



Tenable Enclave Security Container Security 1.6.x User Guide

Last Updated: December 10, 2025



Table of Contents

Welcome to Container Security for Tenable Enclave Security	4
Install Container Security	4
System Requirements	4
Settings and Information	8
Dashboard	9
Vulnerabilities	10
Export a Vulnerability	10
Assets	11
Images	11
View Image Details	11
Export an Image	12
Delete an Image	12
Packages	13
View Package Details	13
Layers	13
View Layer Details	13
Policies	14
Create a Policy	14
View Policy Details	16
Activate or Deactivate a Policy	17
Edit a Policy	19
Scans	20
Create a Scan	20



Configure a CI/CD Scan	22
Configure CI/CD Scan Policies	23
Edit a Scan	28
Run a Scan	28
Delete a Scan	28
Scan Settings	29
Asset Expiration	30
Scanners	33
Scanners	33
Add a Scanner	33
Edit a Scanner	35
Update a Scanner	35
Delete a Scanner	36
Deployments	37
Add a Deployment Scanner	37
Install a Deployment Assessment Agent	38
Edit a Deployment Scanner	43
Delete a Deployment Scanner	44
Reporting	45



Welcome to Container Security for Tenable Enclave Security

Container Security stores and scans container images as the images are built, before production. It provides vulnerability and malware detection, along with continuous monitoring of container images. By integrating with the continuous integration and continuous deployment (CI/CD) systems that build container images, Container Security ensures every container reaching production is secure and compliant with enterprise policy.

Container Security comes bundled with Tenable Enclave Security. For details about Tenable Enclave Security, see the [Tenable Enclave Security user guide](#).

Note: To access Container Security, you must be logged in to Tenable Enclave Security as an organizational user. Admin users do not have access to Container Security.

See the following pages for information about using Container Security.

[Install Container Security](#)

[System Requirements](#)

Install Container Security

For instructions on how to install Tenable Enclave Security, see [Install Tenable Enclave Security](#) in the *Tenable Enclave Security user guide*.

For information about licensing Container Security, see [License Requirements](#) in the *Tenable Enclave Security user guide*.

System Requirements

For more information about Tenable Enclave Security system requirements, see [System Requirements](#) in the *Tenable Enclave Security user guide*.

This page describes the following system requirements:

- [Requirements for Container Security services](#)
 - [Database Changes in Container Security 1.6](#)
- [Self-hosted database requirements](#)



- [Cloud database requirements](#)
 - [AWS](#)
 - [Azure for PostgreSQL flexible servers](#)
 - [GCloud](#)
- [System Requirements](#)

Requirements for Container Security Services

Service Name	# of Assets Managed by Container Security	CPU per pod	Memory per pod
tes-consec-ui	1 to 25,000 images	4000 m	4 GiB
tes-consec-api	1 to 25,000 images	4000 m	6 GiB
tes-consec-tvdl	1 to 25,000 images	4000 m	15 GiB
tes-consec-policy	1 to 25,000 images	4000 m	6 GiB
tes-consec-scan	1 to 25,000 images	4000 m	10 GiB

Database Changes in Container Security 1.6

Beginning in version 1.6, Container Security uses the database only and does not provision Persistent Volume Claims (PVC). When you upgrade to version 1.6, your existing data will be migrated from the PVC to the database.

The following are considerations for upgrading to Container Security 1.6:

- If the migration succeeds, the existing PVC will be deleted after 30 days.
- If the migration fails, the PVC will be deleted after 60 days. The data on the PVC will be recreated in the database when you run your first full scan after upgrading.



- There is no impact to Container Security features if the migration fails. The first full scan may run slower.
- Container Security 1.6 does not support database restore from database backups of previous Container Security versions.

Note: Tenable does not recommend doing a helm rollback to a previous Container Security release after upgrading to version 1.6. This can cause data drift, as previous versions use PVCs for scan data storage.

Self-Hosted Database Requirements

A self-hosted database is a database that you install and manage on your physical server or virtual machine. For example, PostgreSQL on a local server.

Requirements for Container Security self-hosted database

# of Assets Managed by Container Security	CPU	Memory	Disk Space
1 to 1,000 images	2000 m	16 GiB	10 GB
1,001 to 5,000 images	4000 m	32 GiB	15 GB
5,001 to 25,000 images	8000 m	64 GiB	20 GB

Cloud Database Requirements

A cloud database is a database service that is hosted and managed on a cloud platform. For example, AWS, Azure, or GCloud.

Requirements for Container Security database in AWS

# of Assets Managed by Container Security	Instance Type	Read Replica	Disk Space
1 to 1,000 images	db.r6g.large	db.r6g.large	10 GB
1,001 to 5,000 images	db.r6g.xlarge	db.r6g.xlarge	15 GB
5,001 to 25,000 images	db.r6g.2xlarge	db.r6g.2xlarge	20 GB

Requirements for Container Security database in Azure for PostgreSQL flexible servers



# of Assets Managed by Container Security	Instance Type	Read Replica	Disk Space
1 to 1,000 images	E2s_v3 / E2ds_v4	E2s_v3 / E2ds_v4	10 GB
1,001 to 5,000 images	E4s_v3 / E4ds_v4	E4s_v3 / E4ds_v4	15 GB
5,001 to 25,000 images	E8s_v3 / E8ds_v4	E8s_v3 / E8ds_v4	20 GB

Requirements for Container Security database in GCloud

# of Assets Managed by Container Security	Instance Type	Read Replica	Disk Space
1 to 1,000 images	2 vCPU, 16 GB	2 vCPU, 16 GB	10 GB
1,001 to 5,000 images	4 vCPU, 32 GB	4 vCPU, 32 GB	10 GB
5,001 to 25,000 images	8 vCPU, 64 GB	8 vCPU, 64 GB	20 GB



Settings and Information

To view your Container Security settings, in the top navigation, click  **Settings & Information**.

