Tenable Enclave Security Container Security 1.9.x User Guide

Last Updated: August 26, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Container Security for Tenable Enclave Security **6**

Install Container Security 6

System Requirements 7

Requirements for Container Security Services 7

Container Security Agent Requirements 7

Self-Hosted Database Requirements 9

Cloud Database Requirements 10

Settings and Information **12**

Dashboard **13**

Vulnerabilities **14**

Export a Vulnerability 14

Assets **15**

Images 15

View Image Details 16

Export an Image 16

Delete an Image 17

Packages 17

View Package Details 17

Layers 18

View Layer Details 18

Policies **19**

Create a Policy 19

View Policy Details 22

Activate or Deactivate a Policy 23

Edit a Policy 25

Scans **26**

Create a Scan 26

Configure a CI/CD Scan 28

Configure CI/CD Scan Policies 30

Edit a Scan 35

Run a Scan 36

Delete a Scan 36

Scan Settings 37

Scan Inclusion and Exclusion Syntax Examples 39

Asset Expiration 39

Scanners **42**

Scanners 42

Add a Scanner 43

Edit a Scanner 44

Update a Scanner 45

Delete a Scanner 46
Deployments 46
Add a Deployment Scanner 47
Install a Deployment Assessment Agent 48
Edit a Deployment Scanner 53
Delete a Deployment Scanner 54
Reporting **56**
Exposure Response **57**
Tracking Container Images in Container Security Exposure Response 57
Create Initiatives 58
Edit or Delete Initiatives 60
Review Initiatives 61
Findings on Assets 62
How Am I Doing? 62
What's New? 64
My Findings and Affected Assets 65
My Findings 65
My Affected Assets 67
Plugins 68
View the Combination Timeline 69
Manage Combinations 69

Create a Combination 69

Edit a Combination 71

Copy a Shared Combination 71

Delete a Combination 72

Exposure Response Filters 73

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
  - Requirements for Container Security Services
  - Container Security Agent Requirements
  - Self-Hosted Database Requirements
  - Cloud Database 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 system requirements for Container Security services, Container Security agents, and self-hosted and cloud databases.

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	2 cores	2 GiB
tes-consec-api	1 to 25,000 images	2 cores	3 GiB
tes-consec-tvdl	1 to 25,000 images	2 cores	6 GiB
tes-consec-policy	1 to 25,000 images	2 cores	2 GiB
tes-consec-scan	1 to 25,000 images	2 cores	5 GiB
tes-exposure-response	1 to 25,000 images	2 cores	2 GiB
tes-platform-ui	1 to 25,000 images	2 cores	4 GiB

Container Security Agent Requirements

Caution: Do not run other scanners, such as Tenable Nessus, Tenable One Web App Scanning, or other vulnerability assessment tools, on the same instance. These tools are CPU and memory intensive and can cause resource contention. To handle multiple scans concurrently, deploy separate scanner instances rather than sharing resources.

Resource	Recommendation
CPU **Note:** This is a fixed requirement. You must provide additional cores only if you run multiple scanners in parallel.	4 cores
Memory (RAM)	8 GB minimum *-or-* equal to the largest uncompressed layer
Storage **Note:** This requirement accounts for the scanner, temporary layers, and other essential files.	50 GB minimum *-or-* Total compressed image size + uncompressed size of the largest layer **Note:** The agent downloads and temporarily extracts image layers under `/tmp/tes-consec/` on the host running the scan. If you mount dedicated storage, target `/tmp/tes-consec/` or the partition containing `/tmp`. All compressed layers remain on disk for the

Resource	Recommendation
	duration of the scan. Layers are decompressed one at a time and cleaned up before the next begins, so the extra headroom only needs to cover the single largest layer's uncompressed size. For example, an image with 1.5 GB of total compressed layers where the largest layer decompresses to 800 MB requires approximately 2.3 GB free on `/tmp/tes-consec/`.

