# Table of Contents

Welcome to Tenable Core + Tenable Sensor Proxy .......................................................... 6

Get Started .......................................................................................................................... 8

Tenable Core Requirements ............................................................................................... 9

System and License Requirements .................................................................................... 9

Access Requirements ......................................................................................................... 11

Default Security Configuration Standards ........................................................................ 13

Deploy or Install Tenable Core .......................................................................................... 17

Deploy Tenable Core in VMWare ...................................................................................... 18

Deploy Tenable Core in Hyper-V ..................................................................................... 19

Deploy Tenable Core in AWS ........................................................................................... 21

Deploy Tenable Core in AWS with Limited Options ....................................................... 22

Deploy Tenable Core in AWS with Advanced Options .................................................. 23

Deploy Tenable Core in Microsoft Azure ....................................................................... 25

Deploy Tenable Core in Microsoft Azure via the Portal ................................................ 25

Deploy Tenable Core in Microsoft Azure via the CLI .................................................... 26

Install Tenable Core on Tenable-Provided Hardware ..................................................... 27

Configure Tenable Core Multi-Factor Authentication ..................................................... 29

Log In to Tenable Core ...................................................................................................... 31

Create an Initial Administrator User Account ................................................................. 32

Create a Password for the Initial Administrator User Account .................................... 33

Manually Configure a Static IP Address .......................................................................... 35

Disk Management ............................................................................................................. 38

Add or Expand Disk Space ............................................................................................... 39
## Configure Tenable Core

Configure Tenable Core + Tenable Sensor Proxy in the Tenable Core + Tenable Sensor Proxy User Interface

Configure Tenable Cor + Tenable Sensor Proxy in Tenable Core

Start, Stop, or Restart Your Application

Configure a Proxy Server

SNMP Agent Configuration

Configure an SNMP Agent via the User Interface

Configure an SNMP Agent via the CLI

View the System Log

Filter the System Log

Generate a Diagnostic Report

Access the Terminal

## Manage the System

Manage System Storage

Rename a Filesystem

Delete a Filesystem

Manage Updates

Configure Automatic Updates

Configure Your Automatic Update Schedule

Update On Demand

Update Tenable Core Offline

Application Data Backup and Restore

Configure Storage for Tenable Core Backups

Perform an On-Demand Backup
Change the Scheduled Backup Time ................................................................. 63
Restore a Backup ......................................................................................... 65
Manage Certificates ................................................................................... 67
Manage the Server Certificate ................................................................. 68
  Upload a Custom Server Certificate ..................................................... 68
  Remove a Custom Server Certificate ................................................... 70
Upload a Certificate for a Trusted Certificate Authority .............................. 71
Use Different Certificates for Tenable Core and Your Application .................. 72
Manage Services ....................................................................................... 73
  Create a Timer ....................................................................................... 76
Manage System Networking ...................................................................... 76
  Add a Bonded Interface ....................................................................... 77
  Add a Team of Interfaces ..................................................................... 79
  Add a Bridge Network ......................................................................... 80
  Add a VLAN ....................................................................................... 81
Manage User Accounts ............................................................................. 82
  Create New User Account .................................................................. 82
  Edit a User Account ......................................................................... 83
  Delete a User Account ...................................................................... 87
Change Performance Profile ..................................................................... 88
Restart Tenable Core ............................................................................... 89
Shut Down Tenable Core ......................................................................... 90
Edit Your Tenable Core Hostname ............................................................. 91
Edit Your Time Settings .......................................................................... 92
Welcome to Tenable Core + Tenable Sensor Proxy

You can use the Tenable Core operating system to run an instance of Tenable Sensor Proxy in your environment. After you deploy Tenable Core + Tenable Sensor Proxy, you can monitor and manage your Tenable Sensor Proxy processes through the secure Tenable Core platform.

To get started quickly with Tenable Sensor Proxy, see Get Started.

Features

- Secure, stable platform that reduces the time to your first scan.
- Provides automatic application installation and updates via Tenable public repositories.
- Built on Oracle Linux 8.
- Targets Center for Internet Security (CIS) standards for Oracle Linux 8 with SELinux enabled. For more information, see Default Security Configuration Standards.
- Root access is enabled on all builds.

Other Tenable Core Configurations

To run a different Tenable application on Tenable Core, see:

- Tenable Core + Nessus
- Tenable Core + Nessus Network Monitor
- Tenable Core + Tenable OT Security
- Tenable Core + Tenable OT Security Sensor
- Tenable Core + Tenable Security Center
- Tenable Core + Tenable Web App Scanning

Note: Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core, deploy a unique instance for each application.

Tenable Core Operating System Version Support
To see which versions of the products are currently available on each operating system version of Tenable Core, see the Versions page.
Get Started

Tenable recommends the following sequence to deploy and get started with Tenable Core + Tenable Sensor Proxy.

To get started with Tenable Core:

1. Confirm that your environment meets the requirements in Tenable Core Requirements. If necessary, prepare to increase your disk space after you deploy.

2. **Deploy or install** Tenable Core + Tenable Sensor Proxy.

   **Note:** You can also deploy Tenable Core using the command line interface (CLI). For more information, see Deploy Tenable Core in Microsoft Azure via the CLI.

3. (Optional) If you want to increase your disk space to accommodate your organization's data storage needs, do one of the following:
   
   - If you are deploying Tenable Core + Tenable Sensor Proxy as a virtual machine or on hardware, see Disk Management.
   
   - If you are deploying Tenable Core + Tenable Sensor Proxy in a cloud environment, refer to your cloud platform's documentation for information about increasing disk space.

4. (Optional) If the Dynamic Host Configuration Protocol (DHCP) is not available on the network where you deployed Tenable Core, configure an IP address for your Tenable Core + Tenable Sensor Proxy deployment.

5. Log in as a wizard user and create an administrator account, as described in Create an Initial Administrator User Account.

6. (Optional) If necessary, log in as a wizard user and create an administrator account, as described in Create an Initial Administrator User Account.

   **Note:** Create an administrator account if you deployed Tenable Core + Tenable Sensor Proxy via one of the following methods:
   
   - As a virtual machine
   
   - On hardware
If you deployed Tenable Core + Tenable Sensor Proxy in a cloud environment and you did not create a password during deployment, you must [create a password for your administrator account].

7. Log In to Tenable Core with your new administrator credentials.

8. (Optional) If you want to create more user accounts, see Create New User Account.

9. (Optional) If you want to configure Tenable Core to use a proxy server, see Configure a Proxy Server.

10. Configure Sensor Proxy in Tenable Core to meet the specifications you want for your application.

   For more information about configuring and operating Tenable Sensor Proxy, see the Sensor Proxy User Guide.

11. Configure and manage Tenable Core. To access the application interface, see Configure Tenable Core.

### Tenable Core Requirements

**Caution**: CentOS 7 will be end-of-support (EOS) as of June 30, 2024. As such, Tenable will also be ceasing support for all CentOS 7-based Tenable Core images & packages. Moving forward, Tenable urges customers to use our Oracle Linux 8-based Tenable Core images & packages to ensure that you are leveraging supported solutions.

You can deploy Tenable Core + Tenable Sensor Proxy on any system that meets the following Tenable Core and Tenable Sensor Proxy environment requirements.

**Note**: Tenable does not recommend deploying multiple applications on a single instance of Tenable Core. If you want to deploy several applications on Tenable Core, deploy a unique instance for each application.

- System and License Requirements
- Access Requirements
- Default Security Configuration Standards

### System and License Requirements
To install and run Tenable Core + Tenable Sensor Proxy, your application and system must meet the following requirements established for Tenable Sensor Proxy.

**Note:** Tenable Support does not assist with issues related to your host operating system, even if you encounter them during installation or deployment.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core File Format</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware .ova file</td>
<td><a href="#">Deploy Tenable Core in VMware</a></td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V .zip file</td>
<td><a href="#">Deploy Tenable Core in Hyper-V</a></td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure n/a</td>
<td><a href="#">Deploy Tenable Core in Microsoft Azure</a></td>
</tr>
<tr>
<td>Cloud</td>
<td>Amazon Web Services (AWS) n/a</td>
<td><a href="#">Deploy Tenable Core in AWS</a></td>
</tr>
<tr>
<td>Hardware</td>
<td>.iso image</td>
<td><a href="#">Install Tenable Core on Tenable-Provided Hardware</a></td>
</tr>
</tbody>
</table>

**Note:** While you could use the packages to run Tenable Core in other environments, Tenable does not provide documentation for those procedures.

**Software Requirements**

- Set up Tenable Sensor Proxy on your network where sensors can reach it internally and where Tenable Sensor Proxy can reach Tenable Vulnerability Management directly with outbound traffic.

**Note:** Tenable Sensor Proxy does not support content delivery network (CDN)-based scan reports from Tenable Nessus Agents.

**Hardware Requirements**
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Minimum Recommended Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable Sensor Proxy with up to 50,000 sensors</td>
<td>CPU: 4 2GHz cores</td>
</tr>
<tr>
<td></td>
<td>Memory: 8 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Disk space: 100 GB</td>
</tr>
<tr>
<td>Tenable Sensor Proxy with more than 50,000 sensors</td>
<td>CPU: 4 2GHz cores</td>
</tr>
<tr>
<td></td>
<td>Memory: 16 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Disk space: 100 GB</td>
</tr>
</tbody>
</table>

Note: Each instance of Tenable Sensor Proxy can support up to 100,000 linked sensors.

Note: Heavy usage of Tenable Sensor Proxy can cause the NGINX access log to grow substantially. Tenable recommends setting up log rotation to prevent running out of disk space.

Tenable Products

- You must have a Tenable Vulnerability Management account.
- You must have Tenable Nessus Agents or Tenable Nessus scanners.

Access Requirements

Your Tenable Core + Tenable Sensor Proxy deployment must meet the following requirements.

- Internet Requirements
- Port Requirements

Internet Requirements

You must have internet access to download Tenable Core files and perform online installs.

After you transfer a file to your machine, internet access requirements to deploy or update Tenable Core vary depending on your environment.

Note: You need to be able to reach appliance.cloud.tenable.com to install from the online ISOS (and to get online updates) and sensor.cloud.tenable.com to pick up scan jobs.
<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core Format</th>
<th>Internet Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware .ova file</td>
<td>You do not need internet access to deploy or update Tenable Core.</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V .zip file</td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td>Amazon Web Services (AWS) n/a</td>
<td>Requires internet access to deploy or update Tenable Core.</td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure n/a</td>
<td>Requires internet access to install or update Tenable Core.</td>
</tr>
<tr>
<td>Hardware</td>
<td>.iso image</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** You do not need access to the internet when you install updates to Tenable Core + Tenable Sensor Proxy via an offline .iso file. For more information, see [Update Tenable Core Offline](#).

## Port Requirements

Your Tenable Core deployment requires access to specific ports for inbound and outbound traffic.

### Inbound Traffic

Allow inbound traffic to the following ports listed.

**Note:** Inbound traffic refers to traffic from users configuring Tenable Core, etc.

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>Inbound SSH connections.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Inbound communications for linking agents and scanners to Tenable Core + Tenable Sensor Proxy.</td>
</tr>
<tr>
<td>TCP 8000</td>
<td>Inbound HTTPS communications to the Tenable Core interface.</td>
</tr>
</tbody>
</table>

**Note:** Inbound only from the networks that have Agents and Scanner. Not needed from “external” locations.
Outbound Traffic

Allow outbound traffic to the following ports listed.

