Qualys Container Security v1.x

API Release Notes

Version 1.11

August 6, 2021

Qualys Container Security API gives you many ways to integrate your programs and API calls with Qualys capabilities.

What's New

CRS API v1.3 Now Available

Qualys API URL

Container Security supports both API server URLs and API gateway URLs for API requests.

The Qualys API server or gateway 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 URL for Qualys US Platform 2 (https://gateway.qg2.apps.qualys.com) in sample API requests. If you're on another platform, please replace this URL with the appropriate server URL for your account.

Copyright 2021 by Qualys, Inc. All Rights Reserved.

CRS API v1.3 Now Available

Container Runtime Security (CRS) API version 1.3 (/csapi/v1.3/runtime/) is now available. CRS API version 1.2 (/csapi/v1.2/runtime/) will also continue to be supported at this time. We urge customers to start using the v1.3 API. There are many improvements in the new version as you'll see listed below, and the v1.2 API will be deprecated in a future release.

API Changes

You'll see several improvements when using the v1.3 API, including:

Validation Added

We've added validations to the POST and PUT API calls. Now you'll get a JSON 400 error in the API response if a required field is missing or an invalid value is provided. Note that some fields require values to be entered in ALL CAPS and the values are case sensitive. See the field descriptions in the table below for allowed values.

Sample error when invalid parameters are passed during an API request:

```
{
  "Code": 10400,
  "Message": "Bad request",
  "MessageInfo": "For API definition see: ",
  "Status": 400,
  "Error": "Invalid json"
}
```

Use of Camel Case

Field names that appear in the API response across all CRS APIs will now start with a lowercase letter (e.g. policyId and logMode) whereas previously the field names started with an uppercase letter (e.g. PolicyId and LogMode). This is to follow established http standards and provide consistency across APIs. You'll need to adhere to the new formatting when passing values for POST and PUT API requests.

Renamed Fields for Clarity

Some field names were renamed for better clarity like "Default" in the Configuration API is now "isDefaultConfig" and "Mode" in the Policy API is now "policyMode". Also, the fields "DateCreated" and "DateUpdated" were shortened to "created" and "updated", respectively.

Removed Unsupported Fields and API

We removed certain fields that are no longer supported. Sniffing was removed from Configuration APIs, and SyscallGroup was removed from Policy APIs.

Also, the API endpoint to get containers running a policy (/csapi/v1.2/runtime/policies/{policyId}/containers) is not supported in v1.3.

Replaced Integer Values with Friendly String Values

Certain fields that took an integer value in v1.2 will now take a string value in v1.3 to match the value that appears in the UI and to be more user friendly. For example, "logMode" now accepts a string value (e.g. POLICY_MONITOR and POLICY_DENY) and "policyMode" now accepts a string value (e.g. ACTIVE and INACTIVE). See the field descriptions in the table below for all possible values. Note that values are case sensitive.

Configure a List of Ignored System Calls

When creating or updating a policy, you can now define a list of system calls to ignore for the policy by using the ignoredSyscalls input. No events will be created for an ignored system call even if it matches a policy rule. This is also now supported in the UI.

Field Name and Value Changes

See the table below for old and new field names and requirements for each field.

Field Name v1.2	Field Name v1.3	Description
General		
DateCreated	created	Timestamp for when the object was created, in the format: ['YYYY'-'MM'-'DD'T'hh':'mm':'ss'.'sss'Z]
DateUpdated	updated	Timestamp for when the object was last updated, in the format: ['YYYY'-'MM'-'DD'T'hh':'mm':'ss'.'sss'Z]
Configuration APIs		
ID	id	The configuration ID generated by the service.
PolicyID	policyId	(Required) The ID of the security policy for this container. A valid policy ID must be provided, and the specified policy must be present for the user. Sample value: 59c2dc5dc07f870001548489
LogMode	logMode	(Required) Specify a string value to indicate which policy hits (rule matches) get logged. Possible values: NONE, POLICY_MONITOR, POLICY_DENY, POLICY_MONITOR_DENY, POLICY_ALLOW, POLICY_ALL, BEHAVIOR, ALL. Values are case sensitive.
Default	isDefaultConfig	(Required) Set to false by default. Specify true to make this the default configuration for group.
Name	name	Specify a name for the configuration. Enter a maximum of 256 characters.

