Tenable General Requirements

Last Revised: July 14, 2023

Introduction

This document provides information about the hardware, software, and licensing requirements required to deploy Tenable products.

For more information, see:

- Tenable Log Correlation Engine (Formerly LCE)
- Tenable Nessus
- Tenable Nessus Agents
- Tenable Nessus Network Monitor (Formerly NNM)
- Tenable Vulnerability Management (Formerly Tenable.io)
- Tenable Identity Exposure (Formerly Tenable.ad)
- Tenable OT Security (Formerly Tenable.ot)
- Tenable.sc (Formerly Tenable.sc)
- Tenable Core

Tenable Log Correlation Engine (Formerly LCE)

This section includes:

- Tenable Log Correlation Engine Hardware Requirements
- Tenable Log Correlation Engine Software Requirements
- Log Correlation Engine Licensing Requirements

Tenable Log Correlation Engine Hardware Requirements

The following hardware recommendations for Log Correlation Engine are to be used as a general guide. 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 cards will be heavily based on the former. Disk space requirements will vary depending on usage based on the amount and length of time data is stored on the system.

The hardware requirements for Log Correlation Engine change based on the number of events being processed.

Estimating Events

The following table provides the estimated average number of events from various sources.

Devices	Number of Estimated Events
1 workstation/laptop	0.5 events/sec
1 web-facing app server	20 events/sec
1 web-facing firewall/IDS/IPS	75 events/sec
1 internal application server (low volume)	5 events/sec
1 internal application server (high volume: IIS, Exchange, AD)	20 events/sec
1 internal network device	2 events/sec

To convert your event rate to bytes per day, Tenable recommends that you multiply your total events/second by 250 bytes/event and multiply by 86,400 seconds/day. For example, assume 100 events per second: 100 events/second * 250 bytes/event * 86,400 seconds/day = 2,160,000,000 bytes/day.

System Specification

The following table specifies the system requirements based on the number of events the Log Correlation Engine server is processing.

Version	Installation scenario	RAM	Processor	Hard disk	Hard disk space
6.x	One Log Correlation Engine server with PostgreSQL processing less than 5,000 events per second	22 GB	8 cores	10,000 to 15,000 RPM HD, or SSD of equiv. IOPS capability, in RAID 0/10 configuration	2.4 x Licensed storage size
	One Log Correlation Engine server with PostgreSQL processing between 5,000 and 20,000 events per second	30 GB	16 cores	15,000 RPM HD, or SSD of equiv. IOPS capability; RAID 0/10 configuration	
	One Log Correlation Engine server with PostgreSQL processing greater than 20,000 events per second	58 GB or more	24 or more cores	SSD of IOPS capability at least equiv. to a 15,000 RPM HD; RAID 0/10 configuration	

The Log Correlation Engine server requires a minimum of 20 GB of storage space to continue running and storing logs. If less than 1 GB is available, the Log Engine (lced) process will stop gracefully

and refuse to store additional logs. The current system disk space is visible on the **Health and Status** page of the Log Correlation Engine interface.

File System Recommendations

Placing your activeDb on a networked file system (e.g. NFS) will result in inadequate system performance. Tenable recommends that you use EXT3, EXT4, XFS, or ZFS; and that you pay close attention to the mount options. Here are the mount options we suggest using, and the mount options we suggest staying away from:

If your file system is:	It is recommended that you use:	It is not recommended to use:
EXT3, EXT4, XFS	`noatime`	`atime` or `strictatime` or `relatime` or `diratime` or No `*atime` at all.
EXT3	`barrier=0`	`barrier=1`
EXT4	`barrier=0` or `nobarrier`	`barrier=1` or `barrier`
XFS	`nobarrier`	`barrier`
EXT3, EXT4	`data=writeback`	`data=journal` or `data=ordered` or No `data=*` at all.
ZFS	`atime=off`	`atime=on` or `relatime=on` or No `*atime` at all.

ZFS	Hardware-dependent	`compression=gzip` or `compression=gzip-N` or `compression=zle`
		
		`compress=gzip` or `compress=gzip-N` or `compress=zle`

ZFS	`logbias=throughput`	`logbias=latency` or No `logbias` at all.
ZFS	`primarycache=metadata`	`primarycache=all` or `primarycache=none` or No `primarycache=*` at all.
ZFS	Hardware-dependent	`recordsize=512` or `recordsize=1024` or `recordsize=2048` or `recordsize=4096`

Tenable Log Correlation Engine Software Requirements

Version	Software Requirements
6.x	• An active Log Correlation Engine license • RHEL/CentOS 7.x, 64-bit

Additionally, while Log Correlation Engine is active, it requires exclusive access to certain ports. The only services that are required to support remote users are SSH and the Log Correlation Engine interface (lce). If other services are active on the system, conflicts should be avoided on the following default ports:

Ports Log Correlation Engine Receives (Listens) On	
Port	Description
162/UDP	SNMP
514/UDP	Syslog
22/TCP	SSH, for requests from Tenable.sc
601/TCP	Syslog
1243/TCP	Vulnerability detection, if enabled in Tenable.sc
6514/TCP	Encrypted syslog
8836/TCP	Log Correlation Engine Administrative Web UI
31300/TCP	Events from Log Correlation Engine Clients

Ports Log Correlation Engine Sends On	
Port	Description
514/UDP	Syslog (forwarded)
443/TCP	Pull requests to the plugins feed at plugins.nessus.org

601/TCP	Syslog (forwarded)

Ports Log Correlation Engine Uses Over Loopback Interface	
Port	Description
7091/TCP	Internal communication, `showids` to `lce_queryd`
7092/TCP	Internal communication, `lce_tasld` to `lced`

Caution: The system running the Log Correlation Engine can operate a syslog daemon, but the syslog daemon must not be listening on the same port(s) that the Log Correlation Engine server is listening on.

Log Correlation Engine Licensing Requirements

Log Correlation Engine requires an activation code, which may be purchased directly from Tenable Network Security or through Authorized Enterprise Partners. The code will be used when installing and configuring your copy of Log Correlation Engine and each attached Tenable.sc (formerly SecurityCenter).

There is no licensed limit to the number of events or IP addresses that the Log Correlation Engine can be configured to monitor. Instead, Log Correlation Engine is licensed by the maximum amount of storage to be used by the Log Correlation Engine installation.

There are different licenses available for the Log Correlation Engine based on the total amount of storage used by the Log Correlation Engine. The licenses are based on 1 TB, 5 TB, and 10 TB storage sizes. A license for Log Correlation Engine is provided as a part of Tenable.sc CV. There is no difference in the Log Correlation Engine software that is installed, just the maximum storage size that can be used by the Log Correlation Engine. The size limit of the Elasticsearch databases can be configured via the Log Correlation Engine interface. Data that exceeds your license limit will be archived.

Tenable Nessus

This section includes:

- Nessus Licensing Requirements
- Nessus Scanners
    - Tenable Nessus Scanner Hardware Requirements
    - Tenable Nessus Software Requirements

Nessus Licensing Requirements

Nessus is available to operate either as a subscription or managed by Tenable.sc. Nessus requires a plugin feed Activation Code to operate in subscription mode. This code identifies which version of Nessus you are licensed to install and use, and if applicable, how many IP addresses can be scanned, how many remote scanners can be linked to Nessus, and how many Nessus Agents can be linked to Nessus Manager.

It is recommended that you obtain the Activation Code before starting the installation process, as that information will be required before you can authenticate to the Nessus GUI interface.

Additionally, your activation code:

- is a **one-time** code, unless your license or subscription changes, at which point a new activation code will be issued to you.
- must be used with the Nessus installation within 24 hours.
- cannot be shared between scanners.
- is not case sensitive.
- is required to Manage Nessus Offline.

You may purchase a Nessus subscription through the Tenable Online Store at https://store.tenable.com/ or via a purchase order through Authorized Nessus Partners. You will then receive an Activation Code from Tenable. This code will be used when configuring your copy of Nessus for updates.

