Tenable Enclave Security 1.8.x User Guide

Last Updated: February 26, 2026

Table of Contents

Welcome to Tenable Enclave Security

Tenable Enclave Security is a private container platform that you can use to deploy on-prem Tenable products.

- **Products** - These are the Tenable products that you can deploy in Tenable Enclave Security.
  - Security Center in Tenable Enclave Security
  - Container Security in Tenable Enclave Security
- **Utilities** - These are the tools available in Tenable Enclave Security to analyze the data collected by Tenable Security Center or Container Security.
  - Reporting

> **Note:** Log Correlation Engine Event Analysis is not supported in Tenable Enclave Security.

See the following pages for information about installing and using Tenable Enclave Security. For sizing requirements, see Tenable Enclave Security System Requirements.

Before Installation

Tenable Enclave Security System Requirements

License Requirements

Prepare a Kubernetes Cluster

Tenable Enclave Security Helm Charts

External PostgreSQL with Tenable Enclave Security

Install Tenable Enclave Security

Update Tenable Enclave Security

Configure Tenable Enclave Security

Before Installation

System Requirements

See Tenable Enclave Security System Requirements for minimum hardware, software, and cloud requirements, including supported Kubernetes environments.

Get a Tenable Enclave Security License

Before you obtain a Tenable Enclave Security license, you must know the namespace and cluster ID for the Kubernetes environment where you plan to install Tenable Enclave Security. For instructions on how to get a Tenable Enclave Security license, see Licenses.

For license requirements, see License Requirements.

Prepare a Kubernetes Cluster

For details on how to create a new cluster or prepare an existing cluster, see Prepare a Kubernetes Cluster.

Tenable Enclave Security System Requirements

Supported Kubernetes Environments

- **Kubernetes versions:** 1.30 to 1.33 in any of the following environments:
  - Standalone Kubernetes
  - Amazon Elastic Kubernetes Service (EKS)
  - AzureKubernetes Service (AKS)
  - GoogleKubernetes Engine (GKE)
- **Helm versions:** 3.11 and later
- **OpenShift versions:** 4.17 and later

Compatible Tenable Product Versions

The following table shows which versions of Security Center and Container Security are compatible with Tenable Enclave Security.

Tenable Enclave Security Version	Compatible Tenable Product Version
Tenable Enclave Security 1.8.x	Security Center 6.8.0

Tenable Enclave Security Version	Compatible Tenable Product Version
	Container Security 1.8.x

Cloud Requirements

For requirements specific to Tenable Security Center and Container Security, see the following topics:

- Tenable Container Security System Requirements
- Tenable Security Center System Requirements

Tenable strongly recommends using high-performance disks when you deploy Tenable Enclave Security in a Kubernetes cluster. Tenable Enclave Security is a disk-intensive application and using disks with high read/write speeds (for example, SSDs or NVMe SSDs) results in the best performance. The requirements in the following tables are based on AWS M5 or better processor specifications. Using slower processors, like those found in AWS M5a instances, will impact performance for your Tenable Enclave Security deployment.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Enclave Security	CPU	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	8000 m	32 GiB	90 days: 125 GB 180 days: 250 GB
2,501 to 10,000 active IPs	16000 m	64 GiB	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000 active IPs	32000 m	128 GiB	90 days: 2.4 TB 180 days: 5 TB
25,001 to 50,000 active IPs	48000 m	192 GiB	90 days: 4.5 TB 180 days: 9 TB

Requirements When Running Basic Network Scans + Local Checks + 1 Configuration Audit

# of Hosts Managed by Tenable Enclave Security	CPU	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	16000 m	64 GiB	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000 active IPs	32000 m	128 GiB	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000 active IPs	32000 m	128 GiB	90 days: 4.5 TB 180 days: 9 TB
25,001 to 50,000 active IPs	48000 m	192 GiB	90 days: 9 TB 180 days: 18 TB

Container Security in Tenable Enclave Security System Requirements

This page describes the following system requirements:

- Requirements for Container Security services
  - Database Changes in Container Security 1.6
- Self-hosted database requirements
- Cloud database requirements
  - AWS
  - Azure for PostgreSQL flexible servers
  - GCloud

Requirements for Container Security Services

Service Name	# of Assets Managed by Container Security	CPU per pod	Memory per pod
tes-consec-ui	1 to 25,000 images	4000 m	4 GiB

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

Database Changes in Container Security 1.6

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

The following are considerations for upgrading to Container Security 1.6:

- If the migration succeeds, the existing PVC will be deleted after 30 days.
- If the migration fails, the PVC will be deleted after 60 days. The data on the PVC will be recreated in the database when you run your first full scan after upgrading.
- There is no impact to Container Security features if the migration fails. The first full scan may run slower.
- Container Security 1.6 does not support database restore from database backups of previous Container Security versions.

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

Self-Hosted Database Requirements

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

Requirements for Container Security self-hosted database

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

Cloud Database Requirements

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

Requirements for Container Security database in AWS

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

Requirements for Container Security database in Azure for PostgreSQL flexible servers

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

Requirements for Container Security database in GCloud

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

Security Center in Tenable Enclave Security System Requirements

Tenable Security Center in Kubernetes Requirements

> **Note:** Tenable recommends using an empty Kubernetes cluster for Tenable Security Center deployments. These requirements assume that the Kubernetes cluster where you install Tenable Security Center has nothing else installed.

Tenable strongly recommends using high-performance disks when you deploy Tenable Security Center in a Kubernetes cluster. Tenable Security Center is a disk-intensive application and using disks with high read/write speeds (for example, SSDs or NVMe SSDs) results in the best performance. The requirements in the following tables are based on AWS M5 or better processor specifications. Using slower processors, like those found in AWS M5a instances, will impact performance for your Tenable Security Center in Kubernetes deployment.

For supported Kubernetes environments and installation instructions, see Tenable Security Center in Kubernetes.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable Security Center	CPU	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	24000 m	96 GiB	90 days: 125 GB 180 days: 250 GB
2,501 to 10,000 active IPs	48000 m	192 GiB	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000 active IPs	96000 m	384 GiB	90 days: 2.4 TB

# of Hosts Managed by Tenable Security Center	CPU	Memory	Disk Space used for Vulnerability Trending
			180 days: 5 TB
25,001 to 50,000 active IPs	144000 m	576 GiB	90 days: 4.5 TB 180 days: 9 TB

Requirements When Running Basic Network Scans + Local Checks + 1 Configuration Audit

# of Hosts Managed by Tenable Security Center	CPU	Memory	Disk Space used for Vulnerability Trending
1 to 2,500 active IPs	48000 m	192 GiB	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000 active IPs	96000 m	384 GiB	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000 active IPs	96000 m	384 GiB	90 days: 4.5 TB 180 days: 9 TB
25,001 to 50,000 active IPs	144000 m	576 GiB	90 days: 9 TB 180 days: 18 TB

Requirements for Tenable Security Center Services

Service	# of Hosts Managed by Tenable Security Center	CPU per pod	Memory per pod	Default pod replicas	Disk space
Reporting pod	1 to 2,500 active IPs	4 cores	8 GiB	1 per report (max 4)	Uses cluster storage

Service	# of Hosts Managed by Tenable Security Center	CPU per pod	Memory per pod	Default pod replicas	Disk space
					dedicated for the pod until report completion
	2,501 to 10,000 active IPs	8 cores	16 GiB		
	10,001 to 25,000 active IPs	16 cores	32 GiB		
	25,001 to 50,000 active IPs	24 cores	48GiB		
Job manager pod	1 to 50,000 active IPs	4 cores	4 GiB	1	N/A

External PostgreSQL Requirements

You can install Tenable Security Center configured to work with a PostgreSQL instance managed by you. PostgreSQL is required for certain features. For more information about connecting a PostgreSQL database, see Connect an External PostgreSQL Server.

This is a required configuration if you have more than 100K hosts. It is also recommended that `wal_segment_size` is set to be at least 64MB.

If you set up your PostgreSQL instance in a cloud environment, the following are guidelines for choosing your instance size. Note that the disk space in the following table is only for PostgreSQL data, and does not include any other OS or other dependencies you have.

# of Hosts Managed by Tenable Security Center	AWS	Azure	Google Cloud Platform (GCP)	Minimum Disk Space Required for PostgreSQL Data
2,500 active IPs	m6g.xlarge	D4s_v3	t2a-standard-4	20 GB
10,000 active IPs	m6g.2xlarge	D16s_v3	t2a-standard-8	50 GB
25,000 active IPs	m6g.4xlarge	D32s_v3	t2a-standard-16	100 GB
100,000 active IPs	m6g.8xlarge	D48s_v3	t2a-standard-32	400GB
250,000 active IP	m6g.16xlarge	D64s_v3	t2a-standard-48	1 TB

License Requirements

For instructions on how to download the Tenable Enclave Security license key, see Download License Key in the *Tenable Account Management guide*.

