

# One Identity Safeguard for Privileged Sessions 5 LTS

## Sizing Guide for SPS version 5.0 or later

## Copyright 2019 One Identity LLC.

### ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

### Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

### Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). All other trademarks are the property of their respective owners.

### Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

# Contents

<b>Introduction</b> .....	<b>4</b>
<b>Performance metrics</b> .....	<b>5</b>
General performance and capacity information .....	5
Indexer performance .....	6
Audit trail files .....	9
<b>Central search capacity</b> .....	<b>11</b>
<b>Sizing guidelines</b> .....	<b>12</b>
<b>About us</b> .....	<b>13</b>
Contacting us .....	13
Technical support resources .....	13

# Introduction

One Identity provides three different One Identity Safeguard for Privileged Sessions (SPS) appliances (boxes), and deciding which box suits customers' exact requirements best always depends on a great many factors. All boxes have different performance measurements and One Identity's goal is to provide information to help select the most appropriate solution for customers' environment.

For detailed hardware specifications of the three SPS appliances, see [Installation Guide](#).

**It is strongly recommended to always ask One Identity engineers to verify the planned design. Each and every use case is different and there can be case-specific conditions changing the final design. One Identity cannot take responsibility for improper architectural and/or performance design if One Identity has not been asked to verify those.**

Performance capabilities heavily depend on several client-specific technical factors. Consequently, the maximum number of concurrent users served by a given SPS box may vary in each IT environment.

Note that:

- While this document uses the terms "sessions" and "concurrent sessions" when providing figures, "concurrent sessions" also means "concurrent users" (assuming that a single user corresponds to a single session).

There can, of course, be users in the client's system who are not all using session management at once, and there can be users (for example, the admin account) who are able to open multiple sessions concurrently. The rough conversion of one user to one session simply serves as a ballpark estimate when calculating license requirements. Client-specific circumstances can fine-tune this estimate.

- All benchmarks presented in this document assume typical administrative workflows within the sessions.
- All performance tests were carried out without One Identity Safeguard for Privileged Analytics (SPA) configured, so measurement figures provided in this document are only valid for SPS appliances with no SPA used.
- Each column in [Performance metrics](#) on page 5 shows the benchmark for a particular protocol.
- When measuring performance for a given protocol, all sessions audited by SPS during the test were from that protocol only (for example, in the case of SSH measurements, 100% of the sessions was SSH).

# Performance metrics

This section provides detailed performance metrics, as well as capacity information related to indexing, and audit trail files.

## General performance and capacity information

### Pure performance:

- The number of indexer worker threads running inside SPS is 0.
- Real-time alerting (Content policy) is disabled.

**Table 1: Pure performance**

Appliance	Max. RDP sessions	Max. SSH sessions	Max. HTTP sessions
SPS T1	200	1000	500
SPS T4	300	1200	600
SPS T10	500	1500	750

SPS Virtual Appliance (VA) capabilities depend on the resources assigned to the Virtual Machine (VM). For the desired performance, One Identity recommends creating a VM with equivalent or similar resources to those of the corresponding T1 / T4 / T10 hardware appliance.

When calculating the required resources, always take into account the overhead produced by the virtualization layer.

**NOTE:**

Adding more resources than those of a T10 hardware model is not recommended as in certain cases, that can cause a decrease in performance.

### Capacity with real-time alerting:

- SSH: Content policy was enabled on 100% of the sessions, with 4 rules matching 10% of the commands.
- RDP: Content policy was enabled on 100% of the sessions, with 1 rule matching 10% of the window titles.

**Table 2: Capacity with real-time alerting**

Appliance	Max. RDP sessions	Capacity	Max. SSH sessions	Capacity
SPS T1	20	10%	200	20%
SPS T4	90	30%	600	50%
SPS T10	150	30%	1350	90%

SPS Virtual Appliance (VA) capabilities depend on the resources assigned to the Virtual Machine (VM). For the desired performance, One Identity recommends creating a VM with equivalent or similar resources to those of the corresponding T1 / T4 / T10 hardware appliance.

When calculating the required resources, always take into account the overhead produced by the virtualization layer.