> **Note:** If you are using Tenable.sc to manage your Nessus scanners, the Activation Code and plugin updates are managed from Tenable.sc. Nessus needs to be started to be able to communicate with Tenable.sc, which it will normally not do without a valid Activation Code and plugins. To have Nessus ignore this requirement and start (so that it can get the information from Tenable.sc), enter "SecurityCenter" (case sensitive) without quotes into the Activation Code box.

Please refer to the following link for the most current information on obtaining an Activation Code: http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code.

Nessus Scanners

This section includes:

- Tenable Nessus Scanner Hardware Requirements
- Tenable Nessus Software Requirements

Tenable Nessus Scanner Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus deployments include raw network speed, the size of the network being monitored, and the Tenable Nessus configuration.

> **Note:** In addition to the minimum recommended disk spaces listed in the following sections, consider how much additional disk space your organization needs to store Tenable Nessus log files. By default, `nessusd.dump` and `nessusd.messages` can store up to 50 GB of log files each, but you can configure this size to be larger or smaller depending on your organization's needs. For more information, see the `dumpfile_max_files`, `dumpfile_max_size`, `logfile_max_files`, and `logfile_max_size` settings in the *Tenable Nessus User Guide* Advanced Logging Settings.

Tenable Nessus Scanners and Tenable Nessus Professional

The following table lists the hardware requirements for Tenable Nessus scanners and Tenable Nessus Professional.

Scenario	Minimum Recommended Hardware
Scanning up to 50,000 hosts per scan	**CPU:** 4 2GHz cores **Memory:** 4 GB RAM (8 GB RAM recommended) **Disk space:** 30 GB, not including space used by the host operating system > **Note:** Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.
Scanning more than 50,000 hosts per scan	**CPU:** 8 2GHz cores **Memory:** 8 GB RAM (16 GB RAM recommended) **Disk space:** 30 GB, not including space used by the host operating system > **Note:** Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.

Tenable Nessus Manager

The following table lists the hardware requirements for Tenable Nessus Manager.

Note: To view the hardware requirements for Nessus Manager clustering, see Clustering System Requirements.

Scenario	Minimum Recommended Hardware
Nessus Manager with 0-10,000 agents	**CPU**: 4 2GHz cores **Memory:** 16 GB RAM **Disk space:** 5 GB per 5,000 agents per concurrent scan **Note:** Scan results and plugin updates require more disk space over time.
Nessus Manager with 10,001-20,000 agents	**CPU:** 8 2GHz cores **Memory:** 32 GB RAM **Disk space:** 5 GB per 5,000 agents per concurrent scan **Note:** Scan results and plugin updates require more disk space over time. **Note:** Engage with your Tenable representative for large deployments.

Virtual Machines

Tenable Nessus can be installed on a virtual machine that meets the same requirements. If your virtual machine is using Network Address Translation (NAT) to reach the network, many of the Tenable Nessus vulnerability checks, host enumeration, and operating system identification are negatively affected.

Note: Only *one* virtualized Tenable Nessus scanner can be run on any physical host. Tenable Nessus relies on low-level network operations and requires full access to the host's network interface controller (NIC). In a virtualization environment (for example, Hyper-V, Docker), this can cause incorrect scanner behavior, or

host instability, if more than one virtualized Tenable Nessus scanner attempts to share a single physical NIC.

Tenable Nessus Software Requirements

Tenable Nessus supports Linux, Windows, and macOS operating systems.

Note: Microsoft Visual C++ Redistributable 14.22 is included as part of a bundled license package with Nessus.

Tenable Nessus 10.5

Operating System	Supported Versions
Linux	Amazon Linux 2015.03, 2015.09, and 2017.09 (x86_64) Amazon Linux 2 (x86_64, AArch64) Debian 10 and 11 (i386) Debian 10 and 11 / Kali Linux 2020 (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali releases. Fedora 35 (x86_64) Raspberry Pi OS (ARMHF) Red Hat ES 6 (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64, AArch64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 (x86_64, AArch64) Red Hat ES 9 / Oracle Linux 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 9 / Alma Linux 9 (x86_64, AArch64) FreeBSD 12 (AMD64) SUSE Enterprise 12 and 15 SP1 and later (x86_64) Ubuntu 14.04 and 16.04 (i386)

Operating System	Supported Versions
	Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (AArch64, Graviton2)
Windows	Windows 10 (i386) Windows 10, 11, Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022 (x86_64)
macOS	macOS 11, 12, and 13 (x86_64, M1)

Tenable Nessus 10.4

Operating System	Supported Versions
Linux	Debian 9, 10 (i386) Debian 9, 10 / Kali Linux 1, 2019, 2020 (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali releases. Fedora 35 (x86_64) Raspberry Pi OS (ARMHF) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64, AArch64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64, AArch64) Red Hat ES 9 / Oracle Linux 9 (including Unbreakable Enterprise Kernel) (x86_64, AArch64) FreeBSD 12 (AMD64)

Operating System	Supported Versions
	SUSE Enterprise 12 and 15 SP1 and later (x86_64) Ubuntu 14.04 and 16.04 (i386) Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (AArch64, Graviton2)
Windows	Windows 10 (i386) Windows 10, 11, Windows Server 2012 R2, Server 2016, Server 2019, Server 2022 (x86_64)
macOS	macOS 11, 12, and 13 (x86_64, M1)

Tenable Nessus 10.3

Operating System	Supported Versions
Linux	Debian 9, 10 / Kali Linux 1, 2017.3 (i386) Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali releases. Fedora 34 and 35 (x86_64) FreeBSD 11, 12 (AMD64) Raspberry Pi OS (ARMHF) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64, i386) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise

Operating System	Supported Versions
	Kernel) (x86_64) SUSE Enterprise 11, 12, and 15 (x86_64) SUSE Enterprise 11 (i586) Ubuntu 14.04 and 16.04 (i386) Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (AArch64, Graviton2)
Windows	Windows 10 (i386) Windows 10, 11, Windows Server 2012 R2, Server 2016, Server 2019, Server 2022 (x86_64)
macOS	macOS 10.9-10.15, 11, and 12 (x86_64, M1)

Tenable Nessus 10.2

Operating System	Supported Versions
Linux	Debian 9, 10 / Kali Linux 2017 and Rolling (i386) Debian 9, 10 / Kali Linux 2017, 2018, 2019, 2020, and Rolling (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali releases. Fedora 33, 34, and 35 (x86_64) FreeBSD 11, 12 (AMD64) Raspberry Pi OS (ARMHF) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (i386) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64)

Operating System	Supported Versions
	Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) SUSE Enterprise 11 SP4, 12 SP3 and later (x86_64, i586) SUSE Enterprise 15 (i586) Ubuntu 14.04 and 16.04 (i386) Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (Graviton2) Ubuntu 18.0 (ARMv7, Graviton2)
Windows	Windows 10 (i386) Windows 10, 11, Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022 (x86_64)
macOS	macOS 10.9-10.15, 11, and 12 (x86_64, M1)

Tenable Nessus 10.1

Operating System	Supported Versions
Linux	Debian 9, 10 / Kali Linux 2017 and Rolling (i386) Debian 9, 10 / Kali Linux 2017, 2018, 2019, 2020, and Rolling (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali releases. FreeBSD 11, 12 (AMD64) Raspberry Pi OS (ARMHF)

Operating System	Supported Versions
	Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (i386) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) SUSE Enterprise 11 SP4, 12 SP3 and later (x86_64, i586) SUSE Enterprise 15 (i586) Ubuntu 14.04 and 16.04 (i386) Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (Graviton2) Ubuntu 18.0 (ARMv7, Graviton2)
Windows	Windows 10 (i386) Windows 10, 11, Windows Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022 (x86_64)
macOS	macOS 10.9-10.15, 11, and 12 (x86_64, M1)

Tenable Nessus 10.0

Operating System	Supported Versions
Linux	Debian 9, 10 / Kali Linux 2017 and Rolling (i386) Debian 9, 10 / Kali Linux 2017, 2018, 2019, 2020, and Rolling (AMD64) **Note:** Tenable recommends using the debian6_amd64.deb package for rolling Kali

Operating System	Supported Versions
	releases. Raspberry Pi OS (ARMHF) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (i386) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / CentOS 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) FreeBSD 11, 12 (AMD64) SUSE Enterprise 11 SP4, 12 SP3 and later (x86_64, i586) SUSE Enterprise 15 (i586) Ubuntu 14.04 and 16.04 (i386) Ubuntu 14.04, 16.04, 18.04, 20.04 (AMD64) Ubuntu 18.04 (Graviton2)
Windows	Windows 10 (i386) Windows 10, Windows Server 2012, Server 2012 R2, Server 2016, Server 2019 (x86_64)
macOS	macOS 10.9-10.15, 11 (x86_64, M1)

Browsers

Nessus supports the following browsers:

- Google Chrome (76+)
- Apple Safari (10+)

- Mozilla Firefox (50+)
- Microsoft Edge (102+)

PDF Reports

The Nessus PDF report generation feature requires the latest version of Oracle Java or OpenJDK.