This topic breaks down the licensing process for Tenable Enclave Security. It also explains how assets are counted, lists add-on components you can purchase, and describes what happens during license overages or expirations.

Licensing Tenable Enclave Security

To use Tenable Enclave Security, you purchase licenses based on your organizational needs and environmental details. Tenable Enclave Security assigns those licenses to your *assets*, which are assessed hosts from Container Security or Security Center.

> **Note**: Tenable offers simplified pricing to managed security service providers (MSSPs). To learn more, contact your Tenable representative.

Tenable Enclave Security Products

The following table lists Tenable Enclave Security products that require licenses, along with the asset type licensed.

Product	Asset Type
Tenable Security Center	Assessed hosts from Tenable Security Center or imported from other Tenable products.
Container Security	Assessed container images. For more information, contact your Tenable representative.

Reclaiming Licenses

When you purchase Tenable licenses, your total license count is static for the length of your contract unless you purchase more licenses. However, Tenable Enclave Security products reclaim licenses under some conditions—and then reassign them to new assets in the same product so that you do not run out of licenses.

The following table explains how each Tenable Enclave Security product reclaims licenses.

Exceeding the License Limit

To allow for usage spikes due to hardware refreshes, sudden environment growth, or unanticipated threats, you can temporarily exceed your license limits in Tenable Enclave Security:

- **Tenable Security Center** - You can temporarily exceed your licensed IP address count by 10%. If you exceed this number, Tenable Security Center is disabled.

- **Tenable Enclave Security Container Security** - When you scan more assets than you have licensed, Tenable clearly communicates the overage and then reduces functionality in three stages:

Scenario	Result
You scan more assets than are licensed for three consecutive days.	A message appears in Tenable Enclave Security.
You scan more assets than are licensed for 15+ days.	A message and warning about reduced functionality appears in Tenable Enclave Security.

You scan more assets than are licensed for 45+ days.	A message appears in Tenable Enclave Security; scan and export features are disabled.

Tenable Enclave Security generates a warning in the user interface when you approach or exceed the license limit.

> **Tip**: Improper scan hygiene or product misconfigurations can cause scan overages, which result in inflated asset counts. To learn more, see Scan Best Practices.

Expired Licenses

The Tenable Enclave Security licenses you purchase are valid for the length of your contract. 30 days before your license expires, a warning appears in the user interface. During this renewal period, work with your Tenable representative to add or remove products or change your license count.

After your license expires, you can no longer sign in to the Tenable platform.

Prepare a Kubernetes Cluster

To determine whether your existing Kubernetes cluster meets the requirements for use with Tenable Enclave Security, see Tenable Enclave Security System Requirements.

Before you begin

- Configure a routable URL or external gateway.
- Determine whether to create a new Kubernetes or use an existing cluster.

Configure a Kubernetes cluster

1. Create a new Kubernetes cluster. For instructions on how to create a new cluster, see the Kubernetes documentation.

   -or-

   Use an existing cluster. To determine whether your existing cluster meets the requirements for your Tenable Enclave Security deployment, see Tenable Enclave Security System Requirements.

2. Define a default storage class on the cluster. For instructions on how to change the default storage class, see the Kubernetes documentation.

3. Install `cert-manager` in your Kubernetes cluster. For instructions on how to install cert-manager, see the cert-manager documentation.

   > **Note:** if you want to use your own certificates, contact your Tenable Support representative.

4. Install `cert-manager-csi-installer` in your Kubernetes cluster.

   > **Note:** Tenable Enclave Security recommends using the cert-manager CSI driver for provisioning certificates used by its services for mTLS. However, if the CSI driver cannot be installed on your cluster, you can disable the cert-manager CSI driver.

5. Configure the Container Security database. This database contains the data visible in the Container Security UI, including vulnerabilities, images, packages, and layers.

   Tenable recommends you use a managed PostgreSQL database service (for example, RDS, AWS, or GCP). If you want to host the database yourself, see the Kubegres documentation.

   PostgreSQL compatible versions

   - PostgreSQL 14.x
   - PostgreSQL 15.x
   - PostgreSQL 16.x (preferred)
   - PostgreSQL 17.x

6. Create a Kubernetes secret named `tes-pg-secrets` to identify characteristics about the database.

   ```
   kubectl apply --namespace tenable-enclave-security -f tes-pg-secrets.yaml
   ```

   > **Note:** Supported SSL modes include `prefer`, `require`, and `verify-ca`. The default SSL mode for Tenable Enclave Security services is `prefer`.

   The following is an example `tes-pg-secrets.yaml`:

```
apiVersion: v1
kind: Secret
type: Opaque
metadata:
  name: tes-pg-secrets
data:
  # All values below must be base64 encoded strings
  pg_host: # Hostname and optional port (e.g., db.example.com or db.example.com:5432)
  pg_user: # Admin username (must have CREATEDB and CREATEROLE permissions)
  pg_pass: # Password for the pg_user
  pg_ro_host: # Hostname for read-only replica (defaults to pg_host if not applicable)
  pg_ssl_mode: # Optional: SSL level. Use 'prefer' (default), 'require', or 'verify-ca'
  pg_ca_cert: # Required if pg_ssl_mode=verify-ca. The CA certificate content.
```

> **Note:** To encode `pg_ssl_mode` correctly on Linux or macOS, use: `echo -n "verify-ca" | base64` If you omit the `-n` flag, the encoded string will include a hidden "newline" character, which will cause the database driver to reject the SSL mode.

Tenable Enclave Security Helm Charts

Tenable Enclave Security leverages the Helm open-source package manager. When you install, configure, or upgrade Tenable Enclave Security, use this Helm Chart.

To download the Helm Chart for Tenable Enclave Security, go to https://github.com/tenable/helm-charts.

Helm Chart

Helm Chart	Description
tes-operator	Configures the namespace, persistent volume claim, and StatefulSet Pods to pull images from container registries.

`Values.yaml` Configuration

For a complete list of Helm Chart options, see https://github.com/tenable/helm-charts/tree/main/charts/tes-operator.

External PostgreSQL with Tenable Enclave Security

> **Note:** When reviewing external PostgreSQL documentation, ensure that you use the appropriate documentation version for the PostgreSQL version you deployed.

Requirements

Tenable Enclave Security requires a customer-managed PostgreSQL instance. This instance can reside within the same Kubernetes cluster as the Tenable Enclave Security deployment or be hosted externally, provided the services within the Kubernetes cluster have network access to the database instance.

Required Privileges for the Bootstrap User

To complete this setup, the database user must have the following permissions:

- **CREATEDB:** Allows the user to create service-specific databases.
- **CREATEROLE:** Allows the user to create distinct user accounts for those services and set passwords for them.

Required PostgreSQL extensions

- **PGCRYPTO**
- **PG_TRGM**

Functional Overview

Bootstrap User and Permissions

The PostgreSQL user credential you provide via the `tes-pg-secrets` secret acts as a bootstrap administrator. This user must have **CREATEDB** and **CREATEROLE** privileges.

Purpose of the Bootstrap User

Tenable Enclave Security consists of multiple microservices, such as the Tenable Enclave Security operator, Tenable Security Center, and Container Security.

Instead of sharing one set of credentials across all services, the installation process uses the credentials in `tes-pg-secrets` to automatically orchestrate a secure, isolated environment:

- **Dynamic Provisioning:** Upon deployment, a database initialization (DB init) job runs for each logical function. The bootstrap user accesses the database instance.
- **Dedicated Databases:** The process creates a separate, dedicated database for each microservice that requires PostgreSQL access. To maintain security best practices, services do not share databases.
- **Unique Service Credentials:** The process generates a unique application user role and a unique password for each service.
- **Least Privilege Access:** Once configured, individual services use these restricted credentials to operate, not the administrative credentials found in the secret.

Responsibility Matrix

When you use an external PostgreSQL server with Tenable Enclave Security, you are responsible for the following:

- Installing and configuring PostgreSQL.
- Backing up PostgreSQL.
- Securing PostgreSQL.
- Patching and upgrading PostgreSQL.
- Maintaining network connectivity to PostgreSQL from the Kubernetes cluster (for example, firewall rules and security groups).

Tenable is responsible for:

- The databases and structures created by Tenable Enclave Security services within PostgreSQL.

  > **Caution:** Do not directly access or modify any databases created by Tenable Enclave Security services. Unauthorized modifications can compromise data integrity and functionality.

- Data integrity and database-level configuration.

> **Note:** PostgreSQL database names use the namespace where you installed Tenable Enclave Security as a prefix.

