



# Tenable Enclave Security 1.0.x User Guide

---

Last Updated: October 30, 2024

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

# Table of Contents

<b>Tenable Enclave Security 1.0.x User Guide</b> .....	<b>1</b>
<b>Welcome to Tenable Enclave Security</b> .....	<b>4</b>
Before Installation .....	4
System Requirements .....	5
License Requirements .....	7
Prepare a Kubernetes Cluster .....	9
Tenable Enclave Security Helm Charts .....	10
Install Tenable Enclave Security .....	12
Update Tenable Enclave Security .....	17
Configure Tenable Enclave Security .....	18
Troubleshooting Tenable Enclave Security .....	25
<b>Settings and Information</b> .....	<b>28</b>
Access Control .....	28
Users .....	29
Roles .....	29
Groups .....	30
Organizations .....	32
Authentication .....	37
LDAP Authentication .....	37
SAML Authentication .....	38
System Logs .....	38
Licenses .....	38
Configuration .....	39
Edit Plugin and Feed Settings and Schedules .....	47

Configure Plugin Text Translation .....	48
API Key Authentication .....	48
Enable API Key Authentication .....	49
Generate API Keys .....	49
Delete API Keys .....	50
Diagnostics .....	51
Job Queue .....	52
Publishing Sites .....	53
<b>Security Center in Tenable Enclave Security .....</b>	<b>55</b>
<b>Container Security in Tenable Enclave Security .....</b>	<b>56</b>
<b>Reporting .....</b>	<b>57</b>

# 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 [System Requirements](#).

## [Before Installation](#)

### [System Requirements](#)

### [License Requirements](#)

### [Prepare a Kubernetes Cluster](#)

### [Tenable Enclave Security Helm Charts](#)

## [Install Tenable Enclave Security](#)

## [Update Tenable Enclave Security](#)

## [Configure Tenable Enclave Security](#)

## [Troubleshooting Tenable Enclave Security](#)

## Before Installation

## System Requirements

See [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](#).

## System Requirements

## Supported Kubernetes Environments

- **Kubernetes versions:** 1.28 to 1.30 in any of the following environments:
  - Standalone Kubernetes
  - Amazon Elastic Kubernetes Service (EKS)
  - AzureKubernetes Service (AKS)
  - Google Kubernetes Engine (GKE)
- **Helm versions:** 3.11 and later

## Cloud Requirements

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

- [Cloud Requirements](#) in the *Tenable Security Center user guide*.
- [System Requirements](#) in the *Container Security user guide*.

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

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

# of Hosts Managed by Tenable Enclave Security	CPU	Memory	Disk Space used for Vulnerability Trending
			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

## License Requirements

For information on how to obtain a Tenable Enclave Security license, see [Licenses](#).

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. To learn how to use Tenable Enclave Security, see the [Tenable Enclave Security User Guide](#).

## 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.

When your environment expands, so does your asset count, so you purchase more licenses to account for the change. Tenable licenses use progressive pricing, so the more you purchase, the lower the per-unit price. For prices, contact your Tenable representative.

**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
<b>Tenable Security Center</b>	Assessed hosts from Tenable Security Center or imported from other Tenable products.
<b>Container Security</b>	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 [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 [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.
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 postgres database service (for example, RDS, AWS, or GCP). If you want to host the database yourself, see the [Kubegres documentation](#).

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
```

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

```
apiVersion: v1
data:
  pg_host: # base64 encoded hostname and port connection string
  pg_user: # base64 encoded username to use (must have privileges to create databases and users)
  pg_pass: # base64 encoded password for the above username
  pg_ro_host: # base64 encoded read-only host string (can be same as pg_host)
kind: Secret
metadata:
  name: tes-pg-secrets
  namespace: tenable-enclave-security
type: Opaque
```

## 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

**Note:** Tenable Enclave Security does not support changing any values besides the ones listed here.

### Specify CPU and Memory Requests and Limits

The following example is for an environment with 10,000 active IPs. For sizing requirements specific to your needs, see [System Requirements](#).