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	Managed DB Instance Type	Compute Instance Type (Self-Managed)	CPU Cores	Memory	Storage
1 to 1,000 images	db.m6g.xlarge	db.m6g.xlarge	4	16 GiB	10 GB
1,001 to 5,000 images	db.m6g.2xlarge	m6g.2xlarge	8	32 GiB	15 GB
5,001 to 25,000 images	db.m6g.4xlarge	m6g.4xlarge	16	64 GiB	20 GB

Requirements for Container Security database in Azure for PostgreSQL flexible servers

# of Assets Managed by Container Security	Managed DB Instance Type	Compute Instance Type (Self-Managed)	CPU Cores	Memory	Storage
1 to 1,000 images	E2s_ v3/E2ds_v4	D4s_v3	4	16 GiB	10 GB
1,001 to 5,000 images	E4s_ v3/E4ds_v4	D16s_v3	8	32 GiB	15 GB
5,001 to 25,000 images	E8s_ v3/E8ds_v4	D32s_v3	16	64 GiB	20 GB

Requirements for Container Security database in GCloud

# of Assets Managed by Container Security	Managed DB Instance Type	Compute Instance Type (Self-Managed)	CPU Cores	Memory	Storage
1 to 1,000 images	4 vCPU, 16GB	t2a-standard-4	4	16 GiB	10 GB
1,001 to 5,000 images	8 vCPU, 32GB	t2a-standard-8	8	32 GiB	15 GB
5,001 to 25,000 images	16 vCPU, 64GB	t2a-standard-16	16	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.

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
  - Scan Inclusion and Exclusion Syntax Examples
- 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.

   > **Note:** If you selected **AWS ECR** as the **Registry Type**, Container Security does not use the **Username** or **Password** fields. To authenticate to AWS ECR, you must authenticate the scanner machine directly to AWS using AWS credentials (for example, an IAM role, instance profile, or environment-based credentials). Credentials entered in the UI are ignored.

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_`	The `group_operator` field accepts only `AND` and `OR`. The `group_operator`

Field	Description
`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 *LOW*, *MEDIUM*, *HIGH*, and *CRITICAL*.

Field	Description
	• **VPR** - only supports floating point numbers as values, from *0.0* to *10.0*. • **CVSS2** - only supports floating point numbers as values, from *0.0* to *10.0*. • **CVSS3** - only supports floating point numbers as values, from *0.0* to *10.0*. • **EPSS** - only supports floating point numbers as values, from *0.0* to *100.0*.
`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** 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, 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

Option	Description
	20 images will apply.
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.	

Option	Description
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.

Scan Inclusion and Exclusion Syntax Examples

Use the following examples as a guide when you enter registries, repositories, and tags in the Scan Inclusion and Scan Exclusion fields.

Type	Example value	What it matches
Registry	`registry.example.com`	All images from the specified registry.
Registry with port	`registry.example.com:5000`	All images from the specified registry on port 5000.
Repository	`myorg/myimage`	All tags for the specified repository.
Specific image and tag	`myorg/myimage:1.2.3`	Only the exact image and tag specified.
Wildcard (all tags)	`myorg/myimage:*`	All tags for the specified repository.
Wildcard (all repositories)	`myorg/*`	All repositories under the specified organization.

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.

Option	Description
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: • **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 the 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*.

Exposure Response

In the **Exposure Response** section, you create *initiatives*, which are projects to address vulnerabilities in your environment.

In initiatives, you track specific findings using combinations and select pipelines or registries to choose the assets in scope. Then, you assign initiatives to your team, set SLAs, and measure progress through remediation scan results.

You can use the **Exposure Response** section to create, assign, and report on all initiatives. As a initiative owner, you only see and work with your initiatives.

