



## Tenable General Requirements

---

Last Revised: August 08, 2017



<b>Tenable General Requirements</b> .....	<b>1</b>
<b>Introduction</b> .....	<b>3</b>
<b>Nessus</b> .....	<b>4</b>
Nessus Hardware Requirements .....	5
Nessus Software Requirements .....	7
Nessus Licensing Requirements .....	14
<b>SecurityCenter</b> .....	<b>15</b>
SecurityCenter Hardware Requirements .....	16
SecurityCenter Software Requirements .....	18
SecurityCenter Licensing Requirements .....	20
<b>PVS</b> .....	<b>21</b>
PVS Hardware Requirements .....	22
PVS Software Requirements .....	24
PVS Licensing Requirements .....	26
<b>LCE</b> .....	<b>27</b>
Log Correlation Engine Hardware Requirements .....	28
Log Correlation Engine Software Requirements .....	31
LCE Licensing Requirements .....	32

---

# 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:

- [Nessus](#)
- [SecurityCenter](#)
- [Passive Vulnerability Scanner](#)
- [Log Correlation Engine](#)

---

# Nessus

---

This section includes:

- [Nessus Hardware Requirements](#)
- [Nessus Software Requirements](#)
- [Nessus Licensing Requirements](#)

# Nessus 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.

## Nessus Hardware Requirements

Version	Installation Scenario	RAM	Processor	Hard Disk Space
6.5 through 6.11	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	3 - 4 GB (8 GB recommended)	1 dual-core, 2GHz Intel CPU (2 dual-core recommended)	30 GB



Version	Installation Scenario	RAM	Processor	Hard Disk Space
	.pdf report generation.			

## 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 Software Requirements

Nessus supports Mac, Linux, and Windows operating systems.

## Nessus Manager and Nessus Professional

Version	Operating System	Supported 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 <div style="border: 1px solid green; padding: 5px;"><p><b>Tip:</b> 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</p></div>

Version	Operating System	Supported Versions
		server product from the Microsoft Windows family such as Windows Server 2008 R2.
	Mac OS X	Mac OS X 10.10, 10.11, and 10.12 - x86-64
Previous Versions		
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, 14.04, and 16.04 - i386 Ubuntu 11.10, 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



Version	Operating System	Supported Versions
		<p><b>Tip:</b> 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.</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, 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, 14.04, and 16.04 - i386</p> <p>Ubuntu 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, and 16.04 - AMD64</p>

Version	Operating System	Supported Versions
	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> <div style="border: 1px solid green; padding: 5px;"> <p><b>Tip:</b> 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>
	Mac OS X	Mac OS X 10.8, 10.9, 10.10, and 10.11 - x86-64

## Nessus Agents

Version	Operating System	Supported Versions
6.11	Linux	<p>Debian 7, 8, and 9- i386</p> <p>Debian 7, 8, and 9 - 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 - x86_64</p> <p>Fedora 24 and 25 - x86_64</p> <p>Ubuntu 12.04, 12.10, 13.04, 13.10, and 14.04 - i386</p> <p>Ubuntu 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,</p>

Version	Operating System	Supported Versions
		Server 2016, 7, 8, and 10 - x86-64
	Mac OS X	Mac OS X 10.8, 10.9, 10.10, 10.11, and 10.12 - x86-64
Previous Versions		
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	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 - i386
		Debian 6, 7, and 8 - AMD64
		Red Hat ES 5 / CentOS 5 / Oracle Linux 5 (including Unbreakable

Version	Operating System	Supported Versions
		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

## 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+)



Version	Supported Browsers
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 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>

---

# 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"><li>• An Active SecurityCenter license</li><li>• OpenJDK or Oracle Java JRE</li><li>• RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit</li></ul>

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](mailto: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](mailto: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.

Please refer to the following link for the most current information on installing a SecurityCenter license key:

[http://static.tenable.com/prod\\_docs/SecurityCenter\\_5.0\\_Installation.pdf](http://static.tenable.com/prod_docs/SecurityCenter_5.0_Installation.pdf)

## SecurityCenter Continuous View (CV)

Tenable’s SecurityCenter Continuous View (CV) platform provides combined Tenable products, which includes licensing for Nessus, the Passive Vulnerability Scanner (PVS), 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 PVS installations that can be deployed with SecurityCenter CV.

