom": 1542842460000,
  "signatureAlgorithm": "SHA256withRSA",
  "issuer": {
    "organization": "Qualys, Inc.",
    "organizationUnit": [
      "Operations"
    ],
    "name": "Qualys Ops T2v1",
    "country": "US",
    "state": "California",
    "certhash": "8c127eecc4da53a0d064d6c1172396b8d520610da22da549283f07e83dfbf31"
}
"locality": "Redwood City"
},
"rootissuer": {
"organization": "Qualys, Inc.",
"organizationUnit": [
"Operations"
],
"name": "Qualys Ops T2v1",
"country": "US",
"state": "California",
"certhash": "11b3989a1f515aac76c2079d64ef6f4b0e3a0d5f0360837c7a29c5dcf71a555"
},
"locality": "Redwood City"
},
"instanceCount": 1,
"dn": "CN=*.p01.eng.sjc01.qualys.com, OU=Production, O=Qualys, Inc., L=Foster City, ST=California, C=US",
"certhash": "9d576081850549e5b05449b22b5426b5a20c9c19c19c017"
],
"assets": [
{
"netbiosName": "", 
"assetId": "495dfba4-f943-4d66-b88c-6b118262f4eb",
"name": "qualysguard.p01.eng.sjc01.qualys.com",
"operatingSystem": "NetScaler",
"tags": [
{
"name": "Test",
"uuid": "cadd8477-ce01-4d81-a86c-dc909304ed24"
}
],
"hostInstances": [
{
"protocol": "tcp",
"sslProtocols": [
"TLSv1.2",
"TLSv1.1"
],
"port": 443,
"grade": "T",
"service": "http",
"fqdn": "",
"vulnerabilities": [
{  "title": "SSL Certificate - Information",  "severity": 1,  "qid": 86002 },
{  "title": "SSL Server Information Retrieval",  "severity": 1,  "qid": 38116 },
{  "title": "SSL/TLS use of weak RC4(Arcfour) cipher",  "severity": 3,  "qid": 38601 },
{  "title": "SSL Certificate - Self-Signed Certificate",  "severity": 2,  "qid": 38169 },
{  "title": "HTTP Strict Transport Security (HSTS) Support Detected",  "severity": 1,  "qid": 86137 },
{  "title": "SSL Certificate - Signature Verification Failed Vulnerability",  "severity": 2,  "qid": 38173 },
{  "title": "TLS Secure Renegotiation Extension Support Information",  "severity": 1,  "qid": 42350 }
},  "vulnCount": 7 }
]
"created": 1568092607000,
"updated": 1569844893000,
"assetInterfaces": [}
List Certview Certificates

```json
{
    "hostname": "qualysguard.p01.eng.sjc01.qualys.com",
    "address": "10.44.1.66"
}
```

- **Certificate Count**: 0
- **SelfSigned**: false
- **ValidTo**: 1606000860000
- **IssuerCategory**: "unapproved"
- **LastFound**: 1569848930000
- **ExtendedValidation**: false
- **OrderStatus**: ""
- **SerialNumber**: "0236b0afe50fd944522deddb6b81e317"
- **KeyUsage**: [Digital signature, Key encipherment]
- **RawData**: "-----BEGIN CERTIFICATE-----
MIIFXDCCBESgAwIBAgIQAjawr+UP2URSLe3ba4HjFzANBgkqhkiG9w0BAQsFADB
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMS0wKwYDVQQDEy
nADp2QVydCBUZXNOIFN1QT1qSW50ZXJtZWRPcHRlcnNlcmlhbmcgV2Fyb2tzLm
MDAwWhcNMTgxMjI4MTI5NzkuY29tLmNvbS90b29tLmNybC8wMDA0NS5jcmww
MB8GA1UdIwQYMBaAFNZN+TlgbHPDivtMtAvoqMBGA1UDgQWBQQTBgUAMxI6
nEhvxx7ZquAzBnkVHRELDAAgghNxc2Muc4XVhhlzLWRIbW8uY29tghN0YW0u
nhbIzLWRIbW8uY29tMA4GA1UDwEB/wQEAwIwFQADAgDgEBFQcD
nAQYIKwYBBQUHAgEwMQA0DQwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCg

"-----END CERTIFICATE-----
```
Chapter 2 - Certificate API

\n\n---END CERTIFICATE---

"enhancedKeyUsage": [  
  "1.3.6.1.5.5.7.3.1",  
  "1.3.6.1.5.5.7.3.2"
],
"subjectKeyIdentifier": "138225bf99709d02c7bf698f121bf1919ed0bb",
"authKeyIdentifier": "d64f939606c73c322f5ad300c2fa0d5ca754a2a"
}
Chapter 3 - Analyze Certificate API

Use these API functions to analyze information based on host or IP.