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 22</td>
<td>Outbound SSH connections, including remote storage connections.</td>
</tr>
<tr>
<td>TCP 443</td>
<td>Outbound communications to the appliance.cloud.tenable.com and sensor.cloud.tenable.com servers for system updates.</td>
</tr>
<tr>
<td>UDP 53</td>
<td>Outbound DNS communications for and Tenable Core.</td>
</tr>
</tbody>
</table>

Default Security Configuration Standards

By default, Tenable Core applies security configurations based on the following Center for Internet Security (CIS) standards. For more information about CIS standards, see cisecurity.org.

Note: SELinux: is enabled by default on the Tenable Core operating system.

CIS Standards

CIS Benchmarks: Tenable has implemented the following parts of the CIS Level 1 Benchmark on the Tenable Core:

CIS Level 1 - 1.x

- CIS 1.1.1.* (Disable mounting of miscellaneous filesystems)
- CIS 1.1.21 (Ensure sticky bit is set on all world-writable directories)
- CIS 1.4.* (Bootloader adjustments)
  - CIS 1.4.1 Ensure permissions on bootloader config are configured
- CIS 1.7.1.* (Messaging/banners)
  - Ensure message of the day is configured properly
  - Ensure local login warning banner is configured properly
  - Ensure remote login warning banner is configured properly
• Ensure GDM login banner is configured - banner message enabled
• Ensure GDM login banner is configured - banner message text

CIS Level 1 - 2.x
• CIS 2.2.* (disabled packages)
  • x11
  • avahi-server
  • CUPS
  • nfs
  • Rpc

CIS level 1 - 3.x
• CIS 3.1.* (packet redirects)
  • 3.1.2 Ensure packet redirect sending is disabled - 'net.ipv4.conf.all.send_redirects = 0'
  • 3.1.2 Ensure packet redirect sending is disabled - 'net.ipv4.conf.default.send_redirects = 0'
• CIS 3.2.* (ipv4, icmp, etc)
  • 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.all.accept_source_route = 0'
  • 3.2.1 Ensure source routed packets are not accepted - 'net.ipv4.conf.default.accept_source_route = 0'
  • 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.all.accept_redirects = 0'
  • 3.2.2 Ensure ICMP redirects are not accepted - 'net.ipv4.conf.default.accept_redirects = 0'
  • 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.all.secure_redirects = 0'
• 3.2.3 Ensure secure ICMP redirects are not accepted - 'net.ipv4.conf.default.secure_redirects = 0'
• 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.all.log_martians = 1'
• 3.2.4 Ensure suspicious packets are logged - 'net.ipv4.conf.default.log_martians = 1'
• 3.2.5 Ensure broadcast ICMP requests are ignored
• 3.2.6 Ensure bogus ICMP responses are ignored
• 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.all.rp_filter = 1'
• 3.2.7 Ensure Reverse Path Filtering is enabled - 'net.ipv4.conf.default.rp_filter = 1'
• 3.2.8 Ensure TCP SYN Cookies is enabled

• CIS 3.3.* (IPv6)
  • 3.3.1 Ensure IPv6 router advertisements are not accepted
  • 3.3.2 Ensure IPv6 redirects are not accepted

• CIS 3.5.* (network protocols)
  • 3.5.1 Ensure DCCP is disabled
  • 3.5.2 Ensure SCTP is disabled
  • 3.5.3 Ensure RDS is disabled
  • 3.5.4 Ensure TIPC is disabled

CIS Level 1 - 4.x
• CIS 4.2.* (rsyslog)
  • 4.2.1.3 Ensure rsyslog default file permissions configured
  • 4.2.4 Ensure permissions on all logfiles are configured

CIS Level 1 - 5.x
• CIS 5.1.* (cron permissions)
  • 5.1.2 Ensure permissions on /etc/crontab are configured
  • 5.1.3 Ensure permissions on /etc/cron.hourly are configured
  • 5.1.4 Ensure permissions on /etc/cron.daily are configured
  • 5.1.5 Ensure permissions on /etc/cron.weekly are configured
  • 5.1.6 Ensure permissions on /etc/cron.monthly are configured
  • 5.1.7 Ensure permissions on /etc/cron.d are configured
  • 5.1.8 Ensure at/cron is restricted to authorized users - at.allow
  • 5.1.8 Ensure at/cron is restricted to authorized users - at.deny
  • 5.1.8 Ensure at/cron is restricted to authorized users - cron.allow
• CIS 5.3.* (password/pam)
  • 5.3.1 Ensure password creation requirements are configured - dcredit
  • 5.3.1 Ensure password creation requirements are configured - Icredit
  • 5.3.1 Ensure password creation requirements are configured - minlen
  • 5.3.1 Ensure password creation requirements are configured - ocredit
  • 5.3.1 Ensure password creation requirements are configured - ucredit
  • 5.3.2 Lockout for failed password attempts - password-auth 'auth [default=die] pam_fai
  lock.so authfail audit deny=5 unlock_time=900'
  • 5.3.2 Lockout for failed password attempts - password-auth 'auth [success=1
default=bad] pam_unix.so'
  • 5.3.2 Lockout for failed password attempts - password-auth 'auth required pam_fai
  lock.so preauth audit silent deny=5 unlock_time=900'
  • 5.3.2 Lockout for failed password attempts - password-auth 'auth sufficient pam_fai
  lock.so authsuc audit deny=5 unlock_time=900'
- 17 -

• 5.3.2 Lockout for failed password attempts - system-auth 'auth [default=die] pam_faiolock.so authfail audit deny=5 unlock_time=900'

• 5.3.2 Lockout for failed password attempts - system-auth 'auth [success=1 default=bad] pam_unix.so'

• 5.3.2 Lockout for failed password attempts - system-auth 'auth required pam_faiolock.so preauth audit silent deny=5 unlock_time=900'

• 5.3.2 Lockout for failed password attempts - system-auth 'auth sufficient pam_faiolock.so authsuc aid deny=5 unlock_time=900'

• 5.3.3 Ensure password reuse is limited - password-auth

• 5.3.3 Ensure password reuse is limited - system-auth

• CIS 5.4.* (user prefs)
  • 5.4.1.2 Ensure minimum days between password changes is 7 or more
  • 5.4.1.4 Ensure inactive password lock is 30 days or less
  • 5.4.4 Ensure default user umask is 027 or more restrictive - /etc/bashrc

• CIS 5.6.* (wheel group)
  • 5.6 Ensure access to the su command is restricted - pam_wheel.so
  • 5.6 Ensure access to the su command is restricted - wheel group contains root

CIS Level 1 - 6.x

• CIS 6.1.* (misc conf permissions)
  • 6.1.6 Ensure permissions on /etc/passwd- are configured
  • 6.1.8 Ensure permissions on /etc/group- are configured

Deploy or Install Tenable Core

You can run Tenable Core + Tenable Sensor Proxy in the following environments.

Note: Tenable Support does not assist with issues related to your host operating system, even if you encounter them during installation or deployment.
<table>
<thead>
<tr>
<th>Environment</th>
<th>Tenable Core File Format</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine</td>
<td>VMware  .ova file</td>
<td>Deploy Tenable Core in VMware</td>
</tr>
<tr>
<td></td>
<td>Microsoft Hyper-V .zip file</td>
<td>Deploy Tenable Core in Hyper-V</td>
</tr>
<tr>
<td>Cloud</td>
<td>Microsoft Azure n/a</td>
<td>Deploy Tenable Core in Microsoft Azure</td>
</tr>
<tr>
<td>Cloud</td>
<td>Amazon Web Services (AWS) n/a</td>
<td>Deploy Tenable Core in AWS</td>
</tr>
<tr>
<td>Hardware</td>
<td>.iso image</td>
<td>Install Tenable Core on Tenable-Provided Hardware</td>
</tr>
</tbody>
</table>

**Note:** While you could use the packages to run Tenable Core in other environments, Tenable does not provide documentation for those procedures.

### Deploy Tenable Core in VMware

To deploy Tenable Core + Tenable Sensor Proxy as a VMware virtual machine, you must download the Tenable Core + Tenable Sensor Proxy .ova file and deploy it on a hypervisor.

**Before you begin:**

- Confirm your environment will support your intended use of the instance, as described in [License and System Requirements](#).
- Confirm your internet and port access will support your intended use of the instance, as described in [Access Requirements](#).
- For more information on configuring VMware, refer to [Configure vSphere Scanning](#) in the Tenable Nessus user guide.

To deploy Tenable Core + Tenable Sensor Proxy as a VMware virtual machine:
1. Download the **Tenable Core Sensor proxy VMware Image** file from the [Tenable Downloads](#) page.

2. Open your VMware virtual machine in the hypervisor.

3. Import the Tenable Core + Tenable Sensor Proxy VMware .ova file from your computer to your virtual machine. For information about how to import a .ova file to your virtual machine, see the [VMware documentation](#).

4. In the setup prompt, configure the virtual machine to meet your organization's storage needs and requirements, and those described in [License and System Requirements](#).

5. Launch your Tenable Core + Tenable Sensor Proxy instance.

   The virtual machine boot process appears in a terminal window.

   **Note**: The boot process may take several minutes to complete.

   When the virtual machine boot process finishes, the Tenable Core + Tenable Sensor Proxy deployment is complete.

What to do next:

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in [Get Started](#).

---

**Deploy Tenable Core in Hyper-V**

To deploy Tenable Core + Tenable Sensor Proxy as a Microsoft Hyper-V virtual machine, you must download the Tenable Core + Tenable Sensor Proxy .zip file and deploy it on the host where you want to launch Tenable Core + Tenable Sensor Proxy.

**Note**: After you download the .zip file, you can use an external storage device to deploy it on another machine. You do not need internet access on the machine hosting Tenable Core.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in [License and System Requirements](#).
To deploy Tenable Core + Tenable Sensor Proxy as a Hyper-V virtual machine:

1. Download the Tenable Core Sensor Proxy HyperV Image file from the Tenable Downloads page.
2. Navigate to your Hyper-V Manager on the machine where you want to deploy Tenable Core + Tenable Sensor Proxy.
3. Extract the .zip file you previously downloaded. Extracting may take a few minutes.
4. In your Hyper-V Manager, create a new virtual machine.
   The Hyper-V Manager wizard appears.
5. In the setup wizard, adjust the virtual machine configurations to meet your organization's storage needs, and the requirements described in System Requirements

   **Note:** Tenable recommends that you select Generation 1 when the Hyper-V Manager wizard prompts you during the configuration.

6. When prompted to Connect to a Virtual Hard Disk in the wizard, select Use an existing virtual hard disk.
7. Click Browse and select the .vhd file.
8. Click Finish.
   The Hyper-V setup completes.
9. (Optional) If you want to increase the number of CPUs on your virtual machine:
   a. In the Virtual Machines table, right-click the row for your machine and click Settings.
      The settings window appears.
   b. In the Hardware section, click Processor.
   c. Modify the settings as necessary.
   d. Click Ok.
10. In the **Virtual Machines** table, right-click the row for your machine and click **Start** or **Connect**.

    The virtual machine load process appears in a console. The load process may take several minutes to complete.

**What to do next:**

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in Get Started.

**Deploy Tenable Core in AWS**

You can deploy Tenable Core + Tenable Sensor Proxy in Amazon Web Services (AWS) via the AWS Marketplace.

**Before you begin:**

- Confirm your environment will support your intended use of the instance, as described in License and System Requirements.

- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

**To deploy a Tenable Core virtual machine in AWS:**

1. Log in to AWS. For more information, see the AWS Documentation.

2. Navigate to the Amazon Marketplace.

3. In the Amazon Marketplace search bar, type **Tenable Core + Tenable Sensor Proxy**.

4. Click the result for **Tenable Core + Tenable Sensor Proxy**.

    The product overview page appears.

5. Click **Continue to Subscribe**.

    Either a terms and conditions window or the basic configurations page appears.
a. If the terms and conditions window appears, click \textbf{Accept Terms}.

b. Click \textbf{Continue to Configuration}.

The basic configurations page appears.

6. Select the region where you want to operate your virtual machine. AWS preselects fulfillment and software versions for the AMI based on your region.

7. Click \textbf{Continue to Launch}.

The launch options page appears.

8. In the \textbf{Choose Action} drop-down box, select one of the following:

- \textbf{Launch from Website} – Continue deploying in a simplified launch page with limited configuration options. For more information, see \textit{Deploy Tenable Core in AWS with Limited Options}.

- \textbf{Launch through EC2} – Continue deploying in an advanced launch instance wizard with complete configuration options, including options for cloud-init. For more information, see \textit{Deploy Tenable Core in AWS with Advanced Options}.

What to do next:

- \textbf{Create a Password for the Initial Administrator User Account}

\textbf{Deploy Tenable Core in AWS with Limited Options}

When deploying Tenable Core in Amazon Web Services (AWS), you can deploy via Amazon Elastic Cloud Compute (Amazon EC2) using a simplified launch page with limited configuration options. If you need to configure cloud-init or other advanced options, see \textit{Deploy Tenable Core in AWS with Advanced Options}.

Before you begin:

- Begin deploying Tenable Core + Tenable Sensor Proxy, as described in \textit{Deploy Tenable Core in AWS}.

To continue deploying via the website:
1. Click the instance type you want to use to deploy Tenable Core + Tenable Sensor Proxy. AWS preselects your Tenable-recommended instance type.

2. Select the virtual private cloud (VPC) where you want to launch your Tenable Core instance, based on your organization’s network requirements.

   **Tip:** For information about your organization’s network requirements, contact your system administrator.

3. In the **Subnet** section, select the subnet you want to use.

4. In the **Security Group Settings** section, create or select a security group that meets the requirements described in *Port Requirements*.

5. In the **Key Pair Settings** section, select the SSH key pair option you want to use for the default administrator account in Tenable Core.

6. Click **Launch**.

   AWS deploys and launches your Tenable Core instance as a virtual machine in AWS.

**What to do next:**

- [Create a Password for the Initial Administrator User Account](#)

**Deploy Tenable Core in AWS with Advanced Options**

When deploying Tenable Core in Amazon Web Services (AWS), you can deploy via Amazon Elastic Cloud Compute (Amazon EC2) using an advanced launch instance wizard with complete configuration options, including options for cloud-init. If you want a more streamlined experience and you do not need to configure cloud-init options, see [Deploy Tenable Core in AWS with Limited Options](#).

**Before you begin:**

- Begin deploying Tenable Core + Tenable Sensor Proxy, as described in [Deploy Tenable Core in AWS](#).

**To continue deploying via Amazon EC2:**
1. Configure the options based on the specifications you want for your instance and the requirements described in Tenable Core Requirements. For information about specific configurations in AWS, see the AWS Documentation.

2. Click the Configure Instance tab.
   In the Advanced Settings section, in the text box, add more configurations (for example, password, new users, and groups) to your instance. For more information, see the cloud-init Documentation.

3. Click the Configure Instance tab.
   In the Advanced Settings section, in the text box, paste the following:

   ```
   #cloud-config
   runcmd:
   # Link Sensor Proxy to tenable.io
     - /opt/sensor_proxy/sbin/sidecar
       - -link
       - -key
       - "your TVM linking key"
   ```

   **Tip:** You can add more configurations (for example, password, new users, and groups) to your instance by modifying the configurations and values in this text. For more information, see the cloud-init Documentation.

4. Click Launch.
   An SSH key pair window appears.

5. In the drop-down box, select the key pair option you want to use for your instance.
   **Caution:** Do not select the option to proceed without a key pair. If you launch your Tenable Core instance without a key pair you cannot connect to the instance, and you cannot add an SSH key pair later.

6. In the lower-left corner, click Launch Instances.
   AWS deploys and launches your Tenable Core instance as a virtual machine in AWS.

What to do next:
Create a Password for the Initial Administrator User Account

Deploy Tenable Core in Microsoft Azure

It is typically simplest to create and configure Tenable Core + Tenable Sensor Proxy using the Microsoft Azure portal, as described in Deploy Tenable Core in Microsoft Azure via the Portal.

In some cases, you may prefer to use the Microsoft Azure command line interface (CLI) to deploy Tenable Core in Azure, as described in Deploy Tenable Core in Microsoft Azure via the CLI.

Deploy Tenable Core in Microsoft Azure via the Portal

It is typically simplest to create and configure Tenable Core + Tenable Sensor Proxy using the Microsoft Azure portal.

In some cases, you may prefer to use the Microsoft Azure command line interface (CLI) to deploy Tenable Core in Azure, as described in Deploy Tenable Core in Microsoft Azure via the CLI.

Before you begin:

• Confirm your environment will support your intended use of the instance, as described in License and System Requirements.

• Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy a Tenable Core + Tenable Sensor Proxy virtual machine via the Azure portal:

1. Log in to the Microsoft Azure portal. For more information, see the Microsoft Azure Documentation.

2. Create a new resource by searching for the Tenable Core + Tenable Sensor Proxy template.

3. Configure all desired options.

Note: If you want Tenable Core + Tenable Sensor Proxy to link automatically to Tenable Vulnerability Management on first boot, enter the following in the advanced settings using the custom data box:

```bash
#cloud-config
runcmd:
# Link Sensor Proxy to tenable.io
```
4. Start the virtual machine deployment.

   Azure begins the virtual machine deployment. Azure displays a success message when finished.

What to do next:

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in Get Started.

Deploy Tenable Core in Microsoft Azure via the CLI

It is typically simplest to create and configure Tenable Core + Tenable Sensor Proxy using the Microsoft Azure portal, as described in Deploy Tenable Core in Microsoft Azure via the Portal.

In some cases, you may prefer to use the Microsoft Azure command line interface (CLI) to deploy Tenable Core in Azure.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in License and System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy a Tenable Core + Tenable Sensor Proxy virtual machine via the Azure CLI:

1. In a text editor, open a new file.

2. If you want Tenable Core + Tenable Sensor Proxy to link automatically to Tenable Vulnerability Management on first boot, copy and paste the following configuration variables:

   ```
   #cloud-config
   runcmd:
   ```
3. Save and close the configuration file.

4. Log in to the Azure CLI.

5. In the Azure CLI, run the `az vm create` command to deploy the file, using the following variables:

```
az vm create --size <The size of your virtual machine>
   --image
   --resource-group <Your resource group name>
   --location <Your location (for example, eastus)>
   --name <The name you want to call your VM>
   --admin-username <The username for your Tenable Core administrator>
   --admin-password <The password for your Tenable Core administrator>
   --custom-data <The file path to your configuration file>
```

Tip: For more information about the Azure CLI, see the *Microsoft Azure CLI Documentation*.

The system deploys your Tenable Core + Tenable Sensor Proxy virtual machine.

What to do next:

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in Get Started.

Install Tenable Core on Tenable-Provided Hardware
You can install Tenable Core + Tenable Sensor Proxy directly on Tenable-provided hardware using an .iso image. When you install Tenable Core via an .iso image on your computer, Tenable Core replaces your existing operating system with the Tenable Core operating system.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in License and System Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To install Tenable Core + Tenable Sensor Proxy on hardware:

1. Download the Tenable Core Tenable Sensor Proxy Installation ISO file from the Tenable Downloads page.
2. Boot the .iso. For more information, see your environment documentation.

   **Caution:** Booting the .iso replaces your existing operating system with the Tenable Core operating system.

   The installer installs Tenable Core + Tenable Sensor Proxy on your hardware.

3. The installation begins if there are no configuration errors.

   The Installation menu appears if there are configuration errors (such as errors after setting up a Base Repository, for example):
The installation runs and the server restarts.

What to do next:

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in Get Started.

Configure Tenable Core Multi-Factor Authentication

You can log into the Tenable Core user interface with multi-factor authentication (MFA). This topic explains how to configure MFA for Tenable Core and only applies to the user interface. Using MFA requires a Google Authenticator token.

**Note:** Multi-Factor Authentication is only supported on OL8 operating system deployments of Tenable Core.
To enable MFA for Tenable Core user interface login:

1. Install the Oracle EPEL repositories by running the following command:

```
sudo dnf install oracle-epel-release-el8
```

**Note:** It may require several minutes for the install to complete.

2. Disable Oracle EPEL repositories by default by running the following command:

```
sudo dnf config-manager --disable 'ol8_developer_EPEL*'
```

3. Install the Google Authenticator client and dependencies by running the following command:

```
sudo dnf install --enablerepo=ol8_developer_EPEL google-authenticator qrencode
```

4. For each user that needs to use MFA when logging in to the Tenable Core user interface, do one of the following:

   a. Run the following command as the user:

```
google-authenticator -t -d -f -u -w 5
```

   **Note:** If using the Tenable Core user interface terminal, add `-Q utf8` to the `google-authenticator -t -d -f -u -w 5` command.

   **Note:** Running this command for the same user more than once invalidates previous codes.

   i. In your authenticator app, scan the QR code.

   ii. Enter the confirmation code from the app.

   iii. (Optional, but recommended) Save the emergency scratch codes.
b. Alternatively, for full control over the MFA token creation options, run the following command:

```
google-authenticator
```

5. Run the following command:

```
sudo edit /etc/pam.d/cockpit
```

6. Under the `auth substack password-auth` line add:

```
auth required pam_google_authenticator.so
```

7. Confirm that the first six lines of the `/etc/pam.d/cockpit` file look like this:

```
# %PAM-1.0
auth required pam_sepermit.so
auth substack password-auth
auth required pam_google_authenticator.so
auth include postlogin
auth optional pam_ssh_add.so
....... 
```

8. Log into the Tenable Core user interface.

**Log In to Tenable Core**

Log in to Tenable Core to configure and manage your Tenable Core + Tenable Sensor Proxy instance in the Tenable Core interface.

**Before you begin:**

- Deploy Tenable Core + Tenable Sensor Proxy, as described in [Deploy or Install Tenable Core](#).

**Note:** For information on inbound and outbound port requirements, see [Access Requirements](#).
To log in to Tenable Core:

1. Navigate to the URL for your Tenable Core virtual machine.
   The login page appears.
2. In the **User name** field, type your username.
3. In the **Password** field, type your password.
4. Click **Log in**.
   Tenable Core logs you in to the user interface.

To access administrative or limited access modes:

- You can access an administrative access mode by clicking the "Administrative access" button at the top of the page. In administrative access mode, you can switch back to a limited access mode by clicking the "Limited access" button in the same location.

Create an Initial Administrator User Account

The first time you access Tenable Core + Tenable Sensor Proxy, you log in as a wizard user.

Then, you create an initial administrator account.

**Tip:** If you delay creating an initial administrator account, after a few minutes, the system locks you out of the wizard user account. Reboot Tenable Core to proceed with the initial administrator account creation.