```
resources:
  limits:
    cpu: 16000m
    memory: 64Gi
  requests:
    cpu: 16000m
    memory: 64Gi
```

### Specify disk space

```
persistentVolumeClaim:
  size: 900Gi
```

### Specify Service annotations (Optional)

If you are using Kubernetes in a hosted environment and your provider (for example, AWS) supports it, use the following annotation to restrict access to the created load balancer.

```
service:
  annotations:
    service.beta.kubernetes.io/load-balancer-source-ranges: "<IP Range>"
```

### Specify Node Affinity (Optional)

Tenable Enclave Security requires an amd64 node. If you are using Kubernetes in an environment with multiple available node types, or that requires a node affinity policy, you can add the policy to values.yaml. The following is an example policy for Karpenter in AWS and EKS.

```
tes:
  blades:
    global:
      affinity:
        nodeAffinity:
          requiredDuringSchedulingIgnoredDuringExecution:
            nodeSelectorTerms:
              - matchExpressions:
                  - key: kubernetes.io/arch
                    operator: In
                    values:
                      - amd64
                  - key: karpenter.sh/capacity-type
                    operator: In
                    values:
                      - on-demand
```

## 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](#)

### 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. Get the cluster ID using the following command:

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

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 [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 [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](#).

## 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
<b>First Name</b>	The first name for the user.
<b>Last Name</b>	The last name for the user.
<b>User Name</b>	The username for the Super Administrator account.
<b>Password</b>	The unique password for the Super Administrator account.
<b>Confirm Password</b>	The same password you entered in the <b>Password</b> box.

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

For more information about organizations, see [Organizations](#).

## Organization options

Option	Description	Default
<b>General</b>		
<b>Name</b>	The name for the organization.	--
<b>Description</b>	A description for the organization.	--
<b>Address</b>	The address for the organization.	--
<b>City</b>	The city for the organization.	--
<b>State</b>	The city for the organization.	--
<b>Phone</b>	The phone number for the organization.	--
<b>Password Expiration</b>		
<b>Enable Password Expiration</b>	<p>When enabled, the user's password will expire after the number of days specified in the <b>Expiration Days</b> 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.</p> <p>When disabled, the user's password expiration settings will default to the organization settings.</p>	disabled
<b>Expiration Days</b>	The number of days before the user's password expires. You can enter a number between 1 and 365.	--
<b>Container Security</b>		
<b>Scanner Key</b>	The number of days before the user's scanner	90

Option	Description	Default
<b>Expiration</b>	key expires.	
<b>Scanning</b>		
<b>Distribution Method</b>	<p>The scan distribution mode you want to use for this organization:</p> <ul style="list-style-type: none"> <li>• <b>Automatic Distribution Only</b> - The scanner chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan.</li> <li>• <b>Locked Zone</b> - The scanner uses the scan zone(s) you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan.</li> <li>• <b>Selectable Zones</b> - 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 external scanner to see the attack surface from an external attacker's perspective.</li> </ul>	Automatic Distribution Only
<b>Scan Zones</b>	<p>One or more scan zones for the organization.</p> <p>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</p>	--

Option	Description	Default
	more scanners in your deployment. For more information about scan zones, see	
<b>Allow for Automatic Distribution</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• When enabled, the scanner chooses one or more scan zones that you specify in the <b>Restricted Scan Ranges</b> setting.</li> <li>• When disabled, the scanner requires the organizational user to specify a scan zone when configuring a scan.</li> </ul>	disabled
<b>Restricted Scan Ranges</b>	The IP address ranges you do not want users in this organization to scan.	--
<b>Analysis</b>		
<b>Accessible LCEs</b>	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.	--
<b>Accessible Repositories</b>	The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.	--
