Qualys Container Security

Release Notes

Version 1.6.8
August 13, 2020

Here’s what’s new in Container Security 1.6.8!

Introducing Reporting Feature

We are introducing a reporting feature in Container Security. With this release, you can create customizable QQL query driven on-demand report jobs. Reports are driven by reporting templates. Currently we support vulnerability report templates (csv format only - for Images, Containers). Reporting workflows can be performed from the new "Reports" tab in the Container Security UI.

Vulnerability Report Templates

- Image Vulnerability Report
- Container Vulnerability Report

Image Vulnerability Report

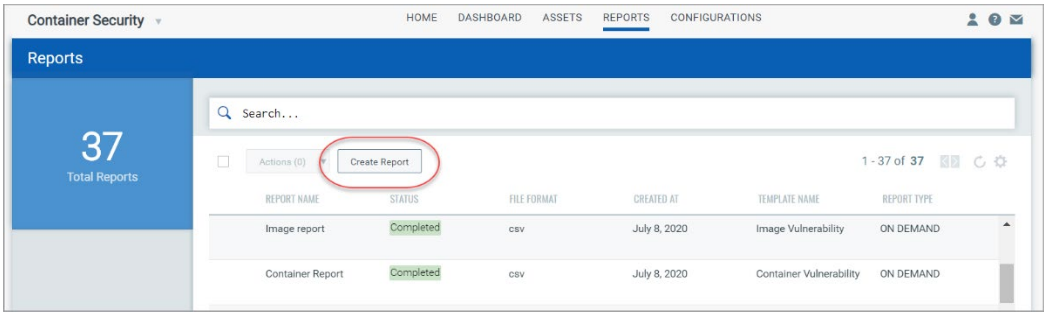
For each row in the report, you'll see image details (e.g. Repository, Image ID, SHA, etc) followed by vulnerability details (e.g. QID, Title, Severity, etc) for a single detected vulnerability. If the image has multiple vulnerabilities it will be listed multiple times (e.g. 10 rows for 10 vulnerabilities on the same image).

Container Vulnerability Report

For each row in the report, you'll see container details (e.g. Container Name, Container ID, Host Name, etc) followed by vulnerability details (e.g. QID, Title, Severity, etc) for a single detected vulnerability. If the container has multiple vulnerabilities it will be listed multiple times (e.g. 10 rows for 10 vulnerabilities on the same container).

How to Create Reports

Go to the Reports section (on the top menu) and click the "Create Report" button.



REPORT NAME	STATUS	FILE FORMAT	CREATED AT	TEMPLATE NAME	REPORT TYPE
Image report	Completed	csv	July 8, 2020	Image Vulnerability	ON DEMAND
Container Report	Completed	csv	July 8, 2020	Container Vulnerability	ON DEMAND

Follow the wizard to give your report a name and description. Then pick a report template for the type of report you want to create: Image Vulnerability or Container Vulnerability.

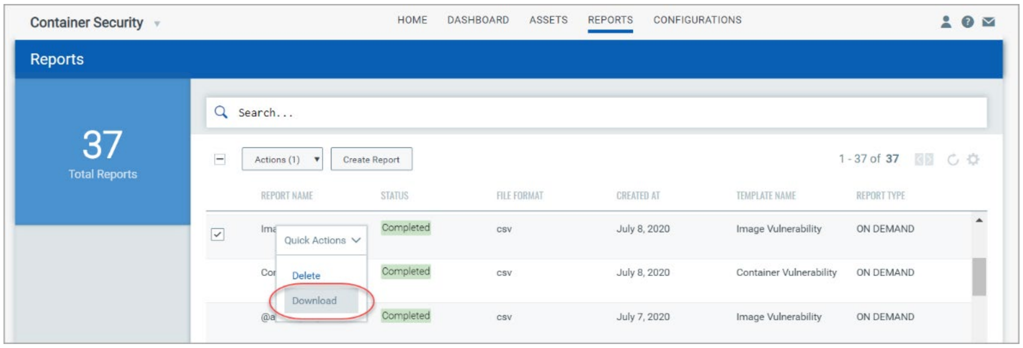
(Optional) Add a search query to limit the report to certain images/containers. For an Image Vulnerability report, only the images that match your query will be included. For a Container Vulnerability report, only the containers that match your query will be included. After entering your query, click Next.

