



Qualys Container Security

Release Notes

Version 1.7

November 20, 2020

Here's what's new in Container Security 1.7!

[Introducing a Policy Editor for Runtime Policies](#)

[View List of Tokens](#)

Container Security 1.7 brings you more improvements and updates! [Learn more](#)

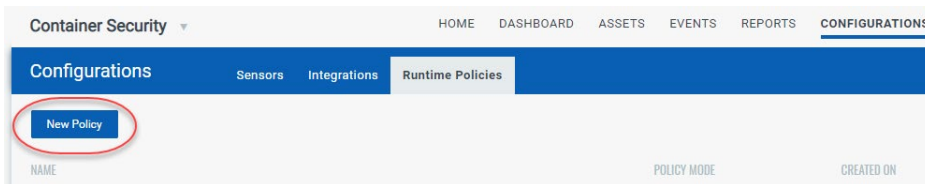
Introducing a Policy Editor for Runtime Policies

Applicable when Container Runtime Security (CRS) is enabled for your subscription.

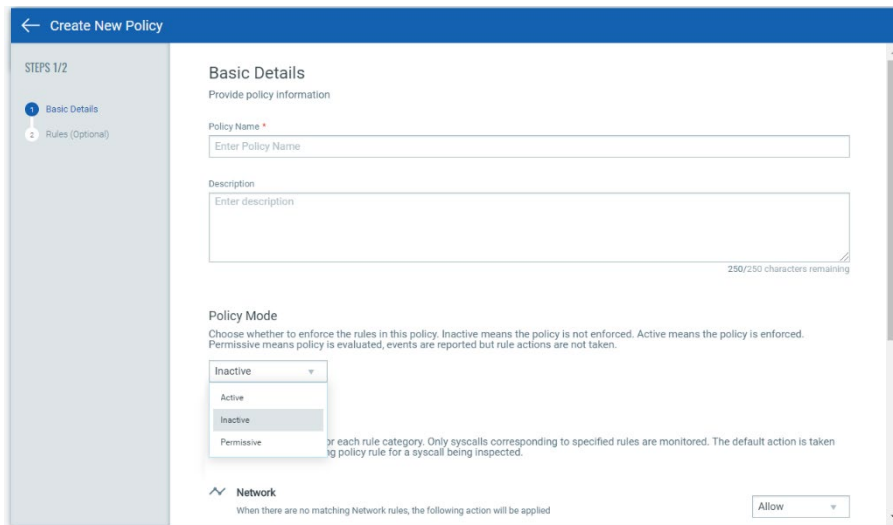
With this release you have the ability to create CRS policies directly from the Container Security UI. You can also now edit and delete policies, as needed. Prior to this release, policies could only be created using the Container Security API. Now all the policy management is in the UI, making managing your policies easier.

Create Policies

Go to **Configurations > Runtime Policies**, and then click the **New Policy** button.



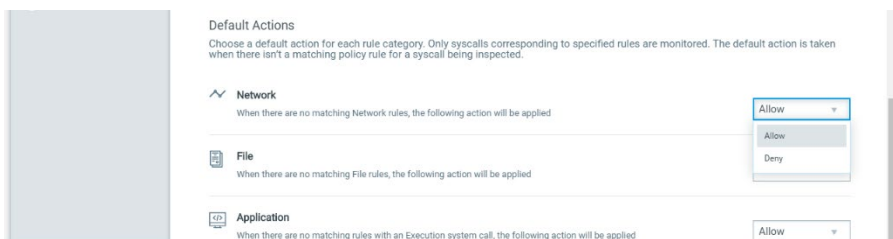
Under **Basic Details**, you'll provide a policy name and description, and choose a policy enforcement mode (Active, Inactive, Permissive). The option you pick determines whether or not the policy rules will be enforced on the containers that are spawned from the image.



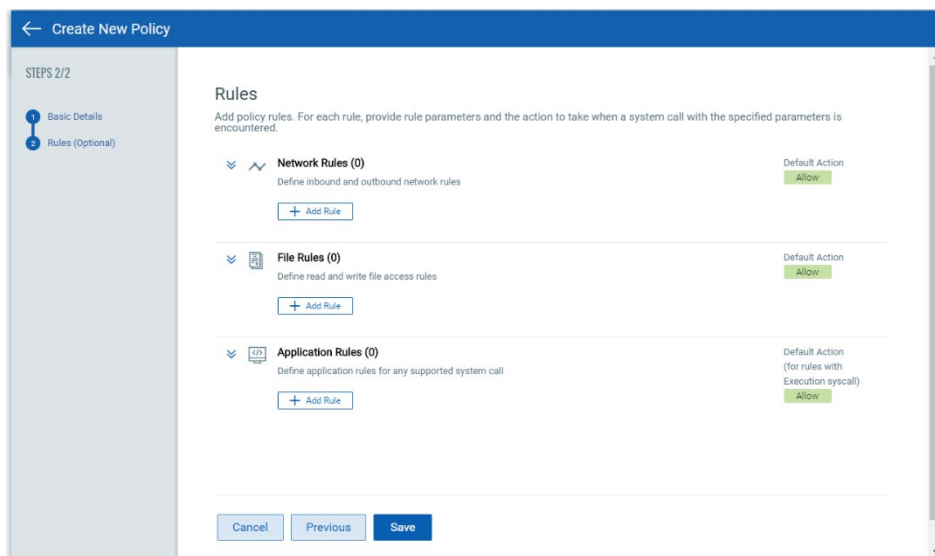
The policy is enforced only when Active is selected.