<b>Accessible Agent Capable Scanners</b>	The Tenable Nessus scanners (with Tenable Nessus Agents enabled) that you want this organization to have access to. Select one or more of the available scanners to allow the	--

Option	Description	Default
	organization to import Tenable Nessus Agent results from the selected scanner.	
<b>Accessible LDAP Scanners</b>	<p>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.</p> <div style="border: 1px solid blue; padding: 5px;"> <p><b>Note:</b> If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.</p> </div>	--
<b>Custom Analysis Links</b>		
<b>Link Name</b>	A name for the custom analysis link. You can use custom analysis links to reference additional data external to Tenable Enclave Security.	--
<b>URL</b>	<p>The custom analysis link URL that will appear in the host vulnerability details.</p> <p>For example,  <a href="http://example.com/index.htm?ip=%ip%">http://example.com/index.htm?ip=%ip%</a>  The %ip% reference is a variable that inserts the IP address of the current host into the specified URI.</p>	--
<b>Vulnerability Weights</b>		
<b>Vulnerability Weights</b>	The vulnerability weighting to apply to vulnerabilities with the specified criticality:	Medium

Option	Description	Default
	<ul style="list-style-type: none"> <li>• <b>Low</b> - The vulnerability weighting to apply to Low criticality vulnerabilities for scoring purposes. (Default: 1)</li> <li>• <b>Medium</b> - The vulnerability weighting to apply to Medium criticality vulnerabilities for scoring purposes. (Default: 3)</li> <li>• <b>High</b> - The vulnerability weighting to apply to High criticality vulnerabilities for scoring purposes. (Default: 10)</li> <li>• <b>Critical</b> - The vulnerability weighting to apply to Critical criticality vulnerabilities for scoring purposes. (Default: 40)</li> </ul>	
<b>Vulnerability Scoring System</b>		
<b>Scoring System</b>	<p>The scoring system the scanner uses to assess the severity of vulnerabilities: <b>CVSS v2</b> or <b>CVSS v3</b>.</p> <div data-bbox="544 1171 1214 1417" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> Changing the Scoring System while the scanner is running certain operations, such as preparing reports or dashboard data, results in data using mixed CVSS v2 and CVSS v3 scores.</p> </div> <div data-bbox="544 1444 1214 1810" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> 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.</p> </div>	CVSS v2

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

## Security Manager Options

Option	Description	Default
<b>Configure Product Access</b>		
<b>Role</b>	The role for the user.	Security Manager
<b>Organization</b>	The organization that the user belongs to.	--
<b>General</b>		
<b>First Name</b>	The first name for the user.	--
<b>Last Name</b>	The last name for the user.	--
<b>Type</b>	<p>The authentication type for the user account:</p> <ul style="list-style-type: none"><li>• <b>Tenable (TNS)</b></li><li>• <b>Lightweight Directory Access Protocol (LDAP)</b></li><li>• <b>Security Assertion Markup Language (SAML)</b></li></ul> <p>You must configure an LDAP server or SAML authentication in order to select <b>LDAP</b> or <b>SAML</b> from the <b>Type</b> drop-down box.</p>	TNS
<b>User Name</b>	The username for the user account. The username is case-sensitive.	--
<b>Password</b>	<p>The password for the user account.</p> <div style="border: 1px solid green; padding: 5px;"><p><b>Tip:</b> Tenable recommends using passwords that meet stringent length and complexity requirements.</p></div>	--
<b>Confirm Password</b>	The same password you entered in the <b>Password</b> box.	--



Option	Description	Default
<b>User Must Change Password</b>	When enabled, the user must change their password when they log in for the first time.	disabled
<b>Time Zone</b>	The time zone for the user.	
<b>Scan Result Default Timeframe</b>	The default <b>Completion Time</b> filter applied when the user accesses or refreshes the scan results.	
<b>Cached Fetching</b>	When enabled, Tenable Enclave Security caches plugin policy information and performs plugin policy downloads once per page load.	
<b>Password Expiration</b>		
<b>Enable Password Expiration</b>	When enabled, the user's password will expire after the number of days specified in the <b>Expiration Days</b> 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
<b>Expiration Days</b>	The number of days before the user's password expires. You can enter a number between 1 and 365.	--

## Troubleshooting Tenable Enclave Security

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

### 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*.

# 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
<b>Super Administrator</b>	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 <a href="#">Configure</a> <a href="#">[[[Undefined variable Tenable.PrivateCloud]]]</a> .