Use this API to retrieve the list of endpoints that are associated with an FQDN in the CertView inventory.

Analyze Certificate Information

/certview/v1/analyze

[POST]

Input Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host (String)</td>
<td>(Required) Host on which scan is executed, it can be IP For example - <a href="http://www.ssllabs.com">www.ssllabs.com</a>, 10.10.10.10</td>
</tr>
<tr>
<td>Authorization</td>
<td>(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with &quot;Bearer&quot; and one space. For example - Bearer authToken</td>
</tr>
</tbody>
</table>

Permissions

- User must be a Super User or must have the CERTVIEW.API.ACCESS permission.

Sample - Host is IP

Request:


Response:

```json
{
  "host": "64.41.200.100",
  "endpoints": [
    {
      "ipAddress": "64.41.200.100",
      "port": 443,
      "service": "http",
      "grade": "A+",
      "gradeTrustIgnored": "A+",
      "hasWarnings": false,
      "exceptional": true
    }
  ]
}
```
Sample - Host is FQDN

Request:
```
```

Response:
```
{
  "host": "www.ssllabs.com",
  "endpoints": [
    {
      "ipAddress": "64.41.200.100",
      "port": 443,
      "service": "http",
      "grade": "A+",
      "gradeTrustIgnored": "A+",
      "hasWarnings": false,
      "isExceptional": true
    },
    {
      "ipAddress": "64.41.200.100",
      "port": 5443,
      "service": "rdp",
      "grade": "A+",
      "gradeTrustIgnored": "A+",
      "hasWarnings": false,
      "isExceptional": true
    },
    {
      "ipAddress": "64.41.200.111",
      "port": 443,
      "service": "http",
      "grade": "A+",
      "gradeTrustIgnored": "A+",
      "hasWarnings": false,
      "isExceptional": true
    }
  ]
}
```
Chapter 4 - Endpoint API

Use these API function to retrieve detailed endpoint information.

List Endpoints

/certview/v1/getEndpointData

[POST]

Input Parameters

<table>
<thead>
<tr>
<th>Authorization (String)</th>
<th>(Required) Authorization token to authenticate to the Qualys Cloud Platform. Prepend token with &quot;Bearer&quot; and one space. For example - Bearer authToken</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip (String)</td>
<td>(Required) Host IP for which the endpoint details are required.</td>
</tr>
<tr>
<td>port (Integer)</td>
<td>Used to filter the endpoint details based on port.</td>
</tr>
<tr>
<td></td>
<td>In Certview scan, we can scan multiple ports as certificates can be found on multiple ports. Define the port number to filter the endpoint data based on port.</td>
</tr>
<tr>
<td>fqdn (String)</td>
<td>Used to filter the endpoint details based on FQDN.</td>
</tr>
<tr>
<td></td>
<td>Note: For filtering based on fqdn, port is required parameter. Also, this field is required if the service or protocol parameter is specified.</td>
</tr>
<tr>
<td>service (String)</td>
<td>Used to filter the endpoint details based on service.</td>
</tr>
<tr>
<td></td>
<td>Note: For filtering based on fqdn, port is required parameter. Also, this field is required if the fqdn or protocol parameter is specified.</td>
</tr>
<tr>
<td>protocol (String)</td>
<td>Used to filter the endpoint details based on protocol.</td>
</tr>
<tr>
<td></td>
<td>Note: For filtering based on fqdn, port is required parameter. Also, this field is required if the service or protocol parameter is specified.</td>
</tr>
</tbody>
</table>

Permissions

- User must be a Super User or must have the CERTVIEW.API.ACCESS permission.