If your organization requires PDF reports, you must install Oracle Java or OpenJDK before installing Tenable Nessus. If you install Oracle Java or OpenJDK after installing Nessus, you need to reinstall Nessus for the PDF report feature to function properly.

Nessus Agents

This section includes:

- Nessus Agent Hardware Requirements
- Nessus Agent Software Requirements
- Nessus Agent Software Footprint

Nessus Agent Hardware Requirements

Tenable Nessus Agents are lightweight and only minimal system resources. Generally, a Tenable Nessus Agent uses 40 MB of RAM (all pageable). A Tenable Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs.

The following table outlines the minimum recommended hardware for operating a Tenable Nessus Agent. You can install Tenable Nessus Agents on a virtual machine that meets the same requirements specified.

Hardware	Minimum Requirement
Processor	1 Dual-core CPU
Processor Speed	> 1 GHz
RAM	> 1 GB
Disk Space	• Agents 7.7.x and earlier: > 1 GB, not including space used by the host operating system • Agents 8.0.x and later: > 3 GB, not including space used by the host operating system • Agents 10.0.x and later: > 2 GB, not including space used by the host operating system The agent may require more space during certain processes, such as a `plugins-code.db` defragmentation operation.
Disk Speed	15-50 IOPS

Nessus Agent Software Requirements

Nessus Agents support Linux, Windows, and macOS operating systems.

Note: Tenable Nessus Agent does not require an external runtime environment, such as Java.

Note: Microsoft Visual C++ Redistributable 14.22 is included as part of a bundled license package with Nessus Agents.

Version	Operating System	Supported Versions
10.4.x	Linux	Amazon Linux 2015.03, 2015.09, 2017.09, 2018.03 (x86_64) Amazon Linux 2 (x86_64, AArch64) Debian 10 / Kali Linux 2017, 2018, 2019, and 2020 (i386) Debian 10 and 11 / Kali Linux 2017, 2018, 2019, and 2020 (x86_64) Fedora 34, 35, and 36 (x86_64) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (AArch64, Graviton2) Red Hat ES 8 and 9 / AlmaLinux 8 and 9 / Oracle Linux 8 and 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 and 9 (x86_64) Red Hat ES 8 and 9 / AlmaLinux 8 and 9 / Oracle Linux 8 and 9 (including Unbreakable Enterprise Kernel) / Rocky Linux 8 and 9 (AArch64, Graviton2) SUSE Enterprise 12 SP4 and later, 15 SP1 and later (x86_64) Ubuntu 14.04, 16.04, 18.04, 20.04, and 22.04 (x86_64)

		Ubuntu 18.04, 20.04, and 22.04 (AArch64, Graviton2)
	Windows	Windows 10 (x86) Windows 10 and 11 (x86_64) Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64) **Note:** Nessus Agent 8.2.0 and later requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Nessus Agent 8.2.0 and later. Current agent installations on Windows that do not meet these requirements will not automatically upgrade past version 8.1.0.
	macOS	macOS 11, 12, and 13 (x86_64) macOS 11, 12, and 13 (Apple Silicon)
Previous Versions		
10.3.x	Linux	Debian 10 / Kali Linux 2019, 2020 (i386) Debian 10 and 11 / Kali Linux 2019, 2020 (x86_64) Fedora 35 and 36 (x86_64) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 (AArch64, Graviton2) Red Hat ES 8 and 9 / AlmaLinux 8.6 and 9 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) / Rocky Linux 8.6 and 9 (x86_64) Red Hat ES 8 and 9 / AlmaLinux 8.6 and 9 / Rocky Linux 8.6 and

		9 (AArch64, Graviton2) SUSE Enterprise 12 SP3 and later, 15 SP1 and later (x86_64) Ubuntu 14.04, 16.04, 18.04, 20.04, and 22.04 (x86_64) Ubuntu 18.04, 20.04, and 22.04 (AArch64, Graviton2)
	Windows	Windows 10 (x86) Windows 10 and 11 (x86_64) Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64) **Note:** Nessus Agent 8.2.0 and later requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Nessus Agent 8.2.0 and later. Current agent installations on Windows that do not meet these requirements will not automatically upgrade past version 8.1.0.
	macOS	macOS 11, 12, and 13 (x86_64) macOS 11, 12, and 13 (Apple Silicon)
10.2.x	Linux	Debian 9 and 10 / Kali Linux 2017.3, 2018, 2019, 2020 (i386) Debian 9, 10, and 11 / Kali Linux 2017.3, 2018, 2019, 2020 (x86_64) Fedora 34, 35, and 36 (x86_64) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (AArch64, Graviton2)

		Red Hat ES 8 and 9 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 and 9 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (AArch64, Graviton2) SUSE Enterprise 12 SP3 and later, 15 (x86_64) Ubuntu 14.04, 16.04, 18.04, 20.04, and 22.04 (x86_64) Ubuntu 18.04, 20.04, and 22.04 (AArch64, Graviton2)
	Windows	Windows 10 (x86) Windows 10, 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64) **Note:** Nessus Agent 8.2.0 and later requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Nessus Agent 8.2.0 and later. Current agent installations on Windows that do not meet these requirements will not automatically upgrade past version 8.1.0.
	macOS	macOS 11, 12, and 13 (x86_64) macOS 11, 12, and 13 (Apple Silicon)
10.1.x	Linux	Debian 9 and 10 / Kali Linux 2017.3, 2018, 2019, 2020 (i386) Debian 9 and 10 / Kali Linux 2017.3, 2017.3, 2018, 2019, 2020 (x86_64) Fedora 33, 34, 35 (x86_64) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64)

		Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) SUSE Enterprise 11 SP4 (x86) SUSE Enterprise 11 SP4, 12 SP3 and later, 15 (x86_64) Ubuntu 14.04, 16.04 (x86) Ubuntu 14.04, 16.04, 18.04, and 20.04 (x86_64) Ubuntu 18.04 (AArch64, Graviton2)
	Windows	Windows 10 (x86) Windows 10 and 11 (x86_64) Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64) **Note:** Nessus Agent 8.2.0 and later requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Nessus Agent 8.2.0 and later. Current agent installations on Windows that do not meet these requirements will not automatically upgrade past version 8.1.0.
	macOS	macOS 11 and 12 (x86_64) macOS 11 and 12 (Apple Silicon)
10.0.x	Linux	Debian 9 and 10 / Kali Linux 2017.3, 2018, 2019, 2020 (i386) Debian 9 and 10 / Kali Linux 2017.3, 2017.3, 2018, 2019, 2020 (x86_64) Fedora 33, 34, 35 (x86_64)

		Red Hat ES 6 /Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86) Red Hat ES 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (x86_64) Red Hat ES 8 / Oracle Linux 8 (including Unbreakable Enterprise Kernel) (x86_64) SUSE Enterprise 11 SP4 (x86) SUSE Enterprise 11 SP4, 12 SP3 and later, 15 (x86_64) Ubuntu 14.04, 16.04 (x86) Ubuntu 14.04, 16.04, 18.04, and 20.04 (x86_64) Ubuntu 18.04 (AArch64, Graviton2)
	Windows	Windows 10 (x86) Windows 10 and 11 (x86_64) Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 (x86_64) **Note:** Nessus Agent 8.2.0 and later requires Windows host systems to be running the latest version of Universal Microsoft C Runtime Library (UCRT) and PowerShell 5.0 or newer. Some older versions of Microsoft Windows require a minimum update to work with Nessus Agent 8.2.0 and later. Current agent installations on Windows that do not meet these requirements will not automatically upgrade past version 8.1.0.
	macOS	macOS 11 and 12 (x86_64) macOS 11 and 12 (Apple Silicon)

Software Footprint

Note: Performance varies by environment and you may or may not see similar results.

