Tenable General Requirements

Last Revised: October 02, 2018

Introduction

This document provides prerequisite information about the hardware, software, and licensing requirements to support a deployment of Tenable products. The goal is to enable Tenable customers to be prepared for product installation. It includes general requirements for the following products:

- Tenable.io
- Nessus
- SecurityCenter
- NNM
- Industrial Security
- LCE

Tenable.io

This section includes:

- Tenable.io System Requirements
- Tenable.io On-prem Environments
- Tenable.io On-prem Licensing Requirements
- Tenable.io WAS Hardware Requirements

Tenable.io System Requirements

Display Settings

Minimum screen resolution: 1440 x 1024

Supported Browsers

- Google Chrome (40+)
- Apple Safari (8+)
- Mozilla Firefox (38+)
- Internet Explorer (11+)

Tenable.io On-prem Environments

Instead of hardware requirements, Tenable provides a transparent look at successful environments where on-prem has been tested. Consider the tested environments below and customize your environment depending on the needs of your organization.

Note: The Small asset size environment is the minimum supported environment for deploying Tenable.io on-prem

Number of Assets	Tested Environment
Small (25,000 - 50,000)	**Processor:** 2 x Intel Xeon E5-2620v4. **Memory:** 4 x 32GB RAM (128GB). **Disk:** 1.5TB usable capacity. For more information, see Raid Controller Guidelines, Disk Space Usage Guidelines, and Disk Speed Guidelines. **Network:** 1 x 1GB.
Medium (50,001 - 75,000)	**Processor:** 2 x Intel Xeon E5-2650v4. **Memory:** 8 x 32GB RAM (256GB). **Disk:** 1.5TB usable capacity). For more information, see Raid Controller Guidelines, Disk Space Usage Guidelines, and Disk Speed Guidelines. **Network:** 1 x 1GB.
Large (75,001 - 100,000)	**Processor:** 2 x Intel Xeon E5-2699v4. **Memory:** 8 x 32GB RAM (256GB). **Disk:** 1.5TB usable capacity. For more information, see Raid Controller Guidelines, Disk Space Usage Guidelines, and Disk Speed Guidelines. **Network:** 1 x 1GB.

Raid Controller Guidelines

Your RAID controller must have Write-Back cache mode enabled and at least 1GB of RAID controller cache, protected by an integrated battery backup unit (BBU).

Disk Space Usage Guidelines

You may want to increase your available disk space depending on your number of assets and expected scan frequency.

On-prem monitors your disk space usage and automatically shuts down the Tenable.io interface if your disk space usage exceeds 90% capacity on a filesystem. After automatic shutdown, power down your server and add disk space. Then, power up the hardware and resize the filesystem.

> **Note:** The following guidelines are based on average-sized scan results. If your scan results are smaller or larger than average, your actual usage varies.

Number of Assets	Disk Space Used if Scanning Daily	Disk Space Used if Scanning Weekly	Disk Space Used if Scanning Monthly
25,000	10950 GB per year	1560 GB per year	360 GB per year
50,000	27375 GB per year	3900 GB per year	900 GB per year
100,000	54750 GB per year	7800 GB per year	1800 GB per year

Disk Speed Guidelines

Tenable runs hardware tests on environments meeting the following disk speeds.

Number of Assets	Maximum Read	Maximum Write
25,000	608 IOPS	204 IOPS
50,000	1703 IOPS	568 IOPS
75,000	1945 IOPS	650 IOPS
100,000	38633 IOPS	12865 IOPS

Tenable recommends estimating your random read and write access performance by running a Flexible I/O workload test:

```
./fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1 --name-
e=test --filename=test --bs=4k --iodepth=64 --size=8G --readwrite=randrw -
-rwmixread=75
```

Browser Requirements

For more information about on-prem configuration interface browser requirements, see http://-cockpit-project.org/running.