You'll see the Report Display page which shows the types of details that will be included in the report (display options are not configurable at this time). Click Next again to review the Report Summary and click Submit to generate your report. Once saved, you cannot edit the report job.

Your report will appear on the reports list with a status of Accepted. The status will change to Completed once the report is done and ready to download.

View & Download Reports

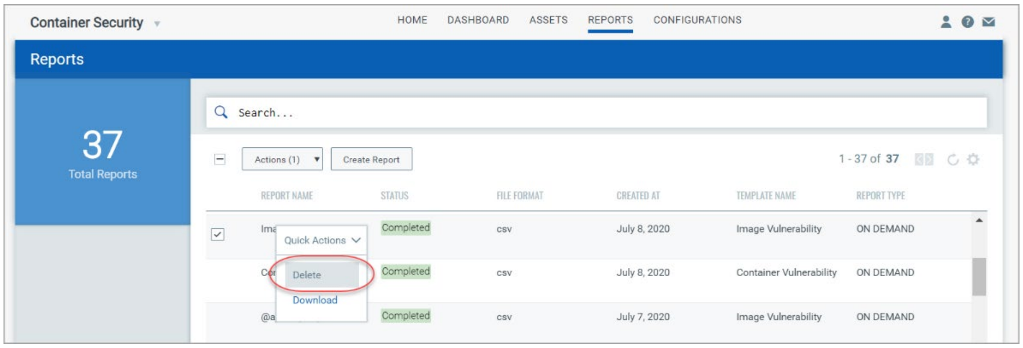
Choose Download from the Quick Actions menu for a completed report. The CSV report will be saved to your local downloads area. (Tip - Use the Search field above the reports list to quickly find a report using the search token reportName.)



	REPORT NAME	STATUS	FILE FORMAT	CREATED AT	TEMPLATE NAME	REPORT TYPE
☑	Ima	Completed	csv	July 8, 2020	Image Vulnerability	ON DEMAND
	Co	Completed	csv	July 8, 2020	Container Vulnerability	ON DEMAND
	@a	Completed	csv	July 7, 2020	Image Vulnerability	ON DEMAND

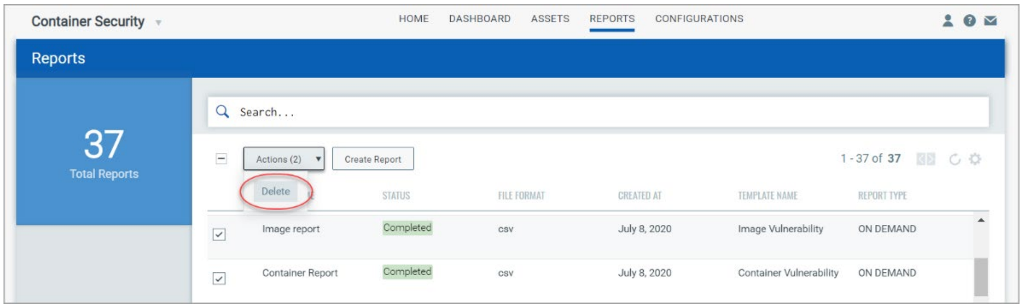
Delete Reports

To delete a single report, choose Delete from the Quick Actions menu.



	REPORT NAME	STATUS	FILE FORMAT	CREATED AT	TEMPLATE NAME	REPORT TYPE
☑	Ima	Completed	csv	July 8, 2020	Image Vulnerability	ON DEMAND
	Co	Completed	csv	July 8, 2020	Container Vulnerability	ON DEMAND
	@a	Completed	csv	July 7, 2020	Image Vulnerability	ON DEMAND

To delete multiple reports in bulk, select each row for the reports you want to delete and choose Actions > Delete above the reports list.



	REPORT NAME	STATUS	FILE FORMAT	CREATED AT	TEMPLATE NAME	REPORT TYPE
☑	Image report	Completed	csv	July 8, 2020	Image Vulnerability	ON DEMAND
☑	Container Report	Completed	csv	July 8, 2020	Container Vulnerability	ON DEMAND

