Qualys Container Security

Release Notes

Version 1.24
April 17, 2023

What's New?

API Changes

Refer to the Container Security API 1.24 Release Notes for the API changes in this release.

Issues Addressed

Qualys Container Security 1.24 brings you many more improvements and updates! Learn more

What's New?

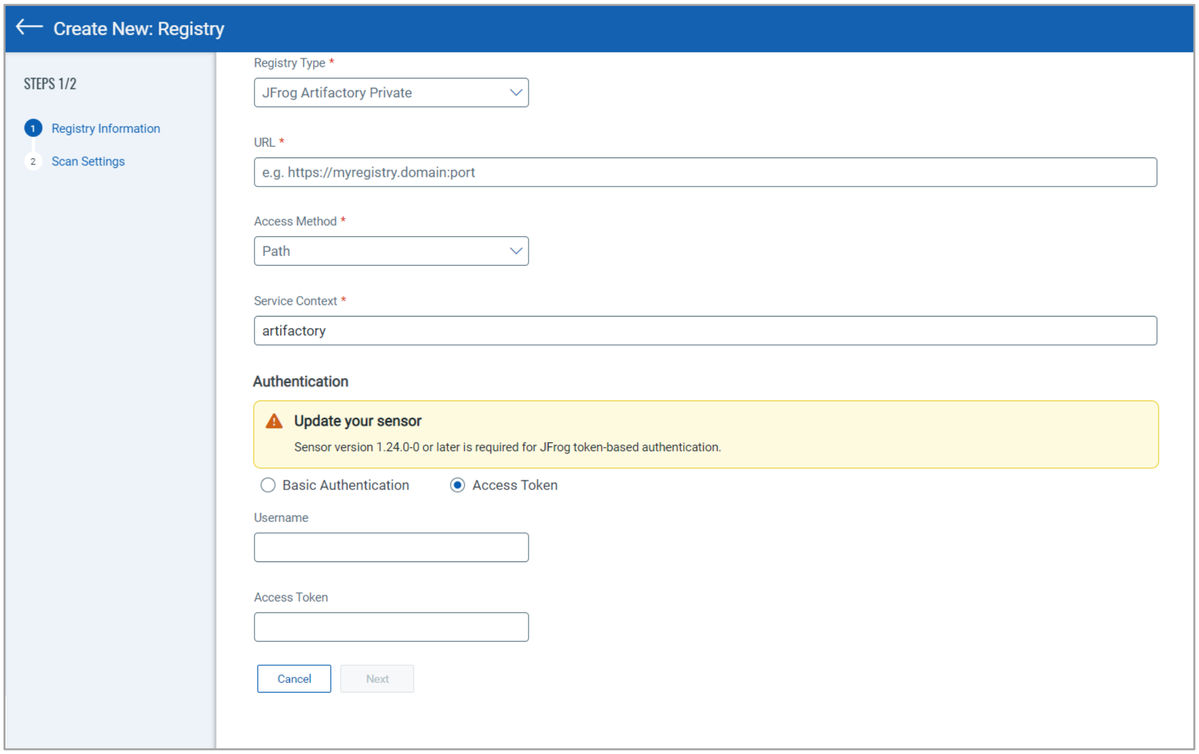
JFrog Private Registry: Authenticating with Non-Admin Credentials and Access Tokens

The registry sensor can now connect with the JFrog Artifactory Private Registry using:

- 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.
- Access tokens. You can generate an access token on the JFrog platform and use it for authenticating the sensor. For more information about JFrog access tokens, see JFrog Documentation.

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

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.



Create New: Registry

STEPS 1/2

1 Registry Information

2 Scan Settings

Registry Type * JFrog Artifactory Private

URL * e.g. https://myregistry.domain:port

Access Method * Path

Service Context * artifactory

Authentication

Update your sensor

Sensor version 1.24.0-0 or later is required for JFrog token-based authentication.

