Table of Contents

Welcome to Tenable Core + Tenable.ot ................................................................. 5
Get Started ........................................................................................................... 6
Tenable Core Requirements .................................................................................. 7
System and License Requirements ...................................................................... 8
Tenable.ot System Requirements .......................................................................... 9
Access Requirements .......................................................................................... 12
Default Security Configuration Standards ........................................................ 14
Deploy or Install Tenable Core ............................................................................. 19
Deploy Tenable Core in VMware ......................................................................... 20
Install Tenable Core on Tenable-Provided Hardware .......................................... 21
Edit the Network Configuration ......................................................................... 23
Edit the Proxy Configuration .............................................................................. 25
Disk Management ............................................................................................... 27
Add or Expand Disk Space .................................................................................. 28
Manually Configure a Static IP Address .............................................................. 30
Create an Initial Administrator User Account ..................................................... 34
Log In to Tenable Core ....................................................................................... 36
Configure Tenable.ot in the Tenable.ot User Interface ....................................... 37
Configure and Manage ......................................................................................... 38
View the Dashboard ............................................................................................ 40
Add a Server ........................................................................................................ 41
Edit a Server ........................................................................................................ 42
Delete a Server .......................................................... 43
Synchronize Accounts .................................................. 44
Manage the System ...................................................... 45
Change Performance Profile ........................................... 47
Restart Tenable Core .................................................... 48
Shut Down Tenable Core ............................................... 49
Edit Your Tenable Core Hostname .................................... 50
Edit Your Time Settings ............................................... 51
View the System Log .................................................... 52
Filter the System Log ................................................... 53
Generate a Diagnostic Report .......................................... 54
View Container Status .................................................. 55
View Tenable.ot Logs .................................................. 56
Manage System Networking ........................................... 57
Add a Bonded Interface ............................................... 59
Add a Team of Interfaces .............................................. 61
Add a Bridge Network .................................................. 62
Add a VLAN .............................................................. 63
Manage System Storage ............................................... 64
Rename a Filesystem .................................................... 65
Delete a Filesystem ..................................................... 66
Manage User Accounts ................................................ 67
Create New User Account ............................................. 68
Edit a User Account .................................................... 69
Welcome to Tenable Core + Tenable.ot

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

To get started quickly with Tenable Core + Tenable.ot, see Get Started.

Features

- Secure, stable platform.
- Provides automatic application installation and updates via Tenable public repositories.
- Built on CentOS 7.
- Targets Center for Internet Security (CIS) standards for RedHat 7 with SELinux enabled. For more information, see Default Security Configuration Standards.
- Root access enabled on 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.sc
- Tenable Core + Tenable.io Web Application 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 (for example, Tenable.sc and Tenable.ot), deploy a unique instance for each application.
Get Started

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

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.ot.

3. (Optional) If you want to increase your disk space to accommodate your organization's data storage needs, see Disk Management and the Tenable.ot User Guide.

4. (Optional) If 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.ot deployment.

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

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

7. In the left navigation bar, click Tenable.ot.

   The Tenable.ot page appears.

8. When prompted, click Install Tenable.ot and allow up to an hour for installation.

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

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

11. Configure Tenable.ot in the Tenable.ot User Interface to meet the specifications you want for your application.

12. Configure and manage Tenable Core. To access the application interface, see Configure and Manage.
Tenable Core Requirements

You can deploy Tenable Core + Tenable.ot on any system that meets the following Tenable Core and Tenable.ot 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 (for example, Tenable.sc and Tenable.ot), 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.ot, your application and system must meet the following requirements.

<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>.ova file</td>
<td>Deploy Tenable Core in VMware</td>
</tr>
<tr>
<td>Tenable-provided hardware</td>
<td>.iso image</td>
<td>Install Tenable Core on Tenable-Provided Hardware</td>
</tr>
</tbody>
</table>

**Note:** Tenable Support does not assist with issues related to your CentOS 7 operating system, even if you encounter them during installation or deployment.

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

Tenable.ot 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 (for example, Tenable.sc and Tenable.ot), deploy a unique instance for each application.

Tenable Core + Tenable.ot ships with the latest version of Tenable.ot included.

**Note:** To update your Tenable.ot application version, contact Tenable Support. You cannot use the Tenable Core interface to update Tenable.ot.

For more information about requirements specifically for Tenable.ot, see [Tenable.ot](#) in the [General Requirements Guide](#).
Tenable.ot System Requirements

You can Install Tenable.ot on a hypervisor\(^1\) or directly on user-supplied hardware running Tenable Core.

**Note:** Tenable strongly discourages running Tenable Core + Tenable.ot in an environment shared with other Tenable applications. (For example, installing two products on the same virtual machine, or in the same Tenable Core system.)

