Qualys Container Security

API Release Notes

Version 1.24

April 17, 2023

Qualys Cloud Suite API gives you many ways to integrate your programs and API calls with Qualys capabilities. 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

Scheduling Vulnerability Reports

JFrog Private Registry: Authenticating with Access Tokens

Fetch a Vulnerability Report in JSON Format

End of Life (EOL) for v1.1 and v1.2 Container Security APIs

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

Scheduling Vulnerability Reports

With this release, you can create schedules to generate image and container vulnerability reports at regular intervals. Generating reports regularly helps you monitor vulnerabilities in your container environment in real time and ensure they are being remediated in a timely manner.

We have introduced the following new APIs to create and manage report schedules:

Create a Report Schedule

Pause or Resume a Report Schedule

Delete a Schedule

List Report Schedules

Create a Report Schedule

API affected	/csapi/v1.3/reports/schedule
Operator	POST
New or Updated APIs	New
DTD or XSD Changes	NA

Creates a new schedule to automatically generate a report on a regular basis.

Input Parameters

Field Name	Mandatory?	Data Type	Description
description	Optional	string	Specify a description for your report (maximum up to 250 characters).
name	Mandatory	string	Specify a title for your report (maximum up to 150 characters).
filter	Optional	string	Specify the columns to include in the report. Multiple columns should be comma-separated. For example, ["repo, "uuid", "qid"}
displayColumns	Mandatory	string	Specify the columns to include in the report. Multiple columns should be comma-separated. When unspecified, ALL report columns will be included. When an empty value is provided, only default columns will be included.
templateName	Mandatory	string	Specify the template for the report. The valid values are: - CS_IMAGE_VULNERABILITY - CS_CONTAINER_VULNERABILITY
eventEndTime	Mandatory	string	Specify the end date and time for the schedule. **Note**: Time must be in UTC.
action	Mandatory	string	Specify the action to perform on the schedule. Currently, the valid value is CREATE.

emailNotification	Mandatory	integer	Specify whether to send an email notification or not. The valid values are 0 or 1.
eventTime	Mandatory	string	Specify the start date and time for the schedule. For example, 2023-02-16T19:30:00Z. **Note**: Time must be in UTC.
reportScheduleDetails	Mandatory	-	Specify the below parameters to define a schedule. Specify null if you do not want to create a recurrent report schedule. In that case, the report is triggered for only once (on the time specified in eventTime).
recurrenceType	Mandatory	string	Specify the recurrence frequency as DAILY or WEEKLY or MONTHLY.
selectedDayOfWeeks	Mandatory	string	Specify a day on which the report is triggered every week. This parameter is valid only if the recurrenceType is WEEKLY. The valid values are the names of days. Specify null if this parameter is not applicable.
monthlyType	Mandatory	string	Specify DAY_OF_WEEK to select the day from a particular week of a month or DAY_OF_MONTH to select a day from a month. This parameter is valid only when the recurrenceType is MONTHLY. Specify null if this parameter is not applicable.

ordinalDayOfMonth	Mandatory	integer	Specify a day of the month. This parameter is valid only when the monthlyType is DAY_OF_MONTH. The valid values are from 1 to 31. Specify null if this parameter is not applicable.
dayOfWeek	Mandatory	string	Specify a day of the week. For example, MONDAY. This parameter is valid only when the monthlyType is DAY_OF_WEEK. The valid values are the names of days. Specify null if this parameter is not applicable.
ordinalDayOfWeek	Mandatory	integer	Specify the number of week in a month. This parameter is valid only when the monthlyType is DAY_OF_WEEK. The valid values are 1, 2, 3, or 4. Specify null if this parameter is not applicable.

