



Qualys Container Security

Release Notes

Version 1.14

February 9, 2022

Here's what's new in Container Security 1.14!

[AWS US GovCloud Registry Support](#)

[Support for RedHat Quay Registry](#)

[Support for JFrog Artifactory Private Registry](#)

[New Option for Optimizing Image Scans](#)

[Search CRS Runtime Policies by Name](#)

Container Security 1.14 brings you more improvements and updates! [Learn more](#)

AWS US GovCloud Registry Support

Now users are able to create and scan AWS US GovCloud based registries. When creating a new AWS ECR registry, you'll see new US GovCloud regions listed and you'll specify the account type (Global or US GovCloud) when setting up your connector. An account type value of null is applied to connectors created prior to this release. Your account type selection determines the AWS credentials that will be used. When the account type is US GovCloud, US GovCloud credentials are used. When the account type is Global or null, Global AWS credentials are used.

When creating an AWS US GovCloud based registry, you must select one of the GovCloud regions. You can choose "US East (GovCloud)" or "US West (GovCloud)".

← Create New: Registry

STEPS 1/2

1 Registry information

2 Scan Settings

Registry sensor not found/unknown
Ensure that registry sensor deployed on the docker host is in running state.

Registry Information
Name and select type of this registry. If Public, add credentials if needed.

Registry Type *

AWS ECR

Region *

Select One...

US East (Ohio)

US East (N. Virginia)

US West (N. California)

US West (Oregon)

US East (GovCloud)

US West (GovCloud)

Asia Pacific (Hong Kong)

Asia Pacific (Mumbai)

Pick a GovCloud region

Create New

Registries can be public or private. Public registries are those hosted on cloud providers such as amazon, azure or google. Private registries are on-premise such as those hosted using artifactory or nexus.

You need different types of credentials to connect to different registries. Credential types supported are Token, BasicAuth, DockerHub, AWS.

In the Connector Details, you'll need to pick an account type: Global or US GovCloud. Your selection must correspond to the region that you selected under Registry Information. If you picked a standard AWS region, pick the Global account type. If you picked a GovCloud region, pick the US GovCloud account type.

← Registry Type: AWS ECR Connector

Connector Details
Give your connector a name and provide a description (optional).

Name *

Description

Specify cross account ARN

Follow steps on the right to create an IAM role in AWS that will give Qualys cross-account access to your AWS resources. Then enter the Role ARN below. Tip - You'll need the Qualys AWS account ID and external ID to complete the steps.

Qualys AWS Account ID

External ID

Role ARN *

e.g. arn:aws:iam::111111111111:role/testRole

Cancel Create Connector

Create A Role For Cross-Account Access

1. Log in to Amazon Web Services (AWS) Console.
2. Go to the IAM service.
3. Go to Roles and click **Create Role**
4. Under "Select type of trusted entity" choose **Another AWS** account. Then:
 - a. Paste in the Qualys AWS Account ID (from connector details).
 - b. Select **Require external ID** and paste in the External ID (from connector details).
 - c. Click **Next: Permissions**
5. Find the policy titled **"AmazonEC2ContainerRegistryReadOnly"** and select the check box next to it.
6. Enter a role name (e.g. CMS) and click **Create role**.
7. Click on the role you just created to view details. Copy the Role ARN value and paste it into the connector details.

Want to create a role using CloudFormation ?

Support for RedHat Quay Registry

The RedHat Quay registry is now supported for the Registry sensor. This new option allows users to scan the images that are stored in the Quay registry.

← Create New: Registry

STEPS 1/2

1 Registry Information

2 Scan Settings

Registry Information

Name and select type of this registry. If Public, add credentials if needed.

Registry Type *

RedHat Quay

URL *

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

Authentication

Username

Password

Cancel Next

Registries can be public or private. Public registries are those hosted on cloud providers such as amazon, azure or google. Private registries are on-premise such as those hosted using artifactory or nexus.

You need different types of credentials to connect to different registries. Credential types supported are Token, BasicAuth, DockerHub, AWS.

To scan images in your RedHat Quay registry, you'll need to complete these steps:

- 1) Download the Registry sensor (Sensor version 1.11 or later). Go to **Configurations > Sensors > Download Sensor** and pick **Registry**. Select the environment where you want to deploy the sensor and follow the installation instructions on the screen. Ensure the registry sensor is in Running state and continue to the next step.
- 2) Add your registry in the Container Security UI and set up a scanning schedule. Go to **Assets > Registries > New Registry**. Choose registry type **RedHat Quay**. Then provide the registry URL (e.g. https://quay.io) and authentication credentials for connecting to your registry. You can provide a standard username and password (for an account with Admin or Super User privileges) or robot account credentials. For a robot account, the username is formatted as UserName+RobotAccountName and the password is the password token value for the robot account.
- 3) After adding registry information, click **Next** to enter scan settings. Like with other registry types, you can choose to scan immediately (On Demand) or on an on-going basis (Automatic). See the online help for guidance on scan settings.