Storage Requirements

Tenable recommends installing Tenable.ot on direct-attached storage (DAS) devices, preferably solid-state drives (SSD), for best performance. Tenable strongly encourages the use of solid state storage (SSS) that have a high drive-writes-per-day (DWPD) rating to ensure longevity.

Tenable does not support installing Tenable.ot on network-attached storage (NAS) devices. Storage area networks (SAN) with a storage latency of 10 milliseconds or less, or Tenable hardware appliances, are a good alternative in such cases.

Disk Space Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for deployments include raw network speed, the size of the network being monitored, and the configuration of the application. Processors, memory, and network card selection are heavily based on these deployment configurations. Disk space requirements vary depending on usage based on the amount and length of time data is stored on the system.

**Note:** Tenable.ot needs to be able to perform full packet captures of monitored traffic\(^2\), and the size of the policy event data stored by Tenable.ot depends on the number of devices and the type of environment.

ICP System Requirement Guidelines (Virtual or Tenable Core)

<table>
<thead>
<tr>
<th>Site Size</th>
<th>Maximum</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage Requirements</th>
<th>Network</th>
</tr>
</thead>
</table>

\(^1\)Hypervisor must be officially supported by VMWare and known to work under Hyper-V, KVM.

\(^2\)Multiply rate (Mbits/sec) \(*\ 2.7\) to get storage (GB/day) - based on a compression factor of 0.25.
## SPAN/TAP

<table>
<thead>
<tr>
<th>SPAN/TAP Throughput (Mbps)</th>
<th>Cores¹</th>
<th>(DDR4)</th>
<th>ments</th>
<th>Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>4 x 2 GHz</td>
<td>12 GB RAM</td>
<td>128 GB</td>
<td>Minimum 4 x 1 Gbps</td>
</tr>
<tr>
<td>Medium</td>
<td>8 x 2 GHz</td>
<td>16 GB RAM</td>
<td>512 GB</td>
<td>Minimum 4 x 1 Gbps</td>
</tr>
<tr>
<td>Large</td>
<td>16 x 2 GHz</td>
<td>32 GB RAM</td>
<td>1 TB</td>
<td>Minimum 4 x 1 Gbps</td>
</tr>
<tr>
<td>XL</td>
<td>32 x 3 GHz</td>
<td>64 GB RAM or more</td>
<td>2 TB or more</td>
<td>Minimum 4 x 1 Gbps</td>
</tr>
</tbody>
</table>

### Disk Partition Requirements

Tenable.ot uses the following mounted partitions:

<table>
<thead>
<tr>
<th>Partition</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>operating system</td>
</tr>
<tr>
<td>/opt</td>
<td>application and database files</td>
</tr>
<tr>
<td>/var/pcap</td>
<td>packet captures (full packet capture, event, query)</td>
</tr>
</tbody>
</table>

The standard install process places these partitions on the same disk. Tenable recommends moving these to partitions on separate disks to increase throughput. Tenable.ot is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance. Tenable recommends using an SSD with high DWPD ratings on customer-supplied hardware installations when using the packet capture feature in Tenable.ot.

**Tip:** Deploying Tenable.ot on a hardware platform configured with a redundant array of independent disks (RAID 0) can dramatically boost performance.
Tip: Tenable does not require RAID disks for even our largest customers. However, in one instance, response times for queries with a faster RAID disk for a customer with more than one million managed vulnerabilities moved from a few seconds to less than a second.

Network Interface Requirements

You must have four network interfaces present on your device before installing Tenable.ot. Tenable recommends the use of gigabit interfaces. The VMWare OVA creates these interfaces automatically. Create these interfaces manually when you are installing the ISO on your own hardware.

Note: Tenable does not provide SR-IOV support for the use of 10 G network cards and does not guarantee 10 G speeds with the use of 10 G network cards.

NIC Requirements

nic0 (192.0.2.5) and nic3 (192.168.3.3) have static IP addresses when you install Tenable Core + Tenable.ot in a hardware environment. Other network interface controllers (NICs) use DHCP.

nic3 (192.168.3.3) has a static IP address when you deploy Tenable Core + Tenable.ot on VMware. Other NICs use DHCP. Confirm that the Tenable Core nic1 MAC address matches the NIC MAC address in your VMware passive scanning configuration. Modify your VMware configuration to match your Tenable Core MAC address if necessary.

For more information, see Manually Configure a Static IP Address, Manage System Networking, and the VMware Documentation.

¹CPU Cores reference PHYSICAL cores, assumes server-class CPU (Xeon, Opteron).
Access Requirements

Your Tenable Core + Tenable.ot deployment must meet the following requirements.

- Internet Requirements
- Port Requirements

Internet Requirements

You must have internet access to download Tenable Core files.

