



Tenable General Requirements

Last Revised: February 20, 2018



| | |
|---|-----------|
| Introduction | 4 |
| Tenable.io | 5 |
| Tenable.io System Requirements | 6 |
| Tenable.io On-prem System Requirements | 7 |
| Tenable.io On-prem Licensing Requirements | 10 |
| Nessus | 11 |
| Nessus Licensing Requirements | 12 |
| Nessus Scanners | 13 |
| Nessus Scanner Hardware Requirements | 14 |
| Nessus Scanner Software Requirements | 16 |
| Nessus Agents | 22 |
| Nessus Agent Hardware Requirements | 23 |
| Nessus Agent Software Requirements | 24 |
| SecurityCenter | 27 |
| SecurityCenter Hardware Requirements | 28 |
| SecurityCenter Software Requirements | 30 |
| SecurityCenter Licensing Requirements | 32 |
| NNM | 33 |
| NNM Hardware Requirements | 34 |
| NNM Software Requirements | 36 |
| NNM Licensing Requirements | 39 |
| Industrial Security | 40 |
| Industrial Security Hardware Requirements | 41 |
| Industrial Security Software Requirements | 42 |



| | |
|--|-----------|
| Industrial Security Licensing Requirements | 43 |
| LCE | 44 |
| Log Correlation Engine Hardware Requirements | 45 |
| Log Correlation Engine Software Requirements | 48 |
| LCE Licensing Requirements | 49 |

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 System Requirements](#)
- [Tenable.io On-prem Licensing Requirements](#)

Tenable.io System Requirements

Display Settings

Minimum screen resolution: 1280 x 1024

Supported Browsers

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

Tenable.io On-prem System Requirements

You can deploy Tenable.io on-prem on dedicated hardware using the on-prem ISO. You cannot deploy on-prem in virtual environments.

Hardware Requirements

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 or fewer) | <p>Processor: Intel® Xeon® E5-2620 v4 2.1GHz, 20M Cache, 8.0GT/s QPI, Turbo, HT, 8C/16T (85W) Max Mem 2133MHz (8 cores).</p> <p>Memory: 4 x 16GB RDIMM, 2400MT/s, Dual Rank, x8 Data Width (64 GB).</p> <p>RAID: 1 x PERC H730 RAID Controller, 1GB NV Cache / Raid 5.</p> <p>Disk Space: 4 x Seagate 1TB 7.2K RPM SATA drives. For more information, see Disk Space Usage Guidelines.</p> |
| Medium (25,001 - 50,000) | <p>Processor: 2 x Intel® Xeon® E5-2620 v4 2.1GHz, 20M Cache, 8.0GT/s QPI, Turbo, HT, 8C/16T (85W) Max Mem 2133MHz (16 cores).</p> <p>Memory: 4 x 32GB RDIMM, 2400MT/s, Dual Rank, x4 Data Width (128 GB).</p> <p>RAID: 1 x PERC H730 RAID Controller, 1GB NV Cache / Raid 10.</p> <p>Disk Space: 8 x 1TB 7.2K RPM SATA 6Gbps 2.5in Hot-plug Hard Drive. For more information, see Disk Space Usage Guidelines.</p> <p>Network: 4 x 1GB.</p> |
| Large (50,001 - | <p>Processor: 2 x Intel® Xeon® E5-2650 v4 2.2GHz, 30M Cache, 9.60GT/s QPI, Turbo, HT,</p> |

| | |
|--------------------------------|---|
| 75,000) | <p>12C/24T (105W) Max Mem 2400MHz (24 total cores).</p> <p>Memory: 8 x 32GB RDIMM, 2400MT/s, Dual Rank, x4 Data Width (256 GB).</p> <p>RAID: 1 x PERC H730 RAID Controller, 1GB NV Cache / Raid 10.</p> <p>Disk Space: 6 x 2TB 7.2K RPM NLSAS 12Gbps 512n 2.5in Hot-plug Hard Drive. For more information, see Disk Space Usage Guidelines.</p> <p>Network: 4 x 1GB.</p> |
| Extra Large (75,001 - 100,000) | <p>Processor: 2 x 2 - Intel Xeon E5-2699 v4 2.2GHz, 55M Cache, 9.60GT/s QPI, Turbo, HT, 22C/44T (145W) Max Mem 2400MHz (44 total cores).</p> <p>Memory: 8 x 32GB RDIMM, 2400MT/s, Dual Rank, x4 Data Width (256 GB).</p> <p>RAID: 1 x PERC H330 Integrated RAID Controller.</p> <p>Disk Space: 4 x 480GB Solid State Drive SATA Read Intensive MLC 6Gbps 2.5in Hot-plug Drive, S3520 and 1 x 1TB 7.2K RPM SATA 6Gbps 2.5in Hot-plug Hard Drive, 13G4 x 480 SSD 7200 RPM SATA, 1 x 1TB 7200 RPM SATA. For more information, see Disk Space Usage Guidelines.</p> <p>Network: 4 x 1GB.</p> |