Field Name v1.2	Field Name v1.3	Description
Policy APIs		
ID	id	The policy ID generated by the service.
Name	name	(Required) The policy name. Enter a maximum of 256 characters.
DefaultNetworkAction	defaultNetworkAction	(Required) The default action when ruleType is NETWORK_OUTBOUND or NETWORK_INBOUND. Possible values: ALLOW or DENY. Values are case sensitive.
DefaultExecuteAction	defaultExecuteAction	(Required) The default action when ruleType is SYSCALL. Possible values: ALLOW or DENY. Values are case sensitive.
DefaultFileAction	defaultFileAction	(Required) The default action when ruleType is READ or WRITE. Possible values: ALLOW or DENY. Values are case sensitive.
IgnoredSyscalls	ignoredSyscalls	Only valid system call names are allowed. Enter a list of values like this: ["sys_read", "sys_write"]
Mode	policyMode	(Required) Specify a string value to indicate the policy mode. Possible values: ACTIVE, INACTIVE, PERMISSIVE. Values are case sensitive.
Description	description	A description for the policy. Enter a maximum of 256 characters.
Policy Rule Parameters		
ID	id	The rule ID generated by the service.
Name	name	(Required) The rule name. Enter a maximum of 256 characters.
InActive	inactive	Specify whether the rule is inactive. Specify false (the default) if the rule is active. Specify true if the rule is not active.
RuleType	ruleType	(Required) Specify the type of rule. Possible values: READ, WRITE, NETWORK_OUTBOUND, NETWORK_INBOUND, SYSCALL. Values are case sensitive.
Program	program	Specify the path to the program that this rule applies to. Wildcards are allowed. The default value is "*".

Field Name v1.2	Field Name v1.3	Description
Action	action	(Required) Specify the action that should be taken if this rule is matched. Possible values: ALLOW, DENY, MONITOR. Values are case sensitive.
Port	port	(Optional when ruleType is NETWORK_OUTBOUND or NETWORK_INBOUND) Specify the network protocol that this rule applies to.
IpAddress	ipAddress	(Required when ruleType is NETWORK_OUTBOUND or NETWORK_INBOUND) Specify the IP address this rule applies to.
File	file	(Required when ruleType is READ or WRITE) Specify the path to the file that the rule applies to.
Syscall	syscall	(Required when ruleType is SYSCALL) The system call provided must be a valid system call name.
Arg1	arg1	(Required when ruleType is SYSCALL) Variable argument. Usage differs depending on rule type. Used only in syscall rules.
Arg2	arg2	Variable argument. Usage differs depending on rule type. Used only in syscall rules.
Arg3	arg3	Variable argument. Usage differs depending on rule type. Used only in syscall rules.

API Samples

See a few samples below using the updated field names and values. Refer to the Container Runtime Security API Guide for samples for all CRS APIs.

Sample create a configuration

/csapi/v1.3/runtime/configs

[POST]

API request:

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/csapi/v1.3/runtime/configs' \
--header 'Authorization: Bearer <token>'
--header 'Content-Type: text/plain' \
--data-raw '{
```

```
  "name": "example configuration",
  "policyId": "59c2dc5dc07f870001548489",
  "logMode": "POLICY_MONITOR",
  "isDefaultConfig": false
}'
```

Response:

```
{
    "id": "5ede0cfff42b100001905d58",
    "created": "2020-06-08T10:03:43.507Z",
    "updated": "2020-06-08T10:03:43.507Z",
    "policyId": "59c2dc5dc07f870001548489",
    "logMode": "POLICY_MONITOR",
    "isDefaultConfig": false,
    "name": "example configuration"
}
```

Sample update a configuration

/csapi/v1.3/runtime/configs/{configId}

[PUT]

API request:

```
curl --location --request PUT
'https://gateway.qg1.apps.qualys.com/csapi/v1.3/runtime/configs/5ede0cfff
42b100001905d58' \
--header 'Authorization: Bearer <token>'\
--header 'Content-Type: text/plain' \
--data-raw '{
  "name": "example configuration",
  "policyId": "59c2dc5dc07f870001548489",
  "logMode": "POLICY_MONITOR",
  "isDefaultConfig": false,
}'
```

Response:

```
{
    "id": "5ede0cfff42b100001905d58",
    "created": "2020-06-08T10:03:43.507Z",
    "updated": "2020-06-08T10:07:44.249Z",
    "policyId": "5e18c86e4e08ce0001368940",
    "logMode": "POLICY_MONITOR",
    "isDefaultConfig": false,
    "name": "example configuration"
}
```

Sample create a new security policy

/csapi/v1.3/runtime/policies

[POST]

API request:

```
curl --location --request POST
'https://gateway.qg1.apps.qualys.com/csapi/v1.3/runtime/policies' \
--header 'Authorization: Bearer <token>'
--header 'Content-Type: text/plain' \
--data-raw '{
    "name": "Prevent Shadow Access To User",
    "created": "2021-06-10T08:14:22.509Z",
    "updated": "2021-06-10T08:14:22.509Z",
    "defaultNetworkAction": "ALLOW",
    "defaultExecuteAction": "ALLOW",
    "defaultFileAction": "ALLOW",
    "rules": [
        {
            "id": "5faa4bdeeda7de00015142c0",
            "name": "Deny access in cat /etc/shadow",
            "created": "2021-06-10T08:14:22.509Z",
            "updated": "2021-06-10T08:14:22.509Z",
            "inactive": false,
            "ruleType": "SYSCALL",
            "program": "*/cat",
            "action": "DENY",
            "file": "/etc/shadow",
            "port": 0,
            "ipAddress": "",
            "syscall": "sys_open",
            "arg1": "/etc/shadow",
            "arg2": "",
            "arg3": ""
        }
    ],
    "ignoredSyscalls": [],
    "policyMode": "ACTIVE",
    "description": "Example policy denies access to /etc/shadow from
program cat"
}'
```

Response:

```
Response Code 200 :
Response Message :

{
```

```
    "id": "5fb5e21f5caea20001fd27ce",
    "name": "Prevent Shadow Access To User",
    "created": "2021-06-19T03:10:23.36Z",
    "updated": "2021-06-19T03:10:23.36Z",
    "defaultNetworkAction": "ALLOW",
    "defaultExecuteAction": "ALLOW",
    "defaultFileAction": "ALLOW",
    "rules": [
        {
            "id": "5faa4bdeeda7de00015142c0",
            "name": "Deny access in cat /etc/shadow",
            "created": "2021-06-19T03:10:23.36Z",
            "updated": "2021-06-19T03:10:23.36Z",
            "inactive": false,
            "ruleType": "SYSCALL",
            "program": "*/cat",
            "action": "DENY",
            "file": "/etc/shadow",
            "port": 0,
            "ipAddress": "",
            "syscall": "sys_open",
            "arg1": "/etc/shadow",
            "arg2": "",
            "arg3": ""
        }
    ],
    "ignoredSyscalls": [],
    "policyMode": "ACTIVE",
    "description": "Example policy denies access to /etc/shadow from
program cat"
}
```


Sample update a security policy

/csapi/v1.3/runtime/policies/{policyId}

[PUT]

API request:

```
curl --location --request PUT
'https://gateway.qg1.apps.qualys.com/csapi/v1.3/runtime/policies/5fb5e21f
5caea20001fd27ce' \
--header 'Authorization: Bearer <token>'
--header 'Content-Type: text/plain' \
--data-raw '{
    "name": "Updated Policy Prevent Shadow Access To User",
    "created": "2021-06-10T08:14:22.509Z",
    "updated": "2021-06-10T08:14:22.509Z",
```

```
    "defaultNetworkAction": "ALLOW",
    "defaultExecuteAction": "ALLOW",
    "defaultFileAction": "ALLOW",
    "rules": [
        {
            "id": "5faa4bdeeda7de00015142c0",
            "name": "Deny access in cat /etc/shadow",
            "created": "2021-06-10T08:14:22.509Z",
            "updated": "2021-06-10T08:14:22.509Z",
            "inactive": false,
            "ruleType": "SYSCALL",
            "program": "*/cat",
            "action": "DENY",
            "file": "/etc/shadow",
            "port": 0,
            "ipAddress": "",
            "syscall": "sys_open",
            "arg1": "/etc/shadow",
            "arg2": "",
            "arg3": ""
        }
    ],
    "ignoredSyscalls": [],
    "policyMode": "ACTIVE",
    "description": "Example policy denies access to /etc/shadow from
program cat"
}'
```

Response:

```
{
    "id": "5fb5e21f5caea20001fd27ce",
    "name": "Updated Policy Prevent Shadow Access To User",
    "created": "2021-06-19T03:10:23.36Z",
    "updated": "2021-06-19T03:13:03.083Z",
    "defaultNetworkAction": "ALLOW",
    "defaultExecuteAction": "ALLOW",
    "defaultFileAction": "ALLOW",
    "rules": [
        {
            "id": "5faa4bdeeda7de00015142c0",
            "name": "Deny access in cat /etc/shadow",
            "created": "2021-06-19T03:10:23.36Z",
            "updated": "2021-06-19T03:13:03.083Z",
            "inactive": false,
            "ruleType": "SYSCALL",
            "program": "*/cat",
            "action": "DENY",
            "file": "/etc/shadow",
```

```
            "port": 0,
            "ipAddress": "",
            "syscall": "sys_open",
            "arg1": "/etc/shadow",
            "arg2": "",
            "arg3": ""
        }
    ],
    "ignoredSyscalls": [],
    "policyMode": "ACTIVE",
    "description": "Example policy denies access to /etc/shadow from
program cat"
}
```