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

<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>Hardware</td>
<td>.iso image</td>
<td>Requires internet access to install or update Tenable Core.</td>
</tr>
</tbody>
</table>

**Tip:** You do not need access to the internet when you install updates to Tenable Core + Tenable.ot 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. Tenable.ot also requires application-specific port access. For more information, see the *Tenable.ot Documentation*.

Inbound Traffic

Allow inbound traffic to the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TCP 22 | Inbound SSH connections.
---|---
TCP 443 | Inbound communications to the Tenable.ot interface.
TCP 8000 | Inbound HTTPS communications to the Tenable Core interface.

### Outbound Traffic

Allow outbound traffic to the following ports:

<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 server for system updates.</td>
</tr>
<tr>
<td>UDP 53</td>
<td>Outbound DNS communications for Tenable.ot 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'
  - 3.2.5 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 - lcredit
  - 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_faillock.so authfail audit deny=5 unlock_time=900'
  - 5.3.2 Lockout for failed password attempts - password-auth 'auth [success=1 default=t=bad] pam_unix.so'
  - 5.3.2 Lockout for failed password attempts - password-auth 'auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900'
  - 5.3.2 Lockout for failed password attempts - password-auth 'auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900'
  - 5.3.2 Lockout for failed password attempts - system-auth 'auth [default=die] pam_faillock.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_faillock.so preauth audit silent deny=5 unlock_time=900'
  - 5.3.2 Lockout for failed password attempts - system-auth 'auth sufficient pam_faillock.so authsucc audit 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.ot in the following environments.

<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>.ova file</td>
<td><a href="#">Deploy Tenable Core in VMware</a></td>
</tr>
<tr>
<td>Tenable-provided hardware</td>
<td>.iso image</td>
<td><a href="#">Install Tenable Core on Tenable-Provided Hardware</a></td>
</tr>
</tbody>
</table>

**Note:** Tenable Support does not assist with issues related to your CentOS 7 operating system, even if you encounter them during installation or deployment.

**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.ot as a VMware virtual machine, you must download the Tenable Core + Tenable.ot .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 System and License Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.

To deploy Tenable Core + Tenable.ot as a VMware virtual machine:

1. Download the Tenable Core + Tenable.ot .ova file.
2. Open your VMware virtual machine in the hypervisor.
3. Import the Tenable Core + Tenable.ot VMware .ova file from your computer to your virtual machine. For information about how to import a .ova file to your virtual machine, see VMware documentation.
4. In the setup prompt, configure the virtual machine to meet your organization's storage needs and requirements, and those described in System and License Requirements.
5. Launch your Tenable Core + Tenable.ot instance.

The virtual machine boot process appears in a terminal window.

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

What to do next:

- Continue getting started with Tenable Core + Tenable.ot, as described in Get Started.
Install Tenable Core on Tenable-Provided Hardware

You can install Tenable Core + Tenable.ot 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.

**Note:** Tenable Core + Tenable.ot requires Tenable-provided hardware. For more information, contact your Tenable representative.

Before you begin:

- Confirm your environment will support your intended use of the instance, as described in System and License Requirements.
- Confirm your internet and port access will support your intended use of the instance, as described in Access Requirements.
- Confirm that Tenable Core + Tenable.ot was not preinstalled on your hardware for any new instance of Tenable Core + Tenable.ot. Not all new instances require manual installation.

To install Tenable Core + Tenable.ot on hardware:

1. Download the Tenable Core + Tenable.ot .iso image.
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.

**Tip:** To monitor the progress of the installation, select Install TenableCore using serial console from the boot menu. For more information about the Tenable.ot serial console, see the Tenable.ot User Guide.

The installer installs Tenable Core + Tenable.ot on your hardware.

The installation begins if there are no configuration errors.

The **Installation** menu appears if there are configuration errors.

If you need to resolve configuration errors with your **Installation source** and/or **Software selection** settings, either Edit the Network Configuration or Edit the Proxy Configuration.
**Caution:** Do not enter any other menus or modify any other settings.

The installation runs and the server restarts.

What to do next:

- Continue getting started with Tenable Core + Tenable.ot, as described in [Get Started](#).
Edit the Network Configuration

During installation, you may need to edit the network configuration settings. Perform this procedure to resolve errors [!] with your 4) Installation source and/or 5) Software selection settings.

Caution: Do not enter any other menus or modify any other settings.

To edit the network configuration:

1. From the Installation menu, press the 8 key.
2. Press the Enter key.
   The Network Configuration menu appears.
3. Press the 2 key.
4. Press the Enter key.
   The Device Configuration menu appears.
5. Review the 1) IPv4 address or "dhcp" for DHCP, 2) IPv4 netmask, 3) IPv4 gateway, and 6) Nameservers settings and, if necessary, edit them.
   For example, you must edit these settings if you are installing Tenable Core on a static network without DHCP.
6. Check 8) Apply configuration in installer.
7. Press the c key until you return to the Installation menu.
8. Press the r key to refresh the menu.
9. Confirm that settings 1-7 show an [x]. If the settings all show an [x] proceed to step 11.
10. If 4) Installation source still shows a [!]:
    Refresh the repository URL:
    a. Press the 4 key.
    b. Press the Enter key.
    The Installation Source menu appears.
c. Press the 3 key.

d. Press the Enter key.