Sample 1: Create a Daily Report Schedule

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports/schedule
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Request Body:

```
{
  "name": "CRS-TEST-15",
  "description": "",
  "templateName": "CS_IMAGE_VULNERABILITY",
  "format": "csv",
```

```
  "reportScheduleDetails": {
    "recurrenceType": "DAILY",
    "selectedDayOfWeeks": null,
    "monthlyType": null,
    "ordinalDayOfMonth": null,
    "dayOfWeek": null,
    "ordinalDayOfWeek": null
  },
  "displayColumns": [
    "imageId",
    "qid"
  ],
  "eventEndTime": "2023-03-25T22:30:00Z",
  "action": "CREATE",
  "emailNotification": 1,
  "eventTime": "2023-02-16T19:30:00Z"
}
```

Response:

```
{
  "reportUuid": "620a2490-c3cc-11ed-bf38-5563a478dc98"
}
```

Sample 2: Create a Weekly Report Schedule

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports/schedule
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Request Body:

```
{
  "name": "CRS-TEST-15",
  "description": "",
  "templateName": "CS_IMAGE_VULNERABILITY",
  "format": "csv",
  "reportScheduleDetails": {
    "recurrenceType": "WEEKLY",
    "selectedDayOfWeeks": "MONDAY",
    "monthlyType": null,
    "ordinalDayOfMonth": null,
    "dayOfWeek": null,
    "ordinalDayOfWeek": null
```

```
  },
  "displayColumns": [
    "imageId",
    "qid"
  ],
  "eventEndTime": "2023-03-25T22:30:00Z",
  "action": "CREATE",
  "emailNotification": 1,
  "eventTime": "2023-02-16T19:30:00Z"
}
```

Response:

```
{
  "reportUuid": "620a2490-c3cc-11ed-bf38-5563a478dc98"
}
```

Sample 3: Create a Monthly Schedule by Specifying a Day of a Month

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports/schedule
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Request Body:

```
{
  "name": "CRS-TEST-15",
  "description": "",
  "templateName": "CS_IMAGE_VULNERABILITY",
  "format": "csv",
  "reportScheduleDetails": {
    "recurrenceType": "MONTHLY",
    "selectedDayOfWeeks": null,
    "monthlyType": "DAY_OF_MONTH",
    "ordinalDayOfMonth": 11,
    "dayOfWeek": null,
    "ordinalDayOfWeek": null
  },
  "displayColumns": [
    "imageId",
    "qid"
  ],
  "eventEndTime": "2023-03-25T22:30:00Z",
  "action": "CREATE",
```

```
  "emailNotification": 1,
  "eventTime": "2023-02-16T19:30:00Z"
}
```

Response:

```
{
  "reportUuid": "620a2490-c3cc-11ed-bf38-5563a478dc98"
}
```

Sample 4: Create a Monthly Schedule by Specifying a Day of a Week

API Request:

```
curl -X POST
"<qualys_base_url>/csapi/v1.3/reports/schedule
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Request Body:

```
{
  "name": "CRS-TEST-15",
  "description": "",
  "templateName": "CS_IMAGE_VULNERABILITY",
  "format": "csv",
  "reportScheduleDetails": {
    "recurrenceType": "MONTHLY",
    "selectedDayOfWeeks": null,
    "monthlyType": "DAY_OF_WEEK",
    "ordinalDayOfMonth": null,
    "dayOfWeek": "SUNDAY",
    "ordinalDayOfWeek": 4
  },
  "displayColumns": [
    "imageId",
    "qid"
  ],
  "eventEndTime": "2023-03-25T22:30:00Z",
  "action": "CREATE",
  "emailNotification": 1,
  "eventTime": "2023-02-16T19:30:00Z"
}
```

Response:

```
{
  "reportUuid": "620a2490-c3cc-11ed-bf38-5563a478dc98"
}
```

Pause or Resume a Report Schedule

API affected	csapi/v1.3/reports/RESUME/schedule/ csapi/v1.3/reports/PAUSE/schedule/
Operator	PUT
New or Updated APIs	New
DTD or XSD Changes	NA

Lets you pause or resume a report schedule.

Input Parameters

Field Name	Mandatory?	Data Type	Description
action	Mandatory	string	Specify the action: PAUSE or RESUME.
reportingScheduleId	Mandatory	string	Specify the UUID of the schedule you want to pause or resume.

Sample 1: Resume a Report Schedule

API Request:

```
curl -X PUT
"<qualys_base_url>csapi/v1.3/reports/RESUME/schedule/620a2490-c3cc-11ed-
bf38-5563a478dc98
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:

```
{
  "data": true,
  "message": "Report schedule state is set to RESUME successfully"
}
```