Installation

You can use any currently supported version of PostgreSQL. Supported versions include:

- PostgreSQL 14.x
- PostgreSQL 15.x
- PostgreSQL 16.x (preferred)
- PostgreSQL 17.x

Tenable follows the PostgreSQL lifecycle and removes support after the final release of a major version. For example, Tenable will not support PostgreSQL 14.x after November 2026.

Review the PostgreSQL documentation for installation instructions. You can use a managed instance of PostgreSQL from a cloud vendor if the instance meets the requirements listed in this document.

> **Note:** If you use an external PostgreSQL database and you uninstall Tenable Enclave Security, the associated PostgreSQL database remains. Contact your database administrator to remove the database and ensure you maintain any required backups.

Configuration

See the System Requirements for specific requirements.

Security

Tenable recommends that you implement a PostgreSQL security baseline if you host your own PostgreSQL instance. Examples include the Center for Internet Security (CIS) PostgreSQL Benchmark or the Crunchy Data PostgreSQL Security Technical Implementation Guide (STIG).

Tenable does not provide support for implementing these benchmarks. Certain configurations may impact Tenable Enclave Security performance or functionality.

Implementation of security benchmarks may require you to add external extensions to PostgreSQL, such as `pgaudit` and `pgcrypto`. Tenable does not provide support or documentation for the installation or configuration of these extensions.

Patching and Upgrades

Note: You must shut down Tenable Security Center before you patch or upgrade PostgreSQL.

Tenable recommends that you:

- Monitor PostgreSQL security updates and apply relevant security patches after testing.
- Back up your Tenable Enclave Security databases before you patch or upgrade PostgreSQL.

Install Tenable Enclave Security

This topic describes how to install Tenable Enclave Security in a Kubernetes cluster. To update an existing Tenable Enclave Security deployment, see Update Tenable Enclave Security.

- Install Tenable Enclave Security
- Install Tenable Enclave Security in an air-gapped environment
- Install Tenable Enclave Security using OpenShift

Before You Begin

- You must have a Kubernetes cluster in a supported Kubernetes environment. For more information, see Supported Kubernetes Environments and Prepare a Kubernetes Cluster.
- Download the kubectl binaries. For more information, see the Kubernetes documentation.
- Update your kubeconfig file to allow kubectl to communicate with the Kubernetes cluster.
- Download the Helm binaries. For more information, see the Helm documentation.

Install Tenable Enclave Security

1. Create a Kubernetes cluster or configure an existing Kubernetes cluster that meets the system requirements for Tenable Enclave Security.
2. In the Kubernetes cluster where you want to install Tenable Enclave Security, create a namespace using the following command:

```
kubectl create namespace tenable-enclave-security
```

In this example, the namespace is *tenable-enclave-security*. You can use a namespace of your choice, just make sure you use the same namespace every time you install or upgrade Tenable Enclave Security.

3. Obtain the namespace ID for the namespace created in step 2:

   ```
   kubectl get namespace tenable-enclave-security --output jsonpath='{.metadata.uid}'
   ```

   > **Tip:** You can disable cluster roles for Tenable Enclave Security using the helm option Tenable Enclave Security Helm Charts.

4. Obtain a Tenable Enclave Security license file and save it to your local environment.

5. Add your license to the namespace that you created in step 2 using the following command:

   ```
   kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
   file=license=directory/license.key
   ```

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

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

7. Update the repository:

   ```
   helm repo update
   ```

8. Install the Helm Chart or upgrade an existing Helm Chart.

   > **Note:** The values in these steps are based on a setup with 10,000 active IP addresses. For minimum requirements for your environment, see Tenable Enclave Security System Requirements.

   a. Create a `values.yaml` file with parameters sized to your deployment. The following is an example `values.yaml`:

      ```
      tes:
      ```

```
blades:
  securitycenter:
    resources:
      limits:
        cpu: 32000m
        memory: 128Gi
      requests:
        cpu: 32000m
        memory: 128Gi
    persistentVolumeClaim:
      size: 5000Gi
```

> **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. For more information, see Values.yaml Configuration.

b. To install the Helm Chart, run the following command:

```
helm install tes-operator --namespace tenable-enclave-security -f values.yaml
tenable/tes-operator
```

9. Push the updated Tenable Enclave Security license file using the following commands:

a.

```
kubectl --namespace tenable-enclave-security delete secret tes-license
```

b.

```
kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
file=license=directory/license.key
```

10. Access Tenable Enclave Security via the URL that you defined in Prepare a Kubernetes Cluster.

Install Tenable Enclave Security in an air-gapped environment

1. Obtain the Helm Charts and publish them locally.

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

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

   b. Update the repository:

```
helm repo update
```

2. Contact your Tenable support representative for a list of required container images and tags for your version of Tenable Enclave Security, and add the container images and tags to your internal image registry.

   (Optional) Use the following script to download tes-operator and all required container images.

   ```
   #!/usr/bin/env bash

   TEMP_DIR=$(mktemp -d)
   ARCHIVE="tes-offline.tar.gz"

   cleanup() {
       rm -rf "$TEMP_DIR"
   }
   trap cleanup EXIT

   helm repo add tenable https://charts.tenable.com
   helm repo add jetstack https://charts.jetstack.io

   helm pull tenable/tes-operator --untar --untardir "$TEMP_DIR"
   helm pull jetstack/cert-manager --untar --untardir "$TEMP_DIR"

   manifest_images=()

   while IFS= read -r line || [[ -n "$line" ]]; do
       if [[ -n "$line" && ! "$line" =~ ^# ]]; then
           manifest_images+=("$line")
       fi
   done < "$TEMP_DIR/tes-operator/image-manifest.txt"

   for IMAGE in "${manifest_images[@]}"; do
     IMAGE_ARCHIVE="$TEMP_DIR/$(echo "$IMAGE" | sed 's/[/:]/_/g').tar"

     echo "Downloading Docker image: $IMAGE"
     (export DOCKER_CLI_HINTS=false; docker pull "$IMAGE")
     echo "Saving Image $IMAGE to $IMAGE_ARCHIVE"
     docker save -o "$IMAGE_ARCHIVE" "$IMAGE"
     printf "\n"
   done

   tar -czf "$ARCHIVE" -C "$TEMP_DIR" .

   echo "TES offline bundle created successfully. Output archive: $ARCHIVE"
   ```

3. Obtain a new license if needed. For more information, see License Tenable Enclave Security Offline.

4. Install the Helm Chart or upgrade an existing Helm Chart.

   > **Note:** The values in these steps are based on a setup with 10,000 active IP addresses. For minimum requirements for your environment, see Tenable Enclave Security System Requirements.

   a. Create a `values.yaml` file with your private registry information. The following is an example `values.yaml` for an air-gapped deployment:

   ```
   operator:
     image:
       registry: some-private-registry.example.com # private image registry hostname
       imagePullSecret: registrypullsecret # private image registry access secret, if needed

   tes:
     blades:
       securitycenter:
         resources:
           limits:
             cpu: 32000m
             memory: 128Gi
           requests:
             cpu: 32000m
             memory: 128Gi
         persistentVolumeClaim:
           size: 5000Gi
   ```

   > **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. For more information, see Values.yaml Configuration.

   b. To install the Helm Chart, run the following command:

   ```
   helm install tes-operator --create-namespace --namespace tenable-enclave-security -f
   values.yaml tenable/tes-operator
   ```

5. Update the repository:

   ```
   helm repo update
   ```

6. Upgrade the Tenable Enclave Security operator using the following command:

   ```
   helm upgrade tes-operator --create-namespace --namespace tenable-enclave-security -f
   values.yaml tenable/tes-operator
   ```

7. Add your license to the namespace using the following command:

   ```
   kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
   file=license=directory/license.key
   ```

8. Access Tenable Enclave Security via the URL that you defined in [Prepare a Kubernetes Cluster]().

Install Tenable Enclave Security using OpenShift

> **Note:** Tenable Enclave Security does not support Network File System (NFS) storage types. If you use NFS persistent storage on the platform where you run Tenable Enclave Security, then Tenable Enclave Security may crash or become unstable.

1. Create an OpenShift cluster that meets the system requirements for Tenable Enclave Security.

2. In the OpenShift cluster where you want to install Tenable Enclave Security, create a namespace using the following command:

   ```
   kubectl create namespace tenable-enclave-security
   ```

   In this example, the namespace is *tenable-enclave-security*. You can use a namespace of your choice, just make sure you use the same namespace every time you install or upgrade Tenable Enclave Security.