**NOTE:**

Adding more resources than those of a T10 hardware model is not recommended as in certain cases, that can cause a decrease in performance.

## Indexer performance

### Indexer performance with `lightweight_indexing`:

When using `lightweight_indexing`, SPS extracts only the executed commands (Command event) and window titles (Window title event) that appear on the screen. It does not index any other screen content (for example, text that is displayed in a terminal or that appears in an RDP window). Note that `lightweight_indexing` is available only in SPS 5 F3 and later. Also, on newly installed 5 F3 and later appliances, `lightweight_indexing` is automatically enabled by default in the Connection policies.

One instance of indexer worker thread can process the following amount of audit trails:

- CLI: 450 hours / day
- Graphical on 1280x1024 screen resolution: 560 hours / day
- HTTP: N/A (HTTP traffic is not indexed when using `lightweight_indexing`)

The SPS appliances can have the following number of indexer worker threads running internally:

**Table 3: Indexer performance with `lightweight_indexing`**

Appliance	# of internal threads	CLI capacity	Graphical capacity
SPS T1	2	900 hours / day	1120 hours / day

Appliance	# of internal threads	CLI capacity	Graphical capacity
SPS T4	1-4 *	450-1800 hours / day	560-2240 hours / day
SPS T10	6-12 *	2700-5400 hours / day	3360-6720 hours / day
SPS Virtual Appliance (VA)	<p>VA capabilities depend on the resources assigned to the Virtual Machine (VM). For the desired performance, One Identity recommends creating a VM with equivalent or similar resources to those of the corresponding T1 / T4 / T10 hardware appliance.</p> <p>When calculating the required resources, always take into account the overhead produced by the virtualization layer.</p> <p><b>NOTE:</b> Adding more resources than those of a T10 hardware model is not recommended as in certain cases, that can cause a decrease in performance.</p>		

\* The lower value shows the maximum number of internal indexer threads on an SPS under high load.

**CAUTION:** Running any number of internal indexer threads is not suggested when real-time alerting is enabled, due to the high CPU usage of both features.

**NOTE:** If the internal indexer of SPS is unable to handle the load, then One Identity recommends running external indexers. In environments with high loads or when using near-real time indexing, running external indexers is the recommended approach.

### Indexer performance with full\_indexing:

When using `full_indexing`, SPS indexes the complete content of the screen, including all events. In SPS version 5 F2 and earlier, only `full_indexing` is available. Using `full_indexing` is slower and requires more resources than `lightweight_indexing`.

One instance of indexer worker thread can process the following amount of audit trails:

- CLI: 600 hours / day
- Graphical on 1280x1024 screen resolution: 100 hours / day
- HTTP: 600 hours / day

SPS appliances can have the following number of indexer worker threads running internally:

**Table 4: Indexer performance with full\_indexing**

Appliance	# of internal threads	CLI capacity	Graphical capacity	HTTP capacity
SPS T1	2	1200 hours / day	200 hours / day	1200 hours / day
SPS T4	1-4 *	600-2400 hours / day	100-400 hours / day	600-2400 hours / day
SPS T10	6-12 *	3600-7200 hours / day	600-1200 hours / day	3600-7200 hours / day

SPS Virtual Appliance (VA) capabilities depend on the resources assigned to the Virtual Machine (VM). For the desired performance, One Identity recommends creating a VM with equivalent or similar resources to those of the corresponding T1 / T4 / T10 hardware appliance.

When calculating the required resources, always take into account the overhead produced by the virtualization layer.

**NOTE:**

Adding more resources than those of a T10 hardware model is not recommended as in certain cases, that can cause a decrease in performance.

\* The lower value shows the maximum number of internal indexer threads on an SPS under high load.

**CAUTION:**

**Running any number of internal indexer threads is not suggested when real-time alerting is enabled, due to the high CPU usage of both features.**

**NOTE:**

If the internal indexer of SPS is unable to handle the load, then One Identity recommends running external indexers.

In environments with high loads or when using near-real time indexing, running external indexers is the recommended approach.

**Using an external indexer:**

Creating an external indexer with equivalent or similar resources to those of the corresponding T1 / T4 / T10 hardware appliance allows you to process roughly the same amount of audit trails as the internal indexer of those hardware models.