When Permissive is selected, the events are reported but actions are not enforced. Note that you can change this at any time after the policy is saved.

Next, choose a default action for each rule category. This is the action that will be taken unless there is a policy rule that overwrites this action. For example, choose Allow as the default action for Network rules to allow all inbound and outbound traffic to/from the instrumented container and then set up a specific rule to deny traffic to a particular IP address and port.



Go to the **Rules** tab to add policy rules. You can add as many rules as you like. Simply click the **Add Rule** button for Network Rule, File Rule or Application Rule.



For each new rule, give the rule a name, choose the rule type, set a rule action, and choose whether the rule is enabled or disabled. When you're done, click **Add Rule** to save it to your policy. Optionally, click **Save and Add another** to save the rule and create another rule of the same type. When you're done adding rules, click **Save**. Your new policy will appear on the **Runtime Policies** list where you can manage it.

Rule Types

Here's a look at the types of rules you can add to your policies and the parameters you'll need to provide for each rule type. For Network and File rules, we watch particular system calls by default. For Application rules, you'll pick the system call the rule applies to.

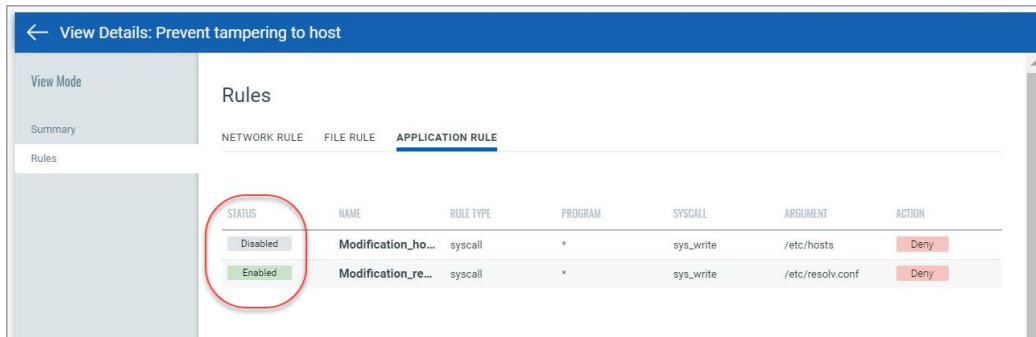
Rule Category	Rule Type	Default System Call	Rule Parameters	Description
Network	Network Outbound	sys_sendto	IP Address & Port (for the destination)	Allow, deny or monitor outbound traffic from the instrumented container to a particular IP and port
Network	Network Inbound	sys_accept	IP Address & Port (for the source)	Allow, deny or monitor inbound traffic from a particular IP and port to the instrumented container
File	Read	sys_open	Program & File	Allow, deny or monitor read access to a particular file by a particular program
File	Write	sys_write	Program & File	Allow, deny or monitor write access to a particular file by a particular program
Application	Syscall	user selected system call	Program, Argument 1, Argument 2, Argument 3	This is an advanced rule type. You must be familiar with the selected system call to know the arguments, if any, that must be defined. Note that rule with an Execution syscall only applies to the parent program defined in the rule and not child programs spun up from the parent program. In other words, the child program may be allowed to execute a file that the parent program is prevented from executing. Use * to prevent all programs from executing a certain file.

Rule Type Changes

You'll notice that some of the rule types have changed. Listener rules are now Network Inbound and Network rules are now Network Outbound. File rules are now Read, and the Write rule type was added.

View Rule Status in Policy Details

Now when you view details for a policy by picking View Details from the Quick Actions menu you'll see the rule status (Enabled or Disabled) in a new column, as shown below.

