



# Qualys Container Security

## Release Notes

Version 1.30

November 1, 2023

### What's New

[Editing Secret Detection System Rules](#)

[Supporting Dynamic Vulnerability Exceptions](#)

### Container Security Sensor Updates

Upgrade your sensor to version 1.30.0 to benefit from the above-mentioned enhancements. Refer to the [Container Security Sensor 1.30 Release Notes](#) for the sensor updates.

### Issues Addressed

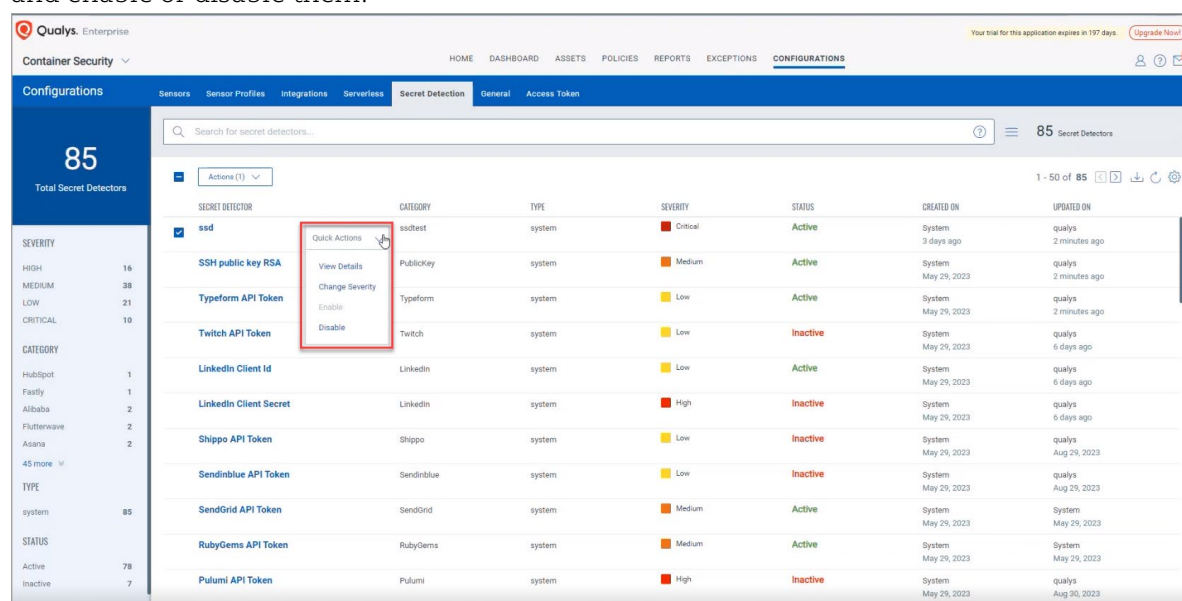
Qualys Container Security 1.30 brings you many more improvements and updates! [Learn more](#).

# What's New

## Editing Secret Detection System Rules

Secret Detectors are sets of rules to discover the presence of sensitive information, such as passwords, API keys, and other credentials, within the container images. Currently, Qualys offers 85 System Secret Detectors to you. These Secret Detectors are displayed under Container Security > Configuration > Secret Detection.

Earlier, System Secret Detectors were not editable. With this release, Container Security now allows you to change the severity of the System Secret Detectors. The new Secret Detection enhancement gives you the flexibility to reduce or increase the severity of the Secret Detectors and enable or disable them.



Disabling a Secret Detector shows its Status as Inactive. Inactive Secret Detectors are skipped from the Sensor scanning. You can use this feature to mask the unwanted or false-positive Secret Detectors.

---

**Note:** Severity or Status changes made in a Secret Detector do not affect any previously scanned images. You need to re-scan the images to reflect the new changes made in a Secret Detector.

---

## Supporting Dynamic Vulnerability Exceptions

We have now introduced a new vulnerability exception type - "Dynamic", which is now the default selection available for Vulnerability Exception type. You can access this option while filling basic details of a new exception.

Qualys Cloud Platform

Your trial for this application expires in 329 days. [Upgrade Now!](#)

← Create New : Vulnerability Exception

STEPS 1/4

- Basic Details
- Scope Details
- Vulnerability List
- Review and Confirm

### Basic Details

Provide the basic details for the vulnerability exception.

Exception Name \*

Enter a name for the exception. 63 characters remaining

Type

Static  **Dynamic**

Reason

False Positive  Risk Accepted  Other

Explanation \*

Describe your reason for this exception. 250 characters remaining

Exception Start Date \*

Exception End Date \*    Never Ends

You can use a specific QQL to automatically apply the dynamic exception to match the QQL Pattern. A query search requires exact string match, and it does not allow wildcard entry.

The newly created images or containers that match search criteria get the vulnerability exception appended automatically. This new exception is applied not just to all future images or containers but also to the images and containers which have been scanned in the past 30 days.

## Issues Addressed

The following issues have been fixed with this release:

- A user was unable to get email notifications of the scheduled reports.
- A user failed to scan images and instead received Poll Timeout error while running the QScanner.
- A signed artifact failed to be deleted from the Registry sensor host after completing a scan.
- The users were unable to run a Force Rescan operation and they had to contact Qualys support for the same. Qualys has enabled Force Re-scan feature for all users.

## Known Issue

- Image artifacts are not ignored for public registry without a force re-scan.