Agents Running Standard Agent Scans

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
~40 MB	~550 MB including plugin updates *	~50 MB RAM	~85 MB RAM	~150 MB RAM	~8 MB/day

*Under certain conditions, disk usage can spike up to 1 GB.

Agents Running Inventory Scans

Agent Footprint on Disk	Total Agent Software Footprint on Disk	Average RAM Usage While Not Scanning	Average RAM Usage While Scanning	Average RAM Usage During Plugin Compilation	Average Network Bandwidth Usage
~40 MB	~150 MB including plugin updates *	~50 MB RAM	~80 MB RAM	~105 MB RAM	~8 MB/day

*Under certain conditions, disk usage can spike up to 200 MB.

For more information about inventory scanning, see Tenable-Provided Nessus Agent Templates in the *Tenable Vulnerability Management User Guide*.

Tenable Nessus Network Monitor (Formerly NNM)

This section includes:

- Tenable Nessus Network Monitor Hardware Requirements
- Tenable Nessus Network Monitor Software Requirements
- Tenable Nessus Network Monitor Licensing Requirements

Tenable Nessus Network Monitor Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus Network Monitor deployments include raw network speed, the size of the network being monitored, and the configuration of Tenable Nessus Network Monitor.

The following chart outlines some basic hardware requirements for operating Tenable Nessus Network Monitor:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	Tenable Nessus Network Monitor managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	2 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor managing more than 50,000 hosts **	4 GB RAM (8 GB RAM recommended)	4 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor running in High Performance mode	16 GB RAM (HugePages memory: 2 GB)	10 2GHz cores with hyper-threading enabled	20 GB HDD minimum

*The ability to monitor a given number of hosts depends on the bandwidth, memory, and processing power available to the system running Tenable Nessus Network Monitor.

**For optimal data collection, Tenable Nessus Network Monitor must be connected to the network segment via a hub, spanned port, or network tap to have a full, continuous view of network traffic.

Note: Research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers. Tenable Nessus Network Monitor supports VMware's vmxnet3 driver.

High Performance Mode

To run Tenable Nessus Network Monitor in High Performance mode, a minimum of two of the following types of Intel NICs are required; one as a management interface and at least one as a monitoring interface:

- e1000 (82540, 82545, 82546)
- e1000e (82571, 82574, 82583, ICH8.ICH10, PCH.PCH2)
- igb (82575, 82576, 82580, I210, I211, I350, I354, DH89xx)
- ixgbe (82598, 82599, X540, X550)
- i40e (X710, XL710)
- NT40A01-4x1

Tenable Nessus Network Monitor Software Requirements

Note: Standard support for Tenable Nessus Network Monitor 5.12 ends 09/30/2022. Tenable recommends updating to Tenable Nessus Network Monitor 6.0.0 or later. Otherwise, you will not be able to report issues and bugs. Users that connect to Tenable Vulnerability Management using a web proxy need to upgrade to Tenable Nessus Network Monitor 6.1.1.

Tenable Nessus Network Monitor is available for the following platforms:

Version	Software Requirements
6.2.x	• Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit • Red Hat Linux ES 8 / CentOS 8 (through 8.7) 64-bit • Red Hat Linux ES 9 64-bit **Note:** For all versions of Red Hat Linux ES and CentOS, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • Microsoft Windows 7, 8, 10, Server 2012, Server 2016, and Server 2019 64-bit **Note:** Tenable Nessus Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. You must download the specific package `vc_redist.x64.exe` from the Microsoft downloads site. **High Performance mode only available on:** • RH7/CentOS7 (RH 7.0 through RH 7.9) : 3.10.0-1160 • RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-348 • RH8 (RH 8.6-8.7): 4.18.0-425
6.1.x	• Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • Red Hat Linux ES 8 / CentOS 8 (through 8.5) 64-bit

	Note: For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • Microsoft Windows 7, 8, 10, Server 2008, Server 2012, Server 2016, and Server 2019 64-bit **Note:** Tenable Nessus Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. You must download the specific package `vc_redist.x64.exe` from the Microsoft downloads site. **High Performance mode only available on:** • RH7/CentOS7 (RH 7.0 through RH7.4) : 3.10.0-693 • RH7/CentOS7 (RH 7.5): 3.10.0-862 • RH7/CentOS7 (RH 7.6): 3.10.0-957 • RH7/CentOS7 (RH 7.7): 3.10.0-1062 • RH7/CentOS7 (RH 7.8): 3.10.0-1127 • RH7/CentOS7 (RH 7.9): 3.10-1160 • RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-348
6.0.x	• Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • Red Hat Linux ES 8 / CentOS 8 (through 8.5) 64-bit **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • macOS 10.9-10.13 64-bit • Microsoft Windows 7, 8, 10, Server 2008, Server 2012, Server 2016, and Server 2019 64-bit **Note:** Tenable Nessus Network Monitor requires Microsoft Visual C++ Redis-

	tributable for Visual Studio 2015, 2017 and 2019. You must download the specific package `vc_redist.x64.exe` from the Microsoft downloads site. **High Performance mode only available on:** • RH7/CentOS7 (RH 7.0 through RH7.4) : 3.10.0-693 • RH7/CentOS7 (RH 7.5): 3.10.0-862 • RH7/CentOS7 (RH 7.6): 3.10.0-957 • RH7/CentOS7 (RH 7.7): 3.10.0-1062 • RH7/CentOS7 (RH 7.8): 3.10.0-1127 • RH7/CentOS7 (RH 7.9): 3.10-1160 • RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-348
Previous Versions	
5.13.x	• Red Hat Linux ES/ CentOS 64-bit • Red Hat Linux ES 7 / CentOS 7 (through 7.9) 64-bit **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • Red Hat Linux ES 8 (through 8.3) 64-bit **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • macOS 10.9-10.13 64-bit • Microsoft Windows 7, 8, 10, Server 2008, Server 2012, Server 2016, and Server 2019 64-bit **Note:** Tenable Nessus Network Monitor requires Microsoft Visual C++ Redistributable for Visual Studio 2015, 2017 and 2019. You must download the specific package `vc_redist.x64.exe` from the Microsoft downloads site.

	High Performance mode only available on: • RH6/CentOS6 (RH 6.0 through RH6.9) : 2.6.32-696 • RH7/CentOS7 (RH 7.0 through RH7.4) : 3.10.0-693 • RH7/CentOS7 (RH 7.5): 3.10.0-862 • RH7/CentOS7 (RH 7.6): 3.10.0-957 • RH7/CentOS7 (RH 7.7): 3.10.0-1062 • RH7/CentOS7 (RH 7.8): 3.10.0-1127 • RH7/CentOS7 (RH 7.9): 3.10-1160 • RH8/CentOS8 (RH 8.0 through 8.5): 4.18.0-240
5.12.x	• Red Hat Linux ES 5 • Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit (through 7.8) **Note:** For this version, Tenable Nessus Network Monitor requires that you have `systemd` and `firewalld` on your system. • macOS 10.9-10.13 64-bit • Microsoft Windows 7, 8, 10, Server 2008, Server 2012, and Server 2016 64-bit OS • Microsoft Visual C++ 2010 Redistributable Package **High Performance mode only available on:** • RH6/CentOS6 (RH6.0 thru RH6.9) : 2.6.32-696 • RH7/CentOS7 (RH7.0 thru RH7.4) : 3.10.0-693 • RH7/CentOS7 (RH7.5): 3.10.0-862 • RH7/CentOS7 (RH 7.6): 3.10.0-957

	• RH7/CentOS7 (RH 7.7): 3.10.0-1062 • RH7/CentOS7 (RH 7.8): 3.10.0-1127

You can use ERSPAN to mirror traffic from one or more source ports on a virtual switch, physical switch, or router and send the traffic to a destination IP host running Tenable Nessus Network Monitor. Tenable Nessus Network Monitor supports the following ERSPAN virtual environments:

- VMware ERSPAN (Transparent Ethernet Bridging)
- Cisco ERSPAN (ERSPAN Type II)

Tip: Refer to the Configuring Virtual Switches for Use with Tenable Nessus Network Monitor document for details on configuring your virtual environment.