Tracking Container Images in Container Security Exposure Response

Exposure Response tracks container images by creating a list of images imported into your Container Security container and grouping them based on the following properties:

- **Image Name**: The specific name assigned to the container image.
- **Distribution**: The Linux distribution or OS variant installed on the asset (for example, Ubuntu, CentOS, Windows Server).
- **Architecture**: The system architecture of the asset's operating system (for example, x86_64).
- **Operating System**: The name and version of the operating system running on the asset. (for example Linux Kernel 3.13).
- **Last Scanned**: The date and time the asset was most recently scanned by Container Security.

When you select a registry or pipeline (Asset Scope), the system applies filters based on these properties to the assets. It then builds a list of assets to apply to an initiative.

Exposure Response assumes that the **Image Name**, **Distribution**, **Architecture**, and **Operating System** remain stable for a given group. The only property that changes regularly is the **Last Scanned** value.

Exposure Response then gathers vulnerability remediation information based on the most recently scanned images daily and applies it to the initiatives.

The following topics explain how to use these tools to create, manage, review, and report on initiatives.

Create Initiatives

In the **Exposure Response** section, your first step is creating an initiative. To do this, add the initiative, define the scope by selecting registries and/or pipelines, and choosing an SLA. Then, add combinations to define the vulnerabilities to track.

Example Initiative

To address recently exploited vulnerabilities on your Headquarters registry, you might create an initiative as follows:

- **Name** – Recently exploited vulnerabilities at HQ
- **Asset Scope** – http://localhost:5000
- **Remediate Within** – 7 days
- **Combinations** – Category is equal to Recently Actively Exploited AND VPR is greater than 6

Before You Begin

Before you create an initiative:

- (Optional) **Create custom combinations** – If you plan to use custom combinations, create them.

Create a New Initiative

To create a new initiative:

1. In the left navigation, click **Exposure Response**.
2. In **My Initiatives**, click ⊕ **New**.

   The **Create New Initiative** pane appears.
3. Set the following options.

Option	Description
Name	Type a name for the initiative.
Description	(Optional) Type a description for the initiative, for example *Reduce my external attack surface*.
Asset Scope	Choose up to ten registries or pipelines to define which assets in your environment are in scope. Search for and select registries or pipelines to assign, for example *EXAMPLE:https://example.com* or *EXAMPLE:https://192.0.2.202:5000*.
Remediate Within	Choose an SLA by which all findings must be remediated. For example, to set an SLA of one week, enter *7*.

4. Under **Assign Combinations**, add up to ten combinations from the following tabs.

Tab	Description

My Combinations	Your personal combinations, which only you can view. You cannot assign personal combinations to initiatives you do not own.
Shared	Organization-wide combinations, which anyone can view or use and which your administrators and the combination owners can update. Updates may change the resources in your initiative. Track updates in the Combination Timeline.
Tenable	Predefined combinations from the Tenable Research Team. These may be updated infrequently, which can change the resources in your initiatives. Track updates in the Combination Timeline.

Note: Initiatives can contain no more than *17* queries across all combinations. For example, if you add four combinations to an initiative—and the combinations have five queries each for a total of 20, a warning appears and you cannot save the initiative.

Note: Initiatives with multiple combinations use a logical OR filter. The data displayed will include all results from each of the individual combinations.

5. Click **Save**.

   The initiative appears in the **My Initiatives** panel.

Edit or Delete Initiatives

You can edit or delete initiatives that you own. This topic contains steps to complete both tasks.

Edit an Initiative

To edit an initiative:

1. In the left navigation, click **Exposure Response**.
2. In **My Initiatives**, click ⋮ in the upper-right corner of the initiative.
3. In the menu that opens, click **Edit**.
4. The **Edit Initiative** panel appears.

   Edit the initiative settings, as described in Create Initiatives.

   > **Note**: You cannot edit an initiative's owner, since the system calculates initiative metrics based on the owner's Tenable permissions.

5. Click **Save**.
6. The system saves the initiative.

Delete an Initiative

To delete an initiative:

1. In the left navigation, click **Exposure Response**.
2. In **My Initiatives**, click ⋮ in the upper-right corner of the initiative.
3. In the menu that opens, click **Delete**.
4. In the box that appears, click **Delete** again.