<b>Organizational Users</b> - Users that belong to an organization.	
<b>Security Manager</b>	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.  The 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.
<b>Auditor</b>	The Auditor role can access summary information to perform third-party

Role	Description
	audits. An Auditor can view dashboards, reports, and logs, but cannot perform scans or create tickets.
<b>Credential Manager</b>	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.
<b>Executive</b>	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.
<b>Security Analyst</b>	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.
<b>Vulnerability Analyst</b>	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.
<b>Custom Role</b>	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
<b>General</b> tab	
<b>Name</b>	The name for the group.
<b>Description</b>	A description for the group (e.g., <b>security team at the central office</b> or <b>executives on the east coast</b> ).
<b>Viewable Hosts</b>	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.
<b>Repositories</b>	The repositories you want to share with the group.
<b>Log Correlation Engines</b>	The Log Correlation Engines you want to assign to the group.
<b>Container Security Resources</b>	The Container Security images you want to be available to users in the group.
<b>Sample Content</b>	<p>When enabled, Tenable provides sample content objects to users in the group:</p> <ul style="list-style-type: none"><li>• sample dashboards (<b>Executive 7 Day</b>, <b>Executive Summary</b>, and <b>Vulnerability Overview</b>)</li><li>• sample reports (<b>Critical and Exploitable Vulnerabilities</b>, <b>Monthly Executive</b>, and <b>Remediation Instructions by Host</b>)</li><li>• sample ARCs (<b>CCC 1: Maintain an Inventory of Software and Hardware</b>, <b>CCC 2: Remove Vulnerabilities and Misconfigurations</b>, <b>CCC 3: Deploy a Secure Network</b>, <b>CCC 4: Authorize Users</b>, and <b>CCC 5: Search for Malware and Intruders</b>)</li><li>• sample assets required for the sample ARCs</li></ul> <p>After enabling <b>Sample Content</b>, you must add a new user to the group before all users in the group can access the sample content.</p>

Option	Description
	<p><b>Note:</b> If a user in a group deletes a sample content object, the object is deleted for all other users in that group.</p> <p><b>Note:</b> If you move a sample content object owner (e.g., move the first user in group A to group B), Tenable Enclave Security:</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. Recreates their dashboards, ARCs, and assets required for ARCs in group B. Tenable Enclave Security does not recreate reports.</li> </ol>
<b>Share to Group</b> tab	
<b>Available Objects</b>	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
<b>General</b>	
<b>Name</b>	(Required) The organization name.
<b>Description</b>	A description for the organization.
<b>Contact Information</b>	The relevant contact information for the organization including address, city, state, country, and phone number.
<b>Password Expiration</b>	
<b>Enable Password Expiration</b>	When enabled, passwords for users in the organization will expire after the number of days specified in the <b>Expiration Days</b> box.
<b>Expiration Days</b>	<p>The number of days before the user's password expires. You can enter a number between 1 and 365.</p> <p>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.</p>
<b>Container Security</b>	
<b>Scanner Key Expiration</b>	The number of days before the user's scanner key expires.
<b>Container Security Resources</b>	The Container Security images you want to be available to users in the group.
<b>Scanning</b>	
<b>Distribution Method</b>	The scan distribution mode you want to use for this organization:


Option	Description
	<ul style="list-style-type: none"> <li>• <b>Automatic Distribution Only:</b> Tenable Enclave Security chooses one or more scan zones to run the scan. Organizational users cannot choose a scan zone when configuring a scan.</li> </ul> <p>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 <a href="#">RFC 1918</a> non-internet-routable address spaces.</p> <ul style="list-style-type: none"> <li>• <b>Locked Zone:</b> Tenable Enclave Security uses the one <b>Available Zone</b> you specify to run the scan. Organizational users cannot modify the scan zone when configuring a scan.</li> <li>• <b>Selectable Zones:</b> Tenable Enclave Security allows organizational users to select a scan zone when configuring a scan.</li> </ul> <p>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 external scanner to see the attack surface from an external attacker’s perspective.</p>
