# Table of Contents

**About this Guide** .................................................................................................................. 4
- About Qualys ....................................................................................................................... 4
- Qualys Support .................................................................................................................. 4
- About Container Security Documentation ........................................................................ 4

**Container Security Overview** ....................................................................................... 5
- Concepts and Terminologies............................................................................................... 6
- What data does Container Security collect? ....................................................................... 8

**Get Started** ...................................................................................................................... 9
- Qualys Subscription and Modules required ........................................................................ 9
- System support ................................................................................................................... 9
- Deploying Container Sensor ............................................................................................... 10
- Sensor network configuration ............................................................................................. 13

**Securing Container Assets** ............................................................................................ 14
- Asset Inventory ................................................................................................................... 14
- Asset Details ....................................................................................................................... 15
- Vulnerability scanning of Docker Images .......................................................................... 19
- Vulnerability scanning of Docker Containers ..................................................................... 20
- Vulnerability scanning of Docker Hosts ............................................................................ 21

**Registry Scanning** ......................................................................................................... 22
- Docker host requirements .................................................................................................. 22
- Installing Registry Sensor .................................................................................................. 22
- Adding a new registry to scan ............................................................................................ 23
- Creating a registry scan schedule ..................................................................................... 24
- Viewing vulnerable registry images .................................................................................. 25

**Administration** ................................................................................................................. 26
- Sensor updates .................................................................................................................... 26
- How to uninstall sensor ..................................................................................................... 27
About this Guide

Welcome to Qualys Container Security! We’ll help you get acquainted with the Qualys solutions for securing your Container environments like Images, Containers and Docker Hosts using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

About Container Security Documentation

This document provides information about using the Qualys Container Security UI to monitor vulnerabilities in Images, Containers, and Registries.

For information on deploying the sensor on MAC, CoreOS, and various orchestrators and cloud environments, refer to the Qualys Container Sensor Deployment Guide.

For information on using the Container Security API, refer to the Qualys Container Security API Guide.

For information on deploying the sensor in CI/CD environments refer to:

- Qualys Vulnerability Analysis Plugin for Jenkins
- Qualys Vulnerability Analysis Plugin for Bamboo
Container Security Overview

Qualys Container Security provides discovery, tracking, and continuously protecting container environments. This addresses vulnerability management for images and containers in their DevOps pipeline and deployments across cloud and on-premise environments.

With this version, Qualys Container Security supports
- Discovery, inventory, and near-real time tracking of container environments
- Vulnerability analysis for images and containers
- Vulnerability analysis for registries
- Integration with CI/CD pipeline using APIs (DevOps flow)
- Uses ‘Container Sensor’ – providing native container support, distributed as a docker image
Concepts and Terminologies

Docker Image
A Docker image is a read-only template. For example, an image could contain an Ubuntu operating system with Apache and your web application installed. Images are used to create Docker containers. Docker provides a simple way to build new images or update existing images, or you can download Docker images that other people have already created. Docker images are the build component of Docker.

An image is a static specification what the container should be in runtime, including the application code inside the container and runtime configuration settings. Docker images contain read-only layers, which means once an image is created it is never modified.

Image is tracked within Qualys Container Security module using Image Id and also a unique identifier generated by Qualys called Image UUID.

Docker Registry
Docker registries hold images. These are public or private stores from which you upload or download images. The public Docker registry is provided with the Docker Hub or from cloud providers like AWS ECR, Azure Container Registry or Google Container Registry. It serves a huge collection of existing images for your use. These can be images you create yourself or you can use images that others have previously created. Docker registries are the distribution component of Docker.

Docker Containers
Docker containers are similar to a directory. A Docker container holds everything that is needed for an application to run. Each container is created from a Docker image. Docker containers can be run, started, stopped, moved, and deleted. Each container is an isolated and secure application platform. Docker containers are the run component of Docker.

A running Docker container is an instantiation of an image. Containers derived from the same image are identical to each other in terms of their application code and runtime dependencies. But unlike images that are read-only, each running container includes a writable layer (a.k.a. the container layer) on top of the read-only content. Runtime
changes, including any writes and updates to data and files, are saved in the container layer only. Thus multiple concurrent running containers that share the same underlying image may have different container layers.

Containers are tracked within Qualys Container Security module using Container Id and also a unique identifier generated by Qualys called Container UUID.