Internet Access Requirements

Your Tenable.io on-prem deployment requires access to the internet, with or without going through a proxy server. On-prem performs best with network speeds of 100 Mbps or above.

Network Requirements

Your Tenable.io on-prem deployment reserves 10.96.0.0/20 and 10.32.0.0/20 for its internal networks. If you want a device to communicate with on-prem, you must place the device outside the 10.96.0.0/20 and 10.32.0.0/20 IP address blocks.

Port Access Requirements

Your Tenable.io on-prem deployment requires access to specific ports for inbound and outbound traffic.

Inbound Traffic

Port	Traffic
22	All SSH connections.
443	The Tenable.io interface and NNM, Nessus scanner, and Nessus agent connections.
3000	The Grafana interface, if enabled.
8000	The Tenable.io on-prem configuration interface.
8900	The Kibana interface, if enabled.

Outbound Traffic

Port	Traffic
22	All SSH connections.
443	The `appliance.cloud.tenable.com` server (for system updates) and the `plugins.nessus.org` server (for activation and plugin updates).

Tenable.io On-prem Licensing Requirements

Tenable.io on-prem requires a Tenable-provided license key. Tenable on-prem licenses are specific to your deployment size and Tenable.io product selections:

- the total number of assets you intend to manage.
- the Tenable.io products you intend to configure.

For information about the on-prem licensing process, see the Tenable.io On-prem User Guide.

Tenable.io Web Application Scanning Hardware Requirements

Scenario	Hardware Recommendations
WAS Scanning up to 4 web applications (maximum allowed)	**CPU:** 4 dual core, 2 GHz **Core Ram:** 16GB RAM **Hard Drive:** 25GB

Nessus

This section includes:

- Nessus Licensing Requirements
- Nessus Scanners
    - Nessus Scanner Hardware Requirements
    - Nessus Scanner Software Requirements
- Nessus Agents
    - Nessus Agent Hardware Requirements
    - Nessus Agent Software Requirements

Nessus Licensing Requirements

Nessus is available to operate either as a subscription or managed by SecurityCenter. 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 Tenable's 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.

> If you are using SecurityCenter to manage your Nessus scanners, the Activation Code and plugin updates are managed from SecurityCenter. Nessus needs to be started to be able to communicate with SecurityCenter, 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 SecurityCenter), 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:

- Nessus Scanner Hardware Requirements
- Nessus Scanner Software Requirements

Nessus Scanner Hardware Requirements

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

Version	Installation Scenario	RAM	Processor	Hard Disk Space
6.5.x and later	Nessus scanning up to 50,000 hosts	4 GB (8 GB recommended)	4 2GHz cores	30 GB
	Nessus scanning more than 50,000 hosts	8 GB (16 GB recommended)	8 2GHz cores	30 GB (Additional space may be needed for reporting)
	Nessus Manager with 0-10,000 agents	16 GB	4 2GHz cores	30 GB (Additional space may be needed for reporting)
	Nessus Manager with up to 20,000 agents	64 GB	8 2GHz cores	30 GB (Additional space may be needed for reporting)
Previous Versions				
6.4.x	Scanning smaller networks	2 GB (4 GB recommended)	1 dual-core, 2GHz Intel CPU (dual-core Intel® for Mac OSX)	30 GB
	Scanning large networks processing audit trails and .pdf files report generation	3 - 4 GB (8 GB recommended)	1 dual-core, 2GHz Intel CPU (2 dual-core recommended)	30 GB

Note: Engage with your Tenable representative for large Nessus Agent deployments.

Virtual Machines

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

Nessus Scanner Software Requirements

Nessus Scanners support Mac, Linux, and Windows operating systems.

Version	Operating System	Supported Versions
7.0	Linux	Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - i386 Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - AMD64 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 6 / CentOS 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 FreeBSD 10 and 11 - AMD64 Fedora 24 and 25 - x86_64 SUSE 11 and 12 Enterprise - i586 SUSE 11 and 12 Enterprise - x86_64 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64
	Windows	Windows 7, 8, and 10 - i386 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64 **Tip:** Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus to not perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems. For increased performance and scan reliability when installing on a Windows platform, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.