○ Basic Authentication ● Access Token

Username

Access Token

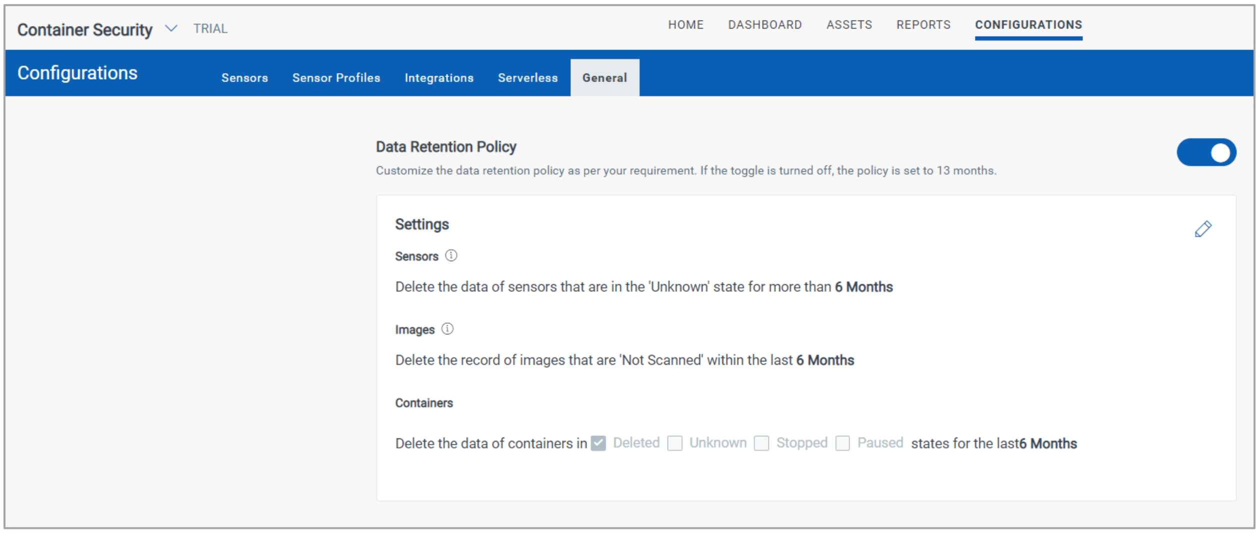
SCA Scanning: Support for CRI-O and Containerd Runtimes

The support for SCA scanning has been extended to the CRI-O and Containerd runtimes, 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.

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.



Data Retention Policy

Customize the data retention policy as per your requirement. If the toggle is turned off, the policy is set to 13 months.

Settings

Sensors ⓘ

Delete the data of sensors that are in the 'Unknown' state for more than **6 Months**

Images ⓘ

Delete the record of images that are 'Not Scanned' within the last **6 Months**

Containers

Delete the data of containers in ☑ Deleted ☐ Unknown ☐ Stopped ☐ Paused states for the last**6 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.

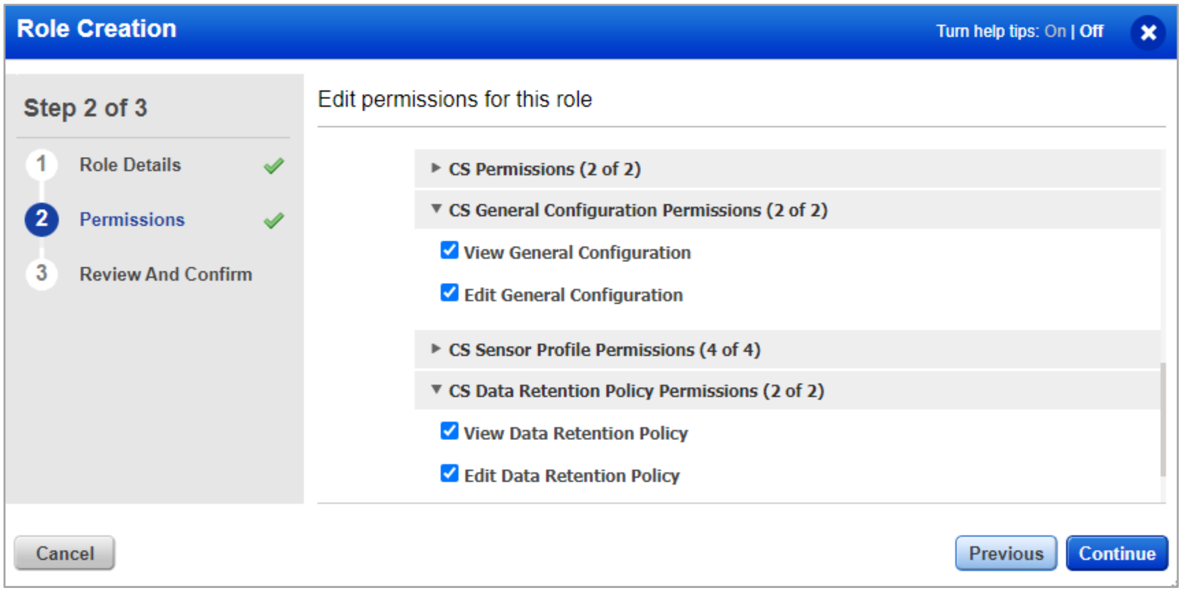
To access the data retention policy options, your role must have the **CS Data Retention Policy Permissions** assigned**.**

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.