<b>Available Zones</b>	One or more scan zones that you want organizational users to have access to when configuring scans.
<b>Allow for Automatic Distribution</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• When enabled, Tenable Enclave Security chooses one or</li> </ul>

Option	Description
	<p>more scan zones as specified by your <b>Restrict to Selected Zones</b> setting.</p> <ul style="list-style-type: none"> <li>When disabled, Tenable Enclave Security requires the organizational user to specify a scan zone when configuring a scan.</li> </ul>
<b>Restrict to Selected Zones</b>	<p>If <b>Allow for Automatic Distribution</b> is enabled, enable or disable this option to specify the zones you want Tenable Enclave Security to choose from when automatically distributing zones.</p> <ul style="list-style-type: none"> <li>When enabled, Tenable Enclave Security chooses from the <b>Available Zones</b> shared with the organization.</li> <li>When disabled, Tenable Enclave Security chooses from all zones on Tenable Enclave Security.</li> </ul>
<b>Restricted Scan Ranges</b>	<p>The IP address ranges you do not want users in this organization to scan.</p>
<b>Analysis</b>	
<b>Accessible Repositories</b>	<p>The repositories that you want this organization to have access to. You can search for the repositories by name or scroll through the list.</p>
<b>Accessible LCEs</b>	<p>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.</p>
<b>Accessible Agent Capable Scanners</b>	<p>The Tenable Nessus scanners (with Tenable Nessus 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 Nessus Agent results from the selected scanner.</p>
<b>Accessible LDAP Servers</b>	<p>The LDAP servers that you want this organization to have</p>

Option	Description
	<p>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.</p> <div data-bbox="602 411 1479 569" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> If you revoke access to an LDAP server, users in the organization cannot authenticate and LDAP query assets cannot run.</p> </div>
<b>Custom Analysis Links</b>	
<p>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 <b>Add Custom Link</b> to create a new option to type the link name and URL to look up additional data external to Tenable Enclave Security.</p> <p>For example: <i>http://example.com/index.htm?ip=%ip%</i></p> <p>The <i>%ip%</i> reference is a variable that inserts the IP address of the current host into the specified URI.</p>	
<b>Vulnerability Weights</b>	
<b>Low</b>	The vulnerability weighting to apply to <b>Low</b> criticality vulnerabilities for scoring purposes. (Default: 1)
<b>Medium</b>	The vulnerability weighting to apply to <b>Medium</b> criticality vulnerabilities for scoring purposes. (Default: 3)
<b>High</b>	The vulnerability weighting to apply to <b>High</b> criticality vulnerabilities for scoring purposes. (Default: 10)
<b>Critical</b>	The vulnerability weighting to apply to <b>Critical</b> criticality vulnerabilities for scoring purposes. (Default: 40)
<b>Vulnerability Scoring System</b>	
<b>Scoring System</b>	The scoring system Tenable Enclave Security uses to assess the severity of vulnerabilities: <b>CVSS v2</b> or <b>CVSS v3</b> .

Option	Description
	<p><b>Note:</b> Changing the <b>Scoring System</b> 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.</p> <p><b>Note:</b> Changing the <b>Scoring System</b> does not impact historical dashboard trend data. For example, if you change the <b>Scoring System</b> from <b>CVSS v2</b> to <b>CVSS v3</b>, dashboard trend data before the change displays CVSS v2 scores while dashboard trend data after the change displays CVSS v3 scores.</p>
<b>Reporting</b>	
<b>Publishing Sites</b>	<p>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.</p> <p>For more information, see <a href="#">Publishing Sites</a>.</p>

## 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.

## License Tenable Enclave Security Online

When you obtain your license, enter the activation code in the Tenable Enclave Security user interface.

## 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
<b>Host</b>	The SMTP server host.	--
<b>Port</b>	The SMTP server port.	--
<b>Authentication Method</b>	<p>The authentication method Tenable Enclave Security uses to connect to the SMTP server:</p> <ul style="list-style-type: none"><li>• <b>None</b> - Tenable Enclave Security does not authenticate the connection.</li><li>• <b>Login</b> - Tenable Enclave Security secures the connection with login authentication.</li><li>• <b>Plain</b> - Tenable Enclave Security secures the connection with plain (username/password) authentication.</li><li>• <b>CRAM-SHA1</b> - Tenable Enclave Security secures the connection with CRAM-SHA1 authentication.</li><li>• <b>CRAM-MD5</b> - Tenable Enclave Security secures the connection with CRAM-SHA1 authentication.</li></ul>	--