Sample 2: Pause a Report Schedule

API Request:

```
curl -X PUT
"<qualys_base_url>/csapi/v1.3/reports/PAUSE/schedule/620a2490-c3cc-11ed-
bf38-5563a478dc98
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:


```
{
  "data": true,
  "message": "Report schedule state is set to RESUME successfully"
}
```

Delete a Report Schedule

API affected	csapi/v1.3/reports/schedule/
Operator	DELETE
New or Updated APIs	New
DTD or XSD Changes	NA

Deletes a report schedule.

Input Parameters

Field Name	Mandatory?	Data Type	Description
reportingScheduleId	Mandatory	string	Specify the UUID of the report schedule.

Sample: Delete a Report Schedule

API Request:

```
curl -X DELETE
"<qualys_base_url>/csapi/v1.3/reports/schedule/620a2490-c3cc-11ed-bf38-
5563a478dc98
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:

```
{
  "data": true,
  "message": "Report schedule state is set to DELETE successfully"
}
```

List Report Schedules

API affected	csapi/v1.3/reports/schedules
Operator	GET
New or Updated APIs	New
DTD or XSD Changes	NA

Retrieves a list of report schedules with their corresponding details from your account. You can also use this API to fetch details of a specific schedule by specifying its UUID.

Input Parameters

Paramter	Mandatory?	Data Type	Description
pageNumber	Optional	integer	Specify the page to be returned.
reportScheduleUuid	Optional	string	If you want to fetch details of a particular schedule, specify the UUID of the schedule.
pageSize	Optional	integer	Specify the number of records to display per page.
sort	Optional	string	Specify how to sort the records in the response. The supported values are: createdDate and name.

Sample 1: List All Report Schedules from Your Account

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports/schedules?pageNumber=1&pageSize=50&
sort=createdDate%20%3Adesc"
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:

```
{
    "data": [
        {
            "name": "CRS-TEST-3",
            "reportScheduleUuid": "bc9cf320-c317-11ed-8d67-39e6329594da",
            "scheduledDatetime": "2023-03-15T09:57:27.000Z",
            "templateName": "CS_IMAGE_VULNERABILITY",
            "resourceId": "bf21812e-92f7-4bcc-be4a-3d2f02642c9c",
```

```
            "action": "CREATE",
            "eventTime": "2023-03-15T09:58:00Z",
            "eventEndTime": "2023-03-22T16:25:00Z",
            "cronExpression": "0 58 9 1/1 * ? *",
            "description": "",
            "createdDateTime": "2023-03-15T09:57:27.000Z",
            "nextFireTime": "2023-03-16T09:58:00.000Z",
            "state": "RESUME",
            "format": "csv",
            "moduleCode": "CS"
        },
        {
            "name": "CRS-TIME-TEST-2",
            "reportScheduleUuid": "b44ebfb0-c316-11ed-8d67-39e6329594da",
            "scheduledDatetime": "2023-03-15T09:50:03.000Z",
            "templateName": "CS_IMAGE_VULNERABILITY",
            "resourceId": "1ffa0872-b92d-40ca-8ab8-593e52ecbd46",
            "action": "CREATE",
            "eventTime": "2023-03-15T09:51:00Z",
            "eventEndTime": "2023-03-16T16:16:00Z",
            "cronExpression": "0 51 9 1/1 * ? *",
            "description": "",
            "createdDateTime": "2023-03-15T09:50:03.000Z",
            "nextFireTime": "2023-03-16T09:51:00.000Z",
            "state": "RESUME",
            "format": "csv",
            "moduleCode": "CS"
        },
        {
            "name": "CRS-TIME-TEST",
            "reportScheduleUuid": "4adc45c0-c316-11ed-8d67-39e6329594da",
            "scheduledDatetime": "2023-03-15T09:47:06.000Z",
            "templateName": "CS_IMAGE_VULNERABILITY",
            "resourceId": "efc13ea6-81ad-4cd5-a1d2-e8031f0401c6",
            "action": "CREATE",
            "eventTime": "2023-03-15T15:16:00Z",
            "eventEndTime": "2023-03-16T16:16:00Z",
            "cronExpression": "0 16 15 1/1 * ? *",
            "description": "",
            "createdDateTime": "2023-03-15T09:47:06.000Z",
            "nextFireTime": "2023-03-16T15:16:00.000Z",
            "state": "RESUME",
            "format": "csv",
            "moduleCode": "CS"
        },
...
    ],
    "count": 150,
    "groups": null
```

```
}
```

