Qualys Certificate View v2.x

API Release Notes

Version 2.7

September 11, 2020

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

What's New

New APIs to Enroll and Renew Certificates

New Error Codes

Qualys API 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.

New APIs to Enroll and Renew Certificates

You can now enroll new or renew existing certificates using the new APIs. The following APIs enable you to complete the end-to-end enrollment or renewal workflow:

- Create Enrollment/Renewal Certificate Request
- Update Certificate Request
- Update Status of Certificate Request
- View Certificate Request
- List DigiCert Organizations
- List DigiCert Products
- List Digicert EV Approvers

Create Enrollment/Renewal Certificate Request

Use this API to enroll or renew certificates

APIs affected	/certview/rest/public/v1/certificates/enrollment/digicert/orders
Method	POST
New or Updated APIs	New

Input Parameters

Input parameters for Create and Update APIs

approverUserNames (array)	(Required) Array of valid user names. User roles must be manager, PKI admin or approvers.
intermediateCA (object)	(Required) Intermediate Certificate Authority information. Make sure: - At least one of the params certhash, commonName or serialNumber is required. - CA is DigiCert's public intermediate CA - CA is configured with CA api key
certhash (string)	(Optional) Secure hash of the certificate
commonName (string)	(Optional) Fully qualified domain name of the Web server that will receive the certificate
serialNumber (string)	(Optional) A short, unique identifier for each certificate generated by the certificate issuer
certificate (object)	(Required)
commonName (string)	(Required) Provide a wildcard character if the product name is of wildcard type.
csr (object)	(Required) Certificate Signing Request Information
autoGenerateCSR (boolean)	(Optional) If this flag is set to True then Qualys will generate csr value and return private key info in the response of the api. If this field is set to True then encoded_csr field can not be set By default the value is set to False.
encodedCSR (string)	(Optional) A valid Encoded Certificate Signing Request
organizationUnits (array)	(Optional) provide value for the OU field for the certificate.
signatureHash (string)	Required) Certificate's signing algorithm hash. Accepted values: SHA-256, SHA-384, SHA-512
renewal (object)	(Optional) Required for certificate renewal request.
digicertPreviousOrderId (integer)	(Required) If the request is a renewal of a previous request then add the previous request id.

renewalOfCertificate (string)	(Required) Provide certhash of the old certificate for which this renewal request is required. Make sure: - certificate is in customer's account - certificate is leaf certificate - certificate is not in IN_RENEWAL status
validity (object)	(Required) Provide any one of the following values: customExpirationDate, validityYears and validityDays params Make sure only one value is provided in a request.
customExpirationDate (date)	(Optional) Expiry date of the certificate.
validityYears (integer)	(Optional) Number of years that the certificate is valid.
validityDays (integer)	(Optional) Number of days that the certificate is valid.
digicertOrganizationId (integer)	(Required) Get organization id using List DigiCert Organizations API
digicertProductNameId (integer)	(Required) Get product name id using List DigiCert Products API
digicertEVApproverUserIds (array)	(Optional) Required when product name is of EV type. Get EV Approvers user id using List Digicert EV Approvers API
comment (string)	(Optional) Any additional comments.

Sample to Submit Certificate Enrollment Request

API request:

```
curl -X POST
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/or
ders" -H "Accept: application/json" -H "Content-Type: application/json" -
d '{ "approverUserNames": [ "quays_sd" ], "certificate": { "commonName":
"p12.test.qualys-demo.com", "csr": { "autoGenerateCSR": true },
"organizationUnits": [ "QA" ], "signatureHash": "SHA-256" }, "comment":
"api test", "digicertOrganizationId": 525858, "digicertProductNameId":
"private_ssl_plus", "intermediateCA": { "certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee" },
"validity": { "validityYears": 1 } }' -H "Authorization: Bearer <jwt
token>"
```

