



Tenable Enclave Security Container Security User Guide

Last Updated: September 23, 2024

This guide describes how to configure and use Container Security for Tenable Enclave Security.

Table of Contents

Tenable Enclave Security Container Security User Guide	1
Welcome to Container Security for Tenable Enclave Security	4
Install Container Security	4
System Requirements	4
Settings and Information	7
Dashboard	8
Vulnerabilities	9
Export a Vulnerability	9
Assets	10
Images	10
View Image Details	11
Export an Image	11
Delete an Image	11
Packages	12
View Package Details	12
Layers	12
View Layer Details	12
Scans	14
Create a Scan	14
Configure a CI/CD Scan	16
Configure CI/CD Scan Policies	17
Edit a Scan	21
Run a Scan	21
Delete a Scan	22

Scan Settings	22
Scanners	24
Add a Scanner	24
Edit a Scanner	25
Update a Scanner	25
Delete a Scanner	27
Reporting	28

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*.

Requirements for Container Security services

Service Name	# of Assets Managed by Container Security	CPU	Memory	Disk Space
tes-consec-ui	1 to 50,000 images	4000 m	4 GiB	--

Service Name	# of Assets Managed by Container Security	CPU	Memory	Disk Space
tes-consec-api	1 to 50,000 images	4000 m	6 GiB	--
tes-consec-tvdl	1 to 1,000 images	4000 m	10 GiB	10 GB
	1,001 to 5,000 images	4000 m	15 GiB	25 GB
	5,001 to 10,000 images	4000 m	30 GiB	50 GB
	10,001 to 25,000 images	4000 m	60 GiB	125 GB
tes-consec-scan	1 to 10,000 images	4000 m	8 GiB	10 GB
	10,001 to 50,000 images	4000 m	12 GiB	10 GB

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

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

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.

Note: Container Security assets do not age out. To manage your license usage, Tenable recommends you periodically delete unused assets.

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.

Note: Container Security assets do not age out. To manage your license usage, Tenable recommends you periodically delete unused assets.

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.

Note: Container Security assets do not age out. To manage your license usage, Tenable recommends you periodically delete unused assets.

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.

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](#)

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

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.

3. Press **Enter**.

Container Security scans the image.

Configure CI/CD 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
<code>policy_groups</code>	A policy json file is a list of <code>policy_groups</code> . Each <code>policy_group</code> is a list of policy entries with boolean operators (<code>group_operator</code>) to join them.
<code>group_operator</code>	The <code>group_operator</code> field accepts only AND and OR. The <code>group_operator</code> applies to the list of entries.
<code>entries</code>	Each entries item contains a <code>label</code> , <code>operator</code> , <code>field</code> , and <code>policy_value</code> .
<code>label</code>	An arbitrary string that describes the policy entry. For example, "Cvssv3 cannot be greater than 7"
<code>operator</code>	The operation that you want to trigger policy violations on. Some fields only support the EQ operator. The following are the supported operators: <ul style="list-style-type: none">• EQ - equal to (=).• NEQ - not equal to (≠).

Field	Description
	<ul style="list-style-type: none"> • GT - greater than (>). • GTE - greater than or equal to (≥). • LT - less than (<). • LTE - less than or equal to (≤).
field	<p>Any of the fields you want to support policy evaluation on. The following are the supported fields:</p> <ul style="list-style-type: none"> • 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 <i>0.0</i> to <i>10.0</i>. • 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"
}
]
}

```

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** page 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	

Option	Description
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.
<p>Scan Inclusion</p> <p>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.</p> <div data-bbox="147 930 1479 1005" style="border: 1px solid #0070C0; padding: 5px;"> <p>Note: Using an asterisk (*) will include all.</p> </div>	
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.
<p>Scan Exclusion</p> <p>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.</p> <div data-bbox="147 1495 1479 1570" style="border: 1px solid #0070C0; padding: 5px;"> <p>Note: Using an asterisk (*) will include all.</p> </div>	
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.

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.

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).

For more information, see the following topics:

[Add a Scanner](#)

[Edit a Scanner](#)

[Update a Scanner](#)

[Delete a Scanner](#)

Add a Scanner

Create a Container Security scanner:

1. On the **Scanners** page, click **Add Scanner**.
2. In the **Scanner Name** box, type a name for the scanner.
3. In the **Description** box, type a description for the scanner.
4. Select a platform for the scanner.
5. Click **Download**.

The 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:

```
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
```

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** page 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** page 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** page 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.

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*.