High Performance Mode

To run Tenable Nessus Network Monitor in High Performance mode, you must enable HugePages support. HugePages is a performance feature of the Linux kernel and is necessary for the large memory pool allocation used for packet buffers. If your Linux kernel does not have HugePages configured, Tenable Nessus Network Monitor automatically configures HugePages per the appropriate settings. Otherwise, if your Linux kernel has defined HugePages, refer to the Configuring HugePages instructions in the Linux Command Line Operations section.

Tenable Nessus Network Monitor Licensing Requirements

Tenable Nessus Network Monitor Subscription

An Tenable Nessus Network Monitor subscription Activation Code is available that enables Tenable Nessus Network Monitor to operate in Standalone mode. This mode enables Tenable Nessus Network Monitor results to be viewed from an HTML interface enabled on the Tenable Nessus Network Monitor server.

Activation Code

To obtain a Trial Activation Code for Tenable Nessus Network Monitor, contact sales@tenable.com. Trial Activation Codes are handled the same way by Tenable Nessus Network Monitor as full Activation Codes, except that Trial Activation Codes allow monitoring for only 30 days. During a trial of Tenable Nessus Network Monitor, all features are available.

Tenable.sc Continuous View

Tenable.sc Continuous View includes Tenable Nessus Network Monitor as part of a bundled license package with Tenable.sc. This license allows an unlimited number of Tenable Nessus Network Monitor deployments to monitor an unlimited number of networks. Tenable.sc CV's IP view is constrained by the license purchased with it.

Note: When activating the Tenable Nessus Network Monitor in host discovery mode, set the activation code to "SecurityCenter" in Tenable Nessus Network Monitor. By default, it is automatically enabled on a new install.

Tenable Vulnerability Management

Tenable Vulnerability Management pushes plugins down to Tenable Nessus Network Monitor. The number of Tenable Nessus Network Monitor deployments is determined by your Tenable Vulnerability Management licensing.

High Performance Mode

Tenable Nessus Network Monitor in High Performance Mode can be licensed in Standalone mode or bundled with Tenable.sc CV.

Tenable Identity Exposure (Formerly Tenable.ad)

For complete information about Tenable Identity Exposure architecture and requirements, see Technical Prerequisites in the Tenable Identity Exposure On-premise Installation Guide.

- Tenable Identity Exposure Hardware Requirements
- Tenable Identity Exposure Network Requirements
- Tenable Identity Exposure Web Portal Requirements

Tenable Identity Exposure Hardware Requirements

Tenable Identity Exposure requires the following hardware:

- Supported Microsoft Windows Operating Systems
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022
- The requirements described in the sizing sections are for the well-being of Tenable Identity Exposure's platform; they do not include the operating system requirements of an application package-based deployment.
- CPU speed must be at least 2.6 GHz.
- Tenable Identity Exposure's platform supports the x86-64 processor architecture (at least Sandy Bridge or Piledriver) with Intel Turbo Boost Technology 2.0.
- One required network interface: you can add other network interfaces for administration, monitoring, or any other reason.

Tenable Identity Exposure Network Requirements

Tenable Identity Exposure requires access to your Active Directory infrastructures to initiate security monitoring. You must allow network flows between the different Tenable Identity Exposure services as described in Network Flow Matrix.

Bandwidth

As a monitoring platform, Tenable Identity Exposure receives Active Directory events continuously. Depending on the scale of the infrastructure, this process can generate a significant volume of data.

You must allocate an appropriate bandwidth to guarantee data transmission to Tenable Identity Exposure for analysis in a reasonable amount of time.

The following table defines the required bandwidth based on the size of the monitored AD.

Active AD Users	Average Number of Objects Received (per minute)	Minimum Bandwidth	Recommended Bandwidth
1 – 5,000	10	1 Mbps/sec	2 Mbps/sec
5,001 – 75,000	150	5 Mbps/sec	10 Mbps/sec
75,001 – 400,000	700	15 Mbps/sec	30 Mbps/sec

Microsoft APIs

To subscribe to the replication flows and begin monitoring them, Tenable Identity Exposure must contact standard directory APIs from Microsoft. Tenable Identity Exposure only requires communication with the Primary Domain Controller emulator (PDCe) with a regular user account. You must also deploy a new group policy object (GPO) to activate the attack detection engine.

Communication with AD

For an on-premises installation, Tenable Identity Exposure is a software package that you deploy on your Windows Server environment. Tenable Identity Exposure must communicate with the monitored Active Directory.

Internet Access

Tenable provides a continuous integration process to allow regular releases of new detection capabilities and features. Tenable recommends that you plan an Internet access to upgrade Tenable Identity Exposure regularly.

Network Protocols

Specific network protocols (such as Syslog, SMTP or HTTP) allow Tenable Identity Exposure to offer native alerting features, the ability to design specific analysis flows bound to a Security Information and Event Management (SIEM) platform, and a REST API that can integrate into a cybersecurity ecosystem.

Tenable Identity Exposure Web Portal Requirements

Tenable Identity Exposure does not require any specific configuration or plugin from client browsers.

Supported Internet Browsers

You must use the most recent version of your supported web browser.

Supported Web Browsers including minimum version	
Microsoft	Edge version 38.14393 or Internet Explorer 11
Google	Chrome version 56.0.2924
Mozilla	Firefox version 52.7.3
Apple	Safari version 11.0

TLS Server Certificate

Tenable Identity Exposure uses SSL/TLS encryption mechanism to access its application.

Tenable strongly recommends using a valid certificate which you provide during installation.

Supported TLS configuration and version

- TLS 1.1 to TLS 1.3
- Self-signed certificate from Tenable
- Certificate issued from your private PKI
- Alternative TLS certificate

Recommended TLS configuration and version

- TLS 1.2
- Certificate issued from your private PKI

TLS certificate update

If you need to change your TLS certificates outside of an upgrade, you can update the CRT and key files under `Tenable\Tenable.ad\Certificates` and restart the services.

Tenable Vulnerability Management (Formerly Tenable.io)

This section includes:

- Tenable Vulnerability Management System Requirements
- Tenable Container Security Requirements
- Container Security Scanner System Requirements

Tenable Vulnerability Management System Requirements

Display Settings

Minimum screen resolution: 1440 x 1024

Supported Browsers

Tenable Vulnerability Management supports the latest versions of the following browsers.

Note: Before reporting issues with Tenable Vulnerability Management, ensure your browser is up to date.

- Google Chrome
- Apple Safari
- Mozilla Firefox
- Microsoft Edge

Note: Tenable Vulnerability Management is not supported on mobile browsers.

Tenable Container Security Requirements

You can access Tenable Container Security from any machine that meets the System Requirements described in the *Tenable Vulnerability Management User Guide*.

Supported Container Image Formats

Tenable Container Security supports the following image formats:

Import and Scan Method	Supported Image Types
Push a Container Image to Tenable Container Security	Docker images
Configure Connectors to Import and Scan Images	Docker images
Configure and Run the Container Security Scanner	• Docker images • Open Containers Initiative (OCI) images

Supported Registries

The container registries that Tenable Container Security supports depends on the method you use to import and scan images.

