



# Qualys Container Security

## Release Notes

Version 1.23

March 08, 2023

### What's New?

[Customizing Data Retention Policy](#)

[Default Landing Page](#)

[Administration: Permissions for General and Data Retention Configurations](#)

[Connecting to JFrog Artifactory Private Registry with Non-Admin Credentials](#)

[Assigning Asset Tags to Images and Containers](#)

[SCA Scanning: Support for containerd Runtime](#)

[Sensor Inactive Window for Registry Sensors](#)

[Performing Only Static Scanning of Container Images](#)

### API Changes

Refer to the [Container Security API 1.23 Release Notes](#) for the API changes in this release.

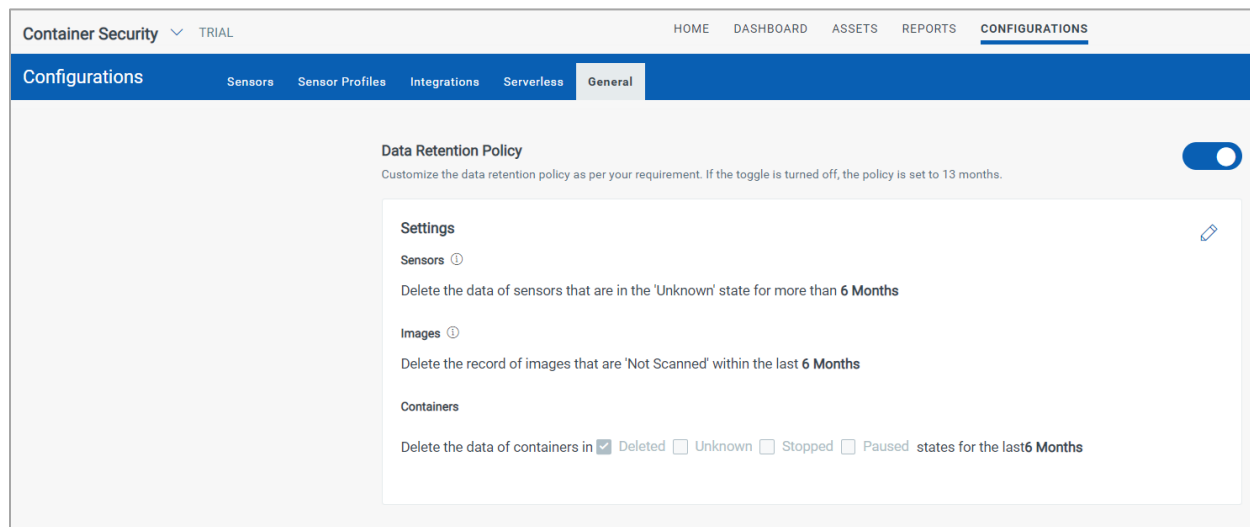
### Issues Addressed

Qualys Container Security 1.23 brings you many more improvements and updates! [Learn more](#)

# What's New?

## Customizing Data Retention Policy

You can now customize the data retention policy for Container security. The data, that is the records of sensors, containers, and images, is purged as per the defined policy. Previously, the default policy was set to purge data after 13 months.



To customize your data retention policy, navigate to **Configurations > General**, turn on the **Data Retention Policy** toggle, and configure the following options:

- **Sensors:** Delete the data of sensors that have been in the **Unknown** state for more than a certain time period.  
Note: This configuration does not apply to the sensors in the AWS Fargate environment. The data retention policy for them is set to 60 days by default.
- **Images:** Delete the record of images that have not been scanned for a certain time period.  
Note: The images that have containers associated with them are not deleted.
- **Containers:** Delete the data of containers that are in the following states for a certain time period:
  - Deleted
  - Unknown
  - Stopped
  - Paused