Version	Operating System	Supported Versions
	Mac OS X	Mac OS X 10.10, 10.11, 10.12, and 10.13 - x86-64
Previous Versions		
6.11	Linux	Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - i386 Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - AMD64 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 6 / CentOS 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 FreeBSD 10 and 11 - AMD64 Fedora 24 and 25 - x86_64 SUSE 11 and 12 Enterprise - i586 SUSE 11 and 12 Enterprise - x86_64 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386 Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64
	Windows	Windows 7, 8, and 10 - i386 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64 **Tip:** Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus to not perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems. For increased performance and scan reliability when installing on a Windows platform, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.

Version	Operating System	Supported Versions
	Mac OS X	Mac OS X 10.10, 10.11, and 10.12 - x86-64
6.9 and 6.10	Linux	Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - i386 Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - AMD64 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 6 / CentOS 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 FreeBSD 10 - AMD64 Fedora 20 and 21 - x86_64 SUSE 10.0 Enterprise - x86_64 SUSE 11 Enterprise - i586 SUSE 11 Enterprise - x86_64 Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04- i386 Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64
	Windows	Windows 7, 8, and 10 - i386 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64 **Tip:** Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus not to perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems.

Version	Operating System	Supported Versions
		For increased performance and scan reliability when installing on a Windows platform, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.
	Mac OS X	Mac OS X 10.8, 10.9, 10.10, 10.11, and 10.12 - x86-64
6.8 and earlier	Linux	Debian 6, 7, and 8 / Kali Linux 1, and 2 - i386 Debian 6, 7, and 8 / Kali Linux 1 and 2 - AMD64 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64 Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386 Red Hat ES 6 / CentOS 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 FreeBSD 10 - AMD64 Fedora 20 and 21 - x86_64 SUSE 10.0 Enterprise - x86_64 SUSE 11 Enterprise - i586 SUSE 11 Enterprise - x86_64 Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - i386 Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64
	Windows	Windows 7, 8, and 10 - i386 Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, and 10 - x86-64

Version	Operating System	Supported Versions
		Tip: Windows Server 2008 R2's bundled version of Microsoft IE does not interface with a Java installation properly. This causes Nessus to not perform as expected in some situations: Microsoft's policy recommends not using MSIE on server operating systems. For increased performance and scan reliability when installing on a Windows platform, it is highly recommended that Nessus be installed on a server product from the Microsoft Windows family such as Windows Server 2008 R2.
	Mac OS X	Mac OS X 10.8, 10.9, 10.10, and 10.11 - x86-64

Browsers

When using the Nessus user interface, the following browsers are supported.

Version	Supported Browsers
6.11	Google Chrome (50+) Apple Safari (10+) Mozilla Firefox (50+) Internet Explorer (11+)
Previous Versions	
6.10	Google Chrome (50+) Apple Safari (9+) Mozilla Firefox (45+) Internet Explorer (9+)
6.9 and earlier	Google Chrome (24+) Apple Safari (6+) Mozilla Firefox (20+) Internet Explorer (9+)

PDF Reports

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

Oracle Java or OpenJDK must be installed prior to the installation of Nessus.

> **Note:** If Oracle Java or OpenJDK is installed after the Nessus installation, Nessus will need to be reinstalled for the PDF report generation to function.

Nessus Agents

This section includes:

Nessus Agent Hardware Requirements

Nessus Agents are designed to be lightweight and to use only minimal system resources. Generally, a Nessus Agent uses 40 MB of RAM (all pageable). A Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs. However, the Nessus Agent process is a low-priority process and yields the CPU whenever asked.

For more information on Nessus Agent resource usage, refer to Software Footprint and Host System Utilization.