Tenable tests and verifies successful import and scanning for the following registries:

Import and Scan Method	Supported Image Types
Push a Container Image to Tenable Container Security	Docker registry
Configure Connectors to Import and Scan Images	• Amazon Web Service (AWS) Elastic Container Registry (ECR) • JFrog Artifactory registry • Docker registry
Configure and Run the Container	• Amazon Web Service (AWS) Elastic Con-

Security Scanner	tainer Registry (ECR) • Azure Container registry • Docker registry • Docker Hub registry • Google Cloud Platform (GCP) Google Container Registry (GCR) • Harbor registry • JFrog Artifactory registry • Nexus Repository Manager registry • Red Hat OpenShift Container Platform registry • Red Hat Quay Container registry

Note: Tenable Container Security supports importing and scanning from tested and verified registries that are compatible with Docker Registry API version 2.0.
If you choose to import and scan images from registries that have not been tested and verified, Tenable Support cannot assist with your configurations.

Port Requirements

The machine where you run Tenable Container Security must allow outbound traffic to TCP port 443 for communications with the `cloud.tenable.com` server.

Container Security Scanner System Requirements

The machine where you want to run the Tenable Container Security Scanner must meet the following requirements:

Software and Hardware Requirements

Deployment Type	Software Requirements	RAM	Temporary Storage	CPU
Local	Able to run Linux containers	2 GB	15 GB	64-bit multi-core, x86 compatible

Internet

The machine where you want to run the Container Security Scanner must have access when you download and run the scanner.

SSL Certificate Requirements

If the registry that hosts your images requires the HTTPS protocol, you must have an SSL certificate signed by a trusted Certificate Authority (CA) installed on the registry. Refer to your registry's documentation for installing an SSL certificate.

Mozilla's CA Certificate Store is the Tenable Container Security Scanner's trusted certificate authority.

Note: If you want the Container Security Scanner to scan the registry without verifying that a trusted CA signed the certificate, you must include the `ALLOW_INSECURE_SSL_REGISTRY` variable when you run the scanner. For more information, see Environment Variables in the *Tenable Container Security User Guide*.

Tenable Web App Scanning Hardware Requirements

Scenario	Hardware Recommendations
Tenable Web App Scanning Scanning up to 4 concurrent web applications	**CPU:** (4) 2 GHz cores **Core Ram:** 16GB RAM **Hard Drive:** 25GB

Tenable OT Security (Formerly Tenable.ot)

For information about Tenable OT Security hardware specifications and requirements, see the Tenable OT Security Physical Hardware Data Sheet on the Tenable Downloads site (requires login).

For Tenable Core-specific requirements when running Tenable Core + Tenable OT Security, see the Tenable Core + Tenable.ot User Guide.

Tenable.sc (Formerly Tenable.sc)

For more information, see:

- Tenable.sc Environment Requirements
- Tenable.sc Cloud Requirements
- Tenable.sc Software Requirements
- Tenable.sc Licensing Requirements

Tenable.sc Environment Requirements

You can run Tenable.sc on hardware, with or without Tenable Core. For more information about Tenable Core, see the Tenable Core User Guide.

Note: Tenable strongly discourages running Tenable.sc or Tenable Core + Tenable.sc in an environment shared with other Tenable applications.

Storage Requirements

Tenable recommends installing Tenable.sc on direct-attached storage (DAS) devices (or storage area networks [SANs], if necessary) with a storage latency of 10 milliseconds or less.

Tenable does not support installing Tenable.sc on network-attached storage (NAS).

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 cards will be heavily based on the former. Disk space requirements will vary depending on usage based on the amount and length of time data is stored on the system.

An important consideration is that Tenable.sc can be configured to save a snapshot of vulnerability archives each day. In addition, the size of the vulnerability data stored by Tenable.sc depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than Open Port plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 2GHz cores	8 GB RAM	90 days: 125 GB 180 days: 250 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 450 GB 180 days: 900 GB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 1.2 TB 180 days: 2.4 TB
100,000 active IPs	32 3GHz cores	64 GB RAM	90 days: 4.5 TB 180 days: 9 TB

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

# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 2GHz cores	8 GB RAM	90 days: 225 GB 180 days: 450 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 900 GB 180 days: 1.8 TB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 2.25 TB 180 days: 4.5 TB
100,000 active IPs	32 3GHz cores	128 GB RAM	90 days: 9 TB 180 days: 18 TB

Disk Partition Requirements

Tenable.sc installs into `/opt/sc`. Tenable highly recommends that you create the `/opt` directory on a separate disk partition. If you want to increase performance, consider using two disks: one for the operating system and one for the system deployed to `/opt`.

Tenable strongly recommends using high performance disks. Tenable.sc is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance.

If required disk space exists outside of the `/opt` file system, mount the desired target directory using the command `mount --bind <olddir> <newdir>`. Make sure that the file system is automatically mounted on reboot by editing the `/etc/fstab` file appropriately.

Note: Tenable.sc does not support using symbolic links for `/opt/sc/`. You can use symbolic links within `/opt/sc/` subdirectories if instructed by Tenable.sc documentation or Tenable Support.

Deploying Tenable.sc on a server configured with RAID disks can also 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 1 million managed vulnerabilities moved from a few seconds to less than a second.

Network Interface Requirements

You can install Tenable.sc in externally connected or air-gapped environments. For more information about special considerations for air-gapped environments, see Considerations for Air-Gapped Environments.

Gigabit or faster network cards are recommended for use on the Tenable.sc server. This is to increase the overall performance of web sessions, emails, Tenable Log Correlation Engine queries, and other network activities.

Tenable.sc Cloud Requirements

The primary method to deploy Tenable.sc in a cloud environment is with Tenable Core + Tenable.sc. For more information, see the Tenable Core User Guide.

However, you can install Tenable.sc in vendor-supported version of your cloud environment that meets the operating system requirements to run Tenable.sc.

The following guidelines can help you install Tenable.sc in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment or an Azure Virtual Machine (Azure Virtual Image) cloud-based environment, but they do not cover all deployment scenarios or cloud environments. For assistance with a different cloud environment, contact Tenable Professional Services.

- Supported Amazon EC2 Instance Types
- Supported Amazon Machine Images (AMIs)
- Supported Azure Instance Types
- Supported Azure Machine Images

Supported Amazon EC2 Instance Types

You can install Tenable.sc in an Amazon Elastic Compute Cloud (Amazon EC2) cloud-based environment that meets all of the following requirements.

Tenable.sc uses a balance of networking and compute resources and requires persistent storage for proper operation. To meet these requirements, Tenable supports installing Tenable.sc on M5 instances with General Purpose SSD (gp2) EBS storage.

Tenable recommends the following Amazon EC2 instance types based on your Tenable.sc deployment size.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.2xlarge	90 days: 125 GB

		180 days: 250 GB
2,501 to 10,000	m5.4xlarge	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000	m5.8xlarge	90 days: 1.2 TB 180 days: 2.4 TB
25,001 to 50,000	m5.12xlarge	90 days: 4.5 TB 180 days: 9 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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

# of Hosts Managed by Tenable.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	m5.4xlarge	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000	m5.8xlarge	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000	m5.8xlarge	90 days: 2.25 TB 180 days: 4.5 TB
25,001 to 50,000	m5.12xlarge	90 days: 9 TB 180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

Supported Amazon Machine Images (AMIs)

Tenable provides an AMI for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Amazon Marketplace AMI for Tenable.sc without Tenable Core:

AMI	Required Configuration Changes
CentOS 7 (x86_64) - with Updates HVM	• This AMI does not include Java, but Tenable.sc requires OpenJDK or the Oracle Java JRE to export PDF reports. You must install OpenJDK or the Oracle Java JRE onto your AMI before hosting Tenable.sc. For more information, see Dependencies. • This AMI configures an SELinux enforcing mode policy, which requires customization to be compatible with Tenable.sc. You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc. • You must confirm this AMI meets all other standard requirements for operating systems. For more information, see Operating System Requirements.

Supported Azure Instance Types

You can install Tenable.sc in an Azure Virtual Machine (Azure Virtual Image) cloud-based environment that meets all of the following requirements.