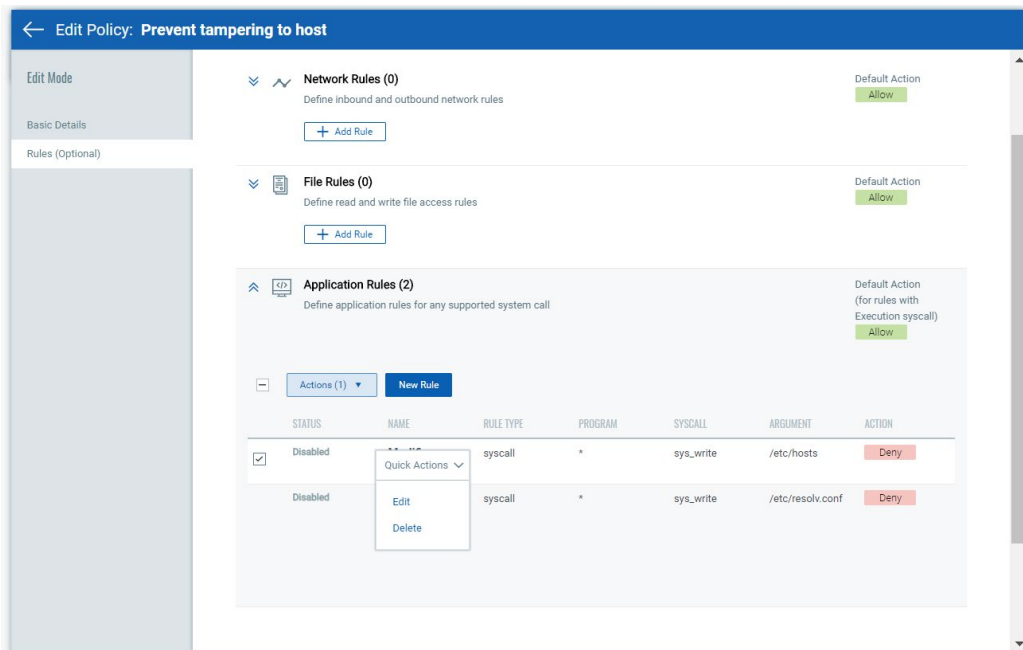


STATUS	NAME	RULE TYPE	PROGRAM	SYSCALL	ARGUMENT	ACTION
Disabled	Modification_ho...	syscall	*	sys_write	/etc/hosts	Deny
Enabled	Modification_re...	syscall	*	sys_write	/etc/resolv.conf	Deny

Edit Policies

Go to **Configurations > Runtime Policies**, and pick **Edit** from the Quick Actions menu to make changes to a policy. You can make changes to any of the policy settings - the policy name, description, policy mode, default actions and policy rules.

On the **Rules** tab, expand the Network Rules, File Rules or Application Rules section to see all the rules for that type. Then edit and delete individual rules. Click **Save** when you're done.



STATUS	NAME	RULE TYPE	PROGRAM	SYSCALL	ARGUMENT	ACTION
Disabled	Modification_ho...	syscall	*	sys_write	/etc/hosts	Deny
Disabled	Modification_re...	syscall	*	sys_write	/etc/resolv.conf	Deny

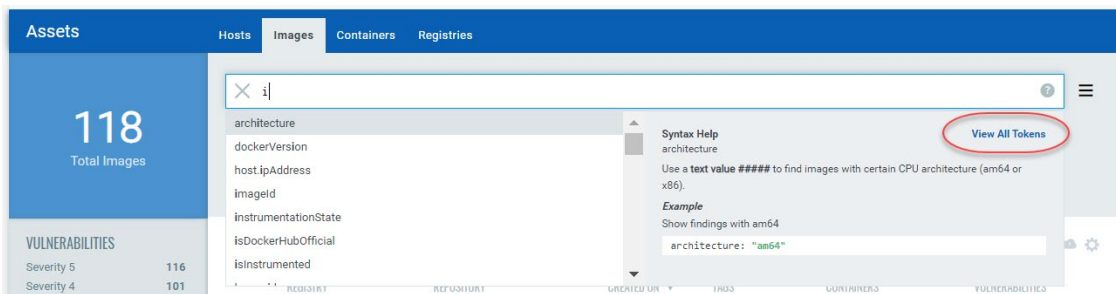
Delete Policies

Go to **Configurations > Runtime Policies**, and pick **Delete** from the Quick Actions menu for the policy you want to remove. Note that you can only delete policies that are not currently associated with instrumented images/containers. You'll see an Error if the policy is associated with an image/container. In this case, you must disassociate the policy and then try again.

Tip - To find instrumented images/containers, go to **Assets > Images** or **Assets > Containers** and use the search query `isInstrumented:true`

View List of Tokens

You can now access a complete list of QQL tokens that are supported for a search query on each tab. Just click the **View All Tokens** link in the token help and the list of all supported tokens for the tab/sub-tab with examples is displayed.



Click **?** in any search bar to see “How to Search” help.

Issues Addressed

- We fixed an issue where users were seeing a Scan Job Error when scanning Azure Registry with more than 100 repositories.
- We fixed an issue where the Created date for a policy was shown as Jan 01, 0001 when the policy name was changed. Now the correct date is shown.
- We fixed an issue where the sensor status was not consistent across the UI and API. Now the same logic is used to show the sensor status on the Sensors list in the UI and the Get sensors list using API.
- Now you'll get a 400 Bad Request error code when a Get Containers API request is missing the container ID.
- Now the response for the API to build a security policy based on container's behavior (`/csapi/v1.2/runtime/containers/{containerSha}/template`) correctly shows PolicyID in the response instead of TemplateID.
- The syntax help for the containerRuntime search token (used to search sensors) has been updated to correctly show possible values in uppercase characters.
- We fixed a typo in the screen text on the Instrument Image page.