The following table outlines the minimum recommended hardware for operating a Nessus Agent. Nessus Agents can be installed 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	< 1 GB
Disk Speed	15-50 IOPS

Nessus Agent Software Requirements

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

Version	Operating System	Supported Versions
7.1	Linux	Amazon Linux 2015.03, 2015.09, and 2017.09 (64-bit) Debian 6, 7, 8, and 9 / Kali Linux 1, 2017.3 (32-bit) Debian 6, 7, 8, and 9 / Kali Linux 1, 2017.3 (64-bit) Fedora 20, 21, 24, 25, 26, and 27 (64-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) (64-bit) SUSE 11 Enterprise (32-bit) SUSE 11 and 12 Enterprise (64-bit) Ubuntu 9.10, 10.04, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04, and 17.10 (32-bit) Ubuntu 9.10, 10.04, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 16.04, and 17.10 (64-bit)
	Windows	Windows Server 2008, 7, 8, and 10 (32-bit) Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 (64-bit)
	Mac OS X	Mac OS X 10.8 - 10.13

Version	Operating System	Supported Versions
Previous Versions		
7.0	Linux	Debian 7, 8, and 9 (32-bit) Debian 7, 8, and 9 (64-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (64-bit) Fedora 24 and 25 (64-bit) Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 (32-bit) Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 (64-bit)
	Windows	Windows Server 2008, 7, 8, and 10 (32-bit) Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 (64-bit)
	Mac OS X	Mac OS X 10.8 - 10.13
6.11	Linux	Debian 7, 8, and 9 (32-bit) Debian 7, 8, and 9 (64-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (64-bit) Fedora 24 and 25 (64-bit) Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04 , and 16.04 (32-bit) Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04 , and 16.04 (64-bit)
	Windows	Windows 7, 8, and 10 (32-bit)

Version	Operating System	Supported Versions
		Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 (64-bit)
	Mac OS X	Mac OS X 10.8 - 10.13
6.9 and 6.10	Linux	Debian 6, 7, and 8 (32-bit) Debian 6, 7, and 8 (64-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (64-bit) Fedora 20 and 21 (64-bit) Ubuntu 10.04 (32-bit) Ubuntu 10.04 (64-bit) Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (32-bit) Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (64-bit)
	Windows	Windows 7, 8, and 10 (32-bit) Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 (64-bit)
	Mac OS X	Mac OS X 10.8 - 10.12
6.8 and earlier	Linux	Debian 6, 7, and 8 (32-bit) Debian 6, 7, and 8 (64-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable

Version	Operating System	Supported Versions
		Enterprise Kernel) (32-bit) Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (32-bit) Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) (64-bit) Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (64-bit) Fedora 20 and 21 (64-bit) Ubuntu 10.04 (32-bit) Ubuntu 10.04 (64-bit) Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (32-bit) Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 (64-bit)
	Windows	Windows 7, 8, and 10 (32-bit) Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, and 10 (64-bit)
	Mac OS X	Mac OS X 10.8 - 10.11

Software Footprint

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

Agent Footprint on Disk	Total Software Footprint on Disk	RAM Usage While Not Scanning	Average RAM Usage While Scanning/Peak	Network Bandwidth Usage
6.6 MB	450 MB including plugin updates	<10%	45 MB RAM	~1.5 MB/day* Expected to be much higher in normal conditions.

*Assuming only one scan a day with no plugin updates. Used `nethogs` program to collect network usage (sent/received) of `nessusd`. After a single scan that detected 66 vulnerabilities on the agent host, 0.855 MB was sent and received (breakdown: .771 MB sent, .084 MB received). After two total scans, 1.551 MB was sent and 0.204 MB was received. Set to > 1 MB day as the polling for jobs adds up (~0.008 MB per poll).

Host System Utilization

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

Generally, a Nessus Agent uses 40 MB of RAM (all pageable). A Nessus Agent uses almost no CPU while idle, but is designed to use up to 100% of CPU when available during jobs. However, the Nessus Agent process is a low-priority process and yields the CPU whenever asked.