## Minimum hardware requirements for running the indexer externally from SPS:

- Available CPU core/thread per indexer worker.
- 2.4 GHz or faster CPU.
- 300 MB RAM per indexer worker.
- There is minimal disk space usage by the indexer workers (only to store the logs).

# Audit trail files

## Size of the audit trail files:

The .zat audit trail files written by SPS is a proprietary binary file format that is compressed on-the-fly. The size of the files heavily depend on the type of actions made by the monitored user, but also on the screen resolution used in graphical connections. If file transferring within a session is also audited by SPS, the size of the transferred file must be calculated in addition.

The typical size of audit trail files, assuming a typical administrative workflow and depending on the terminal window size and the screen resolution is as follows:

- SSH / Telnet: ~15-35 KB / minute (~1-2 MB / hour)
- RDP: ~2-10 MB / minute \*
- Citrix ICA: ~1-5 MB / minute \*
- VNC: ~5-20 MB / minute \*
- HTTP: depends on the monitored web content

### CAUTION:

\* **The screen resolution of graphical sessions has significant impact on the size of the audit trail file. The following examples are for audit trails containing constant activity. Administrative activity is typically not sustained in real life, therefore we calculate with different sizes for disk occupation.**

**More sophisticated disk occupation sizing should be the outcome of Proof of Concept activity.**

- **1024x768: less than 1 MB / minute**
- **1680x931: ~5 MB / minute**
- **1920x1080: ~10 MB / minute**

### **Reference audit trails:**

One Identity partners have access to reference audit trails of both CLI and graphical sessions, showing a sample session of typical administrative usage. One Identity provides reference trails for normal and for heavy usage. To request access to reference audit trails, contact One Identity.

Note that these audit trails contain sustained activity. Hence from a viewpoint of disk occupation, these are not references for sizing.

# Central search capacity

Starting with SPS version 5 F6, it is possible to join multiple SPS nodes into a cluster, monitor their status, and update their configuration from a central location. Starting with version 5 F7, when you have a cluster of nodes set up, you have the possibility to search all session data recorded by all nodes in the cluster on a single node. This is achieved by assigning roles to the individual nodes in your cluster: you can set up one of your SPS nodes to be the Search Master and the rest of the nodes to be Search Minions. Search Minions send session data that they record to the Search Master, and the Search Master acts as a central search node.

Take note of the following capacity requirements when setting up your cluster for central search:

- Only T10 appliances or similarly sized Virtual Appliances (VAs) are supported as Search Master nodes.
- The Search Master node only provides search and reporting functionality and cannot be used to manage production SSH, RDP, and so on traffic.
- At most, 8 appliances (of any kind) can be connected to a single Search Master node.
- The network connection between the Search Minion nodes and the Search Master node must comply with the following requirements if the appliances are operated near their maximum capacity:
  - Must have at least 99.95% annual availability.
  - Must be able to support at least 10MB/sec sustained bandwidth.

In case of an outage:

- A one-time outage of up to 10 hours is handled without the disruption of traffic.
- New connections are no longer accepted and existing connections start to be dropped if the outage is longer than 10 hours.
- Recovery is automatic once the connection is re-established.

When there is a smaller load on the system, these network requirements are different as more limited availability, smaller bandwidth, and more outage time are tolerated.

# Sizing guidelines

In order to scale the appropriate SPS box, One Identity engineers need technical information from the customers including the following:

- The number of concurrent connections going through SPS.
- How many of the concurrent connections are controlled / monitored or just routed through SPS.
- The protocols used for the listed connections.
- The duration of an average working session.
- The type of sessions that should be monitored, for example, system administrator's sessions, or remote scripted commands, or average end-users' sessions (for example, call center or bank employees).
- The preferred screen size and – in the case of graphical sessions – the resolution of the working sessions.

Based on these details, One Identity engineers can recommend an appropriate deployment for you.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

## Contacting us

For sales or other inquiries, visit <https://www.oneidentity.com/company/contact-us.aspx> or call +1-800-306-9329.

## Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at <https://support.oneidentity.com/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos at [www.YouTube.com/OneIdentity](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product