



Qualys Container Security

Release Notes

Version 1.17

August 5, 2022

Here's what's new in Container Security 1.17!

[Introducing Role Based Access Controls](#)

[Introducing Sensor Profiles for Registry Sensors](#)

[Updates to Create/Edit Registry: Name Field Added](#)

Introducing Role Based Access Controls

If you use other Qualys modules, then you're probably already familiar with how the Role Based Access Control (RBAC) model works. With Qualys Cloud Platform 3.12 and Container Security 1.17, the Qualys Container Security module will start using the RBAC model to control access to Container Security features. With RBAC, each user is assigned a pre-defined user role which determines which actions the user can take in the UI and API.

A Manager user (superuser with full permissions and scope) can access the **Administration** utility, has all roles assigned, can add and manage users, can create custom roles and assign roles to users. The first user in a new customer subscription is a Manager user.

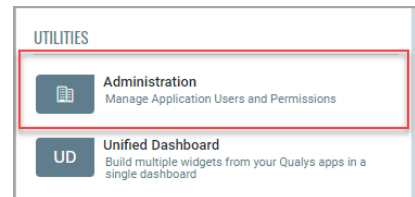
We have the following pre-defined roles for Container Security. These roles are exclusive to the Container Security module. The roles defined in other modules have NO correlation with those defined in Container Security.

- CS Manager: A CS Manager has all Container Security permissions and can perform all actions in the Container Security UI and API. Existing Container Security users will be assigned the CS Manager role automatically, which means all existing users will be able to perform all actions just like in previous releases.
- CS User: The CS User role was existing in the Administration utility prior to this release. This role only has permission to access the Container Security UI, and has no other permissions assigned. Note: This role will not be available in new customer subscriptions created after Container Security 1.17.

How to View Roles and Permissions

Managers can view user roles and permissions from the **Administration** utility. If you need help at any time, please refer to the [Qualys Administration Utility Help](#).

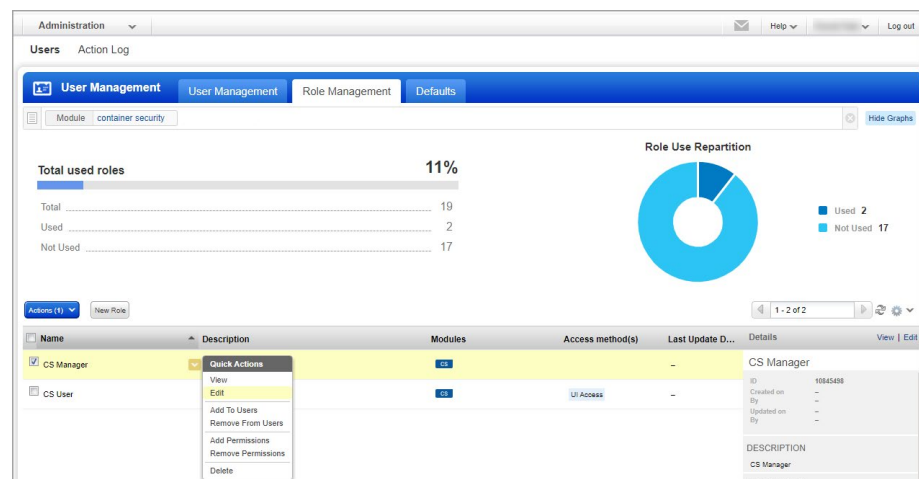
1) Choose **Administration** under **Utilities** from the application picker.



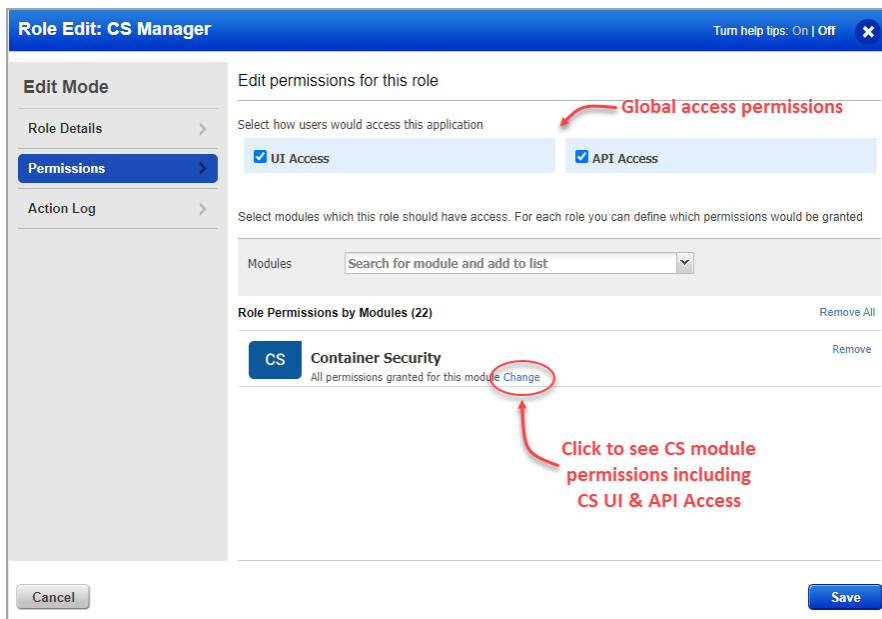
2) Go to the **Users > Role Management** tab. This is where you'll find roles and their related permissions. You can search for the module "container security" to view the Container Security roles.