Before you begin:

- Deploy or install Tenable Core + Tenable Sensor Proxy, as described in **Deploy or Install Tenable Core**.
To create an initial administrator user account:

1. Navigate to the URL for your Tenable Core virtual machine.
   The login page appears.
2. In the User name field, type wizard.
3. In the Password field, type admin.
4. Click Log In.
   The Create New Administrator window appears.
5. In the Username field, type the username you want to use for your administrator account.
6. In the Password field, type a new password for your administrator account.

   **Note:** Your password must meet the following minimum requirements:
   - Minimum 14 characters long
   - Cannot be a palindrome (i.e., a word or phrased spelled the same backward and forward)

7. Click Create Account.
   A confirmation window appears.
8. Click Finish Setup.
   Tenable Core creates your user account.
9. Click Log Out.
   Tenable Core logs you out.

What to do next:
- (Optional) If you want to log in again, see Log In to Tenable Core.
- (Optional) If you want to create another user account, see Create New User Account.

   **Note:** Log in again to create a new user account.

Create a Password for the Initial Administrator User Account
If you deployed Tenable Core + Tenable Sensor Proxy in a cloud environment and did not create a password during deployment, you cannot access the Tenable Core interface. Create a password for your administrator account via SSH to access the Tenable Core interface.

You do not need to create a password via SSH when deploying Tenable Core + Tenable Sensor Proxy in any of the other supported environments.

Before you begin:

- Confirm that you have an SSH client installed that can access your Tenable Core server.

To create a password for the initial administrator user account:

1. Open a connection to Tenable Core with your SSH client via one of the following methods:
   - If your SSH client uses a command-line interface (CLI), run the following command:

     ```
     ssh <your administrator username>@<your Tenable Core hostname or IP address>
     ```

   - If your SSH client uses a user interface, open the interface and follow the prompts to connect to Tenable Core via SSH.

     Tenable Core connects to your SSH client.

     **Note:** When prompted, provide your Tenable Core username via one of the following methods:

     - If you deployed in Amazon Web Service (AWS), type `ec2-user` as your username.
     - If you deployed in Microsoft Azure, type the username you configured during your deployment.

2. Run the `sudo passwd` command.

   ```
   sudo passwd "$USER"
   ```

   The SSH client prompts you to provide a password.

3. Type the password you want to use for your administrator account.
Note: Your password must meet the following minimum requirements:

- Minimum 14 characters long
- Cannot be a palindrome (i.e., a word or phrased spelled the same backward and forward)

4. Press **Enter**.

Tenable Core assigns the password to your administrator account.

5. Run the `exit` command to log out of Tenable Core.

What to do next:

- Continue getting started with Tenable Core + Tenable Sensor Proxy, as described in [Get Started](#).

### Manually Configure a Static IP Address

If you deploy Tenable Core in an environment where DHCP is configured, Tenable Core automatically receives network configurations (including your IP address). If DHCP is not configured, you must manually configure a static IP address in Tenable Core.

For more information about the default NIC configuration in your environment, see [License and System Requirements](#).

Before you begin:

- Deploy or install Tenable Core + Tenable Sensor Proxy, as described in [Deploy or Install Tenable Core](#).

- Contact your network administrator and obtain your network’s netmask and the IP address for your Tenable Core + Tenable Sensor Proxy deployment.

To configure a static IP address manually:

1. In the command-line interface (CLI) in Tenable Core, type the following to log in as a wizard user:
tenable-y3u1xwh1 login: wizard
Password: admin

A prompt appears asking if you want to configure a static IP address.

2. Press the y key.

(Optional) If the prompt does not appear, in the command-line interface (CLI) in Tenable Core, run the following command to access the configuration user interface:

```
  nmtui edit
```

The list of connections page appears.

3. Select the connection you want to configure.

4. Press Tab to select <Edit>.

5. Press Enter.

   The Edit Connection window appears.

6. In the IPv4 Configuration row, press Tab to select <Automatic>.

7. Press Enter.

8. Select <Manual> from the drop-down box.


10. Press Tab to select <Show>.

11. Press Enter.

   More configuration fields appear.

   **Note:** Type the value for each configuration field as four numbers separated by a period. Refer to the examples for each field.

12. In the Addresses field, type the IPv4 IP address for your Tenable Core + Tenable Sensor Proxy deployment, followed by a forward slash and your netmask.

   Example:
13. In the **Gateway** field, type your gateway IP address.  
   Example:  
   
   ![Gateway IP address](192.0.2.57/24)

14. In the **DNS servers** field, type your DNS server IP address.  
   Example:  
   
   ![DNS server IP address](192.0.2.177)

15. Press **Tab** to select <Add...>.  

   **Note**: Complete steps 12-15 only if you have more DNS server IP addresses to add. Repeat for each IP address.

16. Press **Enter**.  
   An empty box appears in the **DNS servers** row.

17. In the new row, type your second DNS server IP address.  
   Example:  
   
   ![Second DNS server IP address](192.0.2.176)

18. Select the check box in the **Require IPv4 addressing for this connection** row.

19. Press **Tab** to select <OK>.  
   The list of connections appears.

20. Press **Tab** to select <Quit>.  

21. Press **Enter**.  
   If you log in with a wizard, a prompt appears asking if you want to create an administrator account.
To create an administrator account, see Create a First-Time User Account.

You are logged out of the wizard account.

22. Log into the CLI using the administrator account.

23. Restart the connection. In the command-line interface (CLI) in Tenable Core, run the following command:

```
$ nmcli connection down "Wired connection 1" && nmcli connection up "Wired connection"
```

**Note:** Restarting the connection enables the system to recognize your static IP address. You can reboot the system instead to trigger the response.

Disk Management

You can use the Tenable Core interface to manage some aspects of your Tenable Core machine disk space. Tenable Core uses Linux logical volume management (LVM) for disk management.

Disk management via the Tenable Core interface assumes you understand basic LVM terminology:

- **Volume group** – A group of one or more physical volumes.
- **Physical volume** – A hard disk, hard disk partition, or RAID unit.
- **Logical volume** – A block of space on the volume group sized to mirror several or all of your physical volumes.
- **File system** – The file system on the logical volume.
- **Mount point** – The location where you mounted the file system in your operating system.

For more information about these concepts, see the general documentation for Linux.

Tenable Core Partitions

Tenable Core deploys with the following preconfigured partitions:

**Note:** This is not a complete list, but an example of the important partitions in Tenable Core.
• /boot
• Swap
• /
• /var/log
• /opt

To add more storage space to Tenable Core (typically, in /opt), add a disk or expand a disk as described in Add or Expand Disk Space.

Add or Expand Disk Space

If you need more space in Tenable Core to meet the requirements, add space to your machine by expanding an existing disk or adding a new disk. For general information about Tenable Core disk management, see Disk Management.

**Caution:** You cannot reassign disk space after you have assigned the space to a file system.

(OL8) To add or expand existing disk space on your Tenable Core machine:

1. Power down your machine, as instructed by your local administrator or the documentation for your local environment.

2. Add a new disk or expand an existing disk in your machine configuration, as instructed by your local administrator or the documentation for your local environment.

3. Power up your machine, as instructed by your local administrator or the documentation for your local environment.

4. Log in to Tenable Core.

   The **System** page appears.

5. In the left navigation bar, click **Storage**.

   The **Storage** page appears.

6. In the **Storage** section, locate the filesystem with /opt as the mount point and note the containing volume group (typically **vg0**).
7. Click the row for the **volume group** that includes your preferred partition as the mount point.

The **LVM2 Volume Group** page appears:
8. Click the **Add Physical Volume** button.

9. Click the checkbox for the space you added.

10. Click **Add**.

The **Volume Group** page appears, updated to show the added space in the **Physical Volumes** section.
11. In the **LVM2 Logical Volumes** section, click the context button for the file system **Name** that includes your preferred partition as the **Mount Point**.

12. Click **Grow**.

   The **Grow Logical Volume** window appears.

13. Use the slider to increase the size of the file system to your desired size (typically, to the new maximum).

14. Click **Grow**.

   The system expands the logical volume and the file system.

   The **Volume Group** page appears, refreshed to reflect the new size.
Configure Tenable Core

You can use the Tenable Core user interface to configure Tenable Core + Tenable Sensor Proxy.

Configure Tenable Core + Tenable Sensor Proxy in the Tenable Core + Tenable Sensor Proxy User Interface

Start, Stop, or Restart Your Application

Configure a Proxy Server

SNMP Agent Configuration

Configure an SNMP Agent via the User Interface

Configure an SNMP Agent via the CLI

View the System Log

Filter the System Log

Generate a Diagnostic Report

Access the Terminal

Configure Tenable Core + Tenable Sensor Proxy in the Tenable Core + Tenable Sensor Proxy User Interface

After you deploy Tenable Core + Tenable Sensor Proxy and complete the initial configuration tasks, complete the configuration steps for Tenable Sensor Proxy.

To configure Tenable Sensor Proxy:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Sensor Proxy.
   The Sensor Proxy page appears.
3. Complete the confirmation tasks for your selected Tenable Sensor Proxy product, as described in Configure Sensor Proxy in the Tenable Sensor Proxy User Guide.

Configure Tenable Cor + Tenable Sensor Proxy in Tenable Core

The Sensor Proxy page displays summary information about your Tenable Sensor Proxy configuration.

To synchronize ports in the Tenable Core + Tenable Sensor Proxy firewall:

1. In the Configuration: section, click the number in the Web Server Port: field.

2. Enter all applicable ports, separating them with commas.

3. Click Save Configuration.
   A success message appears briefly in the dialogue box. The dialogue box then closes.

To link Tenable Core + Tenable Sensor Proxy to the cloud:
1. In the **Link to Cloud:** section, click the number in the **Linking Key:** field.

2. Enter your linking key.

3. Click **Link.**
   
   A success message appears briefly in the dialogue box. The dialogue box then closes.

**Tenable Sensor Proxy Logs**

To view Tenable Sensor Proxy logs:

1. Select the desired log from the drop-down box.

2. Click **View Log.**
   
   The log appears in the text box.

**Start, Stop, or Restart Your Application**

To start, stop, or restart your application via the user interface:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **Tenable Sensor Proxy.**
The application page appears.

3. In the Installation Info section, click Start, Stop, or Restart.

To start, stop, or restart your application via the CLI:

1. Log in to Tenable Core via the Terminal page or command line interface (CLI).

   The command line appears.

2. To change the status of your application, see the Tenable Sensor Proxy Documentation.

Configure a Proxy Server

If your organization configured a proxy server to conceal your IP address, share an internet connection on your local network, or control internet access on your network, set the proxy configuration in Tenable Core.

**Note:** This proxy configuration only applies to updates.

Before you begin:

- Log in to Tenable Core in a browser, as described in Log In to Tenable Core.

To configure a proxy server:

1. In the left navigation bar, click Update Management.

   The Updates page appears.

2. In the Proxy Host box, type the hostname and port for your proxy server in the format `hostname:port` (for example, https://192.0.2.1:2345).

3. (Optional) In the Proxy Username box, type a username for your proxy server.

4. (Optional) In the Proxy Password box, type a password for the proxy.

5. Click Save Proxy.

   The system initiates your proxy configuration.

SNMP Agent Configuration
If your organization uses a Simple Network Monitoring Protocol (SNMP) network management station (NMS) for device monitoring, you can install a net-snmp agent onto Tenable Core to report device data to your NMS.