3. Label the namespace, cert manager, Container Storage Interface (CSI) driver, and persistent CSI driver with a pod security standard of `baseline` or higher using the following commands:

   ```
   kubectl label csidriver csi.cert-manager.io  security.openshift.io/csi-ephemeral-volume-
   profile=baseline

   kubectl label ns tenable-enclave-security pod-security.kubernetes.io/enforce=baseline
   ```

   If you do not want to label the CSI driver, use the `privileged` namespace pod security standard:

   ```
   kubectl label ns tenable-enclave-security pod-security.kubernetes.io/enforce=privileged
   ```

4. Get the cluster ID using the following command:

   ```
   kubectl get namespace kube-system --output jsonpath={.metadata.uid}
   ```

5. Obtain a Tenable Enclave Security license file and save it to your local environment.

6. Add your license to the namespace that you created in step 2 using the following command

   ```
   kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
   file=license=directory/license.key
   ```

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

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

8. Update the repository:

   ```
   helm repo update
   ```

9. Install the Helm Chart or upgrade an existing Helm Chart.

   > **Note:** The values in these steps are based on a setup with 10,000 active IP addresses. For minimum requirements for your environment, see Tenable Enclave Security System Requirements.

   a. Create a `values.yaml` file with parameters sized to your deployment. The following is an example `values.yaml`:

      ```
      tes:
        blades:
          securitycenter:
            resources:
              limits:
                cpu: 32000m
                memory: 128Gi
              requests:
                cpu: 32000m
                memory: 128Gi
            persistentVolumeClaim:
              size: 5000Gi
      ```

> **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. For more information, see Values.yaml Configuration.

b. To install the Helm Chart, run the following command:

```
helm upgrade --install tes-operator --namespace tenable-enclave-security -f values.yaml
tenable/tes-operator
```

10. Push the updated Tenable Enclave Security license file using the following commands:

a.

```
kubectl --namespace tenable-enclave-security delete secret tes-license
```

b.

```
kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
file=license=directory/license.key
```

What to do next

- Configure Tenable Enclave Security using the setup steps in the UI. For more information, see Configure Tenable Enclave Security.

Update Tenable Enclave Security

This topic describes how to update an existing Tenable Enclave Security deployment. To install Tenable Enclave Security for the first time, see Install Tenable Enclave Security.

Update Tenable Enclave Security

1. Obtain a Tenable Enclave Security license file and save it to your local environment.
2. Update the repository:

```
helm repo update
```

3. To update the Helm Chart, run the following command:

```
helm upgrade tes-operator --namespace tenable-enclave-security -f values.yaml tenable/tes-
operator
```

4. If your update includes new licensed products, push your license to the namespace using the following command:

   ```
   kubectl --namespace tenable-enclave-security create secret generic tes-license --from-
   file=license=directory/license.key
   ```

5. Access Tenable Enclave Security via the URL that you defined in Prepare a Kubernetes Cluster.

Configure Tenable Enclave Security

When you access the Tenable Enclave Security user interface for the first time, the **Setup** page appears. On the **Setup** page, you'll create your Super Administrator user account, set up your first organization, and create a Security Manager user account.

Before you begin:

- Install Tenable Enclave Security

Configure Tenable Enclave Security:

1. In a web browser, access Tenable Enclave Security at the URL that you defined in Prepare a Kubernetes Cluster.

2. Set up your Super Administrator user account, and click **Next**.

   Super Administrator options

Option	Description
First Name	The first name for the user.
Last Name	The last name for the user.
User Name	The username for the Super Administrator account.

Option	Description
Password	The unique password for the Super Administrator account.
Confirm Password	The same password you entered in the **Password** box.

3. Set up an organization, and click **Next**.

   For more information about organizations, see Organizations.

Organization options

Option	Description	Default
General		
Name	The name for the organization.	--
Description	A description for the organization.	--
Address	The address for the organization.	--
City	The city for the organization.	--
State	The city for the organization.	--
Phone	The phone number for the organization.	--
Password Expiration		
Enable Password Expiration	When enabled, the user's password will expire after the number of days specified in the **Expiration Days** box. The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the next login. When disabled, the user's password expiration settings will default to the organization settings.	disabled

Option	Description	Default
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365.	--
Container Security		
Scanner Key Expiration	The number of days before the user's scanner key expires.	90
Scanning		
Distribution Method	The scan distribution mode you want to use for this organization: • **Automatic Distribution Only** - The scanner chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan. • **Locked Zone** - The scanner uses the scan zone(s) you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan. • **Selectable Zones** - The scanner allows organizational users to select a scan zone when configuring a scan. This mode allows organizational users to use scanners to run internal and external vulnerability scans and analyze the vulnerability stance from a new perspective. For example, an organizational user can choose an	Automatic Distribution Only

Option	Description	Default
	external scanner to see the attack surface from an external attacker's perspective.	
Scan Zones	One or more scan zones for the organization. Scan zones are areas of your network that you want to target in an active scan, associating an IP address or range of IP addresses with one or more scanners in your deployment. For more information about scan zones, see	--
Allow for Automatic Distribution	Enable or disable this option to specify whether you want the scanner to select one or more scan zones automatically if an organizational user does not specify a scan zone when configuring a scan. • When enabled, the scanner chooses one or more scan zones that you specify in the **Restricted Scan Ranges** setting. • When disabled, the scanner requires the organizational user to specify a scan zone when configuring a scan.	disabled
Restricted Scan Ranges	The IP address ranges you do not want users in this organization to scan.	--
Analysis		
Accessible LCEs	The Log Correlation Engines that you want this organization to have access to. You can search for the Log Correlation Engines by name or scroll through the list.	--

Option	Description	Default
Accessible Repositories	The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.	--
Accessible Agent Capable Scanners	The Tenable Nessus scanners (with Tenable Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the organization to import Tenable Agent results from the selected scanner.	--
Accessible LDAP Scanners	The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets. **Note:** If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.	--
Custom Analysis Links		
Link Name	A name for the custom analysis link. You can use custom analysis links to reference additional data external to Tenable Enclave Security.	--
URL	The custom analysis link URL that will appear in the host vulnerability details. For example,	--

Option	Description	Default
	`http://example.com/index.htm?ip=%ip%` .The *%ip%* reference is a variable that inserts the IP address of the current host into the specified URI.	
Vulnerability Weights		
Vulnerability Weights	The vulnerability weighting to apply to vulnerabilities with the specified criticality: - **Low** - The vulnerability weighting to apply to Low criticality vulnerabilities for scoring purposes. (Default: 1) - **Medium** - The vulnerability weighting to apply to Medium criticality vulnerabilities for scoring purposes. (Default: 3) - **High** - The vulnerability weighting to apply to High criticality vulnerabilities for scoring purposes. (Default: 10) - **Critical** - The vulnerability weighting to apply to Critical criticality vulnerabilities for scoring purposes. (Default: 40)	Medium
Vulnerability Scoring System		
Scoring System	The scoring system the scanner uses to assess the severity of vulnerabilities: **CVSS v2** or **CVSS v3**. **Note:** Changing the Scoring System while the scanner is running certain operations, such as preparing reports or dashboard	CVSS v2

Option	Description	Default
	data, results in data using mixed CVSS v2 and CVSS v3 scores. **Note:** Changing the Scoring System does not impact historical dashboard trend data. For example, if you change the Scoring System from CVSS v2 to CVSS v3, dashboard trend data before the change displays CVSS v2 scores while dashboard trend data after the change displays CVSS v3 scores.	

4. Configure a Security Manager account, and click **Finish**.

Security Manager Options

Option	Description	Default
Configure Product Access		
Role	The role for the user.	Security Manager
Organization	The organization that the user belongs to.	--
General		
First Name	The first name for the user.	--
Last Name	The last name for the user.	--
Type	The authentication type for the user account: • **Tenable (TNS)** • **Lightweight Directory Access Protocol (LDAP)** • **Security Assertion Markup Language (SAML)**	TNS

Option	Description	Default
	You must configure an LDAP server or SAML authentication in order to select **LDAP** or **SAML** from the **Type** drop-down box.	
User Name	The username for the user account. The username is case-sensitive.	--
Password	The password for the user account. **Tip:** Tenable recommends using passwords that meet stringent length and complexity requirements.	--
Confirm Password	The same password you entered in the **Password** box.	--
User Must Change Password	When enabled, the user must change their password when they log in for the first time.	disabled
Time Zone	The time zone for the user.	
Scan Result Default Timeframe	The default **Completion Time** filter applied when the user accesses or refreshes the scan results.	
Cached Fetching	When enabled, Tenable Enclave Security caches plugin policy information and performs plugin policy downloads once per page load.	
Password Expiration		
Enable Password Expiration	When enabled, the user's password will expire after the number of days specified in the **Expiration Days** box. The user will receive daily password expiration notifications at login, starting 14 days before the	disabled

Option	Description	Default
	password expires. After the password expires, the user must change their password at the next login. When disabled, the user's password expiration settings will default to the organization settings.	
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365.	--

Settings and Information

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

For more information, see the following topics:

- Access Control
  - Users
  - Roles
  - Groups
  - Organizations
- Authentication
  - LDAP Authentication
  - SAML Authentication
- System Logs
- Licenses
- Configuration
  - Edit Plugin and Feed Settings and Schedules
  - Configure Plugin Text Translation
  - API Key Authentication
- Diagnostics
- Job Queue
- Publishing Sites

Access Control

To view your users, user roles, groups, and organizations, in the top navigation bar, click ⚙ **Settings & Information** > **Access Control**.