Disk Space Usage Guidelines

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

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 |
|------------------|-----------------------------------|------------------------------------|-------------------------------------|
| 2,000 | 1095 GB per year | 156 GB per year | 36 GB per year |
| 20,000 | 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 |

Browser Requirements

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

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 scanner, 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 |
|------|--|
| 443 | The <code>appliance.cloud.tenable.com</code> server (for system updates) and the <code>plugins.nessus.org</code> 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](#).

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 through 7.0 | Nessus scanning up to 50,000 hosts | 2 GB (4 GB recommended) | 1 dual-core, 2 GHz CPU | 30 GB |
| | Nessus scanning more than 50,000 hosts | 2 GB (8 GB recommended) | 1 dual-core, 2 GHz CPU (2 dual-core recommended) | 30 GB (Additional space may be needed for reporting) |
| | Nessus Manager with up to 10,000 agents | 16 GB | 1 dual-core, 2GHz CPU | 30 GB (Additional space may be needed for reporting) |
| | Nessus Manager with up to 30,000 agents | 64 GB | 1 dual-core, 2GHz CPU | 30 GB (Additional space may be needed for reporting) |
| Previous Versions | | | | |
| 6.4 | 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 report generation. | 3 - 4 GB (8 GB recommended) | 1 dual-core, 2GHz Intel CPU (2 dual-core recommended) | 30 GB |

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 | <p>Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - i386</p> <p>Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - AMD64</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>FreeBSD 10 and 11 - AMD64</p> <p>Fedora 24 and 25 - x86_64</p> <p>SUSE 11 and 12 Enterprise - i586</p> <p>SUSE 11 and 12 Enterprise - x86_64</p> <p>Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386</p> <p>Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64</p> |
| | Windows | <p>Windows 7, 8, and 10 - i386</p> <p>Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64</p> <div style="border: 1px solid green; padding: 10px; margin-top: 10px;"> <p>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.</p> <p>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.</p> </div> |

| 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 | <p>Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - i386</p> <p>Debian 7, 8, and 9 / Kali Linux 1, 2017.1, and Rolling - AMD64</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>FreeBSD 10 and 11 - AMD64</p> <p>Fedora 24 and 25 - x86_64</p> <p>SUSE 11 and 12 Enterprise - i586</p> <p>SUSE 11 and 12 Enterprise - x86_64</p> <p>Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - i386</p> <p>Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64</p> |
| | Windows | <p>Windows 7, 8, and 10 - i386</p> <p>Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>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.</p> <p>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.</p> </div> |

| 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 | <p>Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - i386</p> <p>Debian 6, 7, and 8 / Kali Linux 1, 2, and Rolling - AMD64</p> <p>Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>FreeBSD 10 - AMD64</p> <p>Fedora 20 and 21 - x86_64</p> <p>SUSE 10.0 Enterprise - x86_64</p> <p>SUSE 11 Enterprise - i586</p> <p>SUSE 11 Enterprise - x86_64</p> <p>Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04- i386</p> <p>Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64</p> |
| | Windows | <p>Windows 7, 8, and 10 - i386</p> <p>Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, Server 2016, 7, 8, and 10 - x86-64</p> |

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 |
|-----------------|------------------|---|
| | | <div style="border: 1px solid green; padding: 5px;"> <p>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.</p> </div> |
| | Mac OS X | Mac OS X 10.8, 10.9, 10.10, 10.11, and 10.12 - x86-64 |
| 6.8 and earlier | Linux | <p>Debian 6, 7, and 8 / Kali Linux 1, and 2 - i386</p> <p>Debian 6, 7, and 8 / Kali Linux 1 and 2 - AMD64</p> <p>Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - i386</p> <p>Red Hat ES 6 / CentOS 6 / Oracle Linux 6 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>Red Hat ES 7 / CentOS 7 / Oracle Linux 7 (including Unbreakable Enterprise Kernel) - x86_64</p> <p>FreeBSD 10 - AMD64</p> <p>Fedora 20 and 21 - x86_64</p> <p>SUSE 10.0 Enterprise - x86_64</p> <p>SUSE 11 Enterprise - i586</p> <p>SUSE 11 Enterprise - x86_64</p> <p>Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - i386</p> <p>Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, and 14.04 - AMD64</p> |
| | Windows | <p>Windows 7, 8, and 10 - i386</p> <p>Windows Server 2008, Server 2008 R2*, Server 2012, Server 2012 R2, 7, 8, and 10 - x86-64</p> |

| Version | Operating System | Supported Versions |
|---------|------------------|--|
| | | <p>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.</p> <p>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.</p> |
| | 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 Agent Software Requirements](#)

Nessus Agent Hardware Requirements

The following list 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.