You can use the user interface to configure common SNMPv2 or SNMPv3 settings. To configure other advanced or uncommon SNMP settings, use the CLI.

- Configure an SNMP Agent via the User Interface
- Configure an SNMP Agent via the CLI

To stop, start, restart, or reload the SNMP service in Tenable Core, or to view SNMP logs, see Manage Services.

Configure an SNMP Agent via the User Interface

**Required User Role:** Administrator with Reuse my password for privileged tasks enabled

To install and configure an SNMP agent on Tenable Core via the user interface:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **SNMP**.

   If you already installed an SNMP agent on Tenable Core, the **SNMP** page appears. If you do not have an SNMP agent installed on Tenable Core, the **Install SNMP Packages** window appears.

3. (Optional) In the **Install SNMP Packages** window, click **Install SNMP** to install the SNMP service.
Tenable Core installs the SNMP service and opens inbound ports 161 and 162 on Tenable Core.

The **SNMP** page appears.

4. In the **SNMP common setup** section, configure the contact properties you want to appear on your NMS for this instance of Tenable Core.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact</td>
<td>A name, email address, or other identifier for the person you want to list as the contact for questions about this instance of Tenable Core.</td>
</tr>
<tr>
<td>Location</td>
<td>A geographic, organizational, or other location descriptor for the person you want to list as the contact for questions about this instance of Tenable Core.</td>
</tr>
</tbody>
</table>

5. If you want to grant an SNMPv2c NMS access to Tenable Core, in the **SNMPv2c access control setup** section, configure one or both of the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>read-only access community name</td>
<td>Specifies the read-only community string for the SNMPv2c NMS.</td>
</tr>
<tr>
<td>read-write access community name</td>
<td>Specifies the read-write community string for the SNMPv2c NMS.</td>
</tr>
</tbody>
</table>

6. If you want to grant an SNMPv3 NMS read-only access to Tenable Core, in the **SNMPv3 access control setup** section, configure the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-only Hash algorithm</td>
<td>Specifies the read-only hash algorithm for the SNMPv3 NMS.</td>
</tr>
<tr>
<td>Read-only access username</td>
<td>Specifies the username and password for an account on the SNMPv3 NMS.</td>
</tr>
<tr>
<td>Read-only access user</td>
<td></td>
</tr>
</tbody>
</table>
7. If you want to grant an SNMPv3 NMS read-write access to Tenable Core, in the **SNMPv3 access control setup** section, configure the settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-write Hash algorithm</td>
<td>Specifies the read-write hash algorithm for the SNMPv3 NMS that you want to grant read-write access on Tenable Core.</td>
</tr>
<tr>
<td>Read-write access username</td>
<td>Specifies the username and password for an account on the SNMPv3 NMS.</td>
</tr>
<tr>
<td>Read-write access user password</td>
<td></td>
</tr>
</tbody>
</table>

8. Click **Save Configuration**.

Tenable Core saves your SNMP configuration.

**Configure an SNMP Agent via the CLI**

**Required User Role:** Root user

If your organization uses a Simple Network Monitoring Protocol (SNMP) network management station (NMS) for device monitoring, you can install a `net-snmp` agent onto Tenable Core to report device data to your NMS.

To install and configure an SNMP agent on Tenable Core via the CLI:

1. Prepare the `net-snmp` agent configuration file and add it to Tenable Core, as described in the *Net-SNMP Documentation*.

2. Log in to Tenable Core via the **Terminal** page or command line interface (CLI).

   The command line appears.

3. In the `/etc/snmp/` directory, open the `snmpd.local.conf` file.

   The file opens.
4. Locate the **IncludeFile** line in the file.

5. Comment out the **IncludeFile** line to instruct Tenable Core to ignore all current and future configurations on the **SNMP** page of the Tenable Core user interface.

   Tenable Core ignores SNMP configurations in the Tenable Core user interface.

   **Note:** IP tables may need to be updated to facilitate SNMP communication. Be sure to confirm that your OS configuration allows for this communication.

---

**View the System Log**

You can use the **System Log** page to view errors encountered in the system. The system log lists, categorizes, and stores system issues that have occurred within the last seven days.

To view Tenable Sensor Proxy logs:

1. Select the desired log from the drop-down box.

2. Click **View Log**.
   The log appears in the text box.

3. Click on an individual entry (row) to get additional information.

---

**Filter the System Log**
Several log type filters are available. The **Everything** option is selected by default. Select another option using the drop-down menu at the top of the page. The logs are listed with the most recent entry displayed first. Previous days are divided into sections with the corresponding date displayed in the header.

Filter the logs using the drop-down menu. Click on the date to display the filter options for the logs.

**Generate a Diagnostic Report**

You can use diagnostic reports to assist with troubleshooting Tenable Core.

To generate a diagnostic report for troubleshooting:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **Diagnostic Reports**.
   
   The **Diagnostic Reports** page appears.
3. Click the Run report button.

4. A user interface list appears as the report generates.

5. When the report is complete, the status displays Done.

6. Click the Download button next to each report that you want to download.

   Tenable Core saves and prints the report.

Access the Terminal

The Terminal page provides a console to access a user-specific command-line interface.
# Manage the System

You can use the **Overview** page to view usage statistics and manage system settings.

To manage the Tenable Core system:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The Tenable Core web user interface page appears.

   You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>• View your number of failed services.</td>
</tr>
<tr>
<td></td>
<td>• View your number of available updates.</td>
</tr>
<tr>
<td></td>
<td>• View the date, time, and location of the last successful login.</td>
</tr>
<tr>
<td></td>
<td>• View login history.</td>
</tr>
<tr>
<td>System information</td>
<td>• View your system <strong>Model</strong>.</td>
</tr>
<tr>
<td></td>
<td>• View the <strong>Asset tag</strong> of your system.</td>
</tr>
<tr>
<td></td>
<td>• View the <strong>Machine ID</strong> of your system</td>
</tr>
<tr>
<td></td>
<td>• View the <strong>Uptime</strong> of your system.</td>
</tr>
<tr>
<td></td>
<td>• View your system’s hardware details.</td>
</tr>
<tr>
<td>Usage</td>
<td>• View a graph of the <strong>CPU</strong> usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Memory</strong> usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View metrics and history of usage of your instance.</td>
</tr>
<tr>
<td>Configuration</td>
<td>• View and edit the hostname for your instance, as described in <strong>Edit Your Tenable Core Hostname</strong>.</td>
</tr>
<tr>
<td></td>
<td>• View the <strong>System time</strong>.</td>
</tr>
</tbody>
</table>
Manage System Storage

You can use the Storage page to view real-time system storage graphs, filesystem information, and logs. For more information, see Disk Management.

To manage Tenable Core storage:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Storage.
   
   The Storage page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphs</td>
<td>• View a graph of the Reading storage activity on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Writing storage activity on your instance.</td>
</tr>
<tr>
<td>Filesystems</td>
<td>• View information about each filesystem.</td>
</tr>
<tr>
<td>table</td>
<td>• Click a row to view more details about the filesystem.</td>
</tr>
<tr>
<td></td>
<td>• Rename a filesystem, as described in Rename a Filesystem.</td>
</tr>
<tr>
<td></td>
<td>• Delete a filesystem, as described in Delete a Filesystem.</td>
</tr>
</tbody>
</table>

Rename a Filesystem

To rename a filesystem in Tenable Core:
1. In the left navigation pane, click **Storage**.
   
The **Storage** page appears.

2. In the **File Systems** section, click on the individual file in the file systems list.
   
The details page appears.

3. Click the **Rename** button in the upper right section of the window.
   
A new window appears.

4. Enter the new name for the **File System**.

5. Click **Create**.

   The new name appears on the page.

**Delete a Filesystem**

To delete a filesystem in Tenable Core:

1. In the left navigation pane, click the **Storage** option. The **Storage** page displays.

2. In the **File System** section, click the individual file in the files systems list. The details page appears.

3. Click the red **Delete** button in the system heading.

4. Confirm that you want to delete the **File System**.

   ![Please confirm deletion of centos](image)

   **Caution:** Deleting a volume group erases all data on it.
Manage Updates

You can use the **Updates Management** page to manage your Tenable Core and application updates.

If your deployment is online, Tenable recommends:

- Configuring automatic updates. For more information, see [Configure Automatic Updates](#).
- Performing on-demand updates, as needed. For more information, see [Update On Demand](#).

If your deployment is offline, you can perform offline updates. For more information, see [Update Tenable Core Offline](#).

Configure Automatic Updates

By default, Tenable Core has automatic updates enabled.

If you deploy Tenable Core in an online environment, Tenable recommends keeping automatic updates enabled. When performing an automatic update, Tenable Core retrieves and installs:

- The latest version of Tenable Sensor Proxy.
- The latest version of host operating system included in Tenable Core.
- The latest version of any additional packages required by Tenable Core.
- The latest version of any additional host operating system packages you installed.

To configure automatic updates:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation pane, click **Update Management**.
   
   The **Update Management** page appears.

3. In the **AUTOMATIC UPDATES** section, click the **Edit** link in the **Unit State** row.
   
   The **Services** details page appears, displaying the details for the **Scheduled System Updates** service.

4. Confirm that you have set **Unit State** to enabled (set to enabled by default).
5. Review the schedule for the automatic updates and modify, if needed, as described in Configure Your Automatic Update Schedule.

Configure Your Automatic Update Schedule

By default, Tenable Core has automatic updates set to enabled.

If you deploy Tenable Core in an online environment, Tenable recommends keeping automatic updates enabled.

To configure the schedule for your automatic updates:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The Tenable Core web user interface page appears.

2. In the left navigation pane, click Update Management.
   The Update Management page appears.

3. In the AUTOMATIC UPDATES section, click the link in Timer Config Line.
   The Edit Timer Configuration window appears.

4. Modify the schedule.

   **Note:** If you set both a Day of week and a Day of month, the system only performs updates on days when those two parameters are true. For example, if you set Wednesday as the Day of week and 8 as the Day of month, Tenable Core performs automatic updates only on the 8th of the month if it is a Wednesday.

   **Tip:** Tenable Core uses Eastern Time as your default time zone, unless you modify it as described in Edit Your Time Settings.

5. Click Save.

   Tenable Core modifies the schedule for automatic updates.

Update On Demand

If you deploy Tenable Core in an online environment, you can perform updates on demand. When updating on demand, Tenable Core retrieves and installs the following:
To update on demand:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The Tenable Core web user interface page appears.
2. In the left navigation pane, click Update Management.
   The Update Status section on the page shows the number of available updates.
3. (Optional) Click the button to refresh the page with available updates in the Update Status section
4. Click the Install Updates button.
   Tenable Core installs the updates.
5. Tenable Core confirms your system is up to date and prompts you to reboot, if required by any of the installed updates.
6. If prompted, restart your system.

Update Tenable Core Offline

Tenable recommends applying all offline updates to your Tenable Core machine in chronological order. Do not skip offline updates. There are two methods available to perform an offline update. For information about the contents of individual offline update files, see the Tenable Core Release Notes.

Tip: For more information about updating Tenable Core, see the FAQ.

To upload a Tenable Core offline update .iso file:
1. Navigate to the Tenable Core Offline Update ISO section of the Tenable Downloads page.