Response:

```
{
    "uuid": "cb95d100-ec30-11ea-920d-eb66140967e3",
    "intermediateCA": {
        "name": "DigiCert Test SHA2 Intermediate CA-1",
        "certhash":
```

```
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
    },
    "approverUserNames": [
        "quays_sd"
    ],
    "requesterUserName": "quays_sd",
    "certificate": {
        "commonName": "p12.test.qualys-demo.com",
        "organizationUnits": [
            "QA"
        ],
        "signatureHash": "SHA-256",
        "encodedCSR": "<csr>",
        "privateKey": "<private key>",
        "dnsNames": null
    },
    "renewal": null,
    "validity": {
        "validityYears": 1,
        "validityDays": null,
        "customExpirationDate": null
    },
    "digicertOrganization": {
        "id": 525858
    },
    "digicertProductNameId": "private_ssl_plus",
    "digicertEVApproverUserIds": null,
    "status": "SUBMITTED",
    "caStatus": "",
    "created": "2020-09-01T08:54:50.473+0000",
    "updated": "2020-09-01T08:54:50.473+0000"
}
```


Update Certificate Request

Use this API to edit an existing enrollment/renewal request

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/orders/{certificate_order_uuid}
Method	PUT
New or Updated APIs	New

Refer to Input Parameters

Sample to Update Certificate Request

API request:

```
curl -X PUT
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/or
ders/cb95d100-ec30-11ea-920d-eb66140967e3" -H "Accept: application/json"
-H "Content-Type: application/json" -d '{ "approverUserNames": [
"quays_sd" ], "certificate": { "commonName": "p12.test.qualys-demo.com",
"csr": { "autoGenerateCSR": true }, "organizationUnits": [ "QA" ],
"signatureHash": "SHA-256" }, "comment": "Updated api test comment",
"digicertOrganizationId": 525858, "digicertProductNameId":
"private_ssl_plus", "intermediateCA": { "certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee" },
"validity": { "validityYears": 1 } }' -H "Authorization: Bearer <jwt
token>"
```

Response:


```
{
    "uuid": "cb95d100-ec30-11ea-920d-eb66140967e3",
    "intermediateCA": {
        "name": "DigiCert Test SHA2 Intermediate CA-1",
        "certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
    },
    "approverUserNames": [
        "quays_sd"
    ],
    "requesterUserName": "quays_sd",
    "certificate": {
        "commonName": "p12.test.qualys-demo.com",
        "organizationUnits": [
            "QA"
        ],
        "signatureHash": "SHA-256",
        "encodedCSR": "<csr>",
        "privateKey": "<private key>",
        "dnsNames": null
    },
    "renewal": null,
    "validity": {
        "validityYears": 1,
        "validityDays": null,
        "customExpirationDate": null
    },
    "digicertOrganization": {
        "id": 525858
    },
    "digicertProductNameId": "private_ssl_plus",
```

```
    "digicertEVApproverUserIds": null,
    "status": "SUBMITTED",
    "caStatus": "",
    "created": "2020-09-01T08:54:50.473+0000",
    "updated": "2020-09-01T08:58:58.138+0000"
}
```


Update Status of Certificate Request

Use this API to approve, reject, or cancel an existing enrollment/renewal request

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/orders/{certificate_order_uuid}/status
Method	PUT
New or Updated APIs	New

Input Parameters

Input parameters for Status update API

status (string)	(Required) Provide one of the following: APPROVED, CANCELLED, REJECTED Make sure: - Only one of approvers, pki or manager can approve, reject or cancel - Once approved request can not rejected or canceled
comment (string)	(Required) Comments about status change.

Sample to Update Status of Certificate Request

API request:

```
curl -X PUT
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/or
ders/cb95d100-ec30-11ea-920d-eb66140967e3/status" -H "Accept:
application/json" -H "Content-Type: application/json" -d '{
"comment": "API request Cancelled",
"status": "CANCELLED"
}' -H "Authorization: Bearer <jwt token>"
```

Response:

```
No Content
Response Code: 204
```

View Certificate Request

Use this API to get details for specified request

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/orders/{certificate_order_uuid}
Method	`GET`
New or Updated APIs	New