Note: The **Role Management** tab is only visible if you have a) full permissions and scope, or b) a role with the "Access Role Management Section" permission enabled.

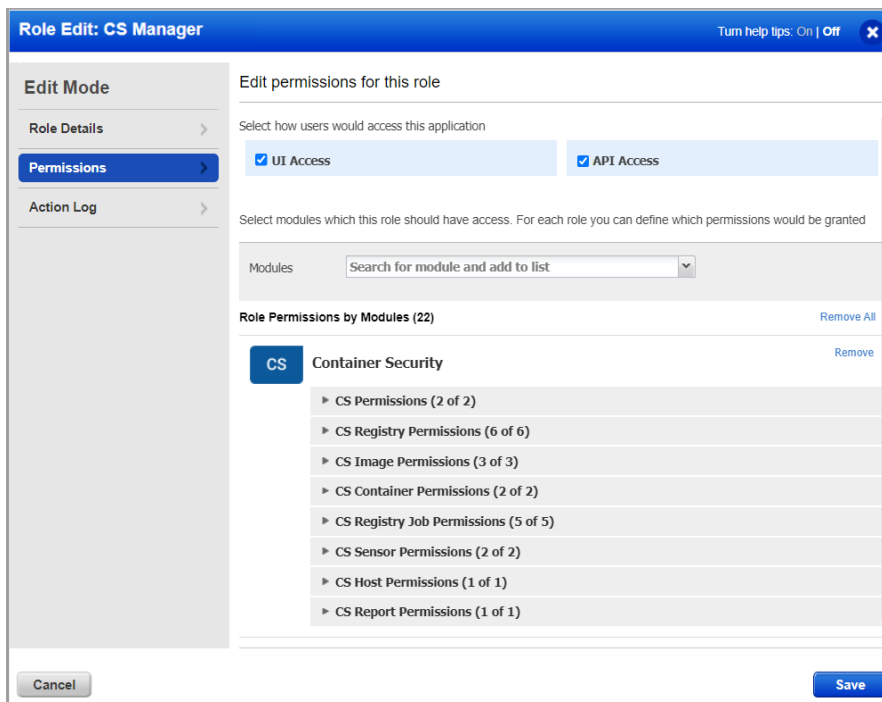
3) Select **View** from the Quick Actions menu for any role in the list to see the permissions associated with the role, or **Edit** to make changes to the permissions. When you change the permissions for a role, all users with the role will be affected by the changes.



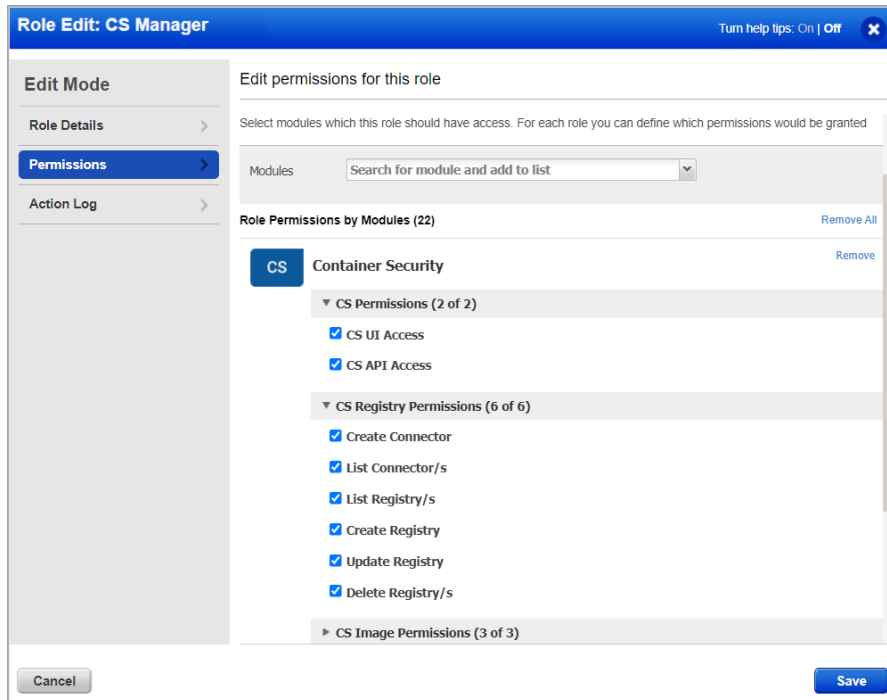
4) Go to the **Permissions** tab to view permissions for the selected role. At the top, you'll see Global UI and API access permissions. For Container Security module access and permissions, click the **Change** link under **Role Permissions by Modules**.