Tenable recommends the following virtual machine instance types based on your Tenable.sc deployment size. You may need to increase the storage allocated to the virtual machine instance depending on usage.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable.sc	Virtual Machine Instance	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 125 GB

		180 days: 250 GB
2,501 to 10,000	D4V2	90 days: 450 GB 180 days: 900 GB
10,001 to 25,000	F16	90 days: 1.2 TB 180 days: 2.4 TB
25,001 to 50,000	F32SV2	90 days: 4.5 TB 180 days: 9 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

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

# of Hosts Managed by Tenable.sc	EC2 Instance Type	Disk Space Used for Vulnerability Trending
1 to 2,500	D3V2	90 days: 225 GB 180 days: 450 GB
2,501 to 10,000	D4V2	90 days: 900 GB 180 days: 1.8 TB
10,001 to 25,000	F16	90 days: 2.25 TB 180 days: 4.5 TB
25,001 to 50,000	D32SV3	90 days: 9 TB 180 days: 18 TB
50,001 or more	For assistance with large enterprise deployments greater than 50,000 active IP addresses, contact your Tenable representative.	

Supported Azure Machine Images

Tenable provides an Azure image for Tenable Core, but not for other cloud deployments without Tenable Core. Tenable supports using the following Azure image for Tenable.sc:

AMI	Required Configuration Changes
CIS CentOS Linux 7 Benchmark L1	• This image does not include Java, but Tenable.sc requires OpenJDK or the Oracle Java JRE to export PDF reports. You must install OpenJDK or the Oracle Java JRE onto your image before hosting Tenable.sc. For more information, see Dependencies. • This image configures an SELinux enforcing mode policy, which requires customization to be compatible with Tenable.sc. You must use the SELinux `sealert` tool to identify errors and solutions. For more information, see Customize SELinux Enforcing Mode Policies for Tenable.sc. • You must confirm this image meets all other standard requirements for operating systems. For more information, see Operating System Requirements.

Tenable.sc Software Requirements

All Tenable.sc versions require an active Tenable.sc license and OpenJDK or Oracle Java JRE. Operating system requirements depend on your Tenable.sc version:

Tenable.sc Version	Operating System Requirements
6.0.0 and later	• Red Hat Enterprise Linux 7 (RHEL 7), 64-bit • Red Hat Enterprise Linux 8 (RHEL 8), 64-bit • Red Hat Enterprise Linux 9 (RHEL 9), 64-bit • CentOS 7, 64-bit • Oracle Linux 8, 64-bit • Oracle Linux 9, 64-bit
5.20.x to 5.23.x	• Red Hat Enterprise Linux 7 (RHEL 7), 64-bit • Red Hat Enterprise Linux 8 (RHEL 8), 64-bit • CentOS 7, 64-bit • Oracle Linux 8, 64-bit
5.19.1	• Red Hat Enterprise Linux 7 (RHEL 7), 64-bit • Red Hat Enterprise Linux 8 (RHEL 8), 64-bit • CentOS 7, 64-bit • Oracle Linux 8, 64-bit
5.17.x to 5.19.0	• Red Hat Enterprise Linux 7 (RHEL 7), 64-bit • Red Hat Enterprise Linux 8 (RHEL 8), 64-bit • CentOS 7, 64-bit
5.12.x to 5.16.x	• Red Hat Enterprise Linux 6 (RHEL 6), 64-bit • Red Hat Enterprise Linux 7 (RHEL 7), 64-bit • CentOS 6, 64-bit

	• CentOS 7, 64-bit

SELinux policy configuration is supported by Tenable in a “Permissive” mode.

Tip: Other SELinux modes are known to work, but the required configuration varies based on policies and custom configurations that may be in place on-site. It is strongly recommended that SELinux implementation configurations are tested prior to deployment on a live network.

Dependencies

Note: Either OpenJDK or the Oracle Java JRE along with their accompanying dependencies must be installed on the system along with any additional Java installations removed for reporting to function properly.

Note: If you are running Tenable.sc 5.20.0, you must upgrade pyTenable to version 1.4.2 or later.

Note: Tenable does not recommend forcing the installation without all required dependencies. If your version of Red Hat or CentOS is missing certain dependencies, it will cause problems that are not readily apparent with a wide variety of functions. Tenable Support has observed different types of failure modes for Tenable.sc when dependencies are missing.

Note: To run Tenable.sc 6.0.0, you must install binutils and initscripts. If you try to migrate from an earlier version of Tenable.sc to Tenable.sc 6.0.0 on a system that does not have binutils or initscripts installed, the migration will fail.

All dependencies must be installed on the system prior to installing the Tenable.sc package. While they are not all required by the installation RPM file, some functionality of Tenable.sc may not work properly if the packages are not installed.

Note: Tenable recommends using the latest stable production version of each package.

Tenable.sc Licensing Requirements

Tenable.sc requires a license key and a maintenance code, which may be purchased directly from Tenable Network Security or via a purchase order through Authorized Enterprise Partners. The license key and maintenance code will be used when installing and configuring your copy of Tenable.sc.

Tenable.sc is licensed by the total number of active IP addresses it manages and the hostname of the system on which it is installed. For example, a customer can purchase a 500 IP Tenable.sc license for the hostname of "security". This key allows that particular server to scan several networks, but as soon as 500 IP addresses are discovered, the license limit becomes active. There is no licensing limit to the number of Tenable Nessus installations that can be deployed with Tenable.sc.

You will need to provide the hostname of the machine on which Tenable.sc will be installed to licenses@tenable.com or on the Tenable Community site, as described in the Tenable Community Guide. This can be obtained by entering the "hostname" command at a system shell prompt.

For more information about license counts and adding licenses to Tenable.sc, see Licenses in the *Tenable.sc User Guide*.

Tenable.sc Plus

The Tenable.sc Plus platform provides combined Tenable products, which includes licensing for Tenable Nessus, the Tenable Nessus Network Monitor, and a Tenable Log Correlation Engine server that are all managed by a Tenable.sc installation. This provides a comprehensive security platform across your IT environment.

Tenable.sc Plus may be purchased directly from Tenable Network Security or via a purchase order through Authorized Enterprise Partners. All license keys and Activation Codes are received from Tenable, and are used when installing and configuring the various Tenable.sc Plus components. There is no licensing limit to the number of Nessus and Tenable Nessus Network Monitor installations that can be deployed with Tenable.sc Plus.

Please see the Tenable Nessus, Tenable Nessus Network Monitor, and Tenable Log Correlation Engine requirements for more information on how each component is licensed for a Tenable.sc Plus purchase.

Tenable Core

This section includes requirements for the following Tenable Core product configurations:

- Tenable Core + Tenable Nessus
- Tenable Core + Tenable Nessus Network Monitor
- Tenable Core + Tenable.sc
- Tenable Core + Tenable Web App Scanning
- Tenable Core + Tenable OT Security

Tenable Core + Tenable Nessus

To install and run Tenable Core + Tenable Nessus, your system must meet requirements established for Tenable Nessus and Tenable Core.

- Tenable Nessus — see below
- Tenable Core — see the Tenable Core + Nessus User Guide

Tenable Core + Tenable Nessus Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus deployments include raw network speed, the size of the network being monitored, and the Tenable Nessus configuration.

Tenable Nessus Scanners and Tenable Nessus Professional Hardware Requirements

Note: The Tenable Core **Disk space** requirement identifies the need for 30 GB of disk space, but this does not include additional space for the OS, etc. which can bring the total to 82 GB for the virtual machine itself.

Scenario	Minimum Recommended Hardware
Scanning up to 50,000 hosts per scan	**CPU:** 4 2GHz cores **Memory:** 4 GB RAM (8 GB RAM recommended) **Disk space:** 30 GB, not including space used by the host operating system **Note:** Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.
Scanning more than 50,000 hosts per scan	**CPU:** 8 2GHz cores **Memory:** 8 GB RAM (16 GB RAM recommended) **Disk space:** 30 GB, not including space used by the host operating system

Scenario	Minimum Recommended Hardware
	Note: Your usage (e.g., scan results, plugin updates, and logs) increases the amount of disk space needed over time.