Input Parameters

Input parameters for View certificate request API

uuid (string)	(Required) UUID of the certificate
approverUserNames (array)	(Required) Array of valid user names. User roles must be manager, PKI admin or approvers.
requesterUserName (string)	Requester user name
intermediateCA (object)	(Required) Intermediate Certificate Authority information. Make sure: - At least one of the params certhash, commonName or serialNumber is required. - CA is DigiCert's public intermediate CA - CA is configured with CA api key
certhash (string)	(Optional) Secure hash of the certificate
commonName (string)	(Optional) Fully qualified domain name of the Web server that will receive the certificate
serialNumber (string)	(Optional) A short, unique identifier for each certificate generated by the certificate issuer
certificate (object)	(Required)
commonName (string)	(Required) Provide a wildcard character if the product name is of wildcard type.
csr (object)	(Required) Certificate Signing Request Information
autoGenerateCSR (boolean)	(Optional) If this flag is set to True then Qualys will generate csr value and return private key info in the response of the api. If this field is set to True then encoded_csr field can not be set By default the value is set to False.
encodedCSR (string)	(Optional) A valid Encoded Certificate Signing Request
organizationUnits (array)	(Optional) provide value for the OU field for the certificate.
signatureHash (string)	Required) Certificate's signing algorithm hash. Accepted values: SHA-256, SHA-384, SHA-512

renewal (object)	(Optional) Required for certificate renewal request.
digicertPreviousOrderId (integer)	(Required) If the request is a renewal of a previous request then add the previous request id.
renewalOfCertificate (string)	(Required) Provide certhash of the old certificate for which this renewal request is required. Make sure: - certificate is in customer's account - certificate is leaf certificate - certificate is not in IN_RENEWAL status
validity (object)	(Required) Provide any one of the following values: customExpirationDate, validityYears and validityDays params Make sure only one value is provided in a request.
customExpirationDate (date)	(Optional) Expiry date of the certificate.
validityYears (integer)	(Optional) Number of years that the certificate is valid.
validityDays (integer)	(Optional) Number of days that the certificate is valid.
digicertOrganizationId (integer)	(Required) Get organization id using List DigiCert Organizations API
digicertProductNameId (integer)	(Required) Get product name id using List DigiCert Products API
digicertEVApproverUserIds (array)	(Optional) Required when product name is of EV type. Get EV Approvers user id using List Digicert EV Approvers API
status (string)	(Optional) Provide any of the following values: CANCELLED, APPROVED, SUBMITTED, ISSUED
caStatus (string)	(Optional) Status from the Certificate Authority
created (date)	(Optional) Date the request was created
updated (date)	(Optionsl) Date the request was updated

Sample to View Certificate Request

API request:

```
curl -X GET
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/or
ders/cb95d100-ec30-11ea-920d-eb66140967e3" -H "Accept: application/json"
-H "Content-Type: application/json" -H "Authorization: Bearer <jwt token>"
```

Response:

```
{
    "uuid": "cb95d100-ec30-11ea-920d-eb66140967e3",
    "intermediateCA": {
        "name": "DigiCert Test SHA2 Intermediate CA-1",
```

```
        "certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
    },
    "approverUserNames": [
        "quays_sd"
    ],
    "requesterUserName": "quays_sd",
    "certificate": {
        "commonName": "p12.test.qualys-demo.com",
        "organizationUnits": [
            "QA"
        ],
        "signatureHash": "SHA-256",
        "encodedCSR": "<csr>",
        "privateKey": null,
        "dnsNames": null
    },
    "renewal": null,
    "validity": {
        "validityYears": 1,
        "validityDays": null,
        "customExpirationDate": null
    },
    "digicertOrganization": {
        "id": 525858
    },
    "digicertProductNameId": "private_ssl_plus",
    "digicertEVApproverUserIds": null,
    "status": "SUBMITTED",
    "caStatus": "",
    "created": "2020-09-01T08:54:50.473+0000",
    "updated": "2020-09-01T08:58:58.138+0000"
}
```


List DigiCert Organizations

Use this API to list Organizations registered with DigiCert

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/organizations
Method	POST
New or Updated APIs	New

Input Parameters

Input parameters for DigiCert APIs. It is required to provide at least one of the params certhash, commonName or serialNumber.

certhash (string)	(Optional) Secure hash of the certificate
commonName (string)	(Optional) Fully qualified domain name of the Web server that will receive the certificate
serialNumber (string)	(Optional) A short, unique identifier for each certificate generated by the certificate issuer

Sample to List DigiCert Organizations

API request:

```
curl -X POST
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/or
ganizations" -H "Accept: application/json" -H "Content-Type:
application/json" -d '{
"certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
}' -H "Authorization: Bearer <jwt token>"
```

Response:

```
{
    "organizations": [
        {
            "id": 525858,
            "status": "active",
            "name": "Qualys, Inc",
            "assumedName": null,
            "displayName": "Qualys, Inc",
            "active": true
        }
    ]
}
```