2. Click and download the offline update .iso file.

3. Upload the file via scp. For example:

```bash
cp local-iso-file.iso user@host:/srv/tenablecore/offlineiso/local-iso-file.iso
```

**Note:** The target line may vary; however, the destination must be the following path:
/srv/tenablecore/offlineiso/tenable-offline-updates.iso

4. Rename the offline update .iso file as `tenable-offline-updates.iso`.

**To update Tenable Core via external media:**

1. Navigate to the Tenable Core Offline Update ISO section of the Tenable Downloads page.

2. Click and download the offline update .iso file.

3. Burn the ISO to media (for example, DVD-DL, BD, or thumb drive).

4. Attach the media to a system and have it mount automatically.

**Note:** By default, the hardening on OL8 operating systems prevents USB media from mounting. In order to use USB drives with a Tenable Core OL8 operating system, the `/etc/modprobe.d/usb-storage.conf` file needs to be removed from that directory.

**What to do next:**

- Update on Demand

**Application Data Backup and Restore**

Backup and restore requires a connection to a remote storage host. When Tenable Core begins a scheduled or on-demand backup, your files are stored temporarily in `/opt/tenablecore/backup/spool` before being sent to the configured remote storage host.

Later, you can restore your backup data by uploading your backup file to Tenable Core.
Note: You can also use local backups in Tenable Core. Remote storage is safer and preferred, but local storage can be enabled. In the user interface you can specify how many backups to keep and download backups that are stored locally. For more information, see Configure Storage for Tenable Core Backups.

For more information, see:

- Configure Storage for Tenable Core Backups
- Perform an On-Demand Backup
- Change the Scheduled Backup Time
- Restore a Backup

If you want to enable or disable a scheduled backup, click Scheduled backups can be configured Here.

Note: During a backup or a restore, Tenable Core stops the Tenable Sensor Proxy application service. You cannot use Tenable Core during this time. After the backup or restore completes, your services restart and Tenable Sensor Proxy resumes normal function.

Tip: A virtual machine snapshot backs up the entire virtual machine (application-installed files, application data, OS files, and configurations.) To take a snapshot of your virtual machine, see Take a Snapshot.

Remote Storage Host Requirements

The location where you store your backups must:

- Have rsync installed.
- Have an SSH server installed and running.
- Have sufficient storage space to hold your application's backup data.
- Have a user with write permissions to manage the remote storage host location.

Note: Tenable Core does not manage your remote storage system. If you have concerns about space on your remote storage system, remove backup files manually when you no longer need them.

Configure Storage for Tenable Core Backups
Before you can back up your application data, you must set the storage location. You can establish a remote storage host with an SSH key and configure Tenable Core to use that host, or you can store backups locally.

Configure remote backup storage

Before you begin:

- Confirm your SSH private key for authenticating to the remote storage host is in OpenSSH key format.
- Prepare your remote storage host environment, as described in the Remote Storage Host Requirements.
- Confirm that you can log in to your remote storage host using SSH key authentication.

Note: There are several ways to create your own SSH private key. These are not Tenable-specific processes. Consult your system administrator.

To configure your remote storage host:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Remote Storage.
   
   The Remote Storage Configuration page appears.

3. In the Remote Host box, type the hostname for the remote storage host where you want to store your backup files.

4. In the Remote Path: box, type the location on the remote host where you want to store your backup files.

5. In the User box, type the username for a user on the remote host with edit permissions for the remote path location.

6. In the SSH private key box, paste the SSH private key for authenticating to the remote storage host.

7. Click Save Configuration.
Configure local backup storage

Storing backups exclusively on the Tenable Core system where the backup is taken is not recommended. Backups should be kept in a separate location in order to avoid data loss in the event that the Tenable Core system becomes unusable.

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Remote Storage.
   The Remote Storage Configuration page appears.

3. In the Storage Mode drop-down menu and select Local.

4. In the left-navigation bar, click Backup/Restore.
   The Backup/Restore page appears.

   In the user interface you can specify how many backups to keep and download backups that are stored locally.

   **Note:** In local storage mode, backups are stored in a folder under /opt.

Any backups that have been taken appear in the list of Available Backups.

**Note:** A fixed number of backups are kept with the oldest ones being deleted. Tenable recommends you make sure there is enough space for that number of backups plus one on the disk that contains /opt.

What to do next:
• Perform a backup, as described in Perform a Backup on Demand.

• (Optional) Change your automatic backup schedule, as described in Change Your Automatic Backup Schedule.

• (Optional) Restore a backup, as described in Restore a Backup.

Perform an On-Demand Backup

Perform a backup of your application data anytime between scheduled backups. For more information about scheduled backups, see Change the Scheduled Backup Time.

Note: During a backup or a restore, Tenable Core stops the Tenable Sensor Proxy application service. You cannot use Tenable Core during this time. After the backup or restore completes, your services restart and Tenable Sensor Proxy resumes normal function.

Before you begin:

• Configure your remote storage host, as described in Configure Storage for Tenable Core Backups.

To perform an on-demand backup:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Backup/Restore.

   The Backup/Restore page appears.

3. In the AVAILABLE MODULES section, select the box next to the application you want to back up.

4. Click Take Backup Now.

   The BACKUP IN PROGRESS window appears. The window disappears after the system completes the backup.

What to do next:

• (Optional) Restore the backup, as described in Restore a Backup.

Change the Scheduled Backup Time
By default, Tenable Core backs up your applications daily at 2:30 AM local time. You can edit your schedule preferences in Tenable Core to change the time and frequency of your scheduled backups.

For more information about managing your time preferences, see Edit Your Time Settings.

**Note:** Tenable Core cannot perform a backup (scheduled or on-demand) until you configure a remote storage host on your computer. For more information, see Configure Storage for Tenable Core Backups.

To change the scheduled backup time:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   
The Tenable Core web user interface page appears.

2. In the left navigation bar, click Backup/Restore.

   The Backup/Restore page appears.

3. In the AUTOMATIC BACKUPS table, locate the Timer Config Line row.

4. Click Edit.

   The EDIT TIMER CONFIGURATION window appears.

5. On the EDIT TIMER CONFIGURATION window, update the configuration based on your desired backup frequency:

   **Note:** If you specify a day of the week and a day of the month for your scheduled backups, Tenable Core performs the backups only when those values overlap. For example, if you specify Monday and 15, Tenable Core performs your backups only on Mondays that fall on the 15th day of the month.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Configuration</th>
</tr>
</thead>
</table>
| Daily     | • In the Day of Week and Day of Month boxes, type an asterisk (*).  
• In the Hour box, type the hour when you want Tenable Core to perform a backup as an integer between 0 and 23.  
• In the Minute box, type the minute when you want Tenable Core to perform a backup as an integer between 0 and 59. |
| Weekly          | • In the **Day of Week** box, type the day of the week when you want Tenable Core to perform a backup (for example, *Monday* or *Mon*).
|                | • In the **Day of Month** box, type an asterisk (*).
|                | • In the **Hour** box, type the hour you want Tenable Core to perform a backup as an integer between 0 and 23.
|                | • In the **Minute** box, type the minute you want Tenable Core to perform a backup as an integer between 0 and 59.
| Monthly        | • In the **Day of Week** box, type an asterisk (*).
|                | • In the **Day of Month** box, type the day of the month when you Tenable Core to perform a backup as an integer (for example, *15*).
|                | • In the **Hour** box, type the hour you want Tenable Core to perform a backup as an integer between 0 and 23.
|                | • In the **Minute** box, type the minute you want Tenable Core to perform a backup as an integer between 0 and 59.

6. Click **Save**.

   Your scheduled backup time updates.

**What to do next:**

• (Optional) Perform an on-demand backup, as described in [Perform a Backup On Demand](#).

• (Optional) Restore the backup, as described in [Restore a Backup](#).

### Restore a Backup

You can restore a backup to return an application to a prior state by uploading a backup to restore, or by restoring from your local storage.

**Note:** During a backup or a restore, Tenable Core stops the Tenable Sensor Proxy application service. You cannot use Tenable Core during this time. After the backup or restore completes, your services restart and Tenable Sensor Proxy resumes normal function.

**Before you begin:**
• Check your firewall settings and confirm that your computer can access port 8090 on Tenable Core, as described in Access Requirements.

**Note:** If you do not confirm this ahead of the backup/restore process Tenable Core provides a link to click which opens a connection-check URL in a new tab so you can accept the certificate for port 8090, and have the restoration process try again.

• For help with issues encountered during the process, refer to the FAQ.

**To upload and restore an application backup:**

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The Tenable Core web user interface page appears.

2. In the left navigation bar, click Backup/Restore.

   The Backup/Restore page appears.

3. In the UPLOAD AND RESTORE section, click Choose a file.

   Your file manager appears.

4. Select the desired backup file.

5. Click Open.

   A details window for the backup appears.

6. If prompted, confirm that you want to upgrade or downgrade your current Tenable Core application version to match the application version from your backup file.

   a. Click Install Correct Version.

      A confirmation window appears.

   b. Click Replace.

      Tenable Core installs the correct version of your application.

      The Restore window appears.

7. Click Restore.

   The system restores your backup to Tenable Core.
Note: Do not log out of Tenable Core or close your browser until after the **Uploading the archive** task is complete. If you end your session early, the restore fails.

When the restore finishes, a success message appears.

**Tip:** If the restore attempt fails, an error message appears with details and remediation instructions. Resolve the errors and click **Retry**.

**To restore a locally stored backup:**

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **Backup/Restore**.

   The **Backup/Restore** page appears.

3. In the **Upload and Restore** section, click **Restore from local backup storage**.

   The **Select Local Backup** pop-up window appears.

4. Select the desired backup file.

5. Click **Restore**.

   A details window for the backup appears.

6. Click **Restore**.

   The system restores your backup to Tenable Core.

**Note:** You can use this feature to restore Tenable Core backups uploaded to the system by tools such as scp or rsync. Store the backups in `/opt/tenablecore/remote-storage/localstorage/` before attempting to restore.

**Manage Certificates**

From the **SSL/TLS Security Certificates** page, you can manage the certificates used by Tenable Core and your application.

[Manage the Server Certificate](#)

[Upload a Certificate for a Trusted Certificate Authority](#)
Use Different Certificates for Tenable Core and Your Application

Manage the Server Certificate

When you first deploy Tenable Core, Tenable provides a default server certificate for accessing the Tenable Core and application interfaces.

**Note:** The default certificate is not signed by a recognized certificate authority (CA). If your browser reports that the Tenable Core or application server certificate is untrusted, Tenable recommends uploading a custom server certificate signed by a trusted certificate authority (CA) for Tenable Core and application use. For more information, see [Upload a Custom Server Certificate](#). Alternatively, you can download the Tenable-provided CA certificate (cacert.pem) for your server certificate and upload it to your browser.

If you upload a custom server certificate signed by a custom CA, you must also provide certificates in the chain to validate your custom server certificate.

For more information, see:

- [Upload a Custom Server Certificate](#)
- [Remove a Custom Server Certificate](#)

Upload a Custom Server Certificate

If you do not want to use the Tenable-provided server certificate, you can upload a custom server certificate to Tenable Core. For more information, see [Manage the Server Certificate](#).

You cannot upload multiple custom server certificates to Tenable Core. Uploading a new file replaces the existing file.

Before you begin:

- Confirm your custom server certificate and key files use the *.der, *.pem, or *.crt extension.
- Move the custom server certificate and key files to a location accessible from your browser.

To upload a custom server certificate for Tenable Core:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation pane, click **SSL/TLS Certificates**.
The SSL/TLS Certificates page appears.