   The system permanently deletes the initiative.

Review Initiatives

On the **Exposure Response** page, review initiatives that you own or have assigned in two sections:

- **My Initiatives** – On the left, view all your initiatives.
- **Initiative Details** – Under My Initiatives, click an initiative to view details.

Initiative Details

The initiative details section contains four panels.

In this section	You can...
Findings on Assets	View a sunburst chart of all findings. In the chart, each segment shows the percentage of assets with a relevant finding, by asset tag or combination.
How Am I Doing?	View a dashboard with at-a-glance metrics and a line chart that tracks finding and remediation trends.
What's New?	View recently identified findings and affected assets.
My Findings and Affected Assets	View all findings and affected assets in two tabs. Refine the displayed items with a query builder and save or share the results.

Findings on Assets

In the **Findings on Assets** panel, view a sunburst chart containing findings and assets. The chart is divided by the combinations used in the initiative.

In the chart, each segment shows the percentage of assets containing a combination. The segment is colored green, yellow, or red to indicate low, medium, or high. Click a segment to open a popup with more details.

How Am I Doing?

In the **How Am I Doing?** panel, view key metrics and an area chart which tracks initiative trends over time.

Key Metrics

At the top of the panel, the following metrics appear.

Metric	Description
Average Age of Vulnerabilities	View the average age of findings in the initiative. This metric is based on the dates that findings were first seen or when they resurfaced.
Average Time to Remediate	View the average time to fix findings since they were discovered on a scan. A finding is marked **Fixed** after being **Active**, **New**, or **Resurfaced**.
Percentage of Findings Remediated	View the percentage of fixed findings in the initiative, including all historic findings.

New Findings vs. Remediations

In the **New Findings vs. Remediations** graph, view the initiative's finding and remediation trends, which change over time as scans run and new assets are found or added.

Do one of the following:

- To change the date range, select **30 Days**, **60 Days**, **90 Days**, or **Custom**.
- To see more details for a date, in the graph, hover on that date.
- To see details about major events, below the graph, click an *event marker* to open an event card.

Event Cards

Below the chart, the following events can appear.

Metric	Description
Asset Count	Appears when the number of affected assets changes by more than 20%.

Combination Changes	Appears when Tenable modifies or removes combinations in the initiative.
Finding Count	Appears when the total findings count changes by more than 20%.
Resurfaced Findings	Appears when the resurfaced findings count changes by more than 20%.

What's New?

In the **What's New** panel, view how an initiative has recently changed. This includes new findings, new affected assets, and new Common Vulnerabilities and Exposures (CVEs) that are now in scope based on the combinations used (for example, a CVE whose VPR increased).

Top New Plugins

In the **Top New Findings** table, view recent findings in the following columns.

Column	Description
VPR	Indicates the Vulnerability Priority Rating (VPR) for the finding.
Plugin	Indicates the plugin that identified the finding. Click a plugin name to view all findings related to that plugin in **My Findings**.
Last Seen	Indicates the date when the finding last appeared on a scan.

Top New Assets

In the **Top New Assets** table, view recent findings in the following columns.

Column	Description

Asset Name	Indicates the name of the affected asset. Click an asset name to view all results for that Asset ID in **My Affected Assets**.
Findings	Indicates the number of findings on the asset.
Last Seen	Indicates the date when the asset last appeared on a scan.

Latest Combination Changes

In the **Latest Combination Changes** section, view CVEs recently found by the combinations in the initiative.

My Findings and Affected Assets

In the **Findings and Affected Assets** panel, view findings and affected assets in two tabs. Filter the items in each tab with the Query Builder, save queries, and export lists of resources.

To learn more, see the following topics.

Topic	Description
My Findings	View all active, new, and resurfaced findings in an initiative.
My Affected Assets	View all affected assets in an initiative.