In the **Settings & Information** menu, you can view the following:

- **Access Control** - For more information, see [Access Control](#) in the *Tenable Enclave Security user guide*.
- **System Logs** - For more information, see [System Logs](#) in the *Tenable Enclave Security user guide*.



Dashboard

The **Dashboard** page in Container Security contains widgets that display high-level information about your containers, images, image repositories, and policies. Click a widget on the dashboard to view details about the item type or to import data items into Container Security.



Vulnerabilities

To view the **Vulnerabilities** page, in the left navigation, click **Vulnerabilities**.

The **Vulnerabilities** page displays a list of all vulnerabilities discovered by Container Security scans.

For more information, see the following topics:

[Export a Vulnerability](#)

Export a Vulnerability

To export a vulnerability:

1. In the left navigation, click **Vulnerabilities**.

The **Vulnerabilities** tab appears, which displays a list of vulnerabilities detected by Container Security.

2. In the table, right-click the row for a vulnerability, and click **Export Vulnerability**.

The **Export** window appears.

3. In the **File Name** box, type a name for the export file.
4. In the **Configuration** section, select the fields you want to include in the export file.
5. Click **Export**.

The export file downloads.



Assets

To view the **Assets** page, in the left navigation, click **Assets**.

On the **Assets** page, you can view the container registries that Container Security is scanning, and the associated images, packages, and layers.

In the left panel, you can search for a registry or repository. Clicking a registry or repository filters the table on the right.

For more information, see the following topics:

[Images](#)

[View Image Details](#)

[Export an Image](#)

[Delete an Image](#)

[Packages](#)

[View Package Details](#)

[Layers](#)

[View Layer Details](#)

Images

To view your images, in the left navigation, click **Assets > Images**.

In the left panel, you can search for a registry or repository. Clicking a registry or repository filters the list of images on the left.

Select **Show Only Base Images** to filter the list by the base image of each registry.

For more information, see the following topics:

[View Image Details](#)

[Export an Image](#)

[Delete an Image](#)

View Image Details



To view the details for an image:

1. In the left navigation, click **Assets > Images**.

The **Images** tab appears, which displays a list of images from your scanned repositories.

2. In the table, click the row for an image.

The right pane appears, which displays details for the image.

Export an Image

To export an image:

1. In the left navigation, click **Assets > Images**.

The **Images** tab appears, which displays a list of images from your scanned repositories.

2. In the table, right-click the row for an image, and click **Export Image**.

The **Export** window appears.

3. In the **File Name** box, type a name for the export file.
4. In the **Configuration** section, select the fields you want to include in the export file.
5. Click **Export**.

The export file downloads.

Delete an Image

Deleting a Container Security image also deletes all associated packages, layers, and vulnerabilities.

To delete an image:

1. In the left navigation, click **Assets > Images**.

The **Images** tab appears, which displays a list of images from your scanned repositories.

2. In the table, right-click the row for an image, and click **Delete**.

A window appears, confirming that you want to delete the asset.

3. Click **Delete**.

The image is deleted, including all of the image's packages, layers, and vulnerabilities.



Packages

To view your packages, in the left navigation, click **Assets > Packages**.

For more information, see the following topic:

[View Package Details](#)

View Package Details

To view the details for a package:

1. In the left navigation, click **Assets > Packages**.

The **Packages** tab appears, which displays a list of packages from your scanned repositories.

2. In the table, click the row for a package.

The right pane appears, which displays details for the package.

Layers

To view your images, in the left navigation, click **Assets > Layers**.

For more information, see the following topics:

[View Layer Details](#)

View Layer Details

To view the details for a layer:

1. In the left navigation, click **Assets > Layers**.

The **Layers** tab appears, which displays a list of layers from your scanned repositories.

2. In the table, click the row for a layer.

The right pane appears, which displays details for the layer.



Policies

Note: The **Policy Builder** replaces the [old method](#) of creating CI/CD scan policies in Container Security.

A Container Security policy defines criteria for CI/CD pipelines or Kubernetes clusters. You can define policies to send alerts or block deployments when a pipeline or cluster does not meet the criteria defined by the policy.

To view your policies, in the left navigation, click **Policies**. The **Policies** page appears.

Create a Policy

Note: The **Policy Builder** replaces the [old method](#) of creating CI/CD scan policies in Container Security.

A Container Security policy defines events that are noteworthy in the network. When an event occurs that meets the conditions outlined in a policy, Container Security logs the event and sends alerts or blocks deployments in accordance with the policy definition.

To create a policy in Container Security:

1. In the left navigation, click **Policies**.

The **Policies** page appears, which displays a list of your policies.

2. At the top of the table, click **Add Policy**.

The **Policy Builder** page appears.