For more information, see the following topics:

- Users
- Roles
- Groups
- Organizations

Users

To view a list of your Tenable Enclave Security users, in the top navigation bar, click ⚙ **Settings & Information** > **Access Control**.

On the **Users** page, you can view your user accounts, add new user accounts, manage user accounts, and delete user accounts.

For information about configuring LDAP and SAML authentication, see Authentication.

Roles

To view your user roles, in the top navigation bar, click ⚙ **Settings & Information** > **Access Control**, then click the **Roles** tab.

This page describes the roles that you can assign to users in Tenable Enclave Security.

Role	Description
Super Administrator	Super Administrator users have the system-provided Super Administrator role and do not belong to any organization. You can create Super Administrator users when you configure Tenable Enclave Security.
Organizational Users - Users that belong to an organization.	
Security Manager	The Security Manager role has full access to all actions at the organization level. A Security Manager has the ability to create new groups and manage existing ones. A Security Manager can also define how users interact with other groups.\n\nThe ability to manage other users and their objects can be configured using group permissions on the Access tab of User add/edit. This includes viewing and stopping running scans and reports.

Role	Description
	The Security Manager role also includes the Exposure Response Manager permission. Exposure Response Managers can edit and delete shared combinations in Container Security.
Auditor	The Auditor role can access summary information to perform third-party audits. An Auditor can view dashboards, reports, and logs, but cannot perform scans or create tickets.
Credential Manager	The Credential Manager role can be used specifically for handling credentials. A Credential Manager can create and share credentials without revealing the contents of the credential. This can be used by someone outside the security team to keep scanning credentials up to date.
Executive	The Executive role is for users who are interested in a high-level overview of their security posture and risk profile. Executives would most likely browse dashboards and review reports, but would not be concerned with monitoring running scans or managing users. Executives would also be able to assign tasks to other users using the ticketing interface.
Security Analyst	The Security Analyst role has permissions to perform all actions at the Organizational level except managing groups and users. A Security Analyst is most likely an advanced user who can be trusted with some system-related tasks such as setting freeze windows or updating plugins. The Security Manager role also includes the Exposure Response Manager permission. Exposure Response Managers can edit and delete shared combinations in Container Security.
Vulnerability Analyst	The Vulnerability Analyst role can perform basic tasks within the application. A Vulnerability Analyst is allowed to view security data, perform scans, share objects, view logs, and work with tickets.
Custom Role	A custom role that you create by enabling or disabling individual permissions.

Groups

To view the **Groups** table, in the top navigation bar, click ⚙ **Settings & Information** > **Access Control**, then click the **Groups** tab.

User groups are a way to group rights to objects within an organization, and then quickly assign these rights to one or more users. A user's group membership determines their access to security data. When a user creates various objects such as reports, scan policies, dashboards, and other similar items, these objects are automatically shared among the group members if the group permissions allow view and control.

Group Options

Option	Description
General tab	
Name	The name for the group.
Description	A description for the group (e.g., **security team at the central office** or **executives on the east coast**).
Viewable Hosts	The IP addresses and agent IDs that are viewable by the group. The selection is made by all defined assets or the selection of one or more asset lists.
Repositories	The repositories you want to share with the group.
Log Correlation Engines	The Log Correlation Engines you want to assign to the group.
Container Security Resources	The Container Security images you want to be available to users in the group.
Sample Content	When enabled, Tenable provides sample content objects to users in the group: • sample dashboards (**Executive 7 Day**, **Executive Summary**, and **Vulnerability Overview**) • sample reports (**Critical and Exploitable Vulnerabilities**, **Monthly Executive**, and **Remediation Instructions by Host**)

Option	Description
	• sample ARCs (**CCC 1: Maintain an Inventory of Software and Hardware**, **CCC 2: Remove Vulnerabilities and Misconfigurations**, **CCC 3: Deploy a Secure Network**, **CCC 4: Authorize Users**, **and CCC 5: Search for Malware and Intruders**) • sample assets required for the sample ARCs After enabling **Sample Content**, you must add a new user to the group before all users in the group can access the sample content. **Note:** If a user in a group deletes a sample content object, the object is deleted for all other users in that group. **Note:** If you move a sample content object owner (e.g., move the first user in group A to group B), Tenable Enclave Security: 1. Assigns their dashboards and ARCs to a new sample content object owner in group A. Tenable Enclave Security does not reassign reports or assets. 2. Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable Enclave Security does not recreate reports.
Share to Group tab	
Available Objects	The list of available objects to be shared with the group on creation or edit in a bulk operation.

Organizations

Required User Role: Administrator

To view your organizations, in the top navigation bar, click ⚙ **Settings & Information** > **Access Control**, then click the **Organizations** tab.

An *organization* is a set of distinct users and groups and the resources (for example, scanners, repositories, and LDAP servers) they have available to them.

The organization is managed primarily by the administrator users and security manager users. The administrator user creates the organization and creates, assigns, and maintains the security manager user account. The security manager user (or any organizational user with appropriate permissions) creates other users within the organization. Groups allow you to manage users and share permissions to resources and objects among the group.

Multiple organizations can share the same repositories, and the vulnerability data associated with the overlapping ranges is shared between each organization. Conversely, organizations can be configured with their own discrete repositories to facilitate situations where data must be kept confidential between different organizational units.

Creation of an organization is a multi-step process. After you create an organization, Tenable Enclave Security prompts you to create the initial security manager user.

To view the users in an organization, filter by the organization on the Users page.

Organization Options

Option	Description
General	
Name	(Required) The organization name.
Description	A description for the organization.
Contact Information	The relevant contact information for the organization including address, city, state, country, and phone number.
Password Expiration	
Enable Password Expiration	When enabled, passwords for users in the organization will expire after the number of days specified in the **Expiration Days** box.
Expiration Days	The number of days before the user's password expires. You can enter a number between 1 and 365. The user will receive daily password expiration notifications at login, starting 14 days before the password expires. After the password expires, the user must change their password at the

Option	Description
	next login.
Container Security	
Scanner Key Expiration	The number of days before the user's scanner key expires.
Container Security Resources	The Container Security images you want to be available to users in the group.
Scanning	
Distribution Method	The scan distribution mode you want to use for this organization: • **Automatic Distribution Only**: Tenable Enclave Security chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan. Tenable Enclave Security distributes targets for scans based on your configured scan zone ranges. This facilitates optimal scanning and is useful if an organization has devices placed behind a firewall or NAT device or has conflicting RFC 1918 non-internet-routable address spaces. • **Locked Zone**: Tenable Enclave Security uses the one **Available Zone** you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan. • **Selectable Zones**: Tenable Enclave Security allows organizational users to select a scan zone when configuring a scan. This mode allows organizational users to use scanners to run internal and external vulnerability scans and analyze the vulnerability stance from a new perspective. For

Option	Description
	example, an organizational user can choose an external scanner to see the attack surface from an external attacker's perspective.
Available Zones	One or more scan zones that you want organizational users to have access to when configuring scans.
Allow for Automatic Distribution	Enable or disable this option to specify whether you want Tenable Enclave Security to select one or more scan zones automatically if an organizational user does not specify a scan zone when configuring a scan. - When enabled, Tenable Enclave Security chooses one or more scan zones as specified by your **Restrict to Selected Zones** setting. - When disabled, Tenable Enclave Security requires the organizational user to specify a scan zone when configuring a scan.
Restrict to Selected Zones	If **Allow for Automatic Distribution** is enabled, enable or disable this option to specify the zones you want Tenable Enclave Security to choose from when automatically distributing zones. - When enabled, Tenable Enclave Security chooses from the **Available Zones** shared with the organization. - When disabled, Tenable Enclave Security chooses from all zones on Tenable Enclave Security.
Restricted Scan Ranges	The IP address ranges you do not want users in this organization to scan.
Analysis	
Accessible Repositories	The repositories that you want this organization to have access to. You can search for the repositories by name or