To measure network utilization when uploading results, Tenable monitored Agent uploads into Tenable.io over a 7 day period. Of over 36,000 uploads observed:

- The average size was 1.6 MB.
- The largest size was 37 MB.
- 90% of uploads were 2.2 MB or less.
- 99% of uploads were 5 MB or less.
- Nessus Agent consumes 40 MB of RAM when dormant.
- The Watchdog service consumes 3 MB.
- Plugins consume approximately 300 MB of disk space (varies based on operating system).
- Scan results from Nessus Agents to Nessus Manager and Tenable.io range between 2-3 MB.
- Check-in frequency starts at 30 seconds and is adjusted by Nessus Manager or Tenable.io based on the management system load (number of agents).

SecurityCenter

This section includes:

- SecurityCenter Hardware Requirements
- SecurityCenter Software Requirements
- SecurityCenter Licensing Requirements

SecurityCenter Hardware Requirements

The following hardware recommendations for SecurityCenter 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 following guidance is intended for typical activities of Tenable customers.

SecurityCenter Full Safe + Local Checks

Version	# of Hosts Managed by SecurityCenter	CPU Cores	Memory	Disk Space used for Vuln Trending
5.x	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

SecurityCenter Full Safe + Local Checks + 1 Configuration Audit

Version	# of Hosts Managed by SecurityCenter	CPU Cores	Memory	Disk Space used for Vuln Trending
5.x	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

In addition to the above guidelines, please consider the following suggestions:

- If the Nessus scanner is deployed on the same system as SecurityCenter, there will be less CPU and memory available during scans, causing slower performance. Use multi-core and/or multiple CPU servers to alleviate this. Placing the scanner on a secondary machine will alleviate performance bottlenecks.
- If one or more Passive Vulnerability Scanners are in use, use multi-core and/or multiple CPU servers to increase performance.
- Use the aggregate of the individual software product resource requirements to determine total hardware system requirements.
- If Nessus or PVS is deployed on the same server as SecurityCenter, consider configuring the server with multiple network cards and IP addresses.

SecurityCenter Software Requirements

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

SecurityCenter Version	Operating System Requirements
5.7.0 and later	• Red Hat Enterprise Linux 6 (64-bit) • Red Hat Enterprise Linux 7 (64-bit) • CentOS 6 (64-bit) • CentOS 7 (64-bit)
5.6.x and earlier	• Red Hat Enterprise Server 5 (64-bit) • Red Hat Enterprise Server 6 (64-bit) • Red Hat Enterprise Server 7 (64-bit) • CentOS 5 (64-bit) • CentOS 6 (64-bit) • CentOS 7 (64-bit)

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

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

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.

Although it is possible to force the installation without all required dependencies, if your version of Red Hat or CentOS is missing certain dependencies, this will cause problems that are not readily apparent with a wide variety of functions. Tenable’s Support team has observed different types of failure modes for SecurityCenter when dependencies to the installation RPM are missing. If you require assistance or guidance in obtaining these dependencies, please contact our Support team at support@tenable.com.

The following programs must be installed on the system prior to installing the SecurityCenter package. While they are not all required by the installation RPM file, some functionality of SecurityCenter may not work properly if the packages are not installed. The packages listed below are among those that are most often not installed by default:

- java-1.7.0-openjdk.x86_64 (or the latest Oracle Java JRE)
- openssh
- expat
- gdbm
- libtool
- libtool-ltdl
- libxml2
- ncurses
- readline
- compat-libstdc++
- libxslt

Using the latest stable production version of each package is recommended.

SecurityCenter Licensing Requirements

SecurityCenter 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 SecurityCenter.

SecurityCenter 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 SecurityCenter 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 Nessus installations that can be deployed with SecurityCenter.

You will need to provide the hostname of the machine on which SecurityCenter will be installed to licenses@tenable.com or within the Activation Codes section of the Tenable Support Portal. This can be obtained by entering the "hostname" command at a system shell prompt. Please see the Nessus section for more information on how to deploy Nessus with SecurityCenter.