3. In the **Details** section, configure the policy category, name, and description.

- a. In the **Category** drop-down, select the policy category:

- **CI/CD** - detect security and quality issues in the build pipeline.
- **Kubernetes** - detect misconfigurations and vulnerabilities in Kubernetes clusters.

- b. In the **Name** box, type a name for the policy.



- c. (Optional) In the **Description** box, type a description for the policy.
 - d. Click **Next**.
4. In the **Definition** section, select how Container Security will enforce the policy, and create a query to define the policy conditions.
- a. In the **Action** section, select the action that occurs when an event meets the policy conditions:
 - **Block Deployment** - if an image meets the policy conditions, Container Security blocks the deployment.
 - or-
 - **Alert** - if an image meets the policy conditions, Container Security sends a notification about the image.

Note: Policy failures will list the events that met the policy conditions. Policy successes will list the events that did not meet the policy conditions, and were therefore successful.

- b. In the **Rule 1** box, type a query or build a query using the drop-down to select filters, operators, and values.
- c. (Optional) To add another query to the policy, click **Add Rule**.

The **And/Or** buttons and **Rule 2** box appear.

- Click **And** or **Or** to define how the policy uses the rules
- In the **Rule 2** box, define a second rule.
- Click **Add Rule** to add as many rules as desired.
- To delete a rule, click the  button to the right of the rule. Each policy must have at least one rule.

- d. Click **Next**.
5. In the **Scope** section, select the pipeline or cluster for the policy.



- a. Enable the **Activate upon completion** setting to XYZ.
- b. Depending on the **Category** you chose in the **Details** section, define the pipeline or cluster for the policy scope:
 - **CI/CD** category
 - In the **Pipeline Type** drop-down, select the type of pipeline to which the policy applies (for example, Jenkins or Azure DevOps).
 - In the **Pipeline Name** drop-down select the pipeline for the policy.
 - (Optional) to add more pipelines, click **Add Pipeline**.
 - (Optional) To delete a pipeline from the policy, click the  button to the right of the **Pipeline Type** box. Each CI/CD policy must specify at least one pipeline.
 - **Kubernetes** category
 - In the **Cluster** drop-down, select one or more clusters for the policy.
 - (Optional) To delete a cluster from the policy, click the X button to the right of the cluster name.
 - (Optional) To delete all clusters from the policy, click the X button on the right side of the **Cluster** drop-down.

6. Click **Save**.

The **Policies** page appears, and the new policy appears in the table. By default, the policy is Inactive.

View Policy Details

Note: The **Policy Builder** replaces the [old method](#) of creating CI/CD scan policies in Container Security.

To view the details for a policy:



1. In the left navigation, click **Policies**.

The **Policies** page appears, which displays a list of your policies.

2. In the table, click the row for the policy you want to view.

The right panel appears, which displays the policy details:

- The **Status** tab displays the policy settings configured in [Create a Policy](#).
 - **Definition** - The policy actions and rules.
 - **Scope** - The pipeline or cluster to which the policy applies.
- The **History** tab displays the policy evaluations and their outcomes. Use the buttons above the tab titles to filter the policy history.
 - Click the **Policy Evaluations** button to view all policy evaluations.
 - Click the **Policy Failures** button to filter the **History** list by the pipelines or clusters that failed to meet the policy conditions.
 - Click the **Policy Success** button to filter the **History** list by the pipelines or clusters that met the policy conditions.
 - In the **History** tab, use the text box to type a custom query or build a query using the drop-down to select filters, operators, and values.
 - Use the drop-down in the **History** tab to sort the list by **Oldest First** or **Newest First**.

Activate or Deactivate a Policy

When you activate a policy, the policy will begin evaluating all CI/CD pipelines or Kubernetes clusters that meet the policy criteria defined in [Create a Policy](#).

To activate an inactive policy:

1. In the left navigation, click **Policies**.

The **Policies** tab appears, which displays a list of your policies.

2. Activate a single policy:



- a. In the table, right-click the row for an inactive policy, and click **Activate Policy**.

-or-

In the row for the inactive policy that you want to activate, click the **⋮** button, and click **Activate Policy**.

-or-

In the row for the inactive policy you want to activate, select the check box, and at the top of the table, click **Activate Policy**.

The policy is activated.

3. Activate multiple policies:

- a. In the row for the inactive policies you want to activate, select the check boxes, and at the top of the table, click **Activate Policies**.

The policies are activated.

To deactivate an active policy:

1. In the left navigation, click **Policies**.

The **Policies** tab appears, which displays a list of your policies.

2. Deactivate a single policy:

- a. In the table, right-click the row for an active policy, and click **Deactivate Policy**.

-or-

In the row for the active policy that you want to deactivate, click the **⋮** button, and click **Deactivate Policy**.

-or-

In the row for the active policy you want to deactivate, select the check box, and at the top of the table, click **Deactivate Policy**.

The policy is activated.

3. Deactivate multiple policies:



- a. In the row for the active policies you want to deactivate, select the check boxes, and at the top of the table, click **Deactivate Policies**.

The policies are deactivated.

Edit a Policy

To edit a policy:

1. In the left navigation, click **Policies**.

The **Policies** tab appears, which displays a list of your policies.