Option	Description
	scroll through the list.
Accessible LCEs	The Log Correlation Engines that you want this organization to have access to. You can search for the Log Correlation Engines by name or scroll through the list.
Accessible Agent Capable Scanners	The Tenable Nessus scanners (with Tenable Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the organization to import Tenable Agent results from the selected scanner.
Accessible LDAP Servers	The LDAP servers that you want this organization to have access to. An organization must have access to an LDAP server to perform LDAP authentication on user accounts within that organization, and to configure LDAP query assets. **Note:** If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.
Custom Analysis Links	
A list of custom analysis links provided to users within the host vulnerability details when analyzing data outside of Tenable Enclave Security is desired. Click **Add Custom Link** to create a new option to type the link name and URL to look up additional data external to Tenable Enclave Security. For example: *http://example.com/index.htm?ip=%ip%* The *%ip%* reference is a variable that inserts the IP address of the current host into the specified URI.	
Vulnerability Weights	
Low	The vulnerability weighting to apply to **Low** criticality vulnerabilities for scoring purposes. (Default: 1)
Medium	The vulnerability weighting to apply to **Medium** criticality

Option	Description
	vulnerabilities for scoring purposes. (Default: 3)
High	The vulnerability weighting to apply to **High** criticality vulnerabilities for scoring purposes. (Default: 10)
Critical	The vulnerability weighting to apply to **Critical** criticality vulnerabilities for scoring purposes. (Default: 40)
Vulnerability Scoring System	
Scoring System	The scoring system Tenable Enclave Security uses to assess the severity of vulnerabilities: **CVSS v2** or **CVSS v3**. **Note:** Changing the **Scoring System** while Tenable Enclave Security is running certain operations, such as preparing reports or dashboard data, results in data using mixed CVSS v2 and CVSS v3 scores. **Note:** Changing the **Scoring System** does not impact historical dashboard trend data. For example, if you change the **Scoring System** from **CVSS v2** to **CVSS v3**, dashboard trend data before the change displays CVSS v2 scores while dashboard trend data after the change displays CVSS v3 scores.
Reporting	
Publishing Sites	You can configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site. For more information, see Publishing Sites.

Authentication

To view your LDAP and SAML configurations, in the top navigation, click ⚙**Settings & Information** > **Authentication**.

For more information, see the following topics:

LDAP Authentication

SAML Authentication

LDAP Authentication

Adding LDAP servers allows you to use one or more external LDAP servers for Tenable Enclave Security user account authentication. LDAP authentication enhances the security of Tenable Enclave Security by inheriting password complexity requirements from environments mandated by security policy.

After you configure an LDAP server, create Tenable Enclave Security user accounts for each LDAP user you want to grant access.

Then, users with LDAP-authenticated accounts can log in to Tenable Enclave Security using the **Sign In Using Identity Provider** button.

> **Note:** Tenable Enclave Security does not support Microsoft Active Directory Lightweight Directory Services (AD LDS) servers for LDAP authentication.

> **Note:** Tenable Enclave Security cannot retrieve more than one page of LDAP results. If Tenable Enclave Security asset list or user authentication queries are not retrieving all expected results, consider modifying your LDAP pagination control settings to increase the results per page.

SAML Authentication

You can configure SAML authentication so that Tenable Enclave Security users can use identity provider-initiated single sign-on (SSO) when logging in to Tenable Enclave Security. Tenable Enclave Security supports SAML 2.0-based authentication (for example, Okta, OneLogin, Microsoft ADFS, or Shibboleth 2.0).

After you configure SAML authentication, create Tenable Enclave Security user accounts for each SAML user you want to grant access.

Then, users with SAML-authenticated accounts can log in to Tenable Enclave Security using the **Sign In Using Identity Provider** button.

System Logs

To view your system logs, in the top navigation, click ⚙**Settings & Information** > **System Logs**.

Tenable Enclave Security logs contain detailed information about functionality to troubleshoot unusual system or user activity. You can use the system logs for debugging and maintaining an audit trail of users who access Tenable Enclave Security or perform basic functions (for example, changing passwords).

Licenses

The **Licenses** page displays your license details and expiration. For information about licensing in Tenable Enclave Security, see License Requirements.

When you obtain a license for Tenable Enclave Security, you will receive an activation code.

Your activation code:

- is a one-time code, unless your license or subscription changes, at which point Tenable issues you a new activation code.
- must be used with the Tenable Enclave Security installation within 24 hours.
- cannot be shared between Tenable Enclave Security deployments.
- is not case-sensitive.
- is required to manage Tenable Enclave Security offline.

Download Tenable Enclave Security License Key

For instructions on how to download the Tenable Enclave Security license key, see Download License Key in the *Tenable Account Management guide*.

License Tenable Enclave Security Online

When you obtain your license, upload the license file to the Tenable Enclave Security user interface.

To upload a license file to Tenable Enclave Security:

1. Log in to Tenable Enclave Security via the user interface with an administrator user account.
2. In the top navigation, click ⚙ **Settings & Information** > **Licenses**.

   The **License Configuration** page appears.

3. Click the **License file** box.

   -or-

   Click **Upload**.

   A file explorer window appears.

4. In the file explorer window, select your license file.

   Your Tenable Enclave Security license is uploaded.

License Tenable Enclave Security Offline

If you want to register an offline Tenable Enclave Security deployment with a license, use the following procedure.

To manage Tenable Enclave Security offline, you need two computers: the Tenable Enclave Security deployment, which is not connected to the internet, and another computer that is connected to the internet.

To register an offline Tenable Enclave Security server's license:

1. Download and copy the license file on a system *with* internet access. Then, download and copy the license to the offline system running Tenable Enclave Security.

2. Register your license on the offline system running Tenable Enclave Security.

Configuration

Required User Role: Administrator

To view your configuration settings, in the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Configuration**.

Mail

The **Mail Configuration** page displays SMTP settings for all email-related Tenable Enclave Security functions. Click the **Test SMTP Settings** button to validate the settings.

Option	Description	Default
Host	The SMTP server host.	--
Port	The SMTP server port.	--
Authentication Method	The authentication method Tenable Enclave Security uses to connect to the SMTP server: • **None** - Tenable Enclave Security does not authenticate the connection. • **Login** - Tenable Enclave Security secures the connection with login authentication. • **Plain** - Tenable Enclave Security secures the connection with plain (username/password) authentication. • **CRAM-SHA1** - Tenable Enclave Security secures the connection with CRAM-SHA1 authentication. • **CRAM-MD5** - Tenable Enclave Security secures the connection with CRAM-SHA1 authentication.	--
Username	The username that Tenable Enclave Security uses to authenticate to the SMTP server. **Note:** Type the **Username** in a format supported by your SMTP server (for example, *username@domain.com* or *domain\username*).	--
Password	The password that Tenable Enclave Security uses to authenticate to the SMTP server.	--
Encryption	The email encryption type: • **None** - Tenable Enclave Security does not encrypt the email. • **TLS** - Tenable Enclave Security forces TLS	--

Option	Description	Default
	encryption for the email. • **SSL** - Tenable Enclave Security forces SSL encryption for the email. • **TLS, if available** - Tenable Enclave Security uses TLS encryption if the receiving server is compatible.	
Return Address	The email address that appear as the sender in the scan results email. **Note:** Use a valid return email address for this option. If this option is empty or the email server requires emails from valid accounts, the email server cannot send the email.	--
Verify Peer	When enabled, Tenable Enclave Security requests peer verification for SMTP servers using SSL or TLS connections.	disabled
Verify Peer Name	When enabled, Tenable Enclave Security requests peer name verification for SMTP servers using SSL or TLS connections.	disabled
Allow Self Signed Certificates	When enabled, Tenable Enclave Security allows connections to the SMTP server using self-signed SSL certificates.	enabled

Miscellaneous

The **Miscellaneous Configuration** page displays options for the web proxy and syslog forwarding.

Web Proxy

Use these settings to configure a web proxy.

Option	Description	Default
Host	The host URL (proxy hostname or IP address) of the web proxy server. The hostname used must resolve properly from the Tenable Enclave Security host.	--
Port	The port of the web proxy server.	--
Authentication Type	The authentication type Tenable Enclave Security uses to connect to the web proxy server. Select one of the following: • **Basic** - Tenable Enclave Security uses basic authentication, which encodes the username and password with Base64. • **NTLM** - Tenable Enclave Security uses NTLM authentication.	--
Username	The username that Tenable Enclave Security uses to authenticate to the web proxy server.	--
Password	The password that Tenable Enclave Security uses to authenticate to the web proxy server.	--

Syslog

Use these settings to allow Tenable Enclave Security to send administrative log events to the local syslog service.

Option	Description	Default
Enable Forwarding	Enables log forwarding options.	disabled
Facility	Type the facility you want to receive the log messages.	*LOG_USER*
Severity	Specifies which syslog message levels you want to	Informational

Option	Description	Default
	forward: **Informational**, **Warning**, or **Critical**.	

License

The **License Configuration** page displays your license details, usage, and expiration dates. For information about licensing in Tenable Enclave Security, see Licenses.

Plugins / Feed

The **Plugins/Feed Configuration** page displays the Plugin Detail Locale for Tenable Enclave Security and the feed and plugin update schedules.