For information about uploading SecurityCenter license activation codes, see the SecurityCenter user guide.

SecurityCenter Continuous View (CV)

Tenable's SecurityCenter Continuous View (CV) platform provides combined Tenable products, which includes licensing for Nessus, the Nessus Network Monitor (NNM), and a Log Correlation Engine (LCE) server, that are managed by a SecurityCenter installation. This provides a comprehensive security platform across your IT environment.

SecurityCenter CV 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 SecurityCenter CV components. There is no licensing limit to the number of Nessus and NNM installations that can be deployed with SecurityCenter CV.

Please see the Nessus, Nessus Network Monitor, and Log Correlation Engine sections in this guide for more information on how each component is licensed for a SecurityCenter CV purchase.

NNM

This section includes:

- NNM Hardware Requirements
- NNM Software Requirements
- NNM Licensing Requirements

NNM Hardware Requirements

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

The following chart outlines some basic hardware requirements for operating NNM:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	NNM managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	2 2GHz cores	20 GB HDD minimum
	NNM managing more than 50,000 hosts **	4 GB RAM (8 GB RAM recommended)	4 2GHz cores	20 GB HDD minimum
	NNM running in High Performance mode	16 GB RAM (HugePages memory: 2 GB)	10 CPUs 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 NNM.

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

> **Note:** Please research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers.

High Performance Mode

To run NNM 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)

NNM Software Requirements

Nessus Network Monitor is available for the following platforms:

Version	Software Requirements
5.5+	• Red Hat Linux ES 5 / CentOS 5 64-bit • Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit • Mac OS X 10.9-10.12 64-bit • Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 • 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) : 3.10.0-693cc • RH7/CentOS7 (RH7.5): 3.10.0-862
Previous Versions	
5.2-5.4	• Red Hat Linux ES 5 / CentOS 5 64-bit • Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit • Mac OS X 10.9-10.12 64-bit • Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 • Microsoft Visual C++ 2010 Redistributable Package **High Performance mode only available on:** • RH6/CentOS6 (RH6.0 thrue RH6.9) : 2.6.32-696 • RH7/CentOS7 (RH7.0 thru RH7.4) : 3.10.0-693cc
5.1	• Red Hat Linux ES 5 / CentOS 5 64-bit

Version	Software Requirements
	• Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit • Mac OS X 10.8 and 10.9 64-bit • Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 • Microsoft Visual C++ 2010 Redistributable Package **High Performance mode only available on:** • CentOS 6.x 64-bit • CentOS 7.x 64-bit • Red Hat ES 6.6+ 64-bit • Red Hat ES 7.x 64-bit • Linux kernel version 2.6.34

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 NNM. The following ERSPAN virtual environments are supported for NNM:

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

Tip: Refer to the Configuring Virtual Switches for Use with NNM document for details on configuring your virtual environment.

High Performance Mode

To run NNM 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, NNM 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.

The following virtual environments are supported for running NNM in High Performance mode:

- VMware ESXi/ESX 5.5
- VMXNET3 network adapter
- VMware ESXi/ESX 6.x

NNM Licensing Requirements

NNM Subscription

A NNM subscription Activation Code is available that enables NNM to operate in Standalone mode. This mode enables NNM results to be viewed from an HTML interface enabled on the NNM server.

Activation Code

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

SecurityCenter Continuous View

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

Nessus Cloud

Nessus Cloud pushes plugins down to NNM. The number of NNM deployments is determined by your Nessus Cloud licensing.

High Performance Mode

NNM in High Performance Mode can be licensed in Standalone mode or bundled with SecurityCenter CV.