Tenable Nessus Manager Hardware Requirements

Scenario	Minimum Recommended Hardware
Nessus Manager with 0-10,000 agents	**CPU**: 4 2GHz cores **Memory:** 16 GB RAM **Disk space:** 5 GB per 5,000 agents per concurrent scan **Note:** Scan results and plugin updates require more disk space over time.
Nessus Manager with 10,001-20,000 agents	**CPU:** 8 2GHz cores **Memory:** 32 GB RAM **Disk space:** 5 GB per 5,000 agents per concurrent scan **Note:** Scan results and plugin updates require more disk space over time. **Note:** Engage with your Tenable representative for large deployments.

Tenable Nessus Supported Browsers

Nessus supports the following browsers:

- Google Chrome (76+)
- Apple Safari (10+)
- Mozilla Firefox (50+)
- Microsoft Edge (102+)

Tenable Core + Tenable Nessus Network Monitor

To install and run Tenable Core + Tenable Nessus Network Monitor, your system must meet requirements established for Tenable Nessus Network Monitor and Tenable Core.

- Tenable Nessus Network Monitor — see below
- Tenable Core — see the Tenable Core + Nessus Network Monitor User Guide

Tenable Core + Tenable Nessus Network Monitor Hardware Requirements

Enterprise networks can vary in performance, capacity, protocols, and overall activity. Resource requirements to consider for Tenable Nessus Network Monitor deployments include raw network speed, the size of the network being monitored, and the configuration of Tenable Nessus Network Monitor.

The following chart outlines some basic hardware requirements for operating Tenable Nessus Network Monitor:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	Tenable Nessus Network Monitor managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	2 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor managing more than 50,000 hosts **	4 GB RAM (8 GB RAM recommended)	4 2GHz cores	20 GB HDD minimum
	Tenable Nessus Network Monitor running in High	16 GB RAM (HugePages memory: 2 GB)	10 2GHz cores with hyper-threading enabled	20 GB HDD minimum

Version	Installation scenario	RAM	Processor	Hard Disk
	Performance mode			

*The ability to monitor a given number of hosts depends on the bandwidth, memory, and processing power available to the system running Tenable Nessus Network Monitor.

**For optimal data collection, Tenable Nessus Network Monitor must be connected to the network segment via a hub, spanned port, or network tap to have a full, continuous view of network traffic.

Note: Research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers. Tenable Nessus Network Monitor supports VMware's vmxnet3 driver.

High Performance Mode

To run Tenable Nessus Network Monitor in High Performance mode, a minimum of two of the following types of Intel NICs are required; one as a management interface and at least one as a monitoring interface:

- e1000 (82540, 82545, 82546)
- e1000e (82571, 82574, 82583, ICH8.ICH10, PCH.PCH2)
- igb (82575, 82576, 82580, I210, I211, I350, I354, DH89xx)
- ixgbe (82598, 82599, X540, X550)
- i40e (X710, XL710)
- NT40A01-4x1

Tenable Core + Tenable.sc

To install and run Tenable Core + Tenable.sc, your system must meet requirements established for Tenable.sc and Tenable Core.

- Tenable.sc — see below
- Tenable Core — see the Tenable Core + Tenable.sc User Guide

Tenable Core + Tenable.sc Hardware Requirements

You can run Tenable.sc on hardware, with or without Tenable Core. For more information about Tenable Core, see the Tenable Core User Guide.

Note: Tenable strongly discourages running Tenable.sc or Tenable Core + Tenable.sc in an environment shared with other Tenable applications.

Storage Requirements

Tenable recommends installing Tenable.sc on direct-attached storage (DAS) devices (or storage area networks [SANs], if necessary) with a storage latency of 10 milliseconds or less.

Tenable does not support installing Tenable.sc on network-attached storage (NAS).

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 cards will be heavily based on the former. Disk space requirements will vary depending on usage based on the amount and length of time data is stored on the system.

An important consideration is that Tenable.sc can be configured to save a snapshot of vulnerability archives each day. In addition, the size of the vulnerability data stored by Tenable.sc depends on the number and types of vulnerabilities, not just the number of hosts. For example, 100 hosts with 100 vulnerabilities each could consume as much data as 1,000 hosts with 10 vulnerabilities each. In addition, the output for vulnerability check plugins that do directory listings, etc. is much larger than Open Port plugins from discovery scans.

For networks of 35,000 to 50,000 hosts, Tenable has encountered data sizes of up to 25 GB. That number is based on storage of 50,000 hosts and approximately 500 KB per host.

Additionally, during active scanning sessions, large scans and multiple smaller scans have been reported to consume as much as 150 GB of disk space as results are acquired. Once a scan has completed and its results are imported, that disk space is freed up.

Requirements When Running Basic Network Scans + Local Checks

# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 2GHz cores	8 GB RAM	90 days: 125 GB 180 days: 250 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 450 GB 180 days: 900 GB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 1.2 TB 180 days: 2.4 TB
100,000 active IPs	32 3GHz cores	64 GB RAM	90 days: 4.5 TB 180 days: 9 TB

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

# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
2,500 active IPs	4 2GHz cores	8 GB RAM	90 days: 225 GB 180 days: 450 GB
10,000 active IPs	8 3GHz cores	16 GB RAM	90 days: 900 GB 180 days: 1.8 TB
25,000 active IPs	16 3GHz cores	32 GB RAM	90 days: 2.25 TB 180 days: 4.5 TB

# of Hosts Managed by Tenable.sc	CPU Cores	Memory	Disk Space used for Vulnerability Trending
100,000 active IPs	32 3GHz cores	128 GB RAM	90 days: 9 TB 180 days: 18 TB

Disk Partition Requirements

Tenable.sc installs into `/opt/sc`. Tenable highly recommends that you create the `/opt` directory on a separate disk partition. If you want to increase performance, consider using two disks: one for the operating system and one for the system deployed to `/opt`.

Tenable strongly recommends using high performance disks. Tenable.sc is a disk-intensive application and using disks with high read/write speeds, such as SSDs, results in the best performance.

If required disk space exists outside of the `/opt` file system, mount the desired target directory using the command `mount --bind <olddir> <newdir>`. Make sure that the file system is automatically mounted on reboot by editing the `/etc/fstab` file appropriately.

Note: Tenable.sc does not support using symbolic links for `/opt/sc/`. You can use symbolic links within `/opt/sc/` subdirectories if instructed by Tenable.sc documentation or Tenable Support.

Deploying Tenable.sc on a server configured with RAID disks can also 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 1 million managed vulnerabilities moved from a few seconds to less than a second.

Network Interface Requirements

You can install Tenable.sc in externally connected or air-gapped environments. For more information about special considerations for air-gapped environments, see Considerations for Air-Gapped Environments.

Gigabit or faster network cards are recommended for use on the Tenable.sc server. This is to increase the overall performance of web sessions, emails, Tenable Log Correlation Engine queries, and other network activities.

Tenable Core + Tenable Web App Scanning

To install and run Tenable Core + Tenable Web App Scanning, your system must meet requirements established for Tenable Web App Scanning and Tenable Core.

- Tenable Web App Scanning — see below
- Tenable Core — see the Tenable Core + Tenable Web App Scanning User Guide

Tenable Core + Tenable Web App Scanning Hardware Requirements

Scenario	Hardware Recommendations
Tenable Web App Scanning Scanning up to 4 concurrent web applications	**CPU:** (4) 2 GHz cores **Core Ram:** 16GB RAM **Hard Drive:** 25GB

Tenable Core + Tenable OT Security

To install and run Tenable Core + Tenable OT Security, your system must meet requirements established for Tenable OT Security and Tenable Core.

- Tenable OT Security — see the Tenable OT Security Physical Hardware Data Sheet on the Tenable Downloads site (requires login)
- Tenable Core — see the Tenable Core + Tenable.ot User Guide