<b>Username</b>	<p>The username that Tenable Enclave Security uses to authenticate to the SMTP server.</p> <div style="border: 1px solid #0070C0; padding: 5px;"><p><b>Note:</b> Type the <b>Username</b> in a format supported by your SMTP server (for example, <i>username@domain.com</i> or <i>domain\username</i>).</p></div>	--
<b>Password</b>	The password that Tenable Enclave Security uses to authenticate to the SMTP server.	--
<b>Encryption</b>	The email encryption type:	--



Option	Description	Default
	<ul style="list-style-type: none"> <li>• <b>None</b> - Tenable Enclave Security does not encrypt the email.</li> <li>• <b>TLS</b> - Tenable Enclave Security forces TLS encryption for the email.</li> <li>• <b>SSL</b> - Tenable Enclave Security forces SSL encryption for the email.</li> <li>• <b>TLS, if available</b> - Tenable Enclave Security uses TLS encryption if the receiving server is compatible.</li> </ul>	
<b>Return Address</b>	<p>The email address that appear as the sender in the scan results email.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p><b>Note:</b> 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.</p> </div>	--
<b>Verify Peer</b>	When enabled, Tenable Enclave Security requests peer verification for SMTP servers using SSL or TLS connections.	disabled
<b>Verify Peer Name</b>	When enabled, Tenable Enclave Security requests peer name verification for SMTP servers using SSL or TLS connections.	disabled
<b>Allow Self Signed Certificates</b>	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
<b>Host</b>	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.	--
<b>Port</b>	The port of the web proxy server.	--
<b>Authentication Type</b>	The authentication type Tenable Enclave Security uses to connect to the web proxy server.  Select one of the following: <ul style="list-style-type: none"><li>• <b>Basic</b> - Tenable Enclave Security uses basic authentication, which encodes the username and password with Base64.</li><li>• <b>NTLM</b> - Tenable Enclave Security uses NTLM authentication.</li></ul>	--
<b>Username</b>	The username that Tenable Enclave Security uses to authenticate to the web proxy server.	--
<b>Password</b>	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
<b>Enable Forwarding</b>	Enables log forwarding options.	disabled
<b>Facility</b>	Type the facility you want to receive the log messages.	<i>LOG_USER</i>

Option	Description	Default
<b>Severity</b>	Specifies which syslog message levels you want to forward: <b>Informational</b> , <b>Warning</b> , or <b>Critical</b> .	Informational

## 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
<b>Tenable Security Center Feed</b>	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-

Update	Description
	required objects, some general plugin information, and updated VPR values.
<b>Active Plugins</b>	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.
<b>Passive Plugins</b>	Retrieves the latest passive plugins feed from Tenable. Tenable Security Center pushes the feed to Tenable Nessus Network Monitor instances.
<b>Event Plugins</b>	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.
<b>WAS Plugins</b>	Retrieves the latest Tenable Web App Scanning plugins from Tenable. Tenable Security Center pushes the feed to Tenable Web App Scanning instances.
<b>TVDL Plugins</b>	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
<b>Session Timeout</b>	The web session timeout in minutes.	60
<b>Maximum Login Attempts</b>	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

Option	Description	Default
<b>Minimum Password Length</b>	This setting defines the minimum number of characters for passwords of accounts created using the local TNS authentication access.	3
<b>Password Complexity</b>	<p>When enabled, user passwords must be at least 4 characters long and contain at least one of each of the following:</p> <ul style="list-style-type: none"> <li>• An uppercase letter</li> <li>• A lowercase letter</li> <li>• A numerical character</li> <li>• A special character</li> </ul> <div data-bbox="444 873 1256 1031" style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> After you enable <b>Password Complexity</b>, Tenable Enclave Security prompts all users to reset their passwords the next time they log in to Tenable Enclave Security.</p> </div> <div data-bbox="444 1052 1256 1251" style="border: 1px solid #0070C0; padding: 5px; margin: 10px 0;"> <p><b>Note:</b> If you enable <b>Password Complexity</b> and set the <b>Minimum Password Length</b> to a value greater than 4, Tenable Enclave Security enforces the longer password requirement.</p> </div>	disabled