   The Installation Source submenu appears.

e. Press the 2 key.

f. Press the Enter key.

   The Specify Repo Options menu appears.

g. Press the c key.

h. Press the Enter key.

   The system refreshes the repository URL and the Installation menu appears.

11. Press the r key to refresh the menu.

12. Press the c key until you return to the Installation menu.
**Edit the Proxy Configuration**

During installation, you may need to edit the proxy configuration settings to identify the proxy you want to use for internet access.

**Caution:** Do not enter any other menus or modify any other settings.

To edit the proxy configuration:

1. From the **Installation** menu, press the 3 key.
2. Press the **Enter** key.
   
   The **Proxy Configuration** menu appears.
3. Type the proxy you want to use. For example, `https://username:password@192.0.2.221:3128`.
   
   **Note:** If your password includes a special character, the special character must be HTML URL encoded.
4. Press the **Enter** key.
5. If your proxy is a man-in-the-middle proxy that intercepts SSL traffic, a prompt appears.
   
   In the prompt:
   1. Type yes.
   2. Press the **Enter** key.

   The system temporarily disables SSL verification. The system automatically re-enables SSL verification after the installation completes.

   The **Installation** menu appears.
6. Press the 4 key.
7. Press the **Enter** key.
   
   The **Installation Source** menu appears.
8. Press the 3 key.
9. Press the **Enter** key.
The **Installation Source** submenu appears.

10. Press the **2** key.

11. Press the **Enter** key.

   The **Specify Repo Options** menu appears.

12. Press the **c** key.

13. Press the **r** key, then the **Enter** key.

14. If necessary, continue pressing the **r** key, then the **Enter** key until 4) **Installation source** no longer says **(Processing...)**.

   The system refreshes the repository URL.
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 general documentation for Linux.

Tenable Core Partitions

Tenable Core deploys with the following preconfigured partitions:

- /boot
- Swap
- /
- /var/log
- /var/pcap
- /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.

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 **Filesystems** section, locate the file system with `/opt` as the **Mount Point** and note the file system **Name** (for example, `/dev/vg0/00`).

   **Tip:** Typically, you want to add space to `/opt`. To add more storage space to a less common partition (for example, `/` or `/var/log`), locate the file system for that partition.

7. Click the row for the file system **Name** that includes your preferred partition as the **Mount Point**.
   
   The **Volume Group** page appears.
8. In the **Physical Volumes** section, click the `+` button.
   
   The **Add Disks** window appears.
9. Click the check box 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 **Logical Volumes** section, expand the section 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.
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 System and License Requirements.

Before you begin:

- Deploy or install Tenable Core + Tenable.ot, 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.ot 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.

9. Press **Enter**.

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.ot deployment, followed by a forward slash and your netmask.

    Example:

    ```
    192.0.2.57
    ```

13. In the **Gateway** field, type your gateway IP address.

    Example:

    ```
    192.0.2.177
    ```

14. In the **DNS servers** field, type your DNS server IP address.

    Example:

    ```
    192.0.2.176
    ```

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:
   