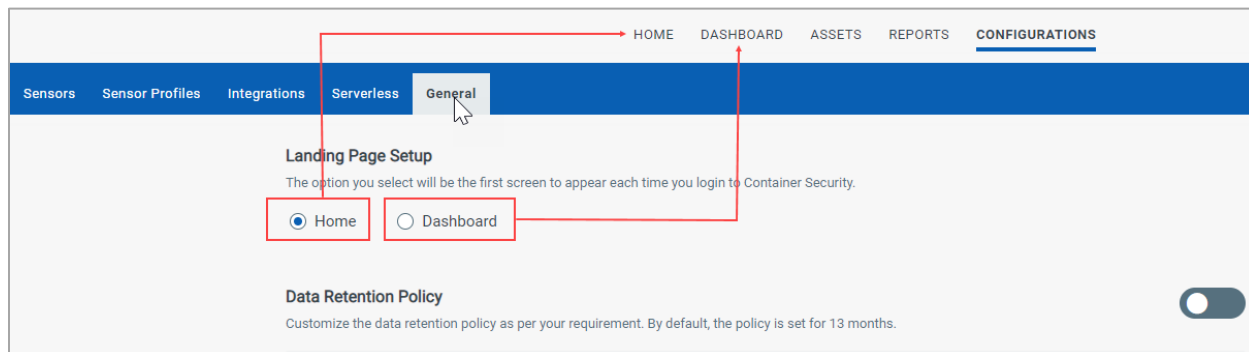
You can select 1 day, 1 week, 1 month, 6 months, or 1 year as the time period for the policy.

If the **Data Retention Policy** toggle is not turned on, the default policy of 13 months is applied.

To access the data retention policy options, your role must have the **CS Data Retention Policy Permissions** assigned.

## Default Landing Page

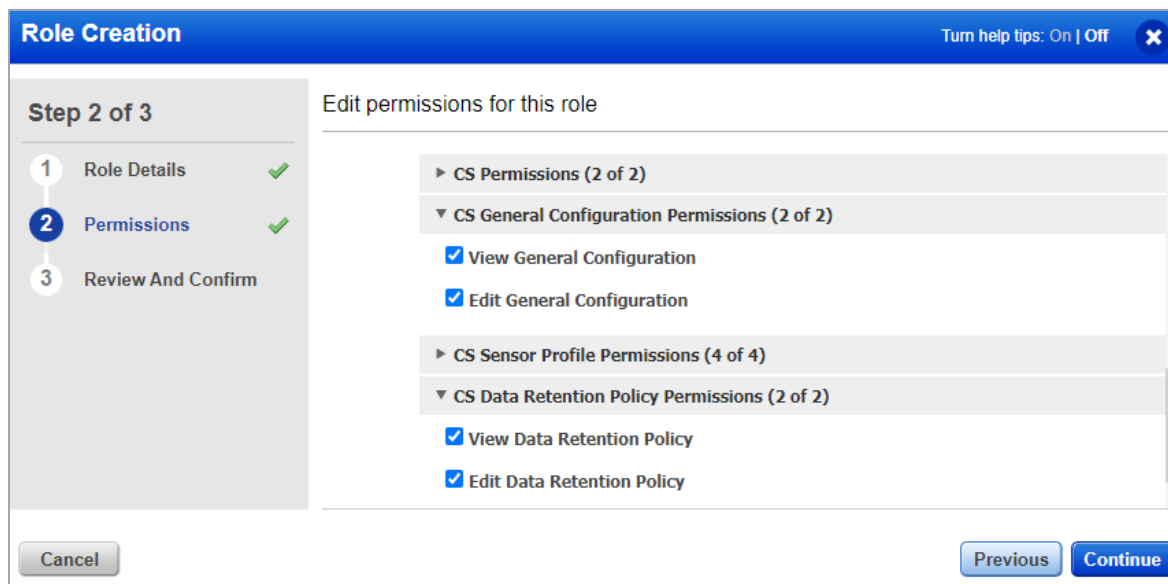
You can now choose between **Home** and **Dashboard** as the default landing page for Container Security. The selected landing page appears as the first screen every time you log in to Container Security.