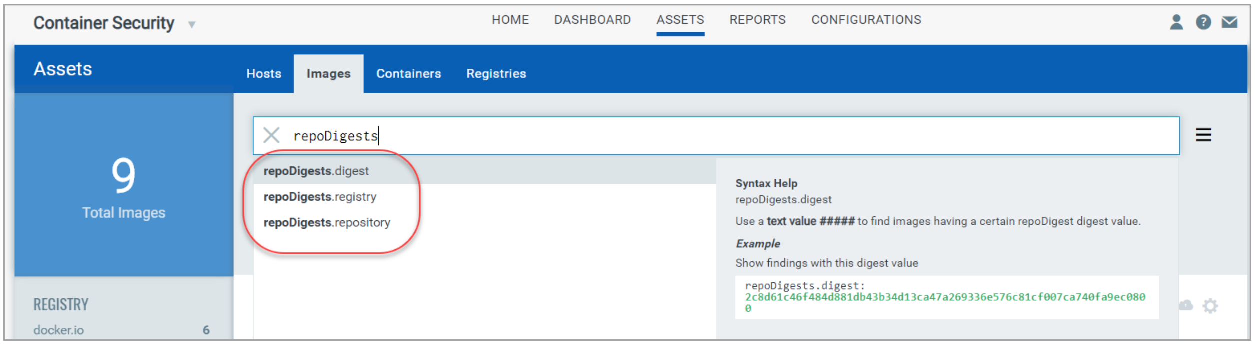
New repoDigest search tokens

These new search tokens are available when searching images:

repoDigests.digest – This token is available to find images with a certain repoDigest digest value.

repoDigests.registry – This token is available to find images with a certain repoDigest registry name.

repoDigests.repository – This token is available to find images with a certain repoDigest repository name.



```
repoDigests
```

- **repoDigests**.digest
- **repoDigests**.registry
- **repoDigests**.repository

Syntax Help
repoDigests.digest

Use a **text value #####** to find images having a certain repoDigest digest value.

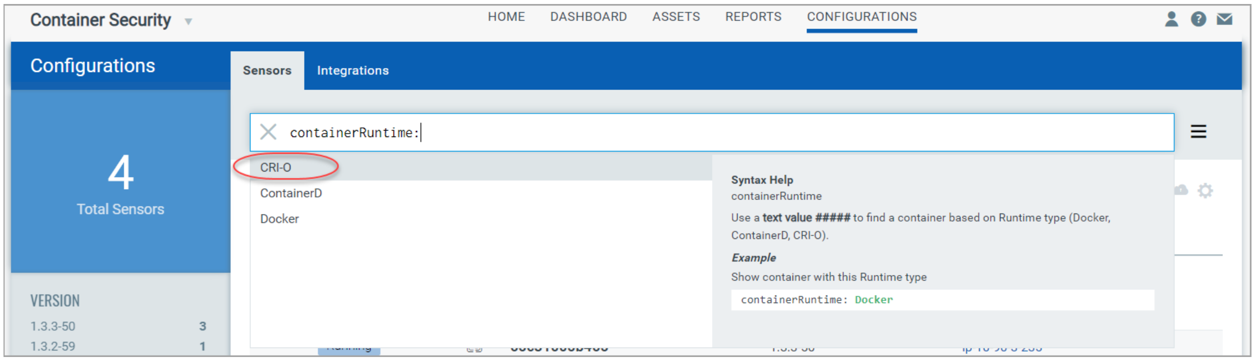
Example

Show findings with this digest value

```
repoDigests.digest:
2c8d61c46f484d881db43b34d13ca47a269336e576c81cf007ca740fa9ec080
0
```

New CRI-O value for containerRuntime search token

When searching sensors, choose CRI-O for the containerRuntime search token to find sensors deployed in a CRI-O environment. You can also find sensors based on the runtime version using the containerRuntimeVersion token.



```
containerRuntime:
```

- CRI-O
- ContainerD
- Docker

Syntax Help
containerRuntime

Use a **text value #####** to find a container based on Runtime type (Docker, ContainerD, CRI-O).

Example

Show container with this Runtime type

```
containerRuntime: Docker
```

Issues Addressed

- We fixed an issue where the Threat section in Vulnerability Details was showing the impact description instead of the threat description.
- We fixed an issue where the sensor search token containerRuntime had a value of DOCKER instead of Docker.
- We fixed an issue where we weren’t saving the default registry value for sensors with containerD runtime.
- Made several fixes to the Sensor Deployment Guide. For example, added that the sensor can run on any operating system that has Docker version 1.12 or later, updated the instructions for deploying the sensor in Kubernetes with Docker Runtime, removed the Docker hub tag value since this can become out of date. Instead, the latest tag should be looked up in Docker hub.