



One Identity Safeguard for Privileged Sessions 6.11.0

Using Splunk with One Identity Safeguard for Privileged Sessions

Copyright 2021 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. All other trademarks are the property of their respective owners.

Legend

-  **WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.**
-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

SPS Using Splunk with One Identity Safeguard for Privileged Sessions
Updated - 19 August 2021, 10:22
Version - 6.11.0

Contents

Introduction	4
The Splunk Add-on	5
Event types	6
The Splunk App	7
Visualizing events and performing gap analysis with the Splunk App	8
Macros and search expressions	10
About us	12
Contacting us	12
Technical support resources	12

Introduction

This document describes how you can use the services of the One Identity Safeguard for Privileged Sessions Add-on for Splunk (the Splunk Add-on) and the One Identity Safeguard for Privileged Sessions App for Splunk (the Splunk App) to process and visualize your events from One Identity Safeguard for Privileged Sessions (SPS).

One Identity Safeguard for Privileged Sessions:

One Identity Safeguard for Privileged Sessions (SPS) controls privileged access to remote IT systems, records activities in searchable, movie-like audit trails, and prevents malicious actions. SPS is a quickly deployable enterprise device, completely independent from clients and servers — integrating seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill down for forensic investigations.

SPS and Splunk Add-on / Splunk App

If you have an SPS device forwarding events to your Splunk, and you want to process and visualize these events with your own, custom dashboards, the Splunk Add-on can provide you with useful event types that you can use in your custom searches. For more information about visualizing events and customizing dashboards, see [The Splunk App](#) and [Macros and search expressions](#).

The Splunk Add-on is an add-on for Splunk that defines useful event types for your sessions originating from SPS. For more information, see [Event types](#).

The Splunk App creates useful dashboards to visualize your sessions audited with SPS.

Also, if you want to use your Microsoft Windows or Linux session logs for gap analysis and you have [the Splunk Add-on for Microsoft Windows](#) or [the Splunk Add-on for Unix and Linux](#) installed, the Splunk App allows you to spot potential audit gaps.

The Splunk Add-on

The Splunk Add-on is an add-on for Splunk that defines useful event types for your sessions originating from SPS. For more information, see [Event types](#).

If you have an SPS device forwarding events to your Splunk, and you want to process and visualize these events with your own, custom dashboards, the Splunk Add-on can provide you with useful event types that you can use in your custom searches. For more information about visualizing events and customizing dashboards, see [The Splunk App](#) and [Macros and search expressions](#).

When using SPS together with the Splunk Add-on, the events originating from SPS are parsed, indexed and labeled with tags. These tags help standardize data coming from various data sources. As a result, custom-searching in Splunk will be more effective.

Prerequisites and restrictions

- Your SPS appliance must be installed and [configured to forward events to Splunk](#), using the **JSON-CIM** format.
- The Splunk Add-on is supported from SPS version 6.0.

Installation and configuration

To install the Splunk Add-on and configure SPS to forward events to Splunk

1. Use your favorite install method to install the app (either by searching for the One Identity Safeguard for Privileged Sessions Add-on for Splunk app on your Splunk web UI, or by navigating to the SplunkBase website and installing [the app](#) manually).
2. Configure SPS to forward events to Splunk. For detailed instructions, see "[Using the universal SIEM forwarder](#)" in the [Administration Guide](#).

Parsing and indexing with the Splunk Add-on

If you want to search for a specific event type in your SPS index (for example, because you want to have a chart on your own dashboard about the distribution of different event types), look at the "Event type name" column in [Event types](#) to filter for the different kinds. As an example, if you would like to count the number of "ServerConnect" events and visualize the results on a graph, you can do so with the following search expression:

```
search index=* | stats count(eval(eventtype=oneidentity_sps_server_connect)) AS count_server_connect BY eventtype
```

Event types

The table below lists the definitions of event types for your sessions originating from SPS and the definitions' descriptions.