- **Processor:** Intel Dual-core
- **Processor Speed:** 2 GHz
- **RAM:** 2GB (4GB recommended)
- **Disk Space:** 30GB

Nessus Agent Software Requirements

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

| Version | Operating System | Supported Versions |
|-------------------|------------------|---|
| 7.0 | Linux | Debian 7, 8, and 9- i386 Debian 7, 8, and 9 - 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 - x86_64 Fedora 24 and 25 - 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 |
| | Mac OS X | Mac OS X 10.8, 10.9, 10.10, 10.11, 10.12, and 10.13 - x86-64 |
| Previous Versions | | |
| 6.11 | Linux | Debian 7, 8, and 9- i386 Debian 7, 8, and 9 - 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 - x86_64 Fedora 24 and 25 - x86_64 |

| Version | Operating System | Supported Versions | |
|--------------|------------------|---|--|
| | | 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 | |
| | Mac OS X | Mac OS X 10.8, 10.9, 10.10, 10.11, 10.12, and 10.13 - x86-64 | |
| 6.9 and 6.10 | Linux | Debian 6, 7, and 8 - i386 Debian 6, 7, and 8 - 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 - x86_64 Fedora 20 and 21 - x86_64 Ubuntu 10.04 - i386 Ubuntu 10.04 - AMD64 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 |
| | | | Mac OS X |

| Version | Operating System | Supported Versions |
|-----------------|------------------|---|
| 6.8 and earlier | Linux | Debian 6, 7, and 8 - i386 Debian 6, 7, and 8 - 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 - x86_64 Fedora 20 and 21 - x86_64 Ubuntu 10.04 - i386 Ubuntu 10.04 - AMD64 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 |
| | Mac OS X | Mac OS X 10.8, 10.9, 10.10, and 10.11 - x86-64 |

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 | 4 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 | 4 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

| Version | Software Requirements |
|---------|--|
| 5.x | <ul style="list-style-type: none">• An Active SecurityCenter license• OpenJDK or Oracle Java JRE• RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit |

SecurityCenter is available for 64-bit versions of Red Hat Enterprise Linux 5, 6, 7. 64-bit versions of CentOS 5, 6, and 7 are also officially supported. 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) | 1 dual-core 2GHz CPU | 20 GB HDD minimum. |
| | NNM 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 |
| | 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 |
|-------------------|--|
| 5.2+ | <ul style="list-style-type: none">• 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 <p>High Performance mode only available on:</p> <ul style="list-style-type: none">• 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 |
| Previous Versions | |
| 5.1 | <ul style="list-style-type: none">• 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 10.8 and 10.9 64-bit• Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012• Microsoft Visual C++ 2010 Redistributable Package <p>High Performance mode only available on:</p> <ul style="list-style-type: none">• CentOS 6.x 64-bit• CentOS 7.x 64-bit• Red Hat ES 6.6+ 64-bit |

| Version | Software Requirements |
|-------------------|--|
| | <ul style="list-style-type: none"> Red Hat ES 7.x 64-bit Linux kernel version 2.6.34. |
| 4.4.x through 5.0 | <ul style="list-style-type: none"> 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 10.8 and 10.9 64-bit Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012 <p>High Performance mode only available on:</p> <ul style="list-style-type: none"> CentOS 6.x 64-bit CentOS 7.x 64-bit Red Hat ES 6.6+ 64-bit Red Hat ES 7.x 64-bit |

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.

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

-
- VMware ESXi/ESX 5.5
 - VMXNET3 network adapter

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 |
|---------|--|
| 1.0 | <ul style="list-style-type: none">• 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: $100 \text{ events/second} * 250 \text{ bytes/event} * 86,400 \text{ seconds/day} = 2,160,000,000 \text{ bytes/day}$.

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 | | | | <p>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.</p> |
| | One LCE server with Elasticsearch processing between 5,000 and 20,000 events per second | 32 GB | 64-bit, 16 cores | HD, or SSD of equiv. IOPS capability, in RAID 0/10 configuration | |
| | 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 |
| | One LCE server processing between 5,000 and 20,000 events | 16 GB | 64-bit, 16 cores | | |
| <p>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.</p> | | | | | |

| 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 | <ul style="list-style-type: none">• 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 | <ul style="list-style-type: none">• 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.