**Docker Host**

Hosts or servers running docker daemon and hosting containers and images. Qualys tracks them as Host Assets, collects the metadata including IP address, DNS and other attributes of the Host. A host in Qualys is identified by a unique identifier Host UUID. The UUID is also stored in a marker file under /usr/local/qualys directory by the Agent or a scan with authentication via a Scanner Appliance.

**Qualys Container Sensor**

The sensor from Qualys is designed for native support of Docker environments. Sensor is packaged and delivered as a Docker Image. Download the image and deploy it as a Container alongside with other application containers on the host.

The sensor is docker based, can be deployed on hosts in your data center or cloud environments like AWS ECS, Azure Container Service or Google Container Service. Sensor currently is only supported on Linux Operating systems and requires docker daemon of version 1.12 and higher to be available.

Since they are docker based, the sensor can be deployed into orchestration tool environments like Kubernetes, Mesos or Docker Swarm just like any other application container.

Upon installation, the sensor does automatic discovery of Images and Containers on the deployed host, provides a vulnerability analysis of them, and additionally it monitors and reports on the docker related events on the host. The sensor lists and scans registries for vulnerable images. The sensor container runs in non-privileged mode. It requires a persistent storage for storing and caching files.
Currently, the sensor only scans Images and Containers, for getting a vulnerability posture on the Host, you would require Qualys Cloud Agents or a scan through Qualys Virtual Scanner Appliance.

**What data does Container Security collect?**

The Qualys Container Security sensor fetches the following information about Images and Containers in your environment:

- **Inventory of Images and Containers** in your environment from commands such as `docker ps` that lists all containers.

- **Metadata information** about Images and Containers from commands such as `docker inspect` and `docker info` that fetches low level information on docker objects.

- **Event information** about Images and Containers from the docker host for docker events like created, started, killed, push, pull, etc.

- **Vulnerabilities** found on Images and Containers. This is the output of the vulnerability management manifests run for identifying vulnerability information in Images and Containers. This is primarily software package listing, services running, ports, etc.

For example, package manager outputs like `rpm -qa`, `npm`. This is supported across various Linux distributions (CentOS, Ubuntu, CoreOS, etc) and across images like Python, NodeJS, Ruby, and so on.
Get Started

This chapter provides an overview of Container Security Sensor installation.

For information on deploying the sensor on MAC, CoreOS, and various orchestrators and cloud environments, refer to the Qualys Container Sensor Deployment Guide.

See About Container Security Documentation

Qualys Subscription and Modules required

You would require “Container Security” (CS) module enabled for your account. Additionally, in order to get vulnerabilities for the hosts that run the containers, you would need to enable Vulnerability Management (VM), either via Scanner Appliance or Cloud Agent.

System support

Container Security supports these systems running Docker version 1.12 or later.

- Ubuntu
- Red Hat Enterprise Linux
- Debian
- CentOS
- MAC
- CoreOS
Deploying Container Sensor

Log into your Qualys portal with your user credentials. Select Container Security from the module picker.

As a first time user, you’ll land directly into the Getting Started page.

Go to Configurations > Sensors, and then click Add New Sensor to download the sensor tar file. You can see various sensor types:

- **General Sensor**: Scan any host other than registry / build (CI/CD).
- **Registry Sensor**: Scan images in a registry (public / private).
- **CI/CD Sensor**: Scan images on CI/CD pipeline (Jenkins / Bamboo).

For Registry you need to append the install command with `--registry-sensor` or `-r`
For CI/CD you need to append the install command with `--cicd-deployed-sensor` or `-c`

Download the QualysContainerSensor.tar.xz file and run the commands generated directly from the screen on the docker host. Note the requirements for installing the sensor, the sensor needs a minimum of 1 GB persistent storage on the host.

A quick overview of the “installsensor.sh” script command line parameters options:

- **ActivationId**: Activation Id for the container sensor, auto-generated based on your subscription.
- **CustomerId**: Qualys subscription’s customerId, auto-generated based on your subscription.
- **Storage**: Directory where the sensor would store the files. Default: `/usr/local/qualys/sensor/data`. Create it if not already available or you can specify a custom directory location.
- **ImageFile**: Location of the Sensor ImageFile, defaults to the local directory [Optional]
- **LogLevel**: Configuration to set the logging level for sensor, accepts 0 to 5 [Optional]
- **HostIdSearchDir**: Directory to map the marker file created by Qualys Agent or Scanner appliance on the host, update if modified [Optional]
- **CpuUsageLimit**: CPU usage limit in percentage for sensor. Valid range is in between 0-100 [Optional]
- **ConcurrentScan**: Number of docker/registry asset scans to run in parallel [Optional]
- **Proxy**: IPv4/IPv6 address or FQDN of the proxy server [Optional]
- **ProxyCertFile** : Proxy certificate file path [Optional]
  ProxyCertFile is applicable only if Proxy has valid certificate file. If this option is not provided then Sensor would try to connect to the server with given https Proxy settings only.