My Findings

In the **My Findings and Affected Assets** section, the **My Findings** tab shows all active, new, or resurfaced findings for that initiative. Refine the results with the Query Builder.

The **My Findings** tab has the following columns, which you can customize using the Columns drop-down.

Column	Description
Plugin ID	The unique identifier for the Tenable plugin that detected the vulnerability.
Plugin Name	The name of the Tenable plugin that detected the finding.
CVEs	The Common Vulnerability and Exposure (CVE) identifier for the finding, as assigned by the CISA-sponsored CVE Program.
VPR	The Tenable-calculated Vulnerability Priority Rating (VPR) score from 0.1 to 10. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
EPSS	The percentage likelihood that a vulnerability will be exploited, based on the third-party Exploit Prediction Scoring System (EPSS).
CVSSv2	The Common Vulnerability Scoring System (CVSS) v2 score for the finding.
CVSSv3	The Common Vulnerability Scoring System (CVSS) v3 score for the finding.
Affected Assets	The count of assets affected by this vulnerability.

Affected Assets

In any findings row, click the drop-down **>** to reveal a table of assets on which that finding appears, with the following columns.

Column	Description
Image Name	The shortened name based on the repository that the image is from. For example, the repository *docker.io/library/api-regression-db* would have the

	image name *library/api-regression-db*.
Operating System	The name and version of the operating system running on the asset, for example *Linux Kernel 3.13*.
Findings Count	The number of findings on the asset.
Last Seen	Indicates the date when the asset last appeared on a scan.

My Affected Assets

In the **My Findings and Affected Assets** section, the **My Affected Assets** tab shows all assets in the initiative with a finding that has not yet been fixed. Refine the results with the Query Builder to provide business context.

The **My Affected Assets** tab has the following columns.

Column	Description
Name	The user-defined hostname or name of the affected asset.
Vulnerabilities	The total count of vulnerabilities detected on the asset.
CVEs	The Common Vulnerability and Exposure (CVE) identifier for the finding on the asset, as assigned by the CISA-sponsored CVE Program.
Tag	Any custom tags applied to the asset within the Tenable environment.
Asset ID	The unique internal identifier Tenable uses to track the asset.
Architecture	The system architecture of the asset's operating system (for example, x86_64).
Distribution	The Linux distribution or OS variant installed on the asset (for example,

	Ubuntu, CentOS, Windows Server).
Operating System	The name and version of the operating system running on the asset, for example *Linux Kernel 3.13*.
Last Scanned	The date and time the asset was most recently scanned by Container Security.
Plugin Count	The number of plugins impacting this image.

Plugins

In any asset row, click the drop-down **>** to reveal a table of plugin results for the findings on that asset, with the following columns.

Column	Description
VPR	The Vulnerability Priority Rating that Tenable calculated for the vulnerability. **Note**: A finding's VPR is based on the VPR of the plugin that identified it. When plugins are associated with multiple vulnerabilities, the highest VPR appears.
Severity	The vulnerability's severity, based on the Common Vulnerability Scoring System (CVSS).
Plugin Name	The name of the Tenable plugin that detected the finding.
Plugin ID	The unique identifier for the Tenable plugin that detected the vulnerability.
Findings	The number of findings detected on the asset.
CVSSv2	The CVSSv2 score for the finding.
CVSSv3	The CVSSv3 score for the finding.

View the Combination Timeline

In the **Combination Timeline** tab, you can view a 30-day timeline of combinations added to or removed from the initiatives you have access to.

- To view the **Combination Timeline**, in the left navigation, click **Exposure Response** > **Combination Timeline**.

On the lower area, in **Combinations with Updates**, view combinations edited in the past 30 days. You may want to do this when the data in one of your initiatives changes significantly, since editing combinations changes initiative data.

In the top-right corner of any combination, click ⋮ to open a menu where you can edit or delete the combination.

Manage Combinations

When you create initiatives, you assign combinations to define what resources they track in your environment. Combinations use *queries* to search for specific findings.