Permissions are grouped by object like registry, image, container, host, etc.



5) Expand any group of permissions to see the individual permissions within the group. Note the **CS UI Access** and **CS API Access** permissions. You'll need to assign these permissions to give users the ability to log into the Container Security UI and API. Click **Save** after making any changes to the role permissions.



How to Remove Permissions from an Existing User

All users existing prior to the Container Security 1.17 release will automatically get the “CS Manager” role which gives them all Container Security permissions. If you want to limit the permissions for a particular user, then you’ll need to create a custom role and select only the permissions the user should be granted. Then, edit the user account from the **Users > User Management** tab in the **Administration** utility. Remove the “CS Manager” role from the user since this gives the user all permissions, and assign the new custom role to the user.

How to Add New Users

Any Manager can add new users and assign them roles and permissions. You can add users from the **Administration** utility.

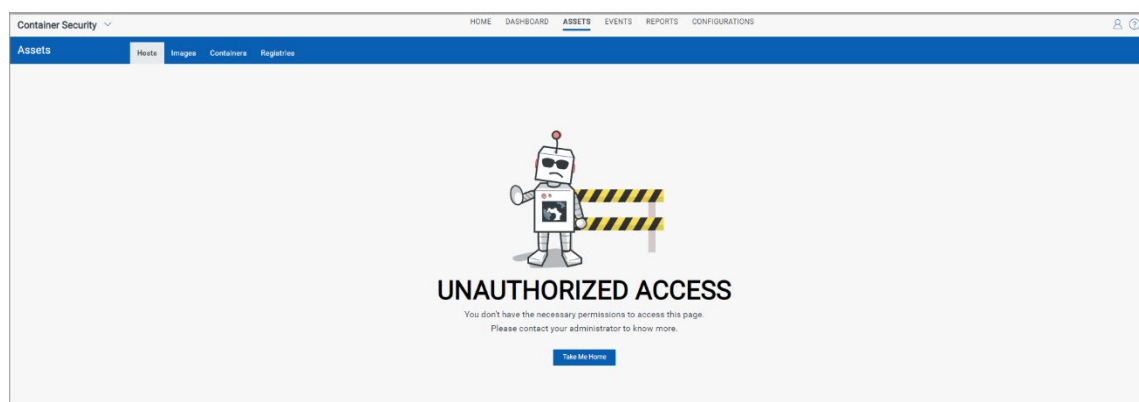
- 1) Choose **Administration** from the application picker.
- 2) Go to the **Users > User Management** tab.
- 3) From the **Create User** menu, choose one of the following options:
 - **Create Reader User** – The user will be assigned the following roles automatically: VM User, Reader, Reporting Reader. The user will not be assigned any Container Security roles/permissions automatically. You’ll need to edit the user account to add CS roles.
 - **Create Manager User** – The user will have all roles assigned, full permissions and scope. Manager users have access to the **Administration** utility.

4) Define the user settings. For help with settings, click the **Launch Help** link in the upper right corner. Once you've added the user, we'll send them a welcome email with login instructions.

5) For a non-Manager user, you'll need to edit the user's settings to assign the user Container Security roles and permissions. From the **User Management** tab, choose **Edit** from the Quick Actions menu. Go to the **Roles and Scopes** tab to assign roles that you've already defined.

When a User Does Not Have Permission to Perform an Action

If a user is not granted a particular permission then the user will not be able to perform the related action from the UI or API. When a user does not have the List permission for an object, then the user will not be able to view the related data list in the UI or fetch the list from the API. In the UI, you'll see an **Unauthorized Access** message when you do not have permission to view the list. In the example below, the user does not have the List Hosts permission.



If the user has the List permission but does not have other permissions like Create, Update, and Delete, then the list will be visible to the user, but the button or menu option for the action will not be visible. For example, if the user does not have the Create Registry permission then the user will not see the New Registry button and will not be able to create registries from the API.