2. In the table, right-click the row for the policy you want to edit, and click **Edit**.

-or-

In the row for the policy you want to edit, select the check box, and at the top of the table, click **Edit**.

-or-

In the row for the policy you want to edit, click the **:** button, and click **Edit**.

The **Edit Policy Builder** window appears.

3. Modify the policy settings as needed. See [Create a Policy](#) for more information about policy settings.
4. Click **Save** to save the policy.



Scans

To view your scans, in the left navigation, click **Scans**.

On the **Scan Management** page, you can configure Container Security scans to collect data about your containers for analysis. Depending on your organization, one person may perform all the steps, or several people may share the steps.

For more information, see the following topics:

[Create a Scan](#)

[Configure a CI/CD Scan](#)

[Configure CI/CD Scan Policies](#)

[Edit a Scan](#)

[Run a Scan](#)

[Delete a Scan](#)

[Scan Settings](#)

[Asset Expiration](#)

Create a Scan

By default, Container Security scans will scan all images in a registry. To scan a single image, see [Configure a CI/CD Scan](#).

Before you begin:

- [Add a Scanner](#).
- Configure [Scan Settings](#).

To create a scan:

1. In the left navigation, click **Scans > Scans**.

The **Scans** tab appears, which displays a list of your scans.

2. At the top of the table, click **Add Scan**.



The **Add Scan** window appears.

3. In the **Name** box, type a name for the scan.
4. In the **Scanner** box, select a Container Security scanner that you configured in [Add a Scanner](#).
5. In the **Registry URL** box, type the URL for the registry that you want to scan.

Note: Scan settings may affect the results of the scan. For more information, see [Scan Settings](#).

6. In the **Registry Type** box, select the type of registry that you want to scan. The following are the available registry types:
 - Docker
 - DockerHub
 - Jfrog
 - Harbor
 - AWS ECR
 - Azure ACR
 - Quay
 - Nexus
7. (Optional) In the **Username** box, type the username that Container Security will use to authenticate to the registry.
8. (Optional) In the **Password** box, type the password that Container Security will use to authenticate to the registry.
9. (Optional) Enable **Schedule Scan**.
 - a. In the **Start On** box, select the date you want the scan to start running.
 - b. In the **Time** box, select the time of day you want the scan to start running.



- c. In the **Time Zone** box, select the time zone for the scan schedule.
- d. In the **Frequency** box, select how often you want the scan to run.

10. Select **Save** to save the scan.

-or-

Select **Save and Run** to start running the scan immediately.

Configure a CI/CD Scan

Note: In Tenable Enclave Security 1.5 and later, this process is replaced by [Scan Policies](#).

This topic describes how to scan a single image. For instructions on how to scan all images in a registry, see [Create a Scan](#).

Before you begin:

- Download the image you want to scan to your local machine.
- [Add a Scanner](#).

Scan a single image:

1. Ensure the image you want to scan is available locally.
 - To pull an image from a registry to the same host as your scanner, use the following command:

```
docker pull <image-name>:<image-tag>
```

Where `<image-name>:<image-tag>` is the image you want to scan.

-or-



- To build an image on the same host as your scanner, use the following command:

```
docker build -f Dockerfile --tag <image-name>:<image-tag> .
```

Where `<image-name>:<image-tag>` is the image you want to scan.

2. In the CLI of the machine where you want to run the scanner, run the customized configuration and command for your deployment type using the following parameters:

```
./consec image \  
--pipeline-name <your-pipeline-name> \  
--pipeline-type JENKINS \  
--policy-config <tes_policy.json> \  
<image-name>:<image-tag>
```

Where:

- `pipeline-name` is the name that appears in the UI.
- `pipeline-type` is the type of CI/CD pipeline provider. If you do not include a pipeline type, this field defaults to *CUSTOM*.
- `policy-config` is the path to the scan policy that you created in [Configure CI/CD Scan Policies](#). If you do not include a scan policy, then the scan will not perform policy configuration.

Note: To scan podman images, use the `--containers-storage` flag.

3. Press **Enter**.

Container Security scans the image.

Configure CI/CD Scan Policies

Note: In Tenable Enclave Security 1.5 and later, this process is replaced by [Scan Policies](#).

Before you can run a Container Security scan, you must create a CI/CD scan policy JSON file. Save this file on the same host as your Container Security scanner that you create in [Add a Scanner](#).

CI/CD scan policy conditions apply to the entire image, not individual plugins.



Structure of a CI/CD Scan Policy JSON File

Field	Description
policy_groups	A policy json file is a list of policy_groups. Each policy_group is a list of policy entries with boolean operators (group_operator) to join them.
group_operator	The group_operator field accepts only AND and OR. The group_operator applies to the list of entries.
entries	Each entries item contains a label, operator, field, and policy_value.
label	An arbitrary string that describes the policy entry. For example, "Cvssv3 cannot be greater than 7"
operator	The operation that you want to trigger policy violations on. Some fields only support the EQ operator. The following are the supported operators: • EQ - equal to (=). • NEQ - not equal to (≠). • GT - greater than (>). • GTE - greater than or equal to (≥). • LT - less than (<). • LTE - less than or equal to (≤).
field	Any of the fields you want to support policy evaluation on. The following are the supported fields: • CVE - only supports operator EQ. • PACKAGE - only supports operator EQ, where the value is of format <package_name>-<package_version>. • IAVM - only supports operator EQ. • SEVERITY - only supports values <i>LOW</i>, <i>MEDIUM</i>, <i>HIGH</i>, and <i>CRITICAL</i>. • VPR - only supports floating point numbers as values, from 0.0 to 10.0.



