



Qualys Container Security

Release Notes

Version 1.31

January 11, 2024

What's New?

[Creating Custom Secret Detectors](#)

[Controlled Access for the Sub-users](#)

[Customized Landing Page for Assets](#)

[Showing "Unknown" Status for the Deleted Scan Jobs under Registries](#)

[Improved Secret Detector Security](#)

[SCA Scan Enablement](#)

Container Security Sensor Updates

Upgrade your sensor to version 1.31.0 to benefit from the above-mentioned enhancements. Refer to the [Container Security Sensor 1.31.0 Release Notes](#) for the sensor updates.

Issues Addressed

Qualys Container Security 1.31 brings you many more improvements and updates! [Learn more](#).

What's New?

Creating Custom Secret Detectors

Starting this release, you can now create, edit, delete custom (non-system) type secret detectors.

Note: You cannot create System type Secret Detector. However, you can edit the Severity, and Status of a System Secret Detector.

In the **Configurations > Secret Detection** tab, you can see the **New Secret Detector** button to create a new secret detector.

The screenshot shows the Qualys Cloud Platform interface for the 'Secret Detection' configuration page. The page has a sidebar with 'Container Security' and a main content area. The main content area has a search bar and a table of secret detectors. A 'New Secret Detector' button is highlighted in the top left corner of the table. The table has columns for 'SECRET DETECTOR', 'CATEGORY', 'TYPE', 'SEVERITY', 'STATUS', 'CREATED BY', and 'UPDATED BY'. The table lists several system detectors, including 'SSH public key DSA', 'SSH public key RSA', 'Typeform API Token', 'Twitch API Token', 'LinkedIn Client Id', and 'LinkedIn Client Secret'.

SECRET DETECTOR	CATEGORY	TYPE	SEVERITY	STATUS	CREATED BY	UPDATED BY
SSH public key DSA	PublicKey	system	High	Active	System	System
SSH public key RSA	PublicKey	system	High	Active	System	System
Typeform API Token	Typeform	system	Low	Active	System	System
Twitch API Token	Twitch	system	Low	Active	System	System
LinkedIn Client Id	LinkedIn	system	Low	Active	System	System
LinkedIn Client Secret	LinkedIn	system	Low	Active	System	System

Fill in the required details for the new secret detector and save the secret detector form. The new Secret Detector will be visible in the Secret Detector's list.

-
- Notes:**
- Wild card characters are disabled for the **Regex** field of a Secret Detector. A query search requires the exact matching of the string (non-wildcard entry) to avoid identification of the redundant entries.
List of un-supported characters in the **Regex** field are as follows.
{".", "\\", ".?", ".*", ".*", "[\\s\\S]", "[\\w\\W]", "[\\d\\D]"}
 - Also, the **Regex** field does not support “\” back-slash character as it can give false-positive search results later.
-

Secret Detector Details

Secret Detector Name *

Enter Secret Detector name

63 characters remaining

Category *

Enter Category

63 characters remaining

Severity *

Critical

▼

Regex *

Enter Regex

256 characters remaining

Status

☒ Active
 ☐ Inactive

Keywords ⓘ

Enter Keywords

Cancel

Save

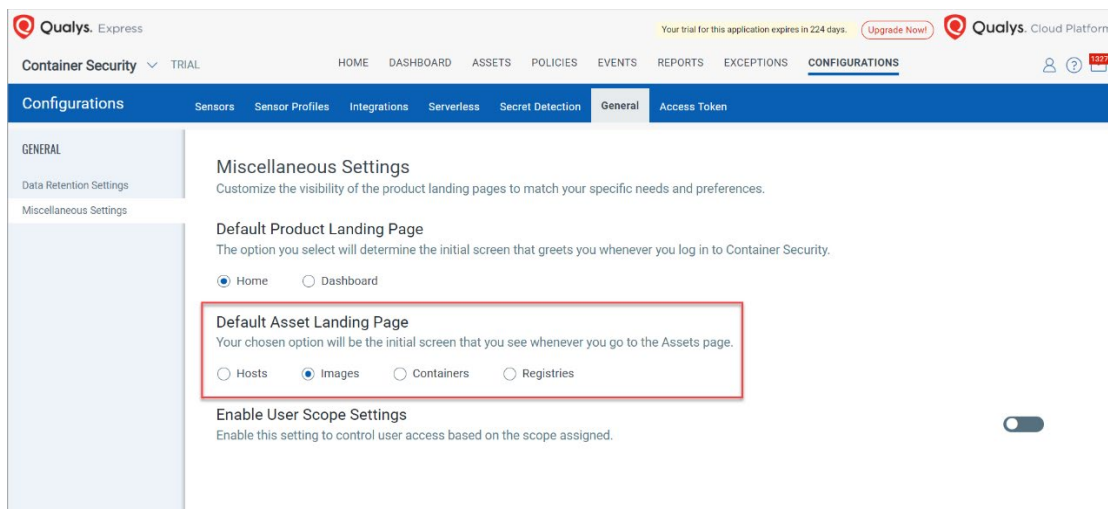
Controlled Access for the Sub-users

With this release, Admins can restrict sub-users access to certain assets. They can achieve this control using a set of tags. Now, all sub-users can only see the assets which are in their scope. Any asset which is beyond their scope will not be visible to them. These assets include images and containers. To understand how to enable the access control, refer to the **Users and Permission** section in the [Container Security Online Help](#).