Event type name	Description
oneidentity_sps_server_connect	ServerConnect event coming from SPS SIEM forwarder
oneidentity_sps_session_closed	SessionClosed event coming from SPS SIEM forwarder
oneidentity_sps_server_authentication_success	ServerAuthenticationSuccess event coming from SPS SIEM forwarder
oneidentity_sps_server_authentication_failure	ServerAuthenticationFailure event coming from SPS SIEM forwarder
oneidentity_sps_gateway_authentication_failure	GatewayAuthenticationFailure event coming from SPS SIEM forwarder
oneidentity_sps_session_scored	SessionScored event coming from SPS SIEM forwarder
oneidentity_sps_command_channel_event	CommandChannelEvent event coming from SPS SIEM forwarder
oneidentity_sps_window_title_channel_event	WindowTitleChannelEvent event coming from SPS SIEM forwarder
oneidentity_sps_rdp_embedded_in_tsg	RdpEmbeddedInTsg event coming from SPS SIEM forwarder
oneidentity_sps_file_transfer	FileTransfer event coming from SPS SIEM forwarder

The Splunk App

The One Identity Safeguard for Privileged Sessions App for Splunk creates useful dashboards to visualize your sessions audited with SPS. With this app, you can get an overview of your audited sessions and pinpoint interesting ones to be able to investigate them further. Also, if you have other sources of information about your audited hosts (for example, Microsoft Windows logs or Unix/Linux logs) as well as those originating from SPS, you can compare the two sources of information and see if all the necessary sessions are audited without audit gaps.

When used together with the Splunk App, you can customize your search with the help of your defined events and visualize your sessions originating from SPS on customized dashboards.

Prerequisites and restrictions

NOTE: It is a prerequisite to have the Splunk Add-on installed for the Splunk App to work. When you install the Splunk App, it is presumed that SPS is already [configured to forward events to Splunk](#) and Splunk already receives these forwarded events. In such a setup, all events from SPS should arrive to a separate index in Splunk (if it's not the case, fix it before installing and setting up the Splunk App).

- If you want to use your Microsoft Windows or Unix / Linux session logs for gap analysis (see [Visualizing events and performing gap analysis with the Splunk App](#)), you need to have [the Splunk Add-on for Microsoft Windows](#) or [the Splunk Add-on for Unix and Linux](#) installed.
- The Splunk App is supported from SPS version 6.0.

Installation and setup

To install and setup the Splunk App

1. Use your favorite install method to install the app (either by searching for the One Identity Safeguard for Privileged Sessions App for Splunk app on your Splunk web UI, or by navigating to the SplunkBase website and installing the [the app](#) manually).
2. On the setup page of the Splunk App, provide the name of the index into which the SPS events will be arriving.
3. (Optional) If such an index does not exist yet and you want to configure forwarding later, just specify an index name of your choice and the Splunk App will create the index for you. In this case, pay attention to forward the events into this index later, when configuring forwarding from SPS.
4. There is another index you can specify, which will be the origin of data coming from logs. You can use this app to spot "audit gaps" (that is, unaudited sessions), but for that to work, you need logs from the hosts directly.
5. (Optional) If you already have forwarders set up to forward logs from your hosts to Splunk, specify the name of the index for the app into which the logs are forwarded.

Visualizing events and performing gap analysis with the Splunk App

Prerequisites and restrictions

- To visualize events from SPS, you must have your SPS [configured to forward events to Splunk](#) and the Splunk Add-on installed.
- To use the gap analysis function, you must have the Splunk App and [the Splunk Add-on for Microsoft Windows](#) or [the Splunk Add-on for Unix and Linux](#) installed.

Installation

For information about the setup process, see [The Splunk App](#).