Field	Description
	• CVSS2 - only supports floating point numbers as values, from <i>0.0</i> to <i>10.0</i>. • CVSS3 - only supports floating point numbers as values, from <i>0.0</i> to <i>10.0</i>. • EPSS - only supports floating point numbers as values, from <i>0.0</i> to <i>100.0</i>.
policy_value	The value you want to match on to trigger a policy violation.

Example CI/CD Scan Policy JSON Files

Simple Policy

The following policy triggers a violation when the CVSS v3 score is greater than or equal to 7.

```
{
  "policy_groups": [
    {
      "entries": [
        {
          "label": "Cvssv3 cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "CVSS3",
          "policy_value": "7"
        }
      ],
      "group_operator": "OR"
    }
  ]
}
```

Policy with AND or OR operators

The following policy triggers a violation when:

- The CVSS v3 score is greater than or equal to 7.
- or-
- The VPR score is greater than or equal to 7.



```
{
  "policy_groups": [
    {
      "entries": [
        {
          "label": "Cvssv3 cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "CVSS3",
          "policy_value": "7"
        },
        {
          "label": "Vpr cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "VPR",
          "policy_value": "7"
        }
      ],
      "group_operator": "OR"
    }
  ]
}
```

The following policy triggers a violation when:

- The CVSS v3 score is greater than or equal to 7.
- and-
- The VPR score is greater than or equal to 7.

```
{
  "policy_groups": [
    {
      "entries": [
        {
          "label": "Cvssv3 cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "CVSS3",
          "policy_value": "7"
        },
        {
          "label": "Vpr cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "VPR",
          "policy_value": "7"
        }
      ],
      "group_operator": "AND"
    },
    {
      "entries": [
        {
          "label": "CVE-123 exists",
          "operator": "EQ",
          "field": "CVE",

```



```
        "policy_value": "123"
      }
    ],
    "group_operator": "OR"
  }
]
```

Complex Nested Policy

The following policy triggers a violation when:

- The CVSS v3 score is greater than or equal to 7, and the VPR score is greater than or equal to 7.
- OR
- The CVE is *cve-123*, or the package is *curl-1.1*.

```
{
  "policy_groups": [
    {
      "entries": [
        {
          "label": "Cvssv3 cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "CVSS3",
          "policy_value": "7"
        },
        {
          "label": "Vpr cannot be greater or equal to 7",
          "operator": "GTE",
          "field": "VPR",
          "policy_value": "7"
        }
      ],
      "group_operator": "AND"
    },
    {
      "entries": [
        {
          "label": "CVE-123 exists",
          "operator": "EQ",
          "field": "CVE",
          "policy_value": "123"
        },
        {
          "label": "curl-1.1 exists",
          "operator": "EQ",
          "field": "PACKAGE",
          "policy_value": "curl-1.1"
        }
      ],
      "group_operator": "OR"
    }
  ]
}
```



```
    "group_operator": "OR"  
  }  
]  
}
```

Edit a Scan

To edit a scan:

1. In the left navigation, click **Scans > Scans**.

The **Scans** tab appears, which displays a list of your scans.

2. In the table, right-click the row for the scan you want to edit, and click **Edit**.

The **Edit Scan** window appears.

3. Modify the scan settings as needed.
4. Select **Save** to save the scan.

-or-

Select **Save and Run** to start running the scan immediately.

Run a Scan

To run a scan:

1. In the left navigation, click **Scans > Scans**.

The **Scans** tab appears, which displays a list of your scans.

2. In the table, right-click the row for a scan, and click **Run**.

The scan starts running.

Delete a Scan

To delete a scan:



1. In the left navigation, click **Scans > Scans**.

The **Scans** tab appears, which displays a list of your scans.

2. In the table, right-click the row for a scan, and click **Delete**.

A window appears, confirming that you want to delete the scan.

3. Click **Delete**.

The scan is deleted.

Scan Settings

The **Scan Settings** tab displays your license utilization and configuration settings for Container Security scans.

The License Utilization section displays your current license usage. For more information, see [License Requirements](#). To reduce your license utilization, delete assets on the **Images** tab of the **Assets** page. For more information, see [Assets](#).

Use the fields below to point to the different registries that you want to scan for images. You can further refine this by explicitly indicating when to scan, the number of scans, and exactly where to scan.

Note: These settings do not apply to active scans. To apply these settings to an active scan, you must stop and restart the scan after saving the settings.

Option	Description
Global Settings	
Images with a build time less than	Images built in the last 90 days are scanned by default. You can customize this setting to scan images built within a minimum of 1 day or a maximum of 10,000 days; otherwise the default of 90 days will apply.
Maximum number of images to scan per repository	The default scan limit is 20 images per repository. You can customize this setting to scan a minimum of 1 image or a maximum of 100,000,000 images; otherwise, the default limit of 20 images will apply.