Support for JFrog Artifactory Private Registry

We now support JFrog Artifactory Private registry for the Registry sensor. This new functionality allows users to scan JFrog Artifactory repositories. The sensor will use the Artifactory Native API with AQL (Artifactory Query Language) for the listing phase of the registry scan to collect image metadata information for the repository provided in the registry scan schedule. The Artifactory Native API provides a more efficient method of finding images which will result in performance improvements. We've also introduced a new Pushed Date filter for On Demand scans that will allow you to filter the images to be scanned based on when each image was pushed into the repository being scanned (see [New Pushed Date Filter Option](#) to learn more).

← Create New: Registry

STEPS 1/2

1 Registry Information

2 Scan Settings

Registry Information

Name and select type of this registry. If Public, add credentials if needed.

Registry Type *
JFrog Artifactory Private

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

Access Method *
Path

Service Context *
artifactory

Authentication

Username

Password

Cancel Next

Registries can be public or private. Public registries are those hosted on cloud providers such as amazon, azure or google. Private registries are on-premise such as those hosted using artifactory or nexus.

You need different types of credentials to connect to different registries. Credential types supported are Token, BasicAuth, DockerHub, AWS.

You'll need to complete these steps:

- 1) Download the Registry sensor (Sensor version 1.11 or later). Go to **Configurations > Sensors > Download Sensor** and pick **Registry**. Select the environment where you want to deploy the sensor and follow the installation instructions on the screen. Ensure the registry sensor is in Running state and continue to the next step.
- 2) Add your registry in the Container Security UI and set up a scanning schedule. Go to **Assets > Registries > New Registry**. Choose registry type **JFrog Artifactory Private**. Provide the following information:

URL - Enter the registry URL.

Access Method - Choose **Path** (for direct access to Docker registries) or **Sub Domain** (for access to Docker registries through a reverse proxy).

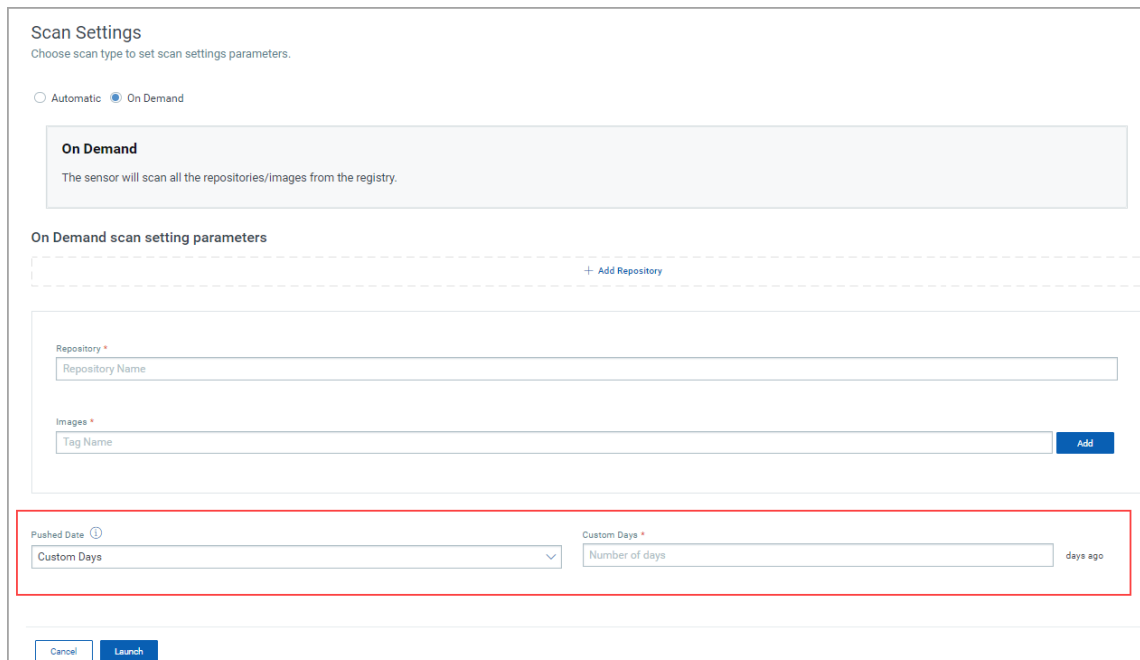
Service Context - Enter the service context value configured as part of the Base URL for reverse proxy configuration.

3) After adding registry information, click **Next** to enter scan settings. Like with other registry types, you can choose to scan immediately (On Demand) or on an on-going basis (Automatic). See the online help for guidance on scan settings.

New Pushed Date Filter Option

When configuring On Demand scan settings for a JFrog Artifactory Private registry, you'll see a new Pushed Date filter option. This option allows you to filter the images to be scanned based on when each image was pushed into the repository being scanned.