Customized Landing Page for Assets

Earlier, **Hosts** page was treated as the default landing page for the **ASSETS** tab. Now, **Images** are treated as the default option. Also, you can choose the default landing page for your ASSETS tab. The following options are available for the ASSETS default landing page – Hosts, Images, Container, and Registries.

To choose the default landing page, go to **Configuration > General > Miscellaneous Settings > Default Asset Landing Page**.



Showing "Unknown" Status for the Deleted Scan Jobs under Registries

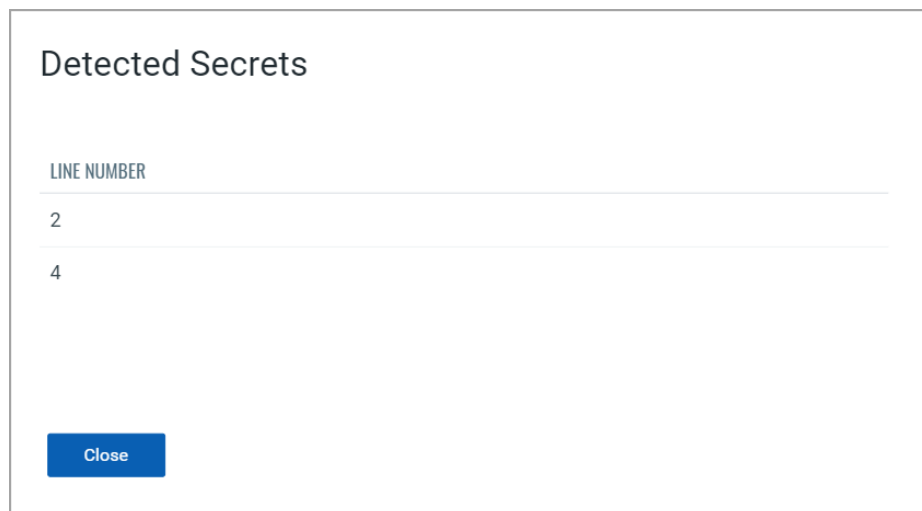
Earlier, if all scan jobs created under a registry are deleted, the status shown was "-". With this release, for registries without any scan jobs, the status shown will be "unknown".

For example, in the image below, the status of "Sub_domain_jfrog" registry - which does not possess any job - shows as "**Unknown**".

REGISTRY NAME	STATUS	REGISTRY	REPOSITORY	TOTAL	SCANNED	VULNERABLE
Jfrog_Test_First	Finished	https://demosecaccount.jfrog.io	0	0	0	0
Docker_Reg_Test_Secrets	Finished	https://registry-1.docker.io	1	0	0	0
Secret_Detection_Scan_Test04	Finished	https://registry-1.docker.io	1	1	1	1
Secret_Detection_02	Error	https://registry-1.docker.io	0	0	0	0
Secret_Detection_Scan_Test01	Cancelled	https://registry-1.docker.io	5	1	1	1
Docker_Hub_Test02_Secret	Finished	https://registry-1.docker.io	1	1	1	1
Docker_Hub_Secret_Detection	Finished	https://registry-1.docker.io	1	1	1	1
DockerHub_Secret	Finished	https://registry-1.docker.io	0	0	0	0
Docker_Force	Error	https://registry-1.docker.io	2	0	0	0
Acun Regression_Test_1_24	Finished	https://cmstestad01.azurecr.io	1	0	0	0
Jfrog_Sub_Domain_Test03	Finished	http://qssensorjfrog.nfab.in03.qualys.com:8000	1	0	0	0
Sub_Domain_jfrog	Unknown	http://qssensorjfrog.nfab.in03.qualys.com:8082	2	0	0	0

Improved Secret Detector Security

With this release, the **Match** column from the **Detected Secrets** window is removed to add extra security to the existing secrets. Now, only the **Line Number** column is displayed. By doing so, we are avoiding unnecessary exposure to the matched secrets. To access the **Detected Secrets** window, go to **Assets > Images with secrets > Image Details > Secrets**.



SCA Scan Enablement

With this release, for all users, the Software Composition Analysis (SCA) scan type is enabled. Earlier, **Dynamic** and **Static** scans were available for the users, and they had to send a request to Qualys to enable the **SCA** scan feature for their accounts. Henceforth, they don't need to send such request for the SCA feature separately.

Issues Addressed

The following issues are fixed in this release:

- The **Repository** page showed the wrong image sha count for the same images which are scanned using registry sensor.
- On Demand/Automatic Scan jobs of some registries failed with this error – “**Unexpected error occurred. Contact Qualys support**”.
- For **vulnerabilities.status:<string value>** token search, the **Images** and **Containers** tab did not show any record even when both assets had suitable matches for the given search token.
- **Last scanned** field in the **Image Summary page** failed to get updated for Registry Force rescan by Tag using regex.
- **Supported OS versions** gave an error when a user tried to access it.
(UI Path: **CONFIGURATIONS > Sensors > Download Sensor > General (Host) > CLUSTER > Kubernetes > System Requirements & Troubleshooting > Supported OS versions**).
- Container Security page under an Asset Details, showed unavailability of the sensor even when a sensor was assigned to that asset.