List DigiCert Products

Use this API to list DigiCert products for your account

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/products
Method	POST
New or Updated APIs	New

Refer to Input Parameters

Sample to List DigiCert Products

API request:

```
curl -X POST
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/pr
oducts" -H "Accept: application/json" -H "Content-Type: application/json"
-d '{
"certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
}' -H "Authorization: Bearer <jwt token>"
```

Response:

```
{
    "products": [
        {
            "groupName": "securesite_ssl_certificate",
            "nameId": "ssl_ev_securesite",
            "name": "Secure Site EV SSL",
            "type": "ssl_certificate",
            "sslCertificateType": null
        },
        {
            "groupName": "securesite_ssl_certificate",
            "nameId": "ssl_ev_securesite_multi_domain",
            "name": "Secure Site EV Multi-Domain SSL",
            "type": "ssl_certificate",
            "sslCertificateType": null
        }
    ]
}
```

List Digicert EV Approvers

Use this API to list EV approvers registered with DigiCert

APIs affected	certview/rest/public/v1/certificates/enrollment/digicert/evApprovers
Method	POST
New or Updated APIs	New

Refer to Input Parameters

Sample to List DigiCert Products

API request:

```
curl -X POST
"https://gateway.qg1.apps.qualys.com/certview/v1/certificates/digicert/ev
Approvers" -H "Accept: application/json" -H "Content-Type:
application/json" -d '{
"certhash":
"a52d05988b61a33d6ac3edb449eb47150fa5b7a26c7dfc4e61f905ca36e165ee"
}' -H "Authorization: Bearer <jwt token>"
```

Response:

```
{
    "evApprovers": [
        {
            "userId": "1541521",
            "name": "John White",
            "firstName": "John",
            "lastName": "White"
        },
        {
            "userId": "1551253",
            "name": "Kelly Smith",
            "firstName": "Kelly",
            "lastName": "Smith"
        }
    ]
}
```

New Error Codes

We have added new error codes to help you easily troubleshoot if you encounter any error.

Here's a list of Certificate View API error codes along with a description of what each code means. For an API request that had an error, you'll find the error code and text in the XML response.

HTTP Status	Error Code	Error Text	Meaning
400 Bad Request	1903	Missing required parameter(s):...	The API request did not contain one or more parameters which are required.
400 Bad Request	1904	Please specify only one of these parameters:...	The API request contained 2 or more parameters from a group from which at most one may be specified.
400 Bad Request	1905	parameter ... has invalid value ...	The API request contained a valid parameter specified with an invalid value.
400 Bad Request	1907	The following combination of key=value pairs is not supported:...	The API request contained an invalid or unsupported combination of parameters. Invalid value for following param. autoGenerateCSR: true and encodedCSR is not null.
400 Bad Request	140001	Malformed json	The json request is not properly formed.
400 (Bad Request)	140002	Field is not editable	The requested field can not be edited.
400 (Bad Request)	140004	Enrollment is not supported for CA	Enrollment/renewal of certificates by the specified CA is currently not supported.
400 (Bad Request)	140005	API key is not configured	Incorrect API details, please verify the API key in the Configuration tab.
400 (Bad Request)	140006	Invalid renewal certificate	Renewal failed due to one of the following reasons: - certificate not found in inventory - certificate is not a leaf certificate - certificate is already in the process of being renewed - certificate is not going to expire in next 60 days
400 (Bad Request)	140007	Certificate order type is not editable	Cannot change an enrollment request to renewal request or vice versa

HTTP Status	Error Code	Error Text	Meaning
403(Forbidden)	2012	User license is not authorized to run this API.	The API request failed because the user's subscription does not have API access enabled.
403(Forbidden)	148100	User does not have required permissions	The API request failed because the user does not have the required permissions. Check user permissions in Admin module
403(Forbidden)	148101	User has exhausted the allocated number of licenses	The API request failed because the order exceeds the allocated license count. Contact your Technical Account Manager for additional licenses
404(Not Found)	148200	Invalid certificate order	Verify the order id
409 Conflict	1920	API resource is not editable	Certificate request can not be updated once it is in the POSTED status.
400 Bad Request	1922	Please specify at least one of the following parameters:...	The API request was missing some required information (but not necessarily a single specific parameter).