Option	Description
Live scans	Enable this setting to perform continuous vulnerability assessment against the existing container image inventory after each plugin feed update. Scheduled scans take priority in the queue over live scans and do not block plugin feed updates. Note: Live scans may take longer to process if they overlap with scheduled scans, because live scans have lower priority.
Scan Inclusion Use these fields to specify the registry, repository, and image tags to include in your scans. Container Security will prioritize matching images to consume available licenses in subsequently scheduled scans. Note: Using an asterisk (*) will include all.	
Registry Name	The name of the registry you want to prioritize in scans.
Repository Name	The name of the repository you want to prioritize in scans.
Tag	The image tags you want to prioritize in scans.
Scan Exclusion Use these fields to specify the registry, repository, and image tags to exclude from your scans. Container Security will exclude matching images from scans, and will not consume licenses in subsequently scheduled scans. Note: Using an asterisk (*) will include all.	
Registry Name	The name of the registry you want to exclude from scans.
Repository Name	The name of the repository you want to exclude from scans.
Tag	The image tags you want to exclude from scans.

Asset Expiration



The **Asset Expiration** tab displays your asset age-out settings for Container Security.

Note: These settings do not apply to active scans. To apply these settings to an active scan, you must stop and restart the scan after saving the settings.

Option	Description
Expiration Policy Settings	
Expire Assets	Enable this setting to set assets to expire relative to the last scan or image build time, as well as a maximum number of days before an asset expires. If you enable this setting and do not configure a schedule, then the assets that meet the Expire Assets criteria will be deleted immediately.
Expire Assets On This setting appears when you enable Expire Assets .	Select whether you want the asset expiration to be based on the last scan time or image build time. • Last Scan Time - The last time the asset was scanned or discovered. • Image Build Time - The last time the asset was built.
Expire Assets Older Than This setting appears when you enable Expire Assets .	Enter the number of days after the Last Scan Time or Image Build Time that you want an asset to expire.
Schedule Expiry	Enable this setting to delete all assets that meet the Expire Assets criteria on a regular interval.
Start On	Select the date for the scheduled expiration.
Time	Select the time for the scheduled expiration.
Time Zone	Select a time zone for the scheduled expiration.
Frequency	Select how often you want the scheduled expiration to run:



Option	Description
	• Once • Daily • Weekly • Monthly • On Demand



Scanners

To view your scanners, in the left navigation, click **Scanners**.

Container Security scanners can scan container images securely without sending the images outside your organization's network. A scanner takes an initial inventory, or snapshot, of the images you want to scan. You can then view the scan data for the images.

On the **Scanners** tab, you can view your Container Security scanners. On the **Deployments** tab, you can view your Container Security deployment scanners.

For more information, see the following topics:

[Scanners](#)

[Add a Scanner](#)

[Edit a Scanner](#)

[Update a Scanner](#)

[Delete a Scanner](#)

[Deployments](#)

[Add a Deployment Scanner](#)

[Install a Deployment Assessment Agent](#)

[Edit a Deployment Scanner](#)

[Delete a Deployment Scanner](#)

Scanners

With Container Security scanners, you can scan:

- A specific image exported from a registry and stored locally on the machine where you install the scanner.
- All images hosted in a specific registry (for example, a Docker registry).

Add a Scanner

Create a Container Security scanner:



1. In the left navigation, click **Scanners**.

The **Scanners > Scanners** tab appears, which displays a list of your scanners.

2. At the top of the table, click **Add Scanner**.

The **Add Scanner** window appears.

3. In the **Scanner Name** box, type a name for the scanner.
4. In the **Description** box, type a description for the scanner.
5. Select a platform for the scanner.
6. Click **Download**.

The scanner downloads to your local machine.

7. Move the scanner to your desired location using the following command:

```
mv ./consec.tar.gz
```

8. Activate the scanner using the following commands:

- a. Untar the Container Security CLI:

```
tar xvpf ./consec.tar.gz
```

- b. Allow executable permissions to the Container Security CLI binary file:

```
chmod +x consec
```

- c. Start the scanner:

```
./consec run
```

-or-

To scan a registry that is using a self-signed certificate, use the following command:



```
./consec run --insecure-registry=true
```

Note: If you are running CI/CD single image scans, you can skip this step. For more information, see [Configure a CI/CD Scan](#).

What to do next:

- [Create a Scan](#).

Edit a Scanner

To edit a scanner:

1. In the left navigation, click **Scanners**.

The **Scanners > Scanners** tab appears, which displays a list of your scanners.

2. In the table, right-click the row for the scanner you want to edit, and click **Edit**.

The **Edit Scanner** window appears.

3. Modify the scanner settings as needed.
4. Click **Save** to save the scan.

Update a Scanner

These steps describe how to update a Container Security scanner. When you update a scanner, a new scanner binary downloads. To start using the new scanner, move the scanner binary to the location you want to use the scanner.

To update a scanner:

1. In the left navigation, click **Scanners**.

The **Scanners > Scanners** tab appears, which displays a list of your scanners.

2. In the table, right-click the row for the scanner you want to update, and click **Update**.

The **Update Scanner** window appears.

3. Select **Refresh Scanner Key** to refresh the scanner key.



Note: Selecting this option will invalidate the existing scanner key.

4. Select **Update to Latest Version** to update the scanner to the latest version of Container Security.

5. Click **Download**.

The updated scanner downloads to your local machine.