Sample with all parameters defined

Request:

curl -X POST
"https://gateway.qgl.apps.qualys.com/certview/v1/getEndpointData"
-H "Accept: application/json" -H "Content-Type: application/json"
-d "{"ip": "64.41.200.100", "port": 443, "fqdn": "", "service": "tcp"}"
-H "Authorization: Bearer <JWT Token>"

Response:
[

{
    "ipAddress": "64.41.200.100",
    "port": 443,
    "service": "http",
    "grade": "A+",
    "gradeTrustIgnored": "A+",
    "hasWarnings": false,
    "isExceptional": true,
    "details": {
        "certChains": ["certIds": [
            "4bda9e40d19260d636042a0e6ad5222a024f05f7001d61220f17e6632428f1d6"
        ],
        "trustPaths": ["certIds": [
            "154c433c491929c5ef686e838e323664a00e6a0d822ccc958fb4dad03e49a08f"
        ],
            "certChains": ["certIds": [
        "4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161"
    ],
    "trustPaths": ["certIds": [
        "4bda9e40d19260d636042a0e6ad5222a024f05f7001d61220f17e6632428f1d6"
    ],
        "154c433c491929c5ef686e838e323664a00e6a0d822ccc958fb4dad03e49a08f"
    ],
            "certChains": ["certIds": [
        "4348a0e9444c78cb265e058d5e8944b4d84f9662bd26db257f8934a443c70161"
    ],
    "trustPaths": ["certIds": [null]
]
"rootStore": "Mozilla",
"isTrusted": true
}
]
]
"noSni": false
]
"protocols": [
{
"id": 771,
"name": "TLS",
"version": "1.2"
},
{
"id": 770,
"name": "TLS",
"version": "1.1"
},
{
"id": 769,
"name": "TLS",
"version": "1.0"
}
],
"suites": [
{
"protocol": 771,
"list": [
{
"name": "DHE-RSA-AES128-SHA",
"cipherStrength": 128,
"kxType": "DH"
},
{
"name": "DHE-RSA-AES256-SHA",
"cipherStrength": 256,
"kxType": "DH"
},
{
"id": 103,
"name": "DHE-RSA-AES128-SHA256",
"cipherStrength": 128,
"kxType": "DH"
}]}
[, 
  {
    "id": 107,
    "name": "DHE-RSA-AES256-SHA256",
    "cipherStrength": 256,
    "kxType": "DH"
  },
  {
    "id": 158,
    "name": "DHE-RSA-AES128-GCM-SHA256",
    "cipherStrength": 128,
    "kxType": "DH"
  },
  {
    "id": 159,
    "name": "DHE-RSA-AES256-GCM-SHA384",
    "cipherStrength": 256,
    "kxType": "DH"
  },
  {
    "id": 49171,
    "name": "ECDHE-RSA-AES128-SHA",
    "cipherStrength": 128,
    "kxType": "ECDH"
  },
  {
    "id": 49172,
    "name": "ECDHE-RSA-AES256-SHA",
    "cipherStrength": 256,
    "kxType": "ECDH"
  },
  {
    "id": 49191,
    "name": "ECDHE-RSA-AES128-SHA256",
    "cipherStrength": 128,
    "kxType": "ECDH"
  },
  {
    "id": 49192,
    "name": "ECDHE-RSA-AES256-SHA384",
    "cipherStrength": 256,
    "kxType": "ECDH"
  },
  {
    "id": 49199,
]
Chapter 4 - Endpoint API
List Endpoints

"name": "ECDHE-RSA-AES128-GCM-SHA256",
"cipherStrength": 128,
"kxType": "ECDH"
},
{
"id": 49200,
"name": "ECDHE-RSA-AES256-GCM-SHA384",
"cipherStrength": 256,
"kxType": "ECDH"
}
]
},
{
"protocol": 770,
"list": [
{
"name": "DHE-RSA-AES128-SHA",
"cipherStrength": 128,
"kxType": "DH"
},
{
"name": "DHE-RSA-AES256-SHA",
"cipherStrength": 256,
"kxType": "DH"
},
{
"name": "ECDHE-RSA-AES128-SHA",
"cipherStrength": 128,
"kxType": "ECDH"
},
{
"name": "ECDHE-RSA-AES256-SHA",
"cipherStrength": 256,
"kxType": "ECDH"
}
]
},
{
"protocol": 769,
"list": [
{
"id": 51,
"name": "DHE-RSA-AES128-SHA",
"cipherStrength": 128,
"kxType": "DH"
}
"id": 57,
"name": "DHE-RSA-AES256-SHA",
"cipherStrength": 256,
"kxType": "DH"
},

"id": 49171,
"name": "ECDHE-RSA-AES128-SHA",
"cipherStrength": 128,
"kxType": "ECDH"
},

"id": 49172,
"name": "ECDHE-RSA-AES256-SHA",
"cipherStrength": 256,
"kxType": "ECDH"
"goldenDoodle": 1,
"supportsCBC": true,
"zeroLengthPaddingOracle": 1,
"sleepingPoodle": 1
]
Appendix A - Error Messages

This appendix describes the types of error messages returned from Certificate View API requests.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Provide an input parameter in correct syntax.</td>
</tr>
<tr>
<td>401</td>
<td>Make sure the user has appropriate permissions to call the Certificates API.</td>
</tr>
<tr>
<td>422</td>
<td>Provide a valid input parameter.</td>
</tr>
<tr>
<td>500</td>
<td>The server encountered an unexpected condition which prevented it from fulfilling the request. Please try again later.</td>
</tr>
</tbody>
</table>