Industrial Security

This section includes:

- Industrial Security Hardware Requirements
- Industrial Security Software Requirements
- Industrial Security Licensing Requirements

Industrial Security Hardware Requirements

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

The following chart outlines some basic hardware requirements for operating Industrial Security:

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	Industrial Security managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	1 dual-core 2GHz CPU	20 GB HDD minimum.
	Industrial Security managing more than 50,000 hosts **	Memory: 4 GB RAM (8 GB RAM recommended)	1 dual-core 2 GHz CPU (2 dual-core recommended)	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 NNM.

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

Note: Please research your VM software vendor for comparative recommendations, as VMs typically see up to a 30% loss in efficiency compared to dedicated servers.

Industrial Security Software Requirements

Industrial Security is available for the following platforms:

Version	Software Requirements
1.2+	• Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit • Microsoft Windows 8, Server 2012 • Microsoft Windows 8, Server 2016
Previous Versions	
1.0-1.1	• Red Hat Linux ES 6 / CentOS 6 64-bit • Red Hat Linux ES 7 / CentOS 7 64-bit • Microsoft Windows 8, Server 2012

Industrial Security Licensing Requirements

Industrial Security Subscription

A Industrial Security subscription Activation Code is available that enables Industrial Security to operate in Standalone mode. This mode enables Industrial Security results to be viewed from an HTML interface enabled on the Industrial Security server.

Activation Code

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

LCE

This section includes:

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

Log Correlation Engine Hardware Requirements

The following hardware recommendations for LCE 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 LCE 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 LCE server is processing.

Version	Installation scenario	RAM	Processor	Hard disk	Hard disk space
5.x	One LCE server with	16 GB	64-bit, 8 cores	10,000 to 15,000 RPM	2x Licensed storage size

Version	Installation scenario	RAM	Processor	Hard disk	Hard disk space
	Elasticsearch processing less than 5,000 events per second			HD, or SSD of equiv. IOPS capability, in RAID 0/10 configuration	**Note:** To query an archived Elasticsearch database, it will need to be restored. The recommended hard disk space does not include optional archiving of logs that exceed the licensed limit.
	One LCE server with Elasticsearch processing between 5,000 and 20,000 events per second	32 GB	64-bit, 16 cores		
	One LCE server with Elasticsearch processing greater than 20,000 events per second	64 GB or more	64-bit, 24 cores or more		
Previous Versions					
4.4.x through 4.8.x	One LCE server processing less than 5,000 events per second	8 GB	64-bit, 8 cores	10,000 to 15,000 RPM HD, or SSD of equiv. IOPS capability, in RAID 0/10 configuration	1.5x Licensed storage size **Note:** Each LCE will use, on average, 1,000,000 inodes per 1TB of licensed storage size. For more information on hardware requirements for your environment, please review Log Correlation Engine 4.6 High Availability Large Scale Deployment Guide.
	One LCE server processing between 5,000 and 20,000 events	16 GB	64-bit, 16 cores		

Version	Installation scenario	RAM	Processor	Hard disk	Hard disk space
	per second				
	One LCE server processing greater than 20,000 events per second	32 GB or more	64-bit, 24 cores or more		

The LCE 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 LCE interface.

Log Correlation Engine Software Requirements

Version	Software Requirements
5.x	• An active LCE license • RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit • Elasticsearch 2.3.3 to 2.4.6 • Java Runtime Environment (JRE) 1.8 update 20 or later
Previous Versions	
4.4.x through 4.8.x	• An active LCE license • RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit

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

Port	Description
UDP	
162	SNMP
514	Syslog messages
TCP	
601	Reliable syslog service messages
1243	Vulnerability detection (if enabled in SecurityCenter)
6514	Encrypted TCP syslog messages
8836	LCE interface
31300	LCE API

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

LCE Licensing Requirements

LCE 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 LCE and each attached SecurityCenter.

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

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

Tenable Core

When installing Tenable Core, use the hardware requirements for the application with which you're installing it. For example, for Tenable Core + Nessus, use Nessus hardware requirements.

Tenable Core for Nessus

Tenable Core for Nessus Network Monitor