## Administration: Permissions for General and Data Retention Configurations

Manager users can now assign new permissions to sub-users to manage the general configurations of Container Security. The following permissions can be assigned:

- **CS General Configuration Permissions:** This allows sub-users to view and edit options in the **Configurations > General** tab, excluding the data retention options. To manage data retention policy options, sub-users must be assigned the CS Data Retention Policy Permissions.
- **CS Data Retention Policy Permissions:** This enables sub-users to view and edit the data retention policy options.



For information about general configurations, see Online help: General Configurations.

## Connecting to JFrog Artifactory Private Registry with Non-Admin Credentials

The registry sensor can now connect with JFrog Artifactory Private Registry with non-admin account credentials. As a result, when adding a JFrog Artifactory Private Registry for scanning, you can now authenticate using the credentials of a non-admin user. The non-admin user must have at least read access to the repositories under consideration.

This new feature allows you to scan your container images stored in JFrog Artifactory Private Registry with minimum privileges.

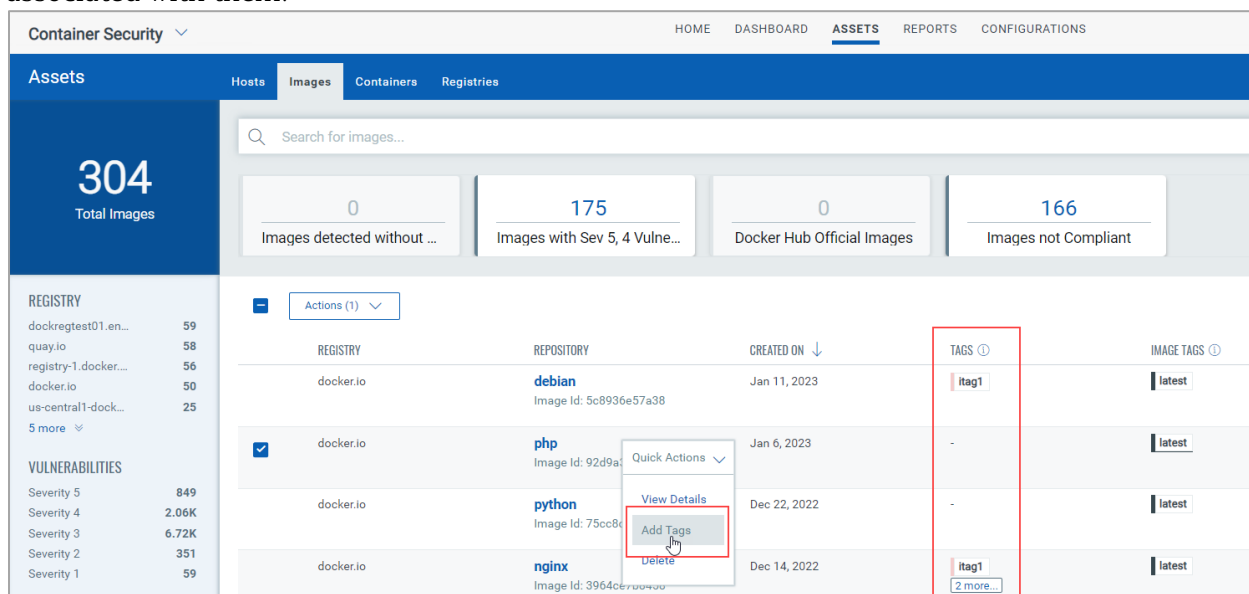
## Assigning Asset Tags to Images and Containers

You can now categorize and organize images and containers by assigning static asset tags to them within Container Security. You can also create new tags on the fly while assigning them. The assigned tags are displayed in the **Tags** column.

### Notes:

- Currently, only static tags are supported for images and containers.
- Only the tags that are created after upgrading to 1.23.0 can be assigned the images and containers.

When adding tags to images, you have the option to pass on the tags to the containers associated with them.