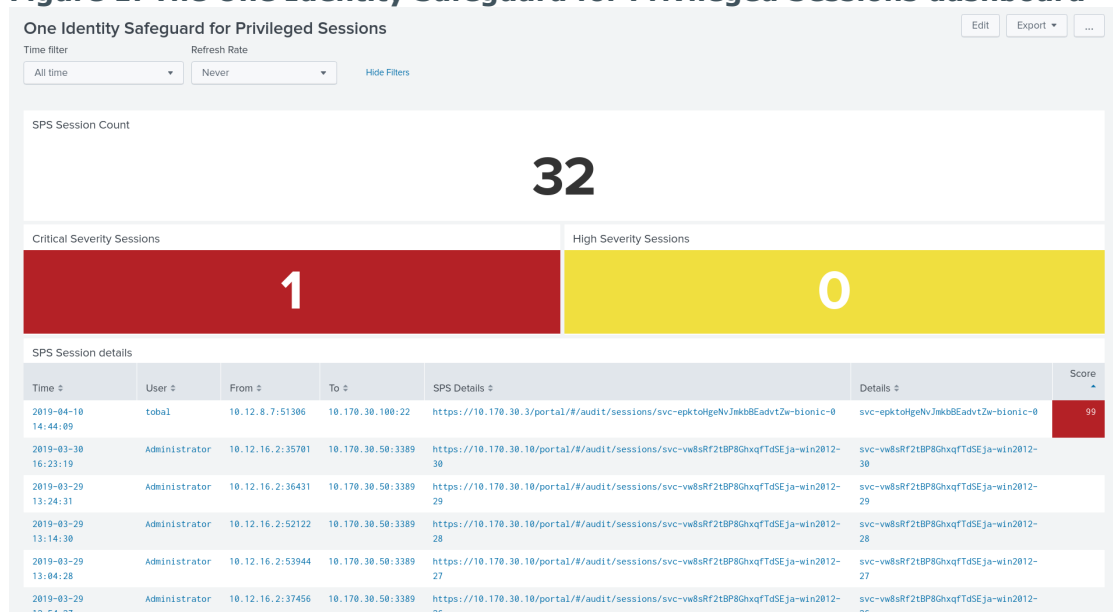
Visualizing events using the One Identity Safeguard for Privileged Sessions dashboard

The One Identity Safeguard for Privileged Sessions dashboard visualizes data from SPS (including your events parsed and indexed by the Splunk Add-on and the metadata that the Splunk Add-on attaches to those events).

To access the One Identity Safeguard for Privileged Sessions dashboard

1. Login to the Splunk Enterprise online administration page.
2. Select **One Identity Safeguard for Privileged Sessions** under **Apps**.

Figure 1: The One Identity Safeguard for Privileged Sessions dashboard



The top filters bar allows you to configure your filters, the middle section shows an overview of logged sessions, and the lower section shows a more detailed list of audited sessions.

Under **Time filter** you can set a time interval in which you want to browse your data, and configure relevant settings. Under **Refresh Rate** you can specify a refresh rate (if you want to). To hide the **Time filter** and **Refresh Rate** items, click **Hide Filters/Show Filters**.

Below the filters bar, you see the details of logged sessions (such as **SPS Session Count**, the number of **Critical Severity Sessions**, and the number of **High Severity Sessions**) in the given time range.

The listed elements below **SPS Session details** show the audited sessions.