You can use the query builder to create your own combinations, apply Tenable combinations, or combine the two. When you create combinations, you can save them as templates to share with your organization.

> **Note**: Exposure Response limits the number of combinations created:
>
> - 50 total combinations per user, and
> - 100 total combinations per organization.

The following sections explain how to use combinations.

Create a Combination

When you create an initiative, unless you want to use existing combinations, you must first create a new combination.

To create new combinations:

1. In the left navigation, click **Exposure Response**.
2. In the left panel, click ⊕**New**.

   The **Create Combination** pane appears. It contains the following options.

Option	Description
Name	Type a combination name.
Description	Type a description, for example *High CvSS score*.
Query	In the query box, define what resources the combination searches for. For example, *CVSSv3 Base Score is greater than 6*. **Note**: For any combination, the system supports a maximum of *six* queries separated by operators.
Add to Initiatives	(Optional) Choose a current initiative in which to add the combination. **Note**: Initiatives with multiple combinations use a logical OR filter. The data displayed will include all results from each of the individual combinations.
Shared	(Optional) Enable this toggle to share the combination with your organization in the **Shared** tab.

3. Click **Save**.

   The combination appears in the left panel under **Personal** or **Shared**.

Edit a Combination

You can edit combinations based on your Tenable user role and the combination status.

- **With the Exposure Response Manager permission:** You can edit any shared non-Tenable combination.
- **Without the Exposure Response Manager permission:**
  - You can edit unshared combinations from **My Combinations**.
  - You can edit shared combinations that you created if they are not in use.

To edit a combination:

1. In the left navigation, click **Exposure Response**.
2. Click **Manage Combinations**.

   The **Manage Combinations** tab appears.
3. In the left pane, in the combination to edit, click ⋮ and select **Edit**.
4. In the **Edit Combination** panel that appears, change the options.

   > **Note**: To remove a combination from a current initiative, edit the initiative instead.
5. Click **Save**.

   The system saves the combination.

Copy a Shared Combination

In the **Exposure Response** section, the **Shared** tab contains combinations shared by your organization. When you want to customize a combination that you did not create, you can copy it to **My Combinations** and then edit the copy.

To copy and edit a shared combination:

1. In the left navigation, click **Exposure Response**.
2. Click **Manage Combinations**.

   The **Manage Combinations** tab appears.
3. In the left panel, click **Shared**.
4. In the left panel, click the template to copy and then, in the right panel, click **Copy to my combinations**.

   The system copies the shared combination.

Delete a Combination

You can delete combinations based on your Tenable user role and the combination status.

- **With the Exposure Response Manager permission:** You can delete any shared non-Tenable combination.

  > **Note**: When a combination is the only data source for an initiative, deleting it pauses the initiative.

- **Without the Exposure Response Manager permission:**
  - You can delete unshared combinations from **My Combinations**.
  - You can delete shared combinations that you created if they are not in use.

To delete a combination:

1. In the left navigation, click **Exposure Response**.
2. Click **Manage Combinations**.

The **Manage Combinations** tab appears.

3. In the left pane, in the combination to edit, click ⋮ and select **Delete**.

4. In the confirmation dialog that appears, click **Delete** again.

   The system deletes the combination.

Exposure Response Filters

In **Exposure Response**, use the query builder to view specific findings or affected assets or choose which vulnerabilities appear in a combination.

> **Tip**: For the fastest results, Tenable recommends using the **Last Seen** filter in all queries to return findings from the last 30 days.

The following table defines the findings filters to use in queries within your **Initiative Activity** pane.