3. Click the System Certificate tab.

4. Locate the Update Certificate section in the SERVER CERTIFICATES section.

```
<table>
<thead>
<tr>
<th>Update Certificate:</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Server Certificate: Choose File No file chosen</td>
</tr>
<tr>
<td>* Server Key: Choose File No file chosen</td>
</tr>
<tr>
<td>Intermediate Certificate: Choose File No file chosen</td>
</tr>
<tr>
<td>Custom Root CA Certificate: Choose File No file chosen</td>
</tr>
</tbody>
</table>

* - Required
```

5. Provide your Server Certificate.
   a. Click Choose File.
      The upload window appears.
   b. Browse to and select the file.
      Tenable Core loads the file.

6. Provide your Server Key.
   a. Click Choose File.
      The upload window appears.
   b. Browse to and select the file.
      Tenable Core loads the file.

7. (Optional) If your custom server certificate is signed by a custom CA that requires an intermediate certificate to validate the custom server certificate, provide your Intermediate Certificate.
a. Click Choose File.
   The upload window appears.

b. Browse to and select the file.
   Tenable Core loads the file.

8. (Optional) If your custom server certificate is signed by a custom CA, upload your **Custom Root CA Certificate**.
   a. Click Choose File.
      The upload window appears.
   b. Browse to and select the file.
      Tenable Core loads the file.

9. Click **Install Server Certificates**.
   Tenable Core uploads the files. A success message appears to confirm the upload succeeded.

10. In the left navigation pane, click **Services**.
    The **Services** page appears.

11. Restart the **Cockpit** service, as described in **Manage Services**.
    The **Cockpit** service restarts and enables the new certificate.

---

### Remove a Custom Server Certificate

If you no longer want to use your custom server certificate for Tenable Core, you can remove the certificate and revert to using a Tenable-provided server certificate. For more information, see **Manage the Server Certificate**.

To remove a custom server certificate and revert to the Tenable-provided default certificate:

1. Log in to Tenable Core via the user interface, as described in **Log In to Tenable Core**.
   The Tenable Core web user interface page appears.
2. In the left navigation pane, click **SSL/TLS Certificates**.

   The **SSL/TLS Certificates** page appears.

3. Click the **System Certificate** tab.

4. In the **SERVER CERTIFICATES** section, in the **Update Certificate** section, click **Reset Server Certificates**.

   A confirmation window appears.

5. Click **Reset**.

   A success message appears to confirm the reset succeeded.

### Upload a Certificate for a Trusted Certificate Authority

You can upload a trusted certificate authority (CA) certificate for any of the following purposes:

- You want to use certificate authentication for user accounts on Tenable Sensor Proxy.

You do not need to upload a trusted CA certificate for any other reasons. You can upload any number of trusted CA certificates to Tenable Core.

**Note:** By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable Sensor Proxy. To decouple the certificates used for your Tenable Core system and your application, see [Use Different Certificates for Tenable Core and Your Application](#).

If you decouple the certificates, Tenable Core disregards the custom CA certificate configuration on the **System Certificate** tab. Tenable Core does not use custom CA certificates for reasons other than the application use.

To view details about an existing certificate, click to expand the **Filename** section for a certificate. To remove an existing certificate, select the certificate and click the **Delete** button.

**Before you begin:**

- Confirm the trusted CA certificate is in `.der`, `.pem`, or `.crt` format.

- Move the trusted CA certificate to a location accessible from your Tenable Core server.

Upload a trusted CA certificate:
1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

   The Tenable Core web user interface page appears.

2. In the left navigation pane, click SSL/TLS Certificates.

   The SSL/TLS Certificates page appears.

3. Click the System Certificate tab.

4. In the TRUSTED CERTIFICATE AUTHORITIES section, in the Add Certificate Authority section, next to Certificate, click Choose File.

   The upload window appears.

5. Browse to and select the certificate file.

   Tenable Core uploads the certificate file.

6. Click Install Certificate Authority.

   A success message appears to confirm the upload succeeded.

**Use Different Certificates for Tenable Core and Your Application**

By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable Sensor Proxy. If needed, you can decouple your system and application certificates and customize them independently.
Before you begin:

- Upload a custom server certificate for Tenable Core, as described in [Upload a Custom Server Certificate](#).

To decouple and customize your application certificates:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
The Tenable Core web user interface page appears.

2. In the left navigation pane, click **SSL/TLS Certificates**.
   
The **SSL/TLS Certificates** page appears.

3. Click the application tab.
   
The application tab appears.

   
The application tab refreshes to display the settings in edit mode.

5. Remain on the application tab and configure the settings for your application-specific server certificate, as described in [Upload a Custom Server Certificate](#).

6. Remain on the application tab and configure the settings for one or more custom certificate authority (CA) certificate, as described in [Upload a Certificate for a Trusted Certificate Authority](#).

   **Note:** If you upload a custom CA certificate on the application tab, Tenable Core disregards the custom CA certificate configuration on the **System Certificate** tab. Tenable Core does not use custom CA certificates for reasons other than the application use described in [Upload a Certificate for a Trusted Certificate Authority](#).

Manage Services

You can use the **Services** page to view information about targets, system services, sockets, timers, and paths.

To manage Tenable Core services:
1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **Services**.

   The **Services** page appears.

You can:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Targets</strong></td>
<td>1. Click <strong>Stop, Start, Restart</strong>, or <strong>Reload</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Restarting a service completely stops and restarts the service. Reloading a service only reloads the service’s configuration files.</td>
</tr>
<tr>
<td></td>
<td>The system changes the status of the service.</td>
</tr>
<tr>
<td><strong>System Services</strong></td>
<td>• View a list of system services.</td>
</tr>
<tr>
<td></td>
<td>• Click a row to view detailed information about a service.</td>
</tr>
<tr>
<td></td>
<td>• To change the status of a service:</td>
</tr>
<tr>
<td></td>
<td>1. Click a row.</td>
</tr>
<tr>
<td></td>
<td>The service details page appears.</td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Stop, Start, Restart</strong>, or <strong>Reload</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Restarting a service completely stops and restarts the service. Reloading a service only reloads the service’s configuration files.</td>
</tr>
<tr>
<td></td>
<td>The system changes the status of the service.</td>
</tr>
<tr>
<td><strong>Sockets</strong></td>
<td>• View a list of socket services.</td>
</tr>
<tr>
<td></td>
<td>• Click a row to view detailed information about a service.</td>
</tr>
<tr>
<td></td>
<td>• To change the status of a service:</td>
</tr>
<tr>
<td></td>
<td>1. Click a row.</td>
</tr>
<tr>
<td>Timers</td>
<td>Paths</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| - View a list of timer services.  
- Click a row to view detailed information about a service.  
- Create a new timer, as described in Create a Timer.  
- To change the status of a service:  
  1. Click a row.  
  
  The service details page appears.  
  2. Click **Stop, Start, Restart, or Reload**.  
  
  **Note:** Restarting a service completely stops and restarts the service. Reloading a service only reloads the service’s configuration files.  
  
  The system changes the status of the service. | - View a list of path services.  
- Click a row to view detailed information about a service.  
- To change the status of a service:  
  1. Click a row.  
  
  The service details page appears.  
  2. Click **Stop, Start, Restart, or Reload**.  
  
  **Note:** Restarting a service completely stops and restarts the service. Reloading a service only reloads the service’s configuration files.  
  
  The system changes the status of the service. |
Create a Timer

To create a timer:

1. In the left navigation pane, click the Services option. The Services page displays.

2. In the Services page heading, click the Create Timers button.
   
   A new window appears.

3. Enter the Service Name, Description, Command, and Run information.

4. Click Save.

   The new timer displays in the enabled section of the list.

Manage System Networking

You can use the Networking page to view real-time system network traffic information, interface connection options, and logs.

To manage Tenable Core system networking:
1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.

The Tenable Core web user interface page appears.

2. In the left navigation bar, click Networking.

The Networking page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Graphs</strong></td>
<td>• View a graph of the Sending (outbound) network traffic on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Receiving (inbound) network traffic on your instance.</td>
</tr>
<tr>
<td><strong>Firewall</strong></td>
<td>• View Firewall rules.</td>
</tr>
<tr>
<td><strong>section</strong></td>
<td>• Add Zones.</td>
</tr>
<tr>
<td></td>
<td>• Add Allowed Services.</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td>• Aggregate multiple network interfaces into a single-bonded interface, as described in Add a Bonded Interface.</td>
</tr>
<tr>
<td><strong>table</strong></td>
<td>• Add a team of interfaces, as described in Add a Team of Interfaces.</td>
</tr>
<tr>
<td></td>
<td>• Add a bridge to create a single aggregate network from multiple communication networks, as described in Add a Bridge Network.</td>
</tr>
<tr>
<td></td>
<td>• Add a VLAN, as described in Add a VLAN.</td>
</tr>
<tr>
<td><strong>Networking</strong></td>
<td>View a log of activity for the system network.</td>
</tr>
<tr>
<td><strong>Logs</strong> table</td>
<td>View a log of activity for the system network.</td>
</tr>
</tbody>
</table>

**Note:** You can only create a new interface by plugging one in, or by adding one to the virtual machine according to the instructions provided by your virtualization tools. This is not provided by Tenable Core.

Add a Bonded Interface
You can add a bond to aggregate multiple network interfaces into a single-bonded interface.

To add a bonded interface to Tenable Core:

1. In the left navigation pane, click the **Networking** option. The **Networking** page displays.

2. In the **Interfaces** heading, click the **Add Bond** button on the **Interfaces** section. A new window appears.

3. Enter a **Name** for the bond.

4. Select the members (interfaces) to bond to in the **Members** section.

5. Select an option for **MAC**.

6. Select the **Mode**.

7. Select a **Primary**.

8. Select the type of **Link Monitoring**. Labeled in the drop-down list is the recommended type.
9. Enter the **Monitoring Intervals** with options to link up or down delay increments.

### Bond Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>bond0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Members</td>
<td></td>
</tr>
<tr>
<td>ens160</td>
<td></td>
</tr>
<tr>
<td>ens32</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td></td>
</tr>
<tr>
<td>Mode</td>
<td>Active Backup</td>
</tr>
<tr>
<td>Primary</td>
<td></td>
</tr>
<tr>
<td>Link Monitoring</td>
<td>MIL (Recommended)</td>
</tr>
<tr>
<td>Monitoring Interval</td>
<td>100</td>
</tr>
<tr>
<td>Link up delay</td>
<td>0</td>
</tr>
<tr>
<td>Link down delay</td>
<td>0</td>
</tr>
</tbody>
</table>

### Add a Team of Interfaces

**To add a team of interfaces to Tenable Core:**

1. In the left navigation pane, click the **Networking** option. The Networking page displays.
2. In the **Interfaces** heading, click the **Add Team** button on the Interfaces section. A new window appears.
3. Enter the **Team Name**.
4. Select the **Ports** needed for the new team.
5. Select the **Runner** and **Link Watch** from the drop-down list.
6. Enter the **Link up** and **Link down delay** increments.

![Team Settings](image)

**Add a Bridge Network**

You can add a bridge to create a single aggregate network from multiple communication networks.

**To add a bridge network to Tenable Core:**

1. In the left navigation pane, click the **Networking** option. The **Networking** page displays.

2. In the **Interfaces** heading, click the **Add Bridge** button on the **Interfaces** section. A new window appears.

3. Enter a **Name** for the bridge.

4. Select the **Ports** that you want to connect to the bridge.

5. Click the box next to **Spanning Tree Protocol (STP)** to get more STP options.
6. Click **Apply** to add the new bridge.