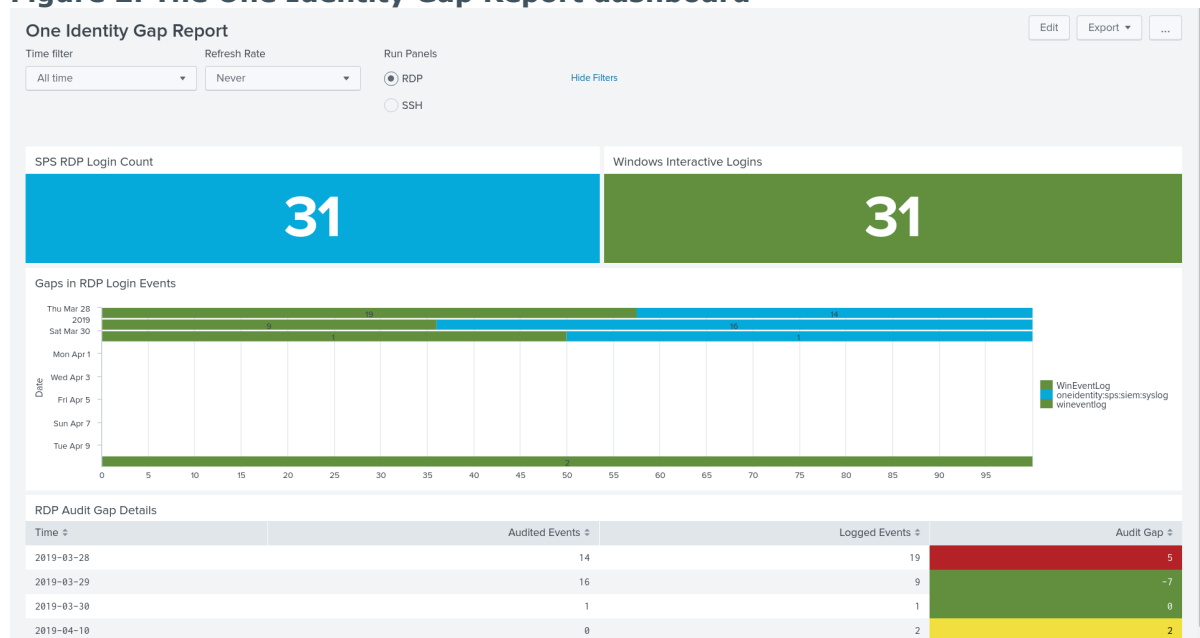
The One Identity Gap Report dashboard

The One Identity Gap Report dashboard allows you to use other sources of information about your audited hosts (for example, Microsoft Windows logs or Unix/Linux logs) as well as those originating from SPS to compare the two sources of information and see if all the necessary sessions are audited without audit gaps.

To access the One Identity Gap Report dashboard

1. Login to the Splunk Enterprise online administration page.
2. Select **One Identity Safeguard for Privileged Sessions** under **Apps**.
3. Click **One Identity Gap Report** on the top tab bar to switch from the the **One Identity Safeguard for Privileged Sessions** dashboard.

Figure 2: The One Identity Gap Report dashboard



The top filters bar allows you to configure your filters and whether you want to visualize your RDP or your SSH sessions, the middle section shows an overview of logged sessions, and the lower section shows a more detailed list of unaudited sessions.

You can set a time interval in which you want to browse your data, and configure relevant settings under the **Time filter**. Under **Refresh Rate** you can specify a refresh rate (if you want to). The **Run Panels** option allows you to switch between RDP and SSH sessions. To hide the **Time filter** and **Refresh Rate** items, click the **Hide Filters/Show Filters**.

Below the filters bar, you see the number of audited sessions (under **SPS RDP Login Count**), and the number of logged sessions (under **Windows Interactive Logins**) in the given time range.

Under **Gaps in RDP Login Events**, a bar chart shows the proportion between audited and logged sessions, by day.

Under **RDP Audit Gap Details**, you can see the specific data (such as **Time** (for the audit gap date), the number of **Audited Events**, the number of **Logged Events** and the number of unaudited sessions, under **Audit Gap**), grouped by day.

Macros and search expressions

If you have the Splunk App installed on your Splunk, but want to build your own custom dashboard, you can use the event types and macros defined by the app. The events originating from SPS are **CIM-compliant** (specifically, they use the **Network Sessions**, the **Network Traffic** and the **Intrusion Detection** data models), so the field names will be familiar. For more information about Splunk's Search Tutorial, click [here](#).

Macros

The table below lists macros defined by the Splunk App and their descriptions.

Macro name	Description
OI_SPS_events	Individual events coming from SPS
OI_SPS_sessions	Sessions audited by SPS (events correlated into full sessions)
OI_SPS_monitored_hosts	Hosts monitored by SPS
OI_SPS_scored_sessions	Sessions audited by SPS which have a score given by SPS analytics
OI_SSH_logins	All SSH sessions coming from SPS
OI_WIN_interactive_logins	All windows interactive logins audited by SPS

Useful search expressions for SPS-specific events

The macros listed in the [Macros](#) section can be used to narrow your search in Splunk for SPS-specific events. You can see a few useful search expressions below.

- **example_user was on server 1.2.3.4**

```
`OI_SPS_events` tag=authentication dest_ip=1.2.3.4 user=example_user
```

- **List users logged onto server 1.2.3.4**

```
`OI_SPS_events` tag=authentication dest_ip=1.2.3.4 | table user | uniq
```

- **Get ID of all sessions with rm command**

```
`OI_SPS_events` eventtype=oneidentity_sps_command_channel_event command=rm |  
table session_id | uniq
```

- **Get ID of sessions with a score higher than 70**

```
`OI_SPS_events` aggregated_score>70 | table session_id | uniq
```

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 and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product