   ```
   192.0.2.8
   ```

18. Select the check the 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 1"
   ```

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

What to do next:
• Confirm that the Tenable Core nic1 MAC address matches the NIC MAC address in your VMware passive scanning configuration. If necessary, modify your VMware configuration to match your Tenable Core MAC address. For more information, see System and License Requirements.
Create an Initial Administrator User Account

The first time you access Tenable Core + Tenable.ot, 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.ot, 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.

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.
Log In to Tenable Core

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

Before you begin:

- Deploy Tenable Core + Tenable.ot, as described in Deploy or Install Tenable Core.

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. Select the Reuse my password for privileged tasks check box.

   **Note:** You cannot configure or manage your instance of Tenable Core + Tenable.ot if you do not select the Reuse my password for privileged tasks check box.

5. Click Log in.

   Tenable Core logs you in to the user interface.
Configure Tenable.ot in the Tenable.ot User Interface

After you deploy Tenable Core + Tenable.ot, you can access the Tenable.ot interface from the Tenable Core interface to configure Tenable.ot.

To access the Tenable.ot interface from the Tenable Core interface:

1. Log in to Tenable Core via the user interface, as described in Log In to Tenable Core.
   - The System page appears.
2. In the left navigation bar, click Tenable.ot.
   - The Tenable.ot page appears.
3. If prompted, provide your Tenable.ot instance password.
   - For more information, contact your Tenable representative.
4. In the Installation Info section, next to URLs, click the URL hyperlink.
   - The Tenable.ot interface appears.
5. Configure Tenable.ot, as described in the Tenable.ot User Guide.
Configure and Manage

You can use the Tenable Core user interface to configure and manage Tenable Core + Tenable.ot.

- View the Dashboard
- Add a Server
- Edit a Server
- Delete a Server
- Synchronize Accounts

Manage the System

- Change Performance Profile
- Restart Tenable Core
- Shut Down Tenable Core
- Edit Your Tenable Core Hostname
- Edit Your Time Settings

- View the System Log
- Filter the System Log
- Generate a Diagnostic Report

View Container Status

- View Tenable.ot Logs

Manage System Networking

- Add a Bonded Interface
- Add a Team of Interfaces
- Add a Bridge Network
- Add a VLAN

Manage System Storage
Rename a Filesystem
Delete a Filesystem
Manage User Accounts
   Create New User Account
   Edit a User Account
   Delete a User Account
Manage Services
   Create a Timer
Access the Terminal
Configure a Proxy Server
Start, Stop, or Restart Your Application
Manage Updates
   Configure Automatic Updates
   Update On Demand
   Update Tenable Core Offline
Manage Certificates
   Manage the Server Certificate
SNMP Agent Configuration
   Configure an SNMP Agent via the User Interface
   Configure an SNMP Agent via the CLI
Take a Virtual Machine Snapshot
View the Dashboard

You can use the **Dashboard** page to view usage statistics and manage your attached servers.

To view the Tenable Core dashboard:

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

2. Hover over the left navigation bar and click **Dashboard**.
   
   The **Dashboard** page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data graphs</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 a graph of the <strong>Network</strong> bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Disk I/O</strong> bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• To change the time range for data displayed in the graph:</td>
</tr>
<tr>
<td></td>
<td>1. In the top-right corner of the graph, click the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>2. Select a time range.</td>
</tr>
<tr>
<td></td>
<td>The system refreshes the graph.</td>
</tr>
<tr>
<td>Servers table</td>
<td>• Add a server, as described in <a href="#">Add a Server</a>.</td>
</tr>
<tr>
<td></td>
<td>• Edit a server, as described in <a href="#">Edit a Server</a>.</td>
</tr>
<tr>
<td></td>
<td>• Delete a server, as described in <a href="#">Delete a Server</a>.</td>
</tr>
<tr>
<td></td>
<td>• Synchronize user accounts, as described in <a href="#">Synchronize Accounts</a>.</td>
</tr>
<tr>
<td></td>
<td>• To view detailed information about a server, click a server row. For</td>
</tr>
<tr>
<td></td>
<td>more information, see <a href="#">System</a>.</td>
</tr>
</tbody>
</table>
Add a Server

To add a server:

**Note:** You can add as many servers to the Dashboard as you want.

1. Hover over the far-left navigation bar.
   The left navigation plane appears.
2. Click **Dashboard**.
   The **Dashboard** page appears.
3. Click the **+** icon.
   The **Add Machine to Dashboard** window appears.
4. In the **Address** field, type the IP address or hostname for the server you want to add.
5. In the **Color** field, click the color you want to represent the server.
6. Click **Add**.
   A confirmation window appears.

**Note:** If Tenable Core cannot establish authentication, the Unknown Host window appears. Contact your administrator to confirm your server’s name or IP address.

7. Click **Connect**.
   A credentials window appears.
8. Type your credentials in the **User name** and **Password** fields.

**Note:** To synchronize your accounts so that your account information and passwords are the same across multiple servers, click the **synchronize accounts and passwords** link. Refer to **Synchronize Accounts** for more information.

9. Click **Log In**.
   Tenable Core adds the server to your list of servers in the **Servers** table.

**Note:** If the server does not appear in the list right away, refresh the browser.
**Edit a Server**

To edit a server:

1. From the top bar in the **Servers** table, click the 📝 icon.
   
   A pencil icon (كتابة) and a trashcan icon (🗑️) appear next to each server name.

2. Click the ☑️ icon.

   The **Edit Server** window appears.

3. Do any of the following:

   - In the **Host Name** box, type the name you want for your server.
   - Update the server color:
     - In the **Color** box, click the color bar.
       
       A color menu appears.
     - Click the color you want to represent the server.
       
       The server color changes.

4. Click **Set**.

   Tenable Core updates your server information.
Delete a Server

To delete a server:

1. From the top bar in the Servers table, click the check mark icon.
   
   A pencil icon and a trashcan icon appear next to each server name.

2. Click the trashcan icon.
   
   The server disappears from the server list.
Synchronize Accounts

If you have multiple user accounts but do not want to manage credentials for each one, you can synchronize your accounts, which allows you to navigate seamlessly between accounts without providing a different username and password for each account.

**Note:** You can synchronize accounts while either adding or editing servers in the Dashboard.

To synchronize accounts:

1. While either adding or editing a server, click the **Synchronize users** link in the dialogue box. The **SYNCHRONIZE USERS** dialogue box appears with a list of your accounts.

   **Note:** If you are adding a server, the linked text in the dialogue box is **synchronize accounts and passwords**.

2. Check the boxes next the accounts you want to synchronize.

3. Click **Synchronize**.
Manage the System

You can use the System 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 System page appears.

You can:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>System details section</td>
<td>• View summary information about your Tenable Core instance.</td>
</tr>
<tr>
<td></td>
<td>• Change the performance profile for your instance, as described in Change Performance Profile.</td>
</tr>
<tr>
<td></td>
<td>• Restart or shut down your instance, as described in Restart Tenable Core and Shut Down Tenable Core.</td>
</tr>
<tr>
<td></td>
<td>• Edit the hostname for your instance, as described in Edit Your Tenable Core Hostname.</td>
</tr>
<tr>
<td></td>
<td>• Edit the time and time zone settings for your instance, as described in Edit Your Time Settings.</td>
</tr>
<tr>
<td>Data graphs</td>
<td>• View a graph of the CPU usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Memory &amp; Swap usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Disk I/O bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the Network Traffic bandwidth usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• To change the time range for data displayed in the graphs:</td>
</tr>
<tr>
<td></td>
<td>1. In the top-right corner of the graph, click the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>2. Select a time range.</td>
</tr>
</tbody>
</table>
The system refreshes the graph.
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 System page appears.

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

3. Click on the link next to the Performance Profile option in the information list to the left of the graph charts. 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.
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 **System** 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 **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.
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 System 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.
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 System page appears.

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

   The System page displays.

3. Click the link next to the Host Name option in the information list to the left of the graph charts.

   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.
Edit Your Time Settings

Caution: Do not edit time settings on Tenable Core + Tenable.ot using any method other than the one described in the following process.

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 System page appears.

2. Access the Tenable.ot interface, as described in Configure Tenable.ot in the Tenable.ot User Interface.
   The Tenable.ot interface appears.

3. Log in to Tenable.ot.

4. Modify your system time settings as described in the Tenable.ot User Guide.
   Tenable Core + Tenable.ot reboots.
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. Click on an individual entry (row) to get additional information.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 24, 2017</td>
<td>11:21</td>
<td>Error probing device: Error sending 8T command IDENTIFY PACKET to /dev/sr2: ATA command failed: error=0x81 count=0x82 status=0x58 (p=io-err)... stored</td>
</tr>
<tr>
<td>August 24, 2017</td>
<td>11:21</td>
<td>Error probing device: Error sending 8T command IDENTIFY PACKET to /dev/sr3: ATA command failed: error=0x81 count=0x82 status=0x58 (p=io-err)... stored</td>
</tr>
<tr>
<td>August 24, 2017</td>
<td>11:21</td>
<td>Error probing device: Error sending 8T command IDENTIFY PACKET to /dev/sr4: ATA command failed: error=0x81 count=0x82 status=0x58 (p=io-err)... stored</td>
</tr>
<tr>
<td>August 24, 2017</td>
<td>11:21</td>
<td>Error probing device: Error sending 8T command IDENTIFY PACKET to /dev/sr5: ATA command failed: error=0x81 count=0x82 status=0x58 (p=io-err)... stored</td>
</tr>
<tr>
<td>August 21, 2017</td>
<td>23:04</td>
<td>Fatal: Read from socket failed: Connection reset by peer [process]</td>
</tr>
<tr>
<td>August 10, 2017</td>
<td>15:55</td>
<td>Failed to start recovery kernel: resuming</td>
</tr>
<tr>
<td>August 10, 2017</td>
<td>15:55</td>
<td>Failed to start Network Manager Wait Online</td>
</tr>
<tr>
<td>August 10, 2017</td>
<td>15:54</td>
<td>pide4: awaken 0000:00:07.3: Host SMBus controller not enabled</td>
</tr>
<tr>
<td>August 10, 2017</td>
<td>15:54</td>
<td>wid 0:0:0:0:3: [wde] Assuming drive cache: write through</td>
</tr>
</tbody>
</table>
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 **System** page appears.

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

3. Click the **Create Report** button.

4. A new window with a status bar appears as the report generates.

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

6. Click the **Download Report** button to save and print the report.
View Container Status

After you deploy Tenable Core + Tenable.ot, you can view container and image status information to troubleshoot issues with Tenable.ot.

To view container status information:

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

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

3. View container status information:

<table>
<thead>
<tr>
<th>Section</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphs</td>
<td>• View a graph of the combined CPU usage on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the combined memory usage on your instance.</td>
</tr>
<tr>
<td>Containers</td>
<td>Expand a row to view details for a container.</td>
</tr>
<tr>
<td>table</td>
<td><strong>Caution:</strong> Tenable does not recommend removing a container or modifying the status of a container unless recommended by Tenable Support.</td>
</tr>
<tr>
<td>Images</td>
<td>Expand a row to view details for an image.</td>
</tr>
<tr>
<td>table</td>
<td><strong>Caution:</strong> Tenable does not recommend removing an image or modifying the status of an image unless recommended by Tenable Support.</td>
</tr>
</tbody>
</table>
View Tenable.ot Logs

If you experience an issue during the Tenable.ot installation process or an issue with the Tenable.ot service, you can view the logs to access more troubleshooting information.

To view logs for Tenable.ot:

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

   The System page appears.

2. In the left navigation bar, click Tenable.ot.

   The Tenable.ot page appears.

3. In the Tenable.ot Logs section, click the drop-down box and select a log type:

   - Tenable.ot Service — Logs related to issues with the Tenable.ot service.
   - Tenable.ot Installation — Logs related to issues during the Tenable Core + Tenable.ot installation.

   The section refreshes to show the logs.

4. (Optional) To filter the logs that appear, select a time range, a Severity, or a Service.

   The page applies the selected filters.