6. Move the scanner to your desired location using the following command:

```
mv ./consec.tar.gz
```

7. Activate the scanner using the following commands:

a. Untar the Container Security CLI using the following command:

```
tar xvpf ./consec.tar.gz
```

b. Allow executable permissions to the Container Security CLI binary file:

```
chmod +x consec
```

c. Start the scanner:

```
./consec run
```

Delete a Scanner

To delete a scanner:

1. In the left navigation, click **Scanners**.

The **Scanners > Scanners** tab appears, which displays a list of your scanners.

2. In the table, right-click the row for the scanner you want to delete, and click **Delete**.

A window appears, confirming that you want to delete the scan.



3. Click **Delete**.

The scanner is deleted.

Deployments

A deployment scanner monitors a cluster for vulnerabilities, misconfigurations, and policy compliance before or during deployments.

On the **Scanners > Deployments** tab, you can view a list of your Container Security deployment scanners. After you create a deployment scanner in Container Security, you must [install a deployment assessment agent](#).

Add a Deployment Scanner

A deployment scanner monitors a cluster for vulnerabilities, misconfigurations, and policy compliance before or during deployments.

To add a deployment scanner:

1. In the left navigation, click **Scanners**.

The **Scanners** page appears.

2. Click the **Deployments** tab.

The **Deployments** tab appears, which displays a list of your deployment scanners.

3. At the top of the table, click **Add Deployment Scanner**.

The **Add Deployment Scanner** window appears.

4. In the **Scanner Name** box, type a name for the deployment scanner.
5. In the **Cluster Name** box, type a name for the cluster to which the deployment scanner is assigned. The text you type in the **Cluster Name** box will be the filename for the generated yaml file.
6. (Optional) In the **Description** box, type a description for the deployment scanner.
7. Click the **Save and Download** button.

The deployment scanner is saved and the scanner configuration yaml file downloads. At the bottom of the **Add Deployment Scanner** window, the **Scanner Information** section appears.



The **Scanner Information** section displays the **Scanner Key**, **Scanner Name**, **Cluster Name**, and **Scanner Key Expiration Date**.

What to do next:

- Use the downloaded scanner configuration yaml file to continue the installation steps in [Install a Deployment Assessment Agent](#).

Install a Deployment Assessment Agent

Deployment assessment agents evaluate the images being deployed in Kubernetes clusters against the image metadata and vulnerability information scanned by Container Security in prior CI/CD and registry scans. You can configure [policies](#) to define the actions taken by deployment assessments.

You can install a deployment assessment agent after you [create a deployment scanner](#) in Container Security.

How does a deployment assessment agent work?

A deployment assessment agent runs as a [dynamic admission controller](#) in a Kubernetes cluster. It receives validating admission webhook HTTP callbacks from the kube-apiserver and applies matching policies configured in Container Security to return results. For more information about creating policies, see [Policies](#).

- The agent receives an [AdmissionReviewRequest](#) for any POD CREATE/UPDATE requests in the cluster for the namespaces being monitored.

Note: You can specify included and excluded namespaces in the helm values during installation. By default, kube-system and the namespace where the deployment assessment agent is installed are excluded from the evaluation.

- The agent extracts all the images in pod spec provided in the AdmissionReviewRequest and reaches out the respective registry to retrieve the image metadata.

Note: If the pod spec refers to an imagePullSecret, the deployment assessment agent attempts to use this secret to access the image in the registry.

- The agent sends the metadata to the Container Security instance to assess the deployment.



- If the image has not been scanned before using Container Security, the deployment is allowed.
- If the image has been scanned before using Container Security, and there is no policy configured, the deployment is allowed.
- If the image has been scanned before using Container Security, and there are configured policies, the policy evaluation determines whether the deployment is allowed or denied.
- If there are multiple policies configured and at least one of them is configured to block, then the deployment is blocked.

Note: The AdmissionReviewRequest does not indicate the architecture of the image or images being deployed. If the image in the registry is a multi-platform image, the deployment assessment agent will attempt to evaluate each architecture in the image manifest. If the policy evaluation fails for any of the platforms, the deployment will be denied.

- The [AdmissionReviewResponse](#) is sent to the kube-apiserver.
- The result of the deployment assessment appears in the Kubernetes events and in the Container Security UI when you [view details for the related policy](#).

Note: If an image being deployed has not been scanned by Container Security in previous CI/CD or registry scans, the images will not appear in the Container Security UI.

This topic describes how to [install a deployment assessment agent](#), and how to [delete a deployment assessment agent](#).

Before You Begin

- The following components must be installed on the Kubernetes cluster that needs to be monitored for deployment assessment:
 - Cert Manager
 - Cert Manager CSI Driver



For more information, see [Prepare a Kubernetes Cluster](#) in the Tenable Enclave Security user guide.

- Container Security must be installed and accessible via the LoadBalancer URL from all the Kubernetes clusters where deployment assessment needs to run.
- [Add a deployment scanner](#) in Container Security.

Install or Upgrade a Deployment Assessment Agent

1. In the Kubernetes cluster where you want to install the deployment assessment agent, create a namespace using the following command:

```
kubectl create namespace tes-deployment-assessment
```

In this example, the namespace is *tes-deployment-assessment*. If you use a different namespace, ensure that you use the same namespace every time you install or upgrade the agent.