Role Creation

Step 2 of 3

1 Role Details ✓
2 Permissions ✓
3 Review And Confirm

Edit permissions for this role

▶ CS Permissions (2 of 2)

▼ CS General Configuration Permissions (2 of 2)

☑ View General Configuration

☑ Edit General Configuration

▶ CS Sensor Profile Permissions (4 of 4)

▼ CS Data Retention Policy Permissions (2 of 2)

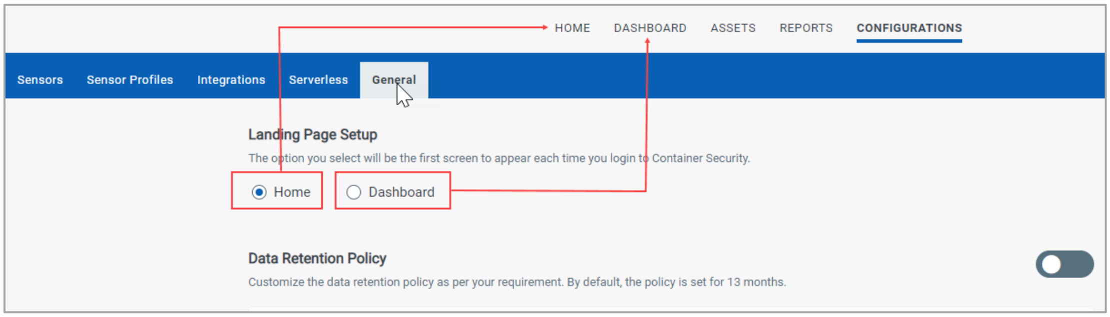
☑ View Data Retention Policy

☑ Edit Data Retention Policy

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

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.



Landing Page Setup

The option you select will be the first screen to appear each time you login to Container Security.

● Home ○ Dashboard

Data Retention Policy

Customize the data retention policy as per your requirement. By default, the policy is set for 13 months.

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.

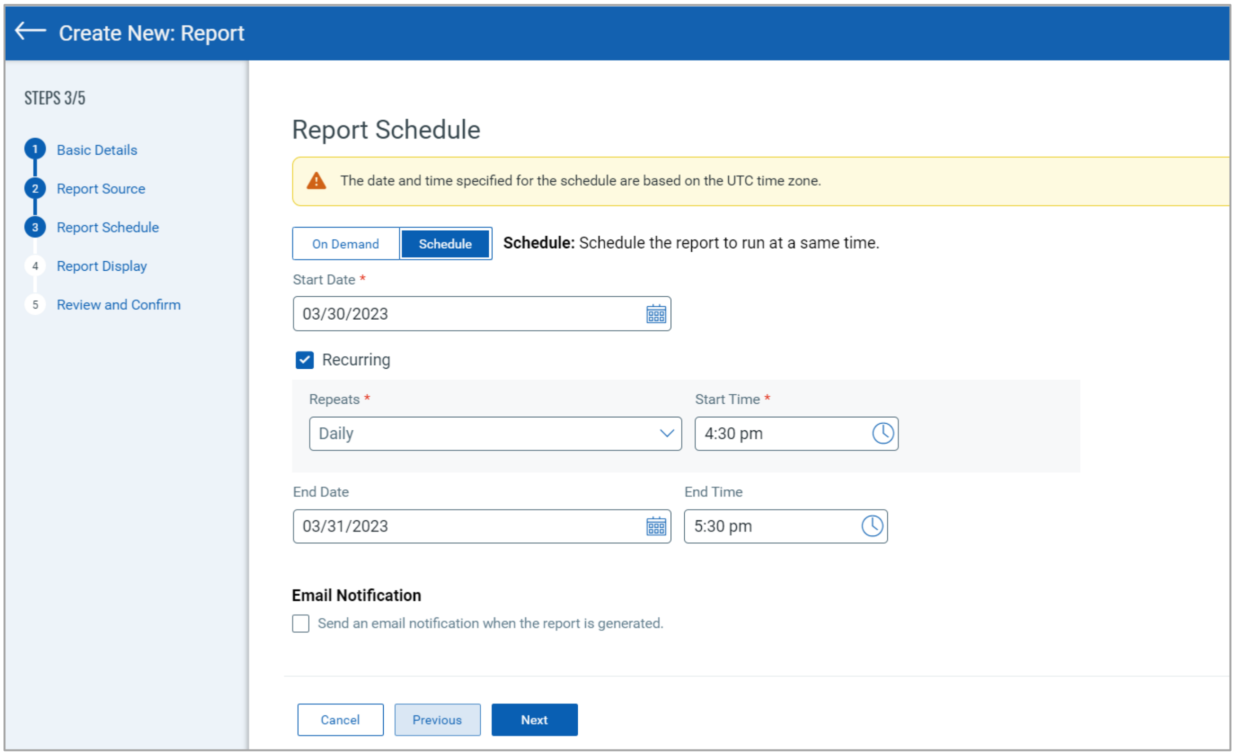
Scheduling Vulnerability Reports

You can now schedule image and container vulnerability reports to run them 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.