Plugin Detail Locale

The local language plugin feature allows you to display portions of plugin data in local languages. When available, translated text displays on all pages where plugin details appear.

Select **Default** to display plugin data in English.

> **Note:** Tenable Enclave Security cannot translate text within custom files. Upload a translated **Active Plugins**`.xml` file to display the file content in a local language.

For more information, see Configure Plugin Text Translation.

Schedules

Tenable Enclave Security automatically updates Tenable Enclave Security feeds, active plugins, passive plugins, and event plugins. If you upload a custom feed or plugin file, the system merges the custom file data with the data contained in the associated automatically updating feed or plugin.

You can upload `tar.gz` files with a maximum size of 1500 MB.

Update	Description
Tenable Security Center Feed	Retrieves the latest Tenable Security Center feed from Tenable. This feed includes data for general use, including templates (for example, dashboards, ARCs, reports, policies, assets, and audit files), template-required objects, some general plugin information, and updated VPR

Update	Description
	values.
Active Plugins	Retrieves the latest active plugins feed (for Tenable Nessus and Tenable Vulnerability Management scanners) from Tenable. Tenable Security Center pushes the feed to Tenable Nessus and Tenable Vulnerability Management scanners.
Passive Plugins	Retrieves the latest passive plugins feed from Tenable. Tenable Security Center pushes the feed to Tenable Network Monitor instances.
Event Plugins	Retrieves the latest event plugins feed from Tenable. Tenable Security Center uses the feed locally with Log Correlation Engine data but does not push the feed to Log Correlation Engine; Log Correlation Engine retrieves the feed directly from Tenable.
WAS Plugins	Retrieves the latest Tenable Web App Scanning plugins from Tenable. Tenable Security Center pushes the feed to Tenable Web App Scanning instances.
TVDL Plugins	Retrieves the latest Container Security plugins from Tenable.

For more information, see Edit Plugin and Feed Settings and Schedules.

Security

Use the Security section to define the Tenable Enclave Security user interface login parameters and options for account logins. You can also configure banners, headers, and classification headers and footers.

Option	Description	Default
Session Timeout	The web session timeout in minutes.	*60*
Maximum Login Attempts	The maximum number of user login attempts Tenable Enclave Security allows before locking out the account. To disable this feature, set the value to *0*.	*20*
Minimum	This setting defines the minimum number of characters	*3*

Option	Description	Default
Password Length	for passwords of accounts created using the local TNS authentication access.	
Password Complexity	When enabled, user passwords must be at least 4 characters long and contain at least one of each of the following: • An uppercase letter • A lowercase letter • A numerical character • A special character **Note:** After you enable **Password Complexity**, Tenable Enclave Security prompts all users to reset their passwords the next time they log in to Tenable Enclave Security. **Note:** If you enable **Password Complexity** and set the **Minimum Password Length** to a value greater than 4, Tenable Enclave Security enforces the longer password requirement.	disabled
Startup Banner Text	Type the text banner that appears before to the login interface.	--
User Text	Adds custom text to the bottom of the user profile menu. You can use the text to identify a company, group, or other organizational information (maximum 128 characters).	--
Classification Type	Adds a header and footer banner to Tenable Enclave Security to indicate the classification of the data accessible via the software. The options are **None**, **Custom, Unclassified**, **Confidential**, **Secret**, **Top Secret**, and **Top Secret – No Foreign**.	None

Option	Description	Default
	If you select **Custom**, the following options appear: • **Custom Text** - Type the text that you want to appear in the banner (maximum 128 characters). • **Text Color** - Select the text color for the banner. • **Background Color** - Select the background color for the banner. **Note:** Custom banners in reports are supported only for Arial Regular font. **Note:** If you set **Classification Type** to an option other than **None**, users can only see the plain report styles. The Tenable report styles do not support the classification banners.	
Allow API Keys	When enabled, allows users to generate API keys as an authentication method for Tenable Enclave Security API requests. For more information, see Enable API Key Authentication.	disabled
Allow Session Management	When enabled, allows administrators to set a session limit for all users.	disabled
Session Limit	Specifies the maximum number of sessions a user can have open at once. If you log in and the session limit has already been reached, Tenable Enclave Security notifies you that the oldest session with that username will be logged out automatically. You can cancel the login or proceed with the login and end the oldest session. **Note:** This behavior is different for Common Access Cards (CAC) logins. Tenable Enclave Security does not check active sessions for CAC authentication.	7

Option	Description	Default
Disable Inactive Users	When enabled, Tenable Enclave Security disables user accounts after a set period of inactivity. You cannot use a disabled user account to log in to Tenable Enclave Security, but other users can use and manage objects owned by the disabled user account.	disabled
Days Users Remain Enabled	When you enable **Disable Inactive Users**, specify the number of inactive days you want to allow before automatically disabling a user account.	*90*
Login Notifications	Sends notifications for each successful and failed login.	

Edit Plugin and Feed Settings and Schedules

Required User Role: Administrator

For more information, see Configuration.

To view and edit plugin and feed settings and schedules:

1. Log in to Tenable Enclave Security via the user interface.
2. In the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Configuration**.

   The **Configuration** page appears.
3. Click the **Plugins/Feed** tile.

   The **Plugins/Feed Configuration** page appears.
4. View the **Plugin Detail Locale** section to see the local language configured for Tenable Enclave Security.
5. Expand the **Schedules** section to show the settings for the plugin feed schedules. For more information about plugin feed schedules, see Schedules.
   a. If you want to update a plugin or feed on demand, click **Update**. You cannot update feeds with invalid activation codes.

        - If there is an update available, the **Update** link will be active.

        - If your plugins or feed are already up to date, the **Update** link will be inactive.

    b. If you want to download the plugins, click **Offline Download Link**.

    c. If you want to upload a custom feed file, click **Choose File**.

    d. Click **Submit**.

        Tenable Enclave Security saves your configuration.

Configure Plugin Text Translation

Required User Role: Administrator

For more information, see Configuration.

To configure plugin text translation:

1. Log in to Tenable Enclave Security via the user interface.

2. In the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Configuration**.

    The **Configuration** page appears.

3. Click the **Plugins/Feed** tile.

    The **Plugins/Feed Configuration** page appears.

4. If you want plugin text to display in a local language, select a language from the **Locale List** box.

5. Click **Apply**.

    Tenable Enclave Security saves your configuration.

6. In the **Schedules** section, in the **Active Plugins** row, click **Update**.

    Tenable Enclave Security updates active plugins to obtain available translations.

API Key Authentication

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable Enclave Security API requests. Without API keys, users must use the `/token` endpoint to log in to the Tenable Enclave Security API and establish a token for subsequent requests.

Tenable Enclave Security attributes actions performed with API keys to the user account associated with the API keys. You can only perform actions allowed by the privileges granted to the user account associated with the API keys.

You can enable the **Allow API Keys** toggle in your Security Settings to allow users to perform API key authentication. Then, users can generate API keys for themselves or for other users. API keys include an access key and secret key that must be used together for API key authentication. For more information, see Enable API Key Authentication and Generate API Keys.

Deleting API keys prevents users from authenticating Tenable Enclave Security API requests with the deleted keys. For more information, see Delete API Keys.

Enable API Key Authentication

You can enable API key authentication to allow users to use API keys as an authentication method for Tenable Enclave Security API requests. For more information, see API Key Authentication.

To allow users to authenticate to the Tenable Enclave Security API using API keys:

1. Log in to Tenable Enclave Security via the user interface.
2. In the top navigation, click ⚙**Settings & Information** > **Miscellaneous** > **Configuration**.

   The **Configuration** page appears.
3. Click the **Security** tile.

   The **Security Configuration** page appears.
4. In the **Authentication Settings** section, enable **Allow API Keys**.
5. Click **Submit**.

   Tenable Enclave Security saves your configuration.

What to do next:

- Generate API keys for a user, as described in Generate API Keys.

Generate API Keys

API keys allow you to authenticate as a specific user for Tenable Enclave Security API requests. Administrators can generate API keys for any user account. Other roles can generate API keys for user accounts with the same role. For more information, see API Key Authentication.

> **Note:** If you generate API keys for a user that already has API keys, the old keys will be replaced. If you delete existing keys or generate new API keys for a user, Tenable Enclave Security deauthorizes API requests attempted with the old keys.

Before you begin:

- Enable API keys to allow users to perform API key authentication, as described in Enable API Key Authentication.

To generate API keys:

1. Log in to Tenable Enclave Security via the user interface.
2. In the top navigation, click ⚙**Settings & Information** > **Access Control** > **Users**.

   The **Users** page appears.
3. Right-click the row for the user for which you want to generate an API key, and click **Generate API Key**.

   -or-

   Select the check box for the user for which you want to generate an API key, and click **API Keys** > **Generate API Key**.