  If only ProxyCertFile is provided without Proxy then Sensor would simply ignore the ProxyCertFile and it would try to connect to the server without any https proxy settings.

- **--silent** or **-s** : Run installsensor.sh in non-interactive mode [Optional]
- **--disable-auto-update** : Do not let sensor update itself automatically [Optional]
- **--cicd-deployed-sensor** or **-c** : Run Sensor in CI/CD environment
- **--registry-sensor** or **-r** : Run sensor to list and scan registry assets
- **--enable-console-logs** : Print logs on console. These logs can be retrieved using the docker logs command.

- **DockerHost** : IPv4 address or FQDN:Port#. The address on which the docker daemon is configured to listen. [optional]

- **DockerSocketDirectory** : Docker socket directory path. [optional]

For more information on installing the registry sensor, see Registry Scanning.

**Proxy Support**

The install script asks for proxy configuration. You need to provide the IP Address/FQDN and port number along with the proxy certificate file path. For example,

Do you want connection via Proxy [y/N]: y
Enter Https Proxy settings [<IP Address>:<Port #>]: 10.xxx.xx.xx:3xxx
Enter Https Proxy certificate file path: /etc/qualys/cloud-agent/cert/ca-bundle.crt

Your proxy server must provide access to the Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. Go to Help > About to see the URL your hosts need to access.
Sensor network configuration

The sensor is pre-configured with the Qualys URL and the subscription details it needs to communicate to. In order for the sensor to communicate to Qualys, the network configuration and firewall needs to provide accessibility to Qualys domain over port 443.

After successful installation of the Sensor, the sensor is listed under Configurations > Sensors where you can see its version, status, etc. and access details.

Additionally, you can Download the sensor from the link under Configurations > Sensors.
Securing Container Assets

Asset Inventory

Upon installation of the sensor, it automatically scans the host for the images and containers that are present on the host. The inventory and the metadata of the inventory is pushed to Qualys portal.

Dashboard

Container security application provides out-of-the box default Security Overview Dashboard providing summary of inventory and security posture across container assets.

The default dashboard provides
- An inventory list of Images, Containers and the Sensors
- Vulnerability summary for all of the images
- Vulnerability summary for all the containers
- Listing of the most popular Images and Containers by Labels
Asset Details

Assets tab lists the Images and Containers discovered along with their metadata information like ports, networks, services, users, installed software, etc. It also lists the registries scanned and the hosts on which the sensor is deployed. The assets are listed along with their associations like associated containers and hosts for an image, other containers from the same parent image. Users can search for images, containers, registries and hosts based on their attributes.

Image Details

Clicking View Details in the Quick Actions menu for an image in the Assets > Images tab, displays comprehensive information about the image.

You can view detailed information about that image, its associations with containers, drift containers, and hosts. Installed Software panel displays software having vulnerabilities, and for which fixes (patches) are available. You can view the vulnerability information such as confirmed vulnerabilities, potential vulnerabilities with their severity. You can
view the age of a vulnerability. The age value is displayed in days. Age is calculated from the point Qualys published the vulnerability. The Layers panel displays a list of layers the image is made of.

**Container Details**

Clicking View Details in the Quick Actions menu for a container in the Assets > Containers tab, displays comprehensive information about the container.

You can view detailed information about that container, its associations with an image, drift containers, and hosts. Installed Software panel displays software having vulnerabilities, and for which fixes (patches) are available. You can view the vulnerability information such as confirmed vulnerabilities, potential vulnerabilities with their severity. You can view the age of a vulnerability. The age value is displayed in days. Age is calculated from the point Qualys published the vulnerability. Services/Users panel displays the list of services available in the container and users associated with the container.
Container “State” is updated based on the docker events (exec_start, kill, destroy, stop) that Qualys Sensor reports to Qualys Cloud Platform.