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 **System** 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 <strong>Sending</strong> (outbound) network traffic on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Receiving</strong> (inbound) network traffic on your instance.</td>
</tr>
<tr>
<td><strong>Firewall section</strong></td>
<td>• View Firewall rules.</td>
</tr>
<tr>
<td></td>
<td>• Add Zones.</td>
</tr>
<tr>
<td></td>
<td>• Add Allowed Services.</td>
</tr>
<tr>
<td><strong>Interfaces table</strong></td>
<td>• Aggregate multiple network interfaces into a single-bonded interface, as described in <a href="#">Add a Bonded Interface</a>.</td>
</tr>
<tr>
<td></td>
<td>• Add a team of interfaces, as described in <a href="#">Add a Team of Interfaces</a>.</td>
</tr>
<tr>
<td></td>
<td>• Add a bridge to create a single aggregate network from multiple communication networks, as described in <a href="#">Add a Bridge Network</a>.</td>
</tr>
<tr>
<td></td>
<td>• Add a VLAN, as described in <a href="#">Add a VLAN</a>.</td>
</tr>
<tr>
<td>Networking Logs table</td>
<td>View a log of activity for the system network.</td>
</tr>
</tbody>
</table>
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>[ens160]</td>
</tr>
<tr>
<td></td>
<td>[ens32]</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.
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.
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 **System** 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><strong>Graphs</strong></td>
<td>• View a graph of the <strong>Reading</strong> storage activity on your instance.</td>
</tr>
<tr>
<td></td>
<td>• View a graph of the <strong>Writing</strong> storage activity on your instance.</td>
</tr>
<tr>
<td><strong>Filesystems table</strong></td>
<td>• View information about each filesystem.</td>
</tr>
<tr>
<td></td>
<td>• Click a row to view more details about the filesystem.</td>
</tr>
<tr>
<td></td>
<td>• Rename a filesystem, as described in <a href="#">Rename a Filesystem</a>.</td>
</tr>
<tr>
<td></td>
<td>• Delete a filesystem, as described in <a href="#">Delete a Filesystem</a>.</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

   This device has filesystems that are currently in use. Proceeding will unmount all filesystems on it.

   Deleting a volume group will erase all data on it.

   Cancel  Delete

   Caution: Deleting a volume group erases all data on it.
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 System 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.

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>
<tr>
<td>Roles</td>
<td>• To grant the user account administrator access, select the <strong>Server Administrator</strong> check box.</td>
</tr>
<tr>
<td></td>
<td>• To remove administrator access from the user account, clear the <strong>Server Administrator</strong> check box.</td>
</tr>
<tr>
<td>Access</td>
<td>• To lock the user account, select the <strong>Lock Account</strong> check box to lock the user account.</td>
</tr>
<tr>
<td></td>
<td>• To unlock the user account, clear the <strong>Lock Account</strong> check box to unlock the user account.</td>
</tr>
<tr>
<td></td>
<td>• To configure the account to remain unlocked indefinitely:</td>
</tr>
</tbody>
</table>

**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 indefinitely.

- 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.
  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 log in 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...
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.
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 System 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>Targets</td>
<td>1. Click Stop, Start, Restart, or Reload.</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>System Services</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 Stop, Start, Restart, or Reload.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Restarting a service completely stops and restarts the service. Reloading a service only reloading the service's configuration files.</td>
</tr>
<tr>
<td></td>
<td>The system changes the status of the service.</td>
</tr>
</tbody>
</table>
| Sockets | • View a list of socket 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. |
| --- | --- |
| Timers | • 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. |
| Paths | • View a list of path services.  
• Click a row to view detailed information about a service.  
• To change the status of a service: |
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 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.
Access the Terminal

The Terminal page provides a console to access a user-specific command-line interface.
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.

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.
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 System page appears.
2. In the left navigation bar, click Tenable.ot.
   
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.ot Documentation.
Manage Updates

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

**Note:** To update your Tenable.ot application version, contact Tenable Support. You cannot use the Tenable Core interface to update Tenable.ot.

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.ot.
- The latest version of CentOS included in Tenable Core.
- The latest version of any additional packages required by Tenable Core.
- The latest version of any additional CentOS packages you installed.

**Note:** To update your Tenable.ot application version, contact Tenable Support. You cannot use the Tenable Core interface to update Tenable.ot.

To configure automatic updates:

1. Log in to Tenable Core via the user interface, as described in [Log In to Tenable Core](#).
   
   The **System** 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 **Scheduled updates can be enabled/disabled Here**.
   
   The **Services** details page appears, displaying the details for the `tenablecore.update.timer` service.

4. Confirm that you have set **Automatic Startup** to enabled.

   **Note:** Tenable does not recommend disabling automatic updates or otherwise modifying **Automatic Startup** for the `tenablecore.update.timer` service.

5. Review the schedule for the automatic updates and modify, if needed, as described in [Configure Your Automatic Update Schedule](#).

What to do next:
• If the update included any of the following packages, restart Tenable Core as described in Start, Stop, or Restart Your Application.
  • kernel
  • glibc
  • linux-firmware
  • systemd
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 System 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:

- The latest version of Tenable.ot.
- The latest version of CentOS included in Tenable Core.
- The latest version of any additional packages required by Tenable Core.
- The latest version of any additional CentOS packages you installed.

**Note:** To update your Tenable.ot application version, contact Tenable Support. You cannot use the Tenable Core interface to update Tenable.ot.

Before you begin:

- Manually refresh the packages:
  
  a. Log in to Tenable Core via [the Terminal page](#) or command line interface (CLI).

  The command line appears.

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