After adding the tags, you can search for images and containers using the following new search tokens:

Search Token	Example	Description
image.tags.name	image.tags.name: TestImage	Shows containers that are associated with images with this tag.

container.tags.name	container.tags.name: TestContainer	Shows images that are associated with containers with this tag.
tags.name	tags.name: Test	Shows images that are assigned with this tag.

For more information, see Online help: [Assign Tags to Assets](#).

## SCA Scanning: Support for containerd Runtime

The support for SCA scanning has been extended to the containerd runtime, making SCA scanning available to a broader range of environments. Previously, it was available only for the docker runtime.

For more information about SCA scanning, see Online help: [SCA Scanning](#).

## Sensor Inactive Window for Registry Sensors

You can now configure a sensor inactive window for registry sensors. Upgrade your registry sensor to version 1.23 or later to take advantage of this feature.

An inactive window for a sensor is a specified period of time during which the sensor is dormant. The purpose of an inactive window is to prevent the sensor from generating data during specific times, such as when routine maintenance is being performed on the system.

For more information about the sensor inactive window, see Online help: [Managing Sensor Profiles](#).

## Performing Only Static Scanning of Container Images

You can now choose to perform only static scanning of your container images. This is useful in ephemeral environments where the nodes may go offline during the launch of the image scan, causing the scanning pods to be left without a node to host them.

You can configure the scanning policy to perform only static scanning using either of the following methods:

- While installing the sensor, specify the scanning policy argument with the appropriate value as shown below:

Sensor Deployment Method	New Argument
Installsensor.sh command (Binary installation)	Specify the following argument in the installsensor.sh script: ScanningPolicy=StaticScanningOnly
Docker run command (Installation from Docker Hub)	Specify the following command line argument while running the docker run command: --scanning-policy StaticScanningOnly

Kubernetes DaemonSet	Add the following argument in the deployment yaml: "--scanning-policy", "StaticScanningOnly"
----------------------	---

- Modify the sensor profile configuration in the UI:

← Create New Profile

STEPS 6/7

- 1 Basic Details
- 2 Assign Registries
- 3 Assign Sensors
- 4 Log Settings
- 5 Sensor Inactive Windows
- 6 Vulnerability Management
- 7 Review

Static scanning is not supported for CRI-O runtime.

### Scan Settings

Configure how the sensors in this profile will collect data for vulnerability management and policy compliance scans.

#### Registry Sensor

##### Configure Image Scans

Indicate whether you want sensors to perform static scanning as a fallback to dynamic scanning for images without a shell. This setting applies when a new image is pulled or the manifest is updated. This setting applies to only vulnerability scans.

Static Scan

- Dynamic Scan
- Dynamic Scan with Static as Fallback
- Static Scan

Cancel Previous Next

## Issues Addressed

The following issues have been fixed with this release:

- Container Security showed incorrect CVSSv3 Base and CVSSv3 Temporal scores for the vulnerabilities that had no scores (null scores) in the knowledgebase.
- Image and container vulnerability reports run through both the UI and API stuck in the **Accepted** state.
- The **Detection Summary** tab on the vulnerability details page showed a blank CVE ID for a vulnerability, while the **Vulnerabilities** tab (listing all vulnerabilities) accurately displayed the CVE ID for the vulnerability.
- The Container Security sensor installed on the CRI-O runtime recorded an inaccurate date and time for a container deletion event.
- The nerdctl utility in the Qualys sensor container included a vulnerable GO package (BTCD).
- The general sensor deployed in a Kubernetes cluster generates pending or non-schedulable scanning Pods on nodes. To avoid generating such Pods, you must ensure the following:
  - Before deleting any pods, validate that no image scanning is running on the node.
  - Avoid running the sensor on short-running nodes.
- If an image is deleted from a host, the association of the host with the image was not automatically removed. As a result, any vulnerabilities associated with the image were still displayed for that host.
- Previously, the registry sensor was unable to perform the "v2/manifests" call when a multi-architecture docker image was detected during the registry scan. The sensor now fetches and lists the image that is compatible with the host architecture from the multi-architecture image.