Filter	Description
Asset ID	The UUID of the asset where a scan detected the finding. This value is unique to Container Security.
CISA KEV	Filter by the presence of the vulnerability in the CISA Known Exploited Vulnerabilities (KEV) Catalog. This helps prioritize risks based on real-world exploitation evidence.
CPE	The Common Platform Enumeration (CPE) identifiers for the vulnerabilities that the plugin detects. You can enter up to 200 values.
CVEs	The Common Vulnerability and Exposure (CVE) IDs for the vulnerabilities that the plugin detects. You can enter up to 200 values.
CVSSv2 Base	A numeric value between 0.0 and 10.0 that represents the intrinsic

Filter	Description
Score	characteristics of a vulnerability independent of any specific environment.
CVSSv2 Temporal Score	The CVSSv2 Temporal Score reflects the current real-world severity of a vulnerability, adjusting the Base Score based on factors that change over time.
CVSSv2 Temporal Vector	The CVSSv2 temporal metrics used to calculate the temporal score for the vulnerability.
CVSSv2 Vector	The raw CVSSv2 metrics for the vulnerability. For more information, see the CVSSv2 documentation on the FIRST website.
CVSSv3 Base Score	A numeric value between 0.0 and 10.0 that represents the intrinsic characteristics of a vulnerability independent of any specific environment.
CVSSv3 Temporal Score	The CVSSv3 temporal score, which is based on characteristics of a vulnerability that change over time but not among user environments.
CVSSv3 Temporal Vector	The CVSSv3 temporal metrics used to calculate the temporal score for the vulnerability.
CVSSv3 Vector	The raw CVSSv3 metrics for the vulnerability.
EPSS Percentile	The Exploit Prediction Scoring System (EPSS) percentile, which indicates how many other vulnerabilities have an EPSS score lower than the current vulnerability.
EPSS Score	The percentage likelihood (0-100) that a vulnerability will be exploited, based on the Exploit Prediction Scoring System (EPSS). You can type a number with up to three decimal places, for example, 75.599.

Filter	Description
Exploit Available	Filter based on whether exploit code is publicly available for the vulnerability.
Exploit Available Calculated	Filter based on the calculated availability of exploit code for the vulnerability, which is determined by Tenable's research.
Exploit Code Maturity	The maturity level of the publicly available exploit code for the vulnerability.
Exploitability Ease	A description of how easy it is to exploit the vulnerability.
IAVM	Filter by the vulnerability's presence on the Information Assurance Vulnerability Management (IAVM) list.
Patch Publication Date	The date on which the vendor published a patch for the vulnerability.
Plugin Family	The family of the plugin that detected the vulnerability. You can enter up to 200 values.
Plugin ID	Filter on the ID of the plugin that detected the vulnerability. You can enter up to 200 values.
Plugin Modification Date	The date on which the plugin that detected the vulnerability was last updated.
Plugin Name	The name of the plugin that detected the vulnerability.

Filter	Description
Plugin Publication Date	The date on which the plugin that detected the vulnerability was published.
Predicted Impact Score	The score representing the potential impact if the vulnerability is exploited.
Product Coverage	Filter based on the Tenable product that detected the vulnerability.
Scan Sources	Filter based on the Tenable sensor or product that generated the vulnerability finding.
Severity	The vulnerability's CVSS-based severity (for example, Critical, High, Medium, Low). For more information, see CVSS vs. VPR.
Threat Intensity Last 28 Days	A measure of the current threat activity related to the vulnerability over the last 28 days.
Threat Recency	Filter based on how recently a threat actor has targeted the vulnerability.
Threat Sources Last 28	The type of threat sources (for example, malware, exploit kits) seen exploiting the vulnerability in the last 28 days.
Vendor Severity	The severity level assigned to the vulnerability by the affected software vendor.
VPR	The Vulnerability Priority Rating that Tenable calculated for the vulnerability.
VPR Age of Vulnerability	The number of days that have passed since the date that the vulnerability was first published.
VPR CVSSv3	The CVSSv3 Impact Score used in the calculation of the Vulnerability

Filter	Description
Impact Score	Priority Rating (VPR).
Vulnerability ID	The unique identifier assigned to the vulnerability by Tenable.
Vulnerability Publication Date	The date when the vulnerability definition was first published (for example, the date the CVE was published).