**Registry Details**

Clicking View Details in the Quick Actions menu for a registry in the Assets > Registries tab, displays comprehensive information about the registry.

You can view detailed information about the registry: number of repositories, total number of images and number of vulnerable images within that registry. The Scan Jobs panel lists the On Demand and Automatic Jobs created for that registry. For more information see **Registry Scanning**.
Host Details

Access the details page for a host from the Sensor details page. Asset Details view displays information about the host on which the sensor is deployed. Besides system, network, and port information, the Asset Details view also displays a list of software installed on the host, vulnerabilities present, certificates, and Threat Protection RTIs (when Qualys TP app is enabled). Container Security panel shows all containers installed on the host, their status, and the images from which the containers are spawned.
Vulnerability scanning of Docker Images

The docker images are scanned to check the presence of any vulnerabilities by the Qualys container sensor. The vulnerabilities panel in Image Details provides a list of vulnerabilities with Severity along with their QIDs. Select Show Patchable Vulnerabilities to view vulnerabilities with available patches.

Qualys scans the docker images for vulnerabilities not through static analysis but via a non-static method, where it looks at the Image as a complete entity. This process is more effective and has lesser false positives (FP) than the more commonly used Static Analysis.

Docker Images are found distributed across the environment from developer laptops, build systems, Image Registry to being cached on the docker hosts running Containers. To scan for vulnerabilities you would need the Container Sensor deployed on the host asset.

To get an inventory of the images and scan them for vulnerabilities, deploy the container sensor on the host. Refer to Deploying Container Sensor for the install instructions and system requirements.

On the local host or laptops

To get an inventory of the images and scan them for vulnerabilities, deploy the container sensor on the local host. Refer to Deploying Container Sensor for the install instructions and system requirements.

To deploy the Sensor on the Mac laptops, there are additional install steps - follow the instructions in the Qualys Container Security Sensor Deployment Guide. See About Container Security Documentation.

Upon Installation the sensor automatically detects the images, and provides inventory and vulnerability scans of the image.
In the CI/CD pipeline

Doing a complete check of vulnerabilities in an image during the build time ensures a lot cleaner operating environment. Qualys Container Security provides a plugin for Jenkins and Bamboo to get the vulnerability analysis of images in the build environment. If you are using other tools you can use the REST APIs available to perform vulnerability analysis on the images.

To start, deploy the Container Sensor on the Build host where the images are being created. The sensor upon install would automatically trigger a vulnerability analysis of the new images found. Use the API or the plugin to look for vulnerabilities in the images. If you are in Jenkins or Bamboo environment, the plugin would provide detail list of the vulnerabilities and its details directly within the plugin, you could optionally access your Qualys subscription to view the full report.

In the Registry

Currently, the Qualys Container Sensor doesn't automatically poll or pull images to do an analysis. Rather you would be needed to deploy the sensor on the host that is configured to pull images from the registry. Either manually or via a cron pull the new images to the host. The sensor does an automatic analysis as soon as it finds a new image. Use the APIs or the Qualys portal to query for the vulnerabilities identified.

Vulnerability scanning of Docker Containers

The containers are scanned to check the presence of any vulnerabilities within the containers. The Vulnerabilities panel in Container Details provides a list of vulnerabilities with Severity along with their QIDs. Select Show Patchable Vulnerabilities to view vulnerabilities with available patches.
**Good to know!**

**Drift Containers** are those which contain vulnerabilities or software, not found in the image from which the container is spawned.

**Rogue Vulnerabilities** are classified as either New, Fixed or Varied. New are those which are newly found on the containers, but were not present in the image from which the container is spawned. Fixed, are the vulnerabilities that are not found in the container but in the image. Varied, are the vulnerabilities that are found in both Containers and Images but the detection varies between them.

**Rogue Software** are classified as new or removed. New, software which are found in the Container but not in the image from which the container is spawned. Fixed, Software not seen in the Container but is present in the parent Image.

**Vulnerability scanning of Docker Hosts**

Container Security Sensor scans Images and Containers for vulnerabilities, and not the actual host machine. You can scan the host via Scanner Appliance or Cloud Agent. Configurations required on the host for using the Cloud Agent are independent of the Sensor. For example, proxy configuration.
Registry Scanning

Registry images are scanned to check the presence of any vulnerabilities by the Qualys container sensor. You can scan public and private registries for vulnerable images. 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.