Sample 2: Fetch Details of a Specific Report Schedule

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports/schedules?pageNumber=1&reportSchedu
leUuid=e82571d0-c2e9-11ed-bf38-
5563a478dc98&pageSize=50&sort=createdDate%20%3Adesc"
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:


```
{
  "data": [
    {
      "name": "CRS-DEMO-DAILY",
      "reportScheduleUuid": "e82571d0-c2e9-11ed-bf38-5563a478dc98",
      "scheduledDatetime": "2023-03-15T04:29:22.000Z",
      "templateName": "CS_IMAGE_VULNERABILITY",
      "resourceId": "487a42bf-fa52-4dab-ac06-aa85598a4873",
      "action": "CREATE",
      "eventTime": "2023-03-14T07:23:54.000Z",
      "eventEndTime": "2023-03-15T07:23:54.000Z",
      "cronExpression": "0 23 7 1/1 * ? *",
      "description": "",
      "createdDateTime": "2023-03-15T04:29:22.000Z",
      "nextFireTime": null,
      "state": "COMPLETED",
      "format": "csv",
      "moduleCode": "CS"
    }
  ],
  "count": 1,
  "groups": null
}
```

JFrog Private Registry: Authenticating with Access Tokens

API affected	csapi/v1.3/registry
Operator	POST, PUT
New or Updated APIs	Updated
DTD or XSD Changes	NA

The registry sensor can now connect with the JFrog Artifactory Private Registry using access tokens. You can generate an access token on the JFrog platform and use it for authenticating the sensor.

It is recommended to use a non-expiring token to avoid the need for repeated authentication. This allows you to maintain a continuous connection without having to repeatedly re-authenticate. If your token has expired, the authentication would fail with an error message.

We have added the following new input parameter to specify the access token.

Input Parameter

Field Name	Mandatory?	Data Type	Description
accessToken	Optional	string	Specify the access token. You need to generate the access token on the JFrog platform.

Sample: Create a JFrog Registry with Access Token Authentication

API Request:

```
curl -X 'POST' \
  '<qualys_base_url>/csapi/v1.3/registry' \
  -H 'accept: application/json' \
  -H 'Authorization: Bearer <token> \
  -H 'Content-Type: application/json' \
  -d '{
   "credential":{
      "username":"<user name>",
      "accessToken":"<access token>"
   },
   "credentialType":"Token",
   "registryType":"ARTIFACTORY_PRIVATE",
   "registryUri":"https://test.jfrog.io",
   "registryName":"JFROG_Test"
} '
```

Response:


```
{
    "registryUuid": "b36965d6-c111-4964-a0ef-6d817454c3c1"
}
Response Code: 200
```

Fetch a Vulnerability Report in JSON Format

API affected	/csapi/v1.3/reports/jsonReport
Operator	GET
New or Updated APIs	New

We have introduced a new API to fetch vulnerability reports in JSON format. This allows you to use the report data seamlessly in further processes such as automation and integrations.

Note: If you want to maintain audit logs for JSON reporting, you need to record the requests and responses at your end.

Input Parameters

Field Name	Mandatory	Data Type	Description
templateName	Yes	string	Specify whether to generate a vulnerability report for images or containers. The valid values are: CS_IMAGE_VULNERABILITY or CS_CONTAINER_VULNERABILITY.
filter	No	string	Provide a QQL query to limit the report to only certain images or containers. Only the images or containers that match your query are included in the report.
paginationQuery	No	string	Provide a query to filter the next page. You can find the pagination query for the next page in the "nexturl" response header.

Sample

Fetch a vulnerability report for all containers in your account.