You can define different schedules as follows:

- A non-recurring schedule to create a report at a future date and time. It allows you to schedule the report in the future.
- Recurring schedules to generate the report regularly at the following time intervals:
  - Daily
  - Weekly
  - Monthly

Note: When specifying the date and time in schedules, you must specify them based on the UTC time zone. For instance, if you are in the UTC+5:30 time zone, you must subtract 5 hours 30 minutes from your local time and specify the adjusted time in the schedule.



Report Schedule

The date and time specified for the schedule are based on the UTC time zone.

Schedule: Schedule the report to run at a same time.

Start Date * 03/30/2023

☑ Recurring

Repeats * Daily

Start Time * 4:30 pm

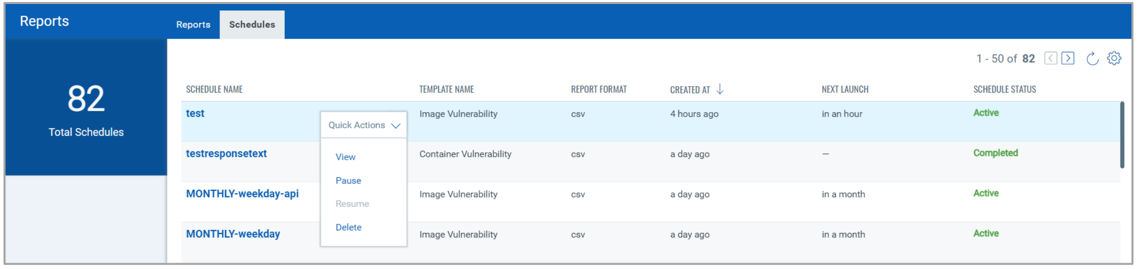
End Date 03/31/2023

End Time 5:30 pm

Email Notification

□ Send an email notification when the report is generated.

Once created, your schedules appear in the **Schedules** tab, where you can perform several actions such as viewing, pausing, resuming, or deleting a schedule. Whenever a schedule is triggered, a report job is generated in the **Reports** tab. The **Report Type** column in the Reports tab allows you to quickly identify whether the report job was triggered by a scheduled or on-demand request.



SCHEDULE NAME	TEMPLATE NAME	REPORT FORMAT	CREATED AT	NEXT LAUNCH	SCHEDULE STATUS
test	Image Vulnerability	csv	4 hours ago	in an hour	Active
testresponsetext	Container Vulnerability	csv	a day ago	–	Completed
MONTHLY-weekday-api	Image Vulnerability	csv	a day ago	in a month	Active
MONTHLY-weekday	Image Vulnerability	csv	a day ago	in a month	Active

Administrators can view the activity logs for any actions performed on reports and schedules in the Administration application. This allows administrators to monitor and keep track of any changes or modifications made to reports and schedules by users.

For more information, see Online Help: Create Vulnerability Reports in Container Security.