   A confirmation window appears.
4. Click **Generate**.

   The **Your API Key** window appears, displaying the access key and secret key for the user.
5. Save the API keys in a safe location.

   > **Note:** You cannot view API secret keys in the Tenable Enclave Security interface after initial generation. If you lose your existing secret key, you must generate new API keys.

Delete API Keys

After you delete a user's API keys, the deleted keys cannot be used for authentication in Tenable Enclave Security API requests. To generate new API keys for a user, see Generate API Keys. For more information, see API Key Authentication.

To delete API keys:

1. Log in to Tenable Enclave Security via the user interface.
2. Click **Users** > **Users**.

   The **Users** page appears.
3. Right-click the row for the user for which you want to delete API keys, and click **Delete API Key**.

   -or-

   Select the check box for the user for which you want to delete API keys, and click **API Keys** > **Delete API Key**.

   A confirmation window appears.
4. Click **Delete**.

   The system deletes the API keys.

Diagnostics

This page displays and creates information that assists in troubleshooting issues that may arise while using Tenable Enclave Security.

To view your diagnostics settings, in the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Diagnostics**.

System Status

You can use this section to view the current status of system functions.

System Function	Description
Correct Java Version	Indicates whether the minimum version of Java required to support Tenable Enclave Security functionality is installed.

System Function	Description
Sufficient Disk Space	Indicates whether you have enough disk space to support Tenable Enclave Security functionality. A red X indicates the disk is at 95% capacity or higher. For more information, see Tenable Enclave Security System Requirements.
Correct RPM Package Installed	Indicates whether you have the correct Tenable Enclave Security RPM installed for your operating system. For more information, see Tenable Enclave Security System Requirements.
Debugging	Indicates whether debugging is enabled. You may experience performance and storage issues if you leave debugging enabled for extended periods of time. For more information, see Debugging Logs.
Migration Errors	Indicates whether an error occurred during a recent Tenable Enclave Security update.
PHP Integrity Errors	Indicates whether any PHP files have been modified from the original version included in the Tenable Enclave Security RPM.

Diagnostics File

You can use this section to generate a diagnostics file for troubleshooting with Tenable Support.

Debugging Logs

You can use this section to enable or disable debugging logs for troubleshooting with Tenable Support.

> **Note:**Tenable does not recommend leaving debugging enabled on Tenable Enclave Security after you send the log files to Tenable Support. You may experience performance and storage issues if you leave debugging enabled for extended periods of time.

Download Debugging Logs

You can use this section to download your debugging logs for troubleshooting with Tenable Support.

Job Queue

To view your job queue, in the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Job Queue**.

The job queue displays a list of Tenable Enclave Security events for review.

To view details for a job, click the row for the job.

If the job is running, you can right-click the row for the job and click **Kill** to stop the process. Avoid killing a job unless absolutely necessary, as killing a job may have undesirable effects on other Tenable Enclave Security processes.

Publishing Sites

To view your publishing sites, in the top navigation, click ⚙ **Settings & Information** > **Miscellaneous** > **Publishing Sites**.

You can configure publishing sites as targets to send report results to a properly configured web server or a Defense Information Systems Agency (DISA) Continuous Monitoring and Risk Scoring (CMRS) site.

Option	Description
Name	Type a name for the publishing site.
Description	Type a description of the publishing site.
Type	The method Tenable Enclave Security uses to publish to the site.
URI	The target address to send the report to when completed.
Use Proxy	When enabled, the publishing site leverages the web proxy defined in the Web Proxy settings.
Authentication	There are two methods of authentication available: **SSL Certificate** and

Option	Description
	Password.
Username	If you select **Password** as the **Authentication** method, the username to authenticate to the target publishing server.
Password	If you select **Password** as the **Authentication** method, the password to authenticate to the target publishing server.
Certificate	If you selected **SSL Certificate** as the **Authentication** method, the certificate you want to use for authentication.
Organizations	Select the organization(s) that are allowed to publish to the configured site.
Verify Host	When enabled, Tenable Enclave Security verifies that the target address specified in the **URI** option matches the CommonName (CN) in the SSL certificate from the target publishing server.

Security Center in Tenable Enclave Security

To access Security Center in Tenable Enclave Security, in the top navigation bar, click ▦ **Workspaces** > **Security Center**.

For Security Center CPU, memory, and disk space requirements, see Security Center in Tenable Enclave Security System Requirements.

For instructions on how to perform tasks in Tenable Security Center, see the Tenable Security Center user guide.

> **Note:** Security Center in Tenable Enclave Security does not support Tenable Log Correlation Engine.

Container Security in Tenable Enclave Security

To access Container Security in Tenable Enclave Security, in the top navigation bar, click ▦ **Workspaces** > Container Security.

For Container Security CPU, memory, and database requirements, see Container Security in Tenable Enclave Security System Requirements.

For instructions on how to perform tasks in Container Security, see the Container Security user guide.

Reporting

To view the **Reports** page, in the top navigation bar, click **Workspaces** > **Reporting**. You can run four reports simultaneously in Tenable Enclave Security.

For more information about reporting, see Reports in the *Tenable Security Center user guide*.

Additional Resources

The topics in this section offer guidance in areas related to Tenable Enclave Security.

- Troubleshooting Tenable Enclave Security
- Access Tenable Security Center Backend

Troubleshooting Tenable Enclave Security

This page describes how to check the container logs and pod status for Tenable Enclave Security for troubleshooting purposes.

Check Container Logs and Pod Status for Security Center

Check the install container logs

Run the following command to check the install container logs:

```
kubectl logs -c sc-install-container tenable-security-center-0 -n tenable
```

If successful, the output looks like this:

```
Security Center install proceeding...
Verifying...                          ########################################
Preparing...                          ########################################
.
.
Security Center install container complete, ready for runtime container.
```

Check the runtime container logs

Run the following command to check the runtime container logs:

```
kubectl logs -c sc-runtime-container tenable-security-center-0 -n tenable
```

If successful, the output looks like this:

```
Replacing System RPM database with persistent backup
Checking for SecurityCenter upgrade in progress:
Checking for active migration:
Installing software updates if availableStarting SecurityCenter services: [  OK  ]
```

Check the pod status

Run the following command to check the pod status:

```
kubectl get all -n tenable
```

If successful, the output looks like this:

```
NAME                              READY     STATUS    RESTARTS    AGE
pod/tenable-security-center-0     1/1       Running   0           4h4m

NAME                 TYPE           CLUSTER-IP      EXTERNAL-IP
        PORT(S)         AGE
service/tenable-sc   LoadBalancer   172.00.00.000   k8s-tenable-security-
center.amazonaws.com   443:12345/TCP   4h4m

NAME                                         READY   AGE
statefulset.apps/tenable-security-center   1/1     4h4m
```

Note: This output is an example of an AWS environment. Your output may vary depending on your AWS and IP ranges, but the Status should be *Running*.

Upgrade Issues

If the new pod does not appear and the **`tes-operator`** logs display the following message when you update the Tenable Enclave Security version:

```
2025/06/25 16:02:02 another operation (install/upgrade/rollback) is in progress
```

This can occur when some of the Helm Charts did not upgrade correctly. To fix the issue, roll back the **`tes`** sub-chart with the following steps:

1. List the charts with the following command:

   ```
   helm list -n tenable-enclave-security -a
   ```

2. If the tes chart is stuck in a pending upgrade, roll back the chart with the following command:

   ```
   helm rollback -n tenable-enclave-security tes
   ```

License Issues

tes-operator logs displaying invalid license error

If the **`tes-operator`** logs display the following error when interpreting the license:

```
2025/07/09 03:29:29 Signature for license is valid.
Interpreting license in key format.
Invalid license:  unexpected end of JSON input
```

This can occur when the license secret is not applied correctly. Refer to step 5 in the Tenable Enclave Security install instructions to ensure that you are applying the license correctly with the expected key.

New license is applied correctly, but not taking effect

Tenable Enclave Security watches for license updates, but if you correctly updated the license in the secret and the license is not taking effect, you can force the operator to pick up the new license by restarting the operator.

1. Get the **`tes-operator`** pod name with the following command:

   ```
   kubectl get po -n tenable-enclave-security
   ```

2. Delete the tes-operator pod with the following command:

   ```
   kubectl delete po -n tenable-enclave-security tes-operator-XXXX
   ```

Access Tenable Security Center Backend

You may need to access the Tenable Security Center Kubernetes runtime container for advanced troubleshooting or to perform maintenance tasks that require command line acess. This includes manually starting, stopping, or restarting services, executing backup and restore operations, or collecting log files or configuration data.

To log in to the Kubernetes runtime container, use the following command:

```
kubectl exec -it -n tenable tenable-security-center-0 -c sc-runtime-container  -- /bin/bash
```