Choose an option from the **Pushed Date** menu. You can choose "All" to scan all images pushed into the repository regardless of the pushed date or "Custom Days" to only scan images pushed into the repository a set number of days ago that you specify.



Scan Settings
Choose scan type to set scan settings parameters.

☐ Automatic ☒ On Demand

On Demand
The sensor will scan all the repositories/images from the registry.

On Demand scan setting parameters

+ Add Repository

Repository *
Repository Name

Images *
Tag Name Add

Pushed Date ⓘ
Custom Days

Custom Days *
Number of days days ago

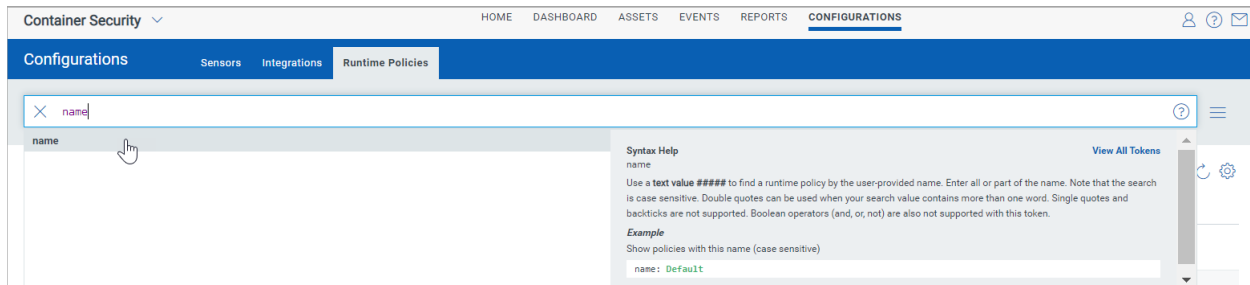
Cancel Launch

New Option for Optimizing Image Scans

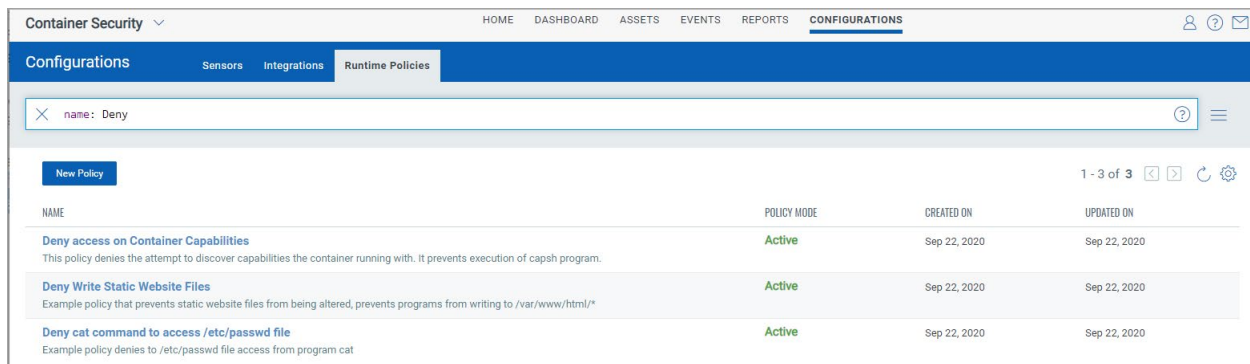
By default, the Container Security Sensor scans every image that it detects on the host. This results in redundant scanning of images. In order to optimize image scans, we've introduced a new argument called "--optimize-image-scans". When you install the General sensor with this new argument, the sensor will communicate with the Qualys Cloud Platform and perform informed scans to avoid redundant image scans. The sensor will determine if the images present on the host are already scanned by other sensors for the same manifest and version and will not scan those images again. Please note that this feature is available for General sensor type only.

Search CRS Runtime Policies by Name

Now you can search the Runtime Policies list by the user-provided policy name. Go to **Configurations > Runtime Policies** and in the search box above the list, type **name** followed by a text value. You can search by all or part of the policy name. Note that the search is case sensitive. See the Syntax Help in the search pane for full details.



In the following example, the user is searching for all policies with Deny in the name.



Issues Addressed

- We fixed the Installation Instructions that appear in the UI on the Download and Deploy Qualys Container Sensor page for MacOS standalone deployment on Docker Hub.
- We fixed an issue where the Download report quick action was not working as expected.
- We fixed an issue where the Created field was being set to null for a registry after the registry was edited and saved.
- We fixed an issue where duplicate entries were shown in the Image Vulnerability Report when an OR operator was used in the search query for the report.
- We fixed an issue for “Fetch a list of reports” API where the API response returned a 200 code and count as “null” if there were zero reports to fetch. Now if the count is zero, you’ll get a 204 code in the response.