Please see the [Nessus](#), [Passive Vulnerability Scanner](#), and [Log Correlation Engine](#) sections in this guide for more information on how each component is licensed for a SecurityCenter CV purchase.

---

# PVS

---

This section includes:

- [PVS Hardware Requirements](#)
- [PVS Software Requirements](#)
- [PVS Licensing Requirements](#)

# PVS Hardware Requirements

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

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

Version	Installation scenario	RAM	Processor	Hard Disk
All Versions	PVS managing up to 50,000 hosts * (**)	2 GB RAM (4 GB RAM recommended)	1 dual-core 2GHz CPU	20 GB HDD minimum.
	PVS 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
	PVS 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 PVS.

\*\*For optimal data collection, PVS 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 PVS 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)

# PVS Software Requirements

The Passive Vulnerability Scanner is available for the following platforms:

Version	Software Requirements
5.1 and later	<ul style="list-style-type: none"><li>• Red Hat Linux ES 5 / CentOS 5 64-bit</li><li>• Red Hat Linux ES 6 / CentOS 6 64-bit</li><li>• Red Hat Linux ES 7 / CentOS 7 64-bit</li><li>• Mac OS X 10.8 and 10.9 64-bit</li><li>• Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012</li></ul> High Performance mode only available on: <ul style="list-style-type: none"><li>• CentOS 6.x 64-bit</li><li>• CentOS 7.x 64-bit</li><li>• Red Hat ES 6.6+ 64-bit</li><li>• Red Hat ES 7.x 64-bit</li><li>• Linux kernel version 2.6.34.</li></ul>
Previous Versions	
4.4.x through 5.0	<ul style="list-style-type: none"><li>• Red Hat Linux ES 5 / CentOS 5 64-bit</li><li>• Red Hat Linux ES 6 / CentOS 6 64-bit</li><li>• Red Hat Linux ES 7 / CentOS 7 64-bit</li><li>• Mac OS X 10.8 and 10.9 64-bit</li><li>• Microsoft Windows Vista, 7, 8, Server 2008, and Server 2012</li></ul> High Performance mode only available on: <ul style="list-style-type: none"><li>• CentOS 6.x 64-bit</li><li>• CentOS 7.x 64-bit</li><li>• Red Hat ES 6.6+ 64-bit</li><li>• Red Hat ES 7.x 64-bit</li></ul>



---

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

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

**Tip:** Refer to the [Configuring Virtual Switches for Use with PVS](#) document for details on configuring your virtual environment.

## High Performance Mode

To run PVS 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 at all, PVS 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 PVS in High Performance mode:

- VMware ESXi/ESX 5.5
- VMXNET3 network adapter

---

# PVS Licensing Requirements

---

## PVS Subscription

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

## Activation Code

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

## SecurityCenter Continuous View

SecurityCenter Continuous View includes PVS as part of a bundled license package with SecurityCenter. This license allows an unlimited number of PVS 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 PVS. The number of PVS deployments is determined by your Nessus Cloud licensing.

## High Performance Mode

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

---

# 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, 3	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		GHz		
	One LCE server with Elasticsearch processing between 5,000 and 20,000 events per second	32 GB	64-bit, 16 cores, 3 GHz	HD, or SSD of equiv. IOPS capability, in RAID 0/10 configuration	<p><b>Note:</b> 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 greater than 20,000 events per second	64 GB or more	64-bit, 24 cores or more, 3 GHz		
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, 3 GHz	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, 3 GHz		

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, 3 GHz		

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"><li>• An active LCE license</li><li>• RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit</li><li>• Elasticsearch 2.3.3 to 2.4.3</li><li>• Java Runtime Environment, latest version</li></ul>
Previous Versions	
4.4.x through 4.8.x	<ul style="list-style-type: none"><li>• An active LCE license</li><li>• RHEL/CentOS 5.x, 6.x, or 7.x, 64-bit</li></ul>

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.