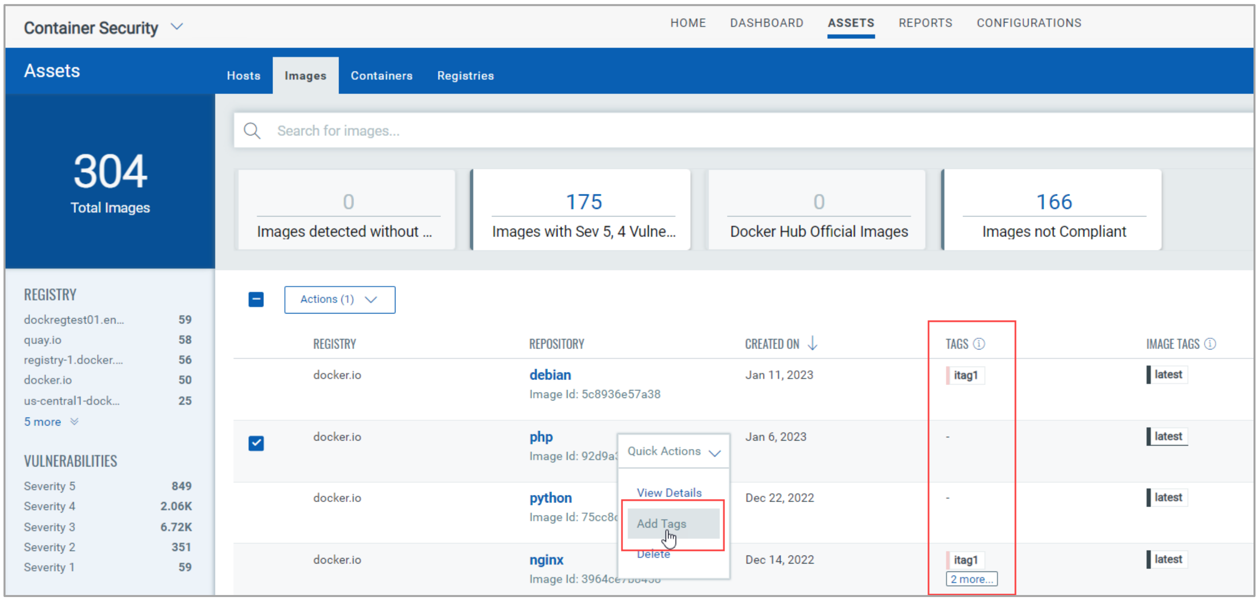
Assigning Asset Tags to Images and Containers

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.



REGISTRY	
dockregtest01.en...	59
quay.io	58
registry-1.docker....	56
docker.io	50
us-central1-dock...	25
5 more	

VULNERABILITIES	
Severity 5	849
Severity 4	2.06K
Severity 3	6.72K
Severity 2	351
Severity 1	59

	REGISTRY	REPOSITORY	CREATED ON	TAGS	IMAGE TAGS
	docker.io	debian Image Id: 5c8936e57a38	Jan 11, 2023	itag1	latest
☑	docker.io	php Image Id: 92d9a	Jan 6, 2023	-	latest
	docker.io	python Image Id: 75cc8	Dec 22, 2022	-	latest
	docker.io	nginx Image Id: 3964ce	Dec 14, 2022	itag1 2 more...	latest

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.

Performing Only Static Scanning of Container Images

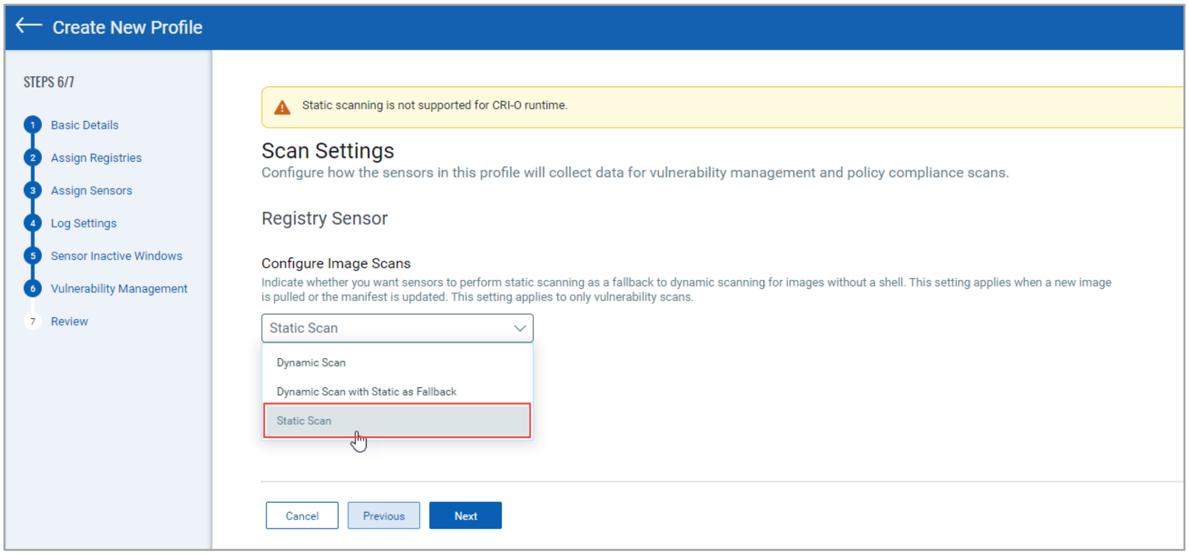
You can now choose to perform only static scanning of your container images. This is useful in ephemeral environments where the nodes may go offline during the launch of the image scan, causing the scanning pods to be left without a node to host them.

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:



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

Issues Addressed

The following issues have been fixed with this release:

- For certain sensors, the sensor UUID and host details did not appear in the UI and API.
- 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.