2. Add the Tenable Helm Charts repository with the following command:

```
helm repo add tenable https://charts.tenable.com
```

3. Update the repository:

```
helm repo update
```

4. In Container Security Container Security, [add a deployment scanner](#) and download the yaml file.
5. Install the Helm Chart or upgrade the existing Helm Chart:
 - a. Create a `values.yaml` file with parameters for your deployment. The following is an example `values.yaml`:

```
# To override image registry and tag
image:
  registry: tenable
```



```
tag: 1.0.0

# To override default resource
resources:
  requests:
    memory: "500Mi"
    cpu: "500m"
  limits:
    memory: "2Gi"
    cpu: "2000m"

# To override include/exclude namespace
# By default, kube-system and the namespace where the agent is being
# deployed is excluded from monitoring.
validatingWebhook:
  # Namespaces to exclude from assessment.
  # release namespace is excluded by default to allow the
  # webhook pod to be deployed.
  excludeNamespaces:
    - kube-system
    - namespace2
  # Namespaces to include in the assessment
  # includeNamespaces:
  #   - namespace1
```

Note: If you create a custom `values.yaml` file, ensure you use the same file every time you upgrade. Otherwise, Tenable uses default values that may not match your configuration.

Deployment Assessment Values.yaml Configuration

ValidatingAdmissionWebhook Configuration

You can override the default `ValidatingAdmissionWebhook` configuration provided in the Helm Charts.

```
validatingWebhook:
  # timeoutSeconds Must be between 1 and 30
  timeoutSeconds: 15
  # Possible values for failurePolicy:
  # - Ignore : means that an error calling the webhook is ignored and the API request is
  # allowed to continue.
  # - Fail : means that an error calling the webhook causes the admission to fail and the
  # API request to be rejected.
  failurePolicy: Ignore
  # Namespaces to exclude from assessment.
  # release namespace is excluded by default to allow the
```



```
# agent pod to be deployed.
excludeNamespaces:
  - kube-system
# Namespaces to include in the assessment
includeNamespaces:
  - app-test
```

Specify Node Affinity

The default Helm Chart for deployment assessment ships with an anti affinity rule to prevent replicas from getting scheduled on the same node. You can specify a node affinity in `values.yaml`.

```
affinity:
  podAntiAffinity:
    requiredDuringSchedulingIgnoredDuringExecution:
      - labelSelector:
          matchLabels:
            app.kubernetes.io/name: tes-deployment-assessment
        topologyKey: kubernetes.io/hostname
```

Image Registry

You can specify a registry to pull the deployment assessment.

```
image:
  registry: tenable
```

Replica Count

Use this option to override the default replica count of 2.

```
replicaCount: 2
```

- b. Install the Helm Chart using the following command, where `{cluster_name.yaml}` is the file you downloaded when you created the deployment scanner:

```
helm upgrade --install tes-deployment-assessment -n tes-deployment-assessment -f
values.yaml -f {cluster_name.yaml} tenable/tes-deployment-assessment
```

Delete a Deployment Assessment Agent



1. In the Kubernetes cluster where the deployment assessment agent is installed, list the charts installed in the namespace with the following command:

```
helm list -n tes-deployment-assessment
```

2. Delete the Helm Chart with the following command:

```
helm delete tes-deployment-assessment -n tes-deployment-assessment
```

3. In the Container Security UI, [delete the deployment scanner](#) from the list.

Edit a Deployment Scanner

To edit a deployment scanner:

1. In the left navigation, click **Scanners**.

The **Scanners** page appears.

2. Click the **Deployments** tab.

The **Deployments** tab appears, which displays a list of your deployment scanners.

3. In the table, right-click the row for the deployment scanner you want to edit, and click **Edit**.

-or-

In the row for the deployment scanner you want to edit, click the **:** button, and click **Edit**.

The **Edit Deployment Scanner** window appears.

4. Modify the deployment scanner name and description as needed.
5. (Optional) Select **Refresh Scanner Key** to generate a new scanner configuration yaml file.

Note: If you select Refresh Scanner Key, this will invalidate the existing scanner key. You will need to update the deployment assessment agent in your cluster using the new scanner configuration yaml file. For instructions, see [Install a Deployment Assessment Agent](#).

6. Click **Save**.

The deployment scanner is saved.



Delete a Deployment Scanner

To delete a scanner:

1. In the left navigation, click **Scanners**.

The **Scanners** page appears.

2. Click the **Deployments** tab.

The **Deployments** tab appears, which displays a list of your deployment scanners.

3. In the table, right-click the row for the deployment scanner you want to delete, and click **Delete**.

-or-

In the row for the deployment scanner you want to delete, click the **:** button, and click **Delete**.

The **Delete Deployment Scanner** window appears, confirming that you want to delete the scan.

4. Click **Delete**.

The scanner is deleted.

What to do next:

- Delete the deployment assessment agent from the cluster using the steps in [Delete a Deployment Assessment Agent](#).



Reporting

You can create reports in Container Security to share data with users in other organizations. Tenable provides reporting through report templates and customizable report formats.

View your Container Security reports

1. In Tenable Enclave Security, in the top navigation bar, click  **Workspaces > Container Security**.

Container Security appears.

2. In the left navigation, click **Reporting**.

The **Reports** page appears.

For more information about reporting, see [Reports](#) in the *Tenable Security Center user guide*.