<b>Startup Banner Text</b>	Type the text banner that appears before to the login interface.	--
<b>User Text</b>	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).	--
<b>Classification Type</b>	Adds a header and footer banner to Tenable Enclave Security to indicate the classification of the data accessible via the software. The options are <b>None</b> , <b>Custom</b> , <b>Unclassified</b> , <b>Confidential</b> , <b>Secret</b> , <b>Top Secret</b> , and <b>Top Secret – No Foreign</b> .	None

Option	Description	Default
	<p>If you select <b>Custom</b>, the following options appear:</p> <ul style="list-style-type: none"> <li>• <b>Custom Text</b> - Type the text that you want to appear in the banner (maximum 128 characters).</li> <li>• <b>Text Color</b> - Select the text color for the banner.</li> <li>• <b>Background Color</b> - Select the background color for the banner.</li> </ul> <div data-bbox="444 632 1256 747" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> Custom banners in reports are supported only for Arial Regular font.</p> </div> <div data-bbox="444 768 1256 921" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> If you set <b>Classification Type</b> to an option other than <b>None</b>, users can only see the plain report styles. The Tenable report styles do not support the classification banners.</p> </div>	
<b>Allow API Keys</b>	<p>When enabled, allows users to generate API keys as an authentication method for Tenable Enclave Security API requests. For more information, see <a href="#">Enable API Key Authentication</a>.</p>	disabled
<b>Allow Session Management</b>	<p>When enabled, allows administrators to set a session limit for all users.</p>	disabled
<b>Session Limit</b>	<p>Specifies the maximum number of sessions a user can have open at once.</p> <p>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.</p> <div data-bbox="444 1688 1256 1841" style="border: 1px solid #0070C0; padding: 5px;"> <p><b>Note:</b> This behavior is different for Common Access Cards (CAC) logins. Tenable Enclave Security does not check active sessions for CAC authentication.</p> </div>	7


Option	Description	Default
<b>Disable Inactive Users</b>	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
<b>Days Users Remain Enabled</b>	When you enable <b>Disable Inactive Users</b> , specify the number of inactive days you want to allow before automatically disabling a user account.	90
<b>Login Notifications</b>	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
<b>Correct Java Version</b>	Indicates whether the minimum version of Java required to support Tenable Enclave Security functionality is installed.
<b>Sufficient Disk Space</b>	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 <a href="#">System Requirements</a> .

System Function	Description
<b>Correct RPM Package Installed</b>	Indicates whether you have the correct Tenable Enclave Security RPM installed for your operating system.  For more information, see <a href="#">System Requirements</a> .
<b>Debugging</b>	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 <a href="#">Debugging Logs</a> .
<b>Migration Errors</b>	Indicates whether an error occurred during a recent Tenable Enclave Security update.
<b>PHP Integrity Errors</b>	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
<b>Name</b>	Type a name for the publishing site.
<b>Description</b>	Type a description of the publishing site.
<b>Type</b>	The method Tenable Enclave Security uses to publish to the site.
<b>URI</b>	The target address to send the report to when completed.
<b>Use Proxy</b>	When enabled, the publishing site leverages the web proxy defined in the <a href="#">Web Proxy</a> settings.
<b>Authentication</b>	There are two methods of authentication available: <b>SSL Certificate</b> and <b>Password</b> .
<b>Username</b>	If you select <b>Password</b> as the <b>Authentication</b> method, the username to authenticate to the target publishing server.
<b>Password</b>	If you select <b>Password</b> as the <b>Authentication</b> method, the password to authenticate to the target publishing server.
<b>Certificate</b>	If you selected <b>SSL Certificate</b> as the <b>Authentication</b> method, the

Option	Description
	certificate you want to use for authentication.
<b>Organizations</b>	Select the organization(s) that are allowed to publish to the configured site.
<b>Verify Host</b>	When enabled, Tenable Enclave Security verifies that the target address specified in the <b>URI</b> 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 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 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..**

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