From the API, when a user makes an API call but doesn't have the required permission, the user will get a **403 FORBIDDEN** error in the response similar to the one shown below. The user will need to reach out to a Manager user to request the permission.

```
"errorCode" : "403 FORBIDDEN",  
"message": "The joe_user user does not have the CS.IMAGE.VIEW permission to perform  
this operation. Ensure that required permissions are assigned to the user",  
"timestamp": 1654169949515
```

Introducing Sensor Profiles for Registry Sensors

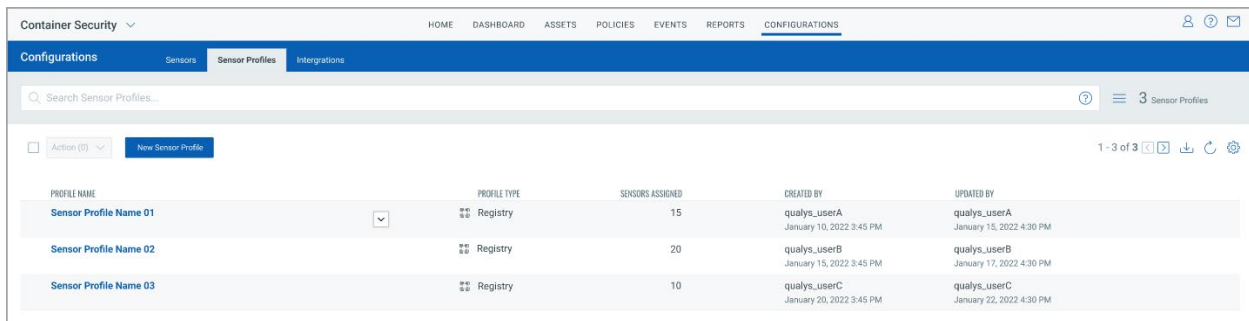
Now users can configure sensor profiles to control which sensors are used for scanning different registries. Each profile associates a list of registries with a list of sensors that can scan them. This is especially useful when you have sensors that don't have Internet access and are not able to scan cloud-based registries. Now you can create a profile with your cloud-based registries and include only the sensors that can reach them for scanning. Using sensor profiles will make registry scanning more efficient and improve performance.

Good to Know

- You can assign only one sensor profile to each registry.
- The same profile can be assigned to multiple registries.
- At scan time, only sensors associated with a registry in the profile will be used for the scan job.
- If a registry is not included in a sensor profile, then any sensor can be used to scan it.

Manage Sensor Profiles

Sensor profiles will be listed under **Configurations** on the new **Sensor Profiles** tab. This is where you'll create profiles and manage your profiles (view, update and delete).



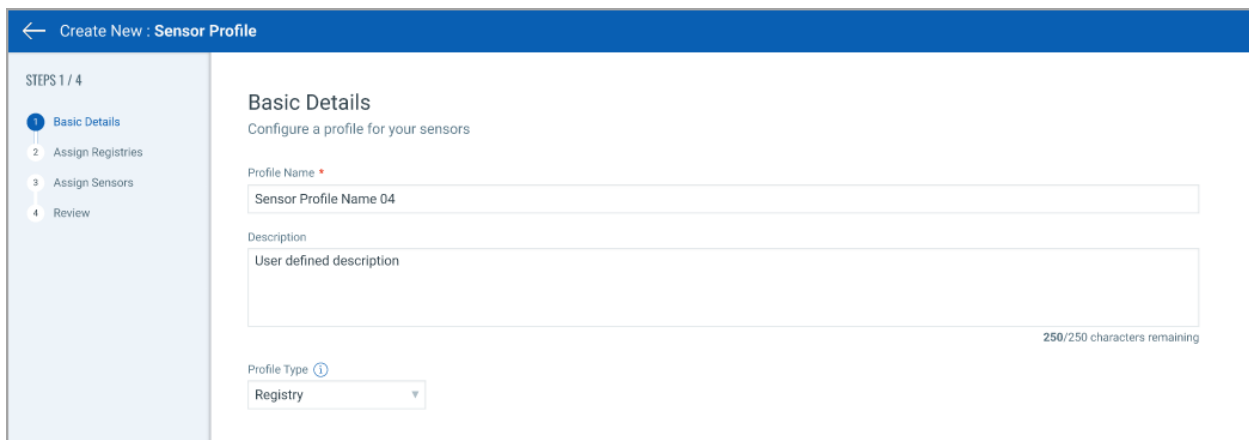
The screenshot shows the 'Configurations' section of the Container Security interface. The 'Sensor Profiles' tab is active, displaying a table with the following data:

PROFILE NAME	PROFILE TYPE	SENSORS ASSIGNED	CREATED BY	UPDATED BY
Sensor Profile Name 01	Registry	15	qualys_userA January 10, 2022 3:45 PM	qualys_userA January 15, 2022 4:30 PM
Sensor Profile Name 02	Registry	20	qualys_userB January 15, 2022 3:45 PM	qualys_userB January 17, 2022 4:30 PM
Sensor Profile Name 03	Registry	10	qualys_userC January 20, 2022 3:45 PM	qualys_userC January 22, 2022 4:30 PM

Create New Sensor Profiles

To create a new profile, go to **Configurations > Sensor Profiles**, and click **New Sensor Profile**.

On the **Basic Details** tab, give your profile a name and a description (optional). Then choose the profile type. Only "Registry" profile type is supported at this time.



The screenshot shows the 'Create New Sensor Profile' form. The 'Basic Details' tab is active, and the form contains the following fields:

- Profile Name:** Sensor Profile Name 04
- Description:** User defined description (250/250 characters remaining)
- Profile Type:** Registry

On the **Assign Registries** tab, add one or more registries to the profile. These are the registries that will be scanned by the sensors added to the same profile.

REGISTRY NAME	REGISTRY URI	TYPE	TOTAL IMAGES
<input type="checkbox"/> Registry Name 01	https://registry-1.docker.io Last Scanned on: Feb 08, 2022	Docker V2-Private	15
<input type="checkbox"/> Registry Name 02	https://registry-1.docker.io Last Scanned on: Feb 08, 2022	Google Cloud Registry	15
<input type="checkbox"/> Registry Name 03	https://registry-1.docker.io Last Scanned on: Feb 08, 2022	Google Cloud Registry	20
<input type="checkbox"/> Registry Name 04	https://registry-1.docker.io Last Scanned on: Feb 08, 2022	AWS ECR	15
<input type="checkbox"/> Registry Name 05	https://registry-1.docker.io Last Scanned on: Feb 08, 2022	Google Cloud Registry	26

On the **Assign Sensors** tab, add one or more sensors to the profile. These are the sensors that will be used to scan the registries in profile.

SENSOR	STATUS	ARCHITECTURE	VERSION	HOST
<input type="checkbox"/> 234adcaa50r4 qualys-container-sensor Created On: Jan 05, 2022	Running 30 minute ago	x86_64	1.10.1-0	qualys-virtual-machine 10.115.108.126
<input type="checkbox"/> 456adcaa50u8 qualys-container-sensor Created On: Jan 05, 2022	Running 40 minute ago	x86_64	1.10.1-0	suse12sp4ent2 10.115.108.126
<input type="checkbox"/> 789adcaa50s3 qualys-container-sensor Created On: Jan 05, 2022	Running 45 minute ago	x86_64	1.10.1-0	suse12sp4ent3 10.115.108.126
<input type="checkbox"/> 123adcaa50d4 qualys-container-sensor Created On: Jan 05, 2022	Running 28 minute ago	x86_64	1.10.1-0	suse12sp4ent5 10.115.108.126
<input type="checkbox"/> 549adcaaa450 qualys-container-sensor Created On: Jan 05, 2022	Running 17 minute ago	x86_64	1.10.1-0	suse12sp4ent6 10.115.108.126

Finally, on the **Review** tab, review all the details and click **Done** to save your profile. Your profile will be added to the **Sensor Profiles** list.

Search Sensor Profiles

The search field at the top of the **Sensor Profiles** list allows you to find sensor profiles by different criteria like the user-provided profile name, the profile UUID and the user login of the user who created or last updated the profile.

Updates to Create/Edit Registry: Name Field Added

Starting in this release, when adding a new registry to your account, you can give your registry a name. This will allow you to add the registry by name to sensor profiles.

← Create New: Registry

STEPS 1/2

1. Registry Information
2. Scan Settings

Registry sensor required.
Ensure that a registry sensor is deployed on a docker host which has access to the registry to pull images to scan.

Registry Information

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

Registry Name * ⓘ
Registry_Samplename 44 characters remaining

Registry Type *
Azure Container Registry

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

To authenticate, connect to Azure Container Registry

Connector *
Find Connector Create New

Cancel Next

← Edit: test

Edit Mode

Basic Information

Scan Jobs

Registry Information

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

Registry Name * ⓘ
test 59 characters remaining

Registry Type
Docker Hub

URL
https://registry-1.docker.io

Organization Name

Authentication

Username
qualysdemo

Password

Cancel Save