![Bridge Settings](image)

**Add a VLAN**

To add a VLAN to Tenable Core:

1. Click the **Add VLAN** button on the Interfaces section. A new window appears.
2. Select the **Parent** from the drop-down list.
3. Enter the **VLAN Id** and name.
4. Click **Apply** to add the **VLAN**.
5. The new **VLAN** displays in the **Interface** list.

![VLAN Settings](image)

**Manage User Accounts**

You can use the **Accounts** page to manage user accounts for your Tenable Core instance.

To manage Tenable Core user accounts:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation bar, click **Accounts**.
   
   The **Accounts** page appears.

   Do any of the following:

   - Create a new user account, as described in [Create New User Account](#).
   - Edit a user account, as described in [Edit a User Account](#).
   - Delete a user account, as described in [Delete a User Account](#).

**Create New User Account**

**Required User Role:** Administrator

You can create a new user account from the **Accounts** page.

To create a new user account:
1. Log in to Tenable Core, as described in Log In to Tenable Core.

2. In the left navigation bar, click Accounts.

   The Accounts page appears.

3. Click Create New Account.

   The Create New Account window appears.

4. In the Full Name box, type the user's full name.

5. In the User Name box, type a username for the user account.

6. In the Password box, type a password for the user account.

   **Note:** Your password must meet the following minimum requirements:
   - Minimum 14 characters long
   - Cannot be a palindrome (i.e., a word or phrased spelled the same backward and forward)

7. In the Confirm box, retype the password.

8. Click Create.

   Tenable Core creates the new account and displays it on the Accounts page.

What to do next:
- (Optional) If you want to configure the user account, see Edit a User Account.
- (Optional) If you want to delete the user account, see Delete a User Account.

**Edit a User Account**

**Required User Role:** Administrator

You can edit a user account configuration, including the user's full name, password, roles, access, and public SSH keys.

Before you begin:

To edit a user account:
1. Log in to Tenable Core, as described in Log In to Tenable Core.

2. In the left navigation bar, click Accounts.

   The Accounts page appears.

3. Click the user account you want to edit.

   The account page for the user account appears.

4. On the user account page, you can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Name</td>
<td>Type a name for the user account.</td>
</tr>
</tbody>
</table>
| Roles | • To grant the user account administrator access, select the Server Administrator check box.  
• To remove administrator access from the user account, clear the Server Administrator check box. |
| Access | • To lock the user account, select the Lock Account check box to lock the user account.  
• To unlock the user account, clear the Lock Account check box to unlock the user account.  
• To configure the account to remain unlocked indefinitely:  

   Note: If you do not configure the account to remain unlocked indefinitely, Tenable Core automatically locks the account on the set expiration date.  

   1. Click Never lock account.  
      
      The Account Expiration window appears.  

   2. Select the Never lock account option.  

   3. Click Change.  

   Tenable Core sets the account to remain unlocked |
• Select an expiration date for the account:

1. Click **Never lock account**.

   The **Account Expiration** window appears.

2. Select the **Lock account on** option.

3. Click the box next to the **Lock account on** option.

   A calendar drop-down box appears.

4. In the calendar drop-down box, select the date when you want the account to age out.

5. Click **Change**.

   Tenable Core sets the expiration date for the user account.

### Password

• To set a new user account password:

1. Click **Set Password**.

   The **Set Password** window appears.

2. In the **New Password** box, type the password you want to use for the account.

   **Note**: Your password must meet the following minimum requirements:
   - Minimum 14 characters long
   - Cannot be a palindrome (i.e., a word or phrased spelled the same backward and forward)

3. Click **Set**.

   Tenable Core updates the user account password.

• To force a user to change their user account password:
1. Click **Force Change**.
   
   The **Force password change** window appears.

2. Click **Reset**.
   
   Tenable Core disables the password for the user account. The user must change the password on the next login attempt.

- Configure the user account password to remain active indefinitely:

  **Note**: If you do not configure the password to remain active indefinitely, Tenable Core automatically ages out the password on the set expiration date.

  1. Click **Never expire password**.
     
     The **Password Expiration** window appears.

  2. Select the **Never expire password** option.

  3. Click **Change**.
     
     Tenable Core sets the password to remain active indefinitely.

- Select an expiration date for the user account password:

  1. Click **Never expire password**.
     
     The **Password Expiration** window appears.

  2. Select the **Require password change every [blank] days** option.

  3. In the **Require password change every [blank] days** section, type the number of days that you want to pass between password expiration dates (for example, type 90 if you want the password to age out every 90 days).
4. Click **Change**.

   Tenable Core sets the expiration date for the user account password.

### Authorized Public SSH Keys

- To add a public SSH key to the user account:
  1. In the **Authorized Public SSH Keys** table, click the + icon.
     
     The **Add public key** window appears.
  2. In the text box, type or paste your public SSH key.
  3. Click **Add key**.
     
     Tenable Core adds the SSH key to the user account.

- To remove a public SSH key:
  1. In the **Authorized Public SSH Keys** table, next to the key you want to remove, click the - icon.
     
     Tenable Core removes the SSH key from your account.

## Delete a User Account

**Required User Role:** Administrator

You can delete a user account from the **Accounts** page.

To delete a new user account:

1. Log in to Tenable Core in a browser, as described in [Log In to Tenable Core](#).

2. In the left navigation bar, click **Accounts**.

   The **Accounts** page appears.

3. Click the user account you want to delete.

   The account page for the user account appears.

4. In the upper-right corner, click **Delete**.
The delete window for the user account appears.

5. (Optional), if you want to delete files attached to the user account, select the **Delete Files** check box.

   **Note:** This file deletion is permanent. If you do not delete them, the files remain attached to the Tenable Core instance, along with their existing access permissions. Users who were previously granted access can still access the files.

6. Click **Delete**.
   Tenable Core delete the user account.

### Change Performance Profile

To change the performance profile for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   The Tenable Core web user interface page appears.

2. In the left navigation pane, click the **Overview** option.
   The **Overview** page displays.

3. Click on the **edit** link next to the **Performance profile** option in the **Configuration** tile. A new window appears displaying **Performance Profile** options.

4. Select the desired **Performance Profile**. The recommended profile is labeled in the list.
5. Click **Change Profile** to confirm the new selection.

![Change Performance Profile](image)

### Restart Tenable Core

**To restart your Tenable Core instance:**

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The Tenable Core web user interface page appears.

2. In the left navigation pane, click the **System** option.
   
   The **System** page displays.

3. Click the **Restart** button or select it from the drop-down box.
   
   A new window appears.

4. Enter a message for the users in the text box.

5. Select the delay time from the drop-down menu. This is the time that the restart begins.
   
   Choose from one of the minute increments or enter a specific time. There is also an option to restart immediately with no delay.
6. Click the **Restart** button to initiate and save the updated information.

![Restart](image)

**Shut Down Tenable Core**

To shut down your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The Tenable Core web user interface page appears.

2. In the left navigation pane, click the **System** option.

   The **System** page displays.

3. Next to the **Power Options** item, click the arrow by **Restart** to display the drop-down menu. Select **Shut Down**.

   A new window appears.

4. Enter a message for the users in the text box.

5. Select the delay time from the drop-down menu. This is the time that the shutdown begins. Choose from one of the minute increments or enter a specific time. There is also an option to **Shut Down** immediately with no delay.
6. Click **Shut Down** to initiate and save the updated information.

![Shut Down](image)

**Edit Your Tenable Core Hostname**

To edit the hostname for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
The Tenable Core web user interface page appears.

2. In the left navigation pane, click the **Overview** option.
   
The **Overview** page displays.

3. Click the **edit** link next to the **Hostname** option in the **Configuration** tile.
   
   A new window appears with the options to enter or edit the **Pretty Host Name** and **Real Host Name**.

4. Enter the **Pretty Host Name** for the machine.
   
The **Real Host Name** updates as you enter the **Pretty Host Name**.

5. Click **Change** to update the name.
The new name displays next to the **Hostname** option.

<table>
<thead>
<tr>
<th>Change Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pretty Host Name</strong></td>
</tr>
<tr>
<td><strong>Real Host Name</strong></td>
</tr>
</tbody>
</table>

---

**Edit Your Time Settings**

To edit the system time and time zone settings for your Tenable Core instance:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).

   The Tenable Core web user interface page appears.

2. In the left navigation pane, click the **Overview** option.

   The **Overview** page displays.

3. Next to **System time**, click the link.

   The **Change System Time** window appears.

4. In the **Time Zone** drop-down box, select your time zone.

   **Tip:** Type the first few letters of the desired time zone to filter the list.

5. In the **Set Time** drop-down box, select your preferred method for time synchronization.

   **Tip:** By default, Tenable Core is set to **Automatically using NTP**.

6. Click **Change**.

   Tenable Core saves the change.
FAQ

When are Tenable Core offline update ISOs released?

Tenable Core releases offline updates throughout the year on a quarterly basis, within three weeks after the end of a quarter.

Can I skip offline updates?

Tenable recommends that you apply updates in order. Tenable does not test, or support, skipping updates. If you have an old version of Tenable Core, it is best to back up the data and restore it on a newer version of Tenable Core.

Does Tenable provide old Tenable Core ISOs?

The downloads page has the current ISO and images from the last four quarters. Tenable does not provide any ISOs older than what is available on the downloads page. If you are looking for an older ISO to downgrade one of the products, you can follow the Tenable Core documentation.

How can I find out what updates are in an offline Tenable Core ISO?

The release notes for offline ISOs have a section for package updates that are present in the ISO.

How long does it take for a Tenable software update to be available in Tenable Core?

Tenable Core holds a new version of Tenable Nessus until the general availability (GA) date in Tenable Vulnerability Management. This is usually a week after the stand-alone Tenable Nessus GA. Releases for other products on Tenable Core usually occur within 24 hours of the GA date. To see which versions of the products are currently available on each operating system version of Tenable Core, see the Versions page.

How can I disable or reenable automatic updates?

Automatic update configuration is in Tenable Core documentation.

Can I use a local repository for software updates?
Tenable Core does not support this feature. Tenable encourages you to submit a feature request.

**How long will Tenable Core support RHEL/CentOS 7?**

Tenable Core bases off of CentOS 7 and support ends when RHEL 7 support officially ends.

**Why is Tenable Security Center down every morning?**

Tenable Core shuts down Tenable Security Center if you have automatic updates enabled while detecting an updated version. If the update fails for any reason, or stalls because a service is not stopping, Tenable Security Center remains down pending user intervention. Automatic backups can also shut down Tenable Security Center, and if a problem occurs, it may not properly restart.

**Does Tenable support X software that I installed on my Tenable Core instance?**

You can install any software you wish on Tenable Core instances. Tenable does not support the additional software, but fully supports Tenable Core and the installed product in that situation. Tenable reserves the right to require that you remove the additional software if it is impacting an issue you are having, and requesting support for.

**Do any services need to be enabled to allow access to cockpit (https://ip.address:8000)?**

No. Cockpit is enabled by default and services start automatically on boot. Any messages regarding cockpit on system boot can be disregarded.

**How do I reset my administrator password in Tenable Core?**

The process to reset your password is in this Tenable Community Knowledge Article.

**How can I connect to port 8090 during the Tenable Core backup/restore process?**
If you did not confirm access to port 8090, during the process Tenable Core provides a link to click which opens that connection-check URL in a new tab so you can accept the certificate for that port and have the restoration process try again. See Backup/Restore.