Docker host requirements

As a prerequisite you must install the registry sensor on a docker host which has access to the registry to pull images to scan.

Docker host configuration

Docker version - 1.12 or later.

Disk space on docker host - Minimum 20 GB of free space on the partition where docker is installed. This is required to scan registry images. Additionally, 1 GB of free space is required for persistent storage.

Connectivity - Docker host should have connectivity to the Registry to be scanned.

To validate connectivity, perform a successful docker login from the host to the Registry.

docker login <registryurl> (No protocol)

For Example,

docker login myregistry.com:5001

Installing Registry Sensor

To download the sensor, simply go to Configurations > Sensors, click Add New Sensor and then select Registry Sensor.

You need to append --registry-sensor or -r to the sensor install command to install the sensor for registry scan.
Adding a new registry to scan

You need to add a registry in order to scan it for vulnerabilities. Go to Assets > Registries, and click New Registry. Ensure that registry sensor deployed on the docker host is in running state.

In order to perform vulnerability analysis you need to connect to the registries using credentials. You need different types of credentials to connect to different registries. Credential types supported are Token, BasicAuth, DockerHub, AWS.
For AWS ECR, you can create a connector to connect to your AWS account.

Creating a registry scan schedule

You can choose to scan immediately (On Demand scan) or on an ongoing basis (Automatic scan).

On Demand scan allows you to scan repositories as well as specific images within those repositories.

With Automatic scan, you can scan entire repositories at a set time every day.

You can cancel an ongoing scan by editing the registry and then using the Cancel option from the Quick Actions menu of a scan job. You cannot cancel jobs which are in “Error” or “Finished” state.

Use the Rescan option to restart an OnDemand scan. You cannot restart jobs which are in “Queued” or “Running” state.
Note: You must provide the full repository path up till the last sub-directory containing the images you want to scan.

Tip: The following command helps you to get a list of full repository names that are part of a registry.

curl -u <username>:<password> https://<registry-url>/v2/_catalog

**Viewing vulnerable registry images**

Once you connect to the registry, Container Security pulls the inventory data and performs vulnerability scans on repositories and images within the registries. Vulnerable images are listed on the **Images** tab.

To get the total count of vulnerable images in a registry, go to Registries tab, and click **View Details** in the Quick Actions Menu of a registry. The Scan Jobs panel shows a list of schedules created for scanning the registry.
Administration

For information on sensor installation and troubleshooting, refer to the Qualys container Security Sensor Deployment Guide. See About Container Security Documentation.

Sensor updates

When an update is available you’ll see “Update Available” next to the sensor name.

![Sensor update screenshot]

Container sensor update is otherwise automatic, however if you are currently using the beta version of the sensor you need to update to the latest sensor version manually. Automatic update kicks off once you are on a version higher than the beta.

To manually update the sensor from beta to the latest version, download the QualysContainerSensor.tar.xz file from Qualys Cloud Portal and then run the following commands directly from the screen on the docker host.

Untar the sensor package:

```
sudo tar -xvf QualysContainerSensor.tar.xz
```

Launch the new sensor:

```
sudo ./installsensor.sh ActivationId=5e7e422a-a1ca-403f-9274-506622dc5b28 CustomerId=a8cf7043-0245-6f1d-82f8-97f784652b93 Storage=/usr/local/qualys/sensor/data -s
```

Enter Y at the prompt asking you to upgrade 'Qualys-Container-Sensor' from version x.x.x to x.x.x.

The install script asks for proxy configuration. If you want to configure proxy, see Proxy Support.

Note: Once you have upgraded from the beta version to a higher version, future updates of Sensor are automatic.
**How to uninstall sensor**

The QualysContainerSensor.tar.xz file (which you download for sensor installation from Qualys Cloud Platform) has the script `uninstallsensor.sh` for uninstalling the sensor.

To uninstall a sensor:

If the docker host is configured to communicate over docker.sock, use the following command:

```
./uninstallsensor.sh -s
```

If the docker host is configured to communicate over TCP socket then provide the address on which docker daemon is configured to listen:

```
./uninstallsensor.sh DockerHost=<IPv4 address or FQDN>:<Port#> -s
```

For example,

```
./uninstallsensor.sh DockerHost=10.115.27.54:3128 -s
```

Follow the on-screen prompts to uninstall the sensor. Qualys recommends not to clear the persistent storage.