API Request:

```
curl -X GET
"<qualys_base_url>/csapi/v1.3/reports/jsonReport?templateName=CS_IMAGE_VU
LNERABILITY%20OR%20CS_CONTAINER_VULNERABILITY"
-H "accept: application/*"
-H "Authorization: Bearer <token>"
```

Response:


```
{
    "data": [
        {
            "uuid": "000061b2-b8be-37ed-9196-dc8bbf372fe1",
            "sha":
"a39b0473439ca693b7f36941ac25ce8a27a74538a29bad17c6638f2f521d6e86",
            "containerId": "a39b0473439c",
            "name": "k8s_calico-kube-controllers_calico-kube-controllers-
7dddfdd6c9-qltv4_calico-system_9793b2c9-58f0-4acc-8ded-8a52b3283d43_111",
            "imageId": "c95ddb97ba59",
            "created": "2022-11-24 06:25:10 +0000 UTC",
            "hostName": "ip-10-82-8-106",
            "hostIp": "10.82.8.106",
            "state": "STOPPED",
            "stateChanged": "2022-11-28 06:41:00 +0000 UTC",
            "lastScanned": "",
            "updated": "2022-11-28 06:41:01 +0000 UTC",
            "hostArchitecture": ["x86_64"
                                ],
            "podName": "",
            "podUuid": "",
            "podNameSpace": "",
            "podLabel": "",
            "podController": "",
            "nodeName": "",
            "nodeIsMaster": "",
            "repository": "",
            "qid": null,
            "title": null,
            "severity": null,
            "category": null,
            "cveids": null,
            "vendorReference": null,
            "cvssBase": null,
            "cvssTemporal": null,
            "cvss3Base": null,
            "cvss3Temporal": null,
            "threat": null,
            "impact": null,
            "solution": null,
            "exploitability": null,
            "associatedMalwares": null,
            "software": null,
            "result": null
        },
        {
            "uuid": "01c85531-614e-3661-afe9-4854159310e6",
```

```
            "sha":
"9adb5c83e17cce411ee6ff2a16e8860436f227048bce1ae3586384e5c13f7f83",
            "containerId": "9adb5c83e17c",
            "name": "k8s_calico-typha_calico-typha-5879f89c49-
lqst4_calico-system_fece47ba-4d8d-457a-aa55-dfcfb892fd1a_24",
            "imageId": "9507cf15077f",
            "created": "2022-11-29 04:59:48 +0000 UTC",
            "hostName": "ip-10-82-10-7",
            "hostIp": "10.82.10.7",
            "state": "STOPPED",
            "stateChanged": "2022-12-12 05:30:08 +0000 UTC",
            "lastScanned": "",
            "updated": "2022-12-12 05:30:14 +0000 UTC",
            "hostArchitecture": [
                "x86_64"
            ],
            "podName": "calico-typha-5879f89c49-lqst4",
            "podUuid": "fece47ba-4d8d-457a-aa55-dfcfb892fd1a",
            "podNameSpace": "calico-system",
           "podLabel": " key:k8s-app value:calico-typha, key:pod-template-
hash value:5879f89c49",
            "podController": " uuid:15ad4899-c983-420a-87a4-cb221ada80ef
name:calico-typha type:Deployment, uuid:89f97929-dfc7-4b74-8678-
aec16e46bebd name:calico-typha-5879f89c49 type:ReplicaSet",
            "nodeName": "ip-10-82-10-7",
            "nodeIsMaster": "true",
            "repository": "",
            "qid": null,
            "title": null,
            "severity": null,
            "category": null,
            "cveids": null,
            "vendorReference": null,
            "cvssBase": null,
            "cvssTemporal": null,
            "cvss3Base": null,
            "cvss3Temporal": null,
            "threat": null,
            "impact": null,
            "solution": null,
            "exploitability": null,
            "associatedMalwares": null,
            "software": null,
            "result": null
        }
    ],
    "resourceType": "Container Vulnerability",
    "count": 2000
}
```

End of Life (EOL) for v1.1 and v1.2 Container Security APIs

The End of Life (EOL) for Container Security API versions 1.1 and 1.2 takes effect starting from Container Security release 1.23. That means all API endpoints containing v1.1 or v1.2 in the API path for containers, images, registries, and sensors will no longer be supported.

It is recommended to use the equivalent v1.3 APIs to perform all of your Container Security operations.

This change was communicated in advance through a notification dated December 07, 2022. For more information, see Qualys Cloud Platform API Deprecation Notice.