  ```
  sed -i.orig '/self.cache_age == 0/s/=/>/' /usr/share/PackageKit/helpers/yum/yumBackend.py
  ```

To update on demand:

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

   The **System** page appears.

2. In the left navigation pane, click **Software Updates**.

   The **Software Updates** page appears.

3. Click **Check for Updates**.

   The page refreshes and displays available updates.
4. If updates are available, click **Install all updates**.

   Tenable Core performs the updates.

What to do next:

- If the update included any of the following packages, restart Tenable Core as described in **Start, Stop, or Restart Your Application**.
  
  - kernel
  
  - glibc
  
  - linux-firmware
  
  - systemd
Update Tenable Core Offline

To perform an offline update of Tenable Core + Tenable.ot, contact Tenable Support.
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
Manage the Server Certificate

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

**Tip:** By default, Tenable Core uses separate certificates for Tenable Core and Tenable.ot. For information about the Tenable.ot application certificate, see the *Tenable.ot Documentation*.

**Note:** The default certificate is not signed by a recognized certificate authority (CA). If your browser reports that the Tenable Core server certificate is untrusted, Tenable recommends uploading a custom server certificate signed by a trusted certificate authority (CA) for Tenable Core 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.

Tip: By default, Tenable Core uses the same certificates for Tenable Core as well as Tenable.ot.

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 System 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.
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 System 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.
**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

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 SNMPv2c or SNMPv3 settings. To configure other advanced or uncommon SNMP settings, use the CLI as described in [Configure an SNMP Agent via the CLI](#).

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 **System** 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>
</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 password</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</td>
<td>Specifies the username and password for an account on the SNMPv3 NMS.</td>
</tr>
<tr>
<td>access username</td>
<td>SNMPv3 NMS.</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Read-write</td>
<td></td>
</tr>
<tr>
<td>access user pass-word</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.
Take a Virtual Machine Snapshot

You can take a snapshot to back up your entire machine, including application-installed files, application data, OS files, and configurations.

Before you begin:

- Stop your instance of Tenable Core + Tenable.ot, as described in Start, Stop and Restart Tenable Core.

To take a snapshot of Tenable Core:

1. Take a snapshot, as described in the documentation for your environment.
FAQ

When are Tenable Core offline update ISOs released?

Tenable Core releases offline updates throughout the year on a quarterly basis, within two 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 Nessus until the general availability (GA) date in Tenable.io. This is usually a week after the stand-alone Nessus GA. Releases for other products on Tenable Core usually occur within 24 hours of the GA date.

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.sc down every morning?
Tenable Core shuts down Tenable.sc 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.sc remains down pending user intervention. Automatic backups can also shut down Tenable.sc, 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.

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

The process to reset your password is in this [Tenable Community Knowledge Article](#).