One Identity Safeguard for Privileged Sessions 5 LTS

Release Notes

December 2018

These release notes provide information about the One Identity Safeguard for Privileged Sessions release.

About this release

Welcome to One Identity Safeguard for Privileged Sessions. This document describes what is new in the latest version of One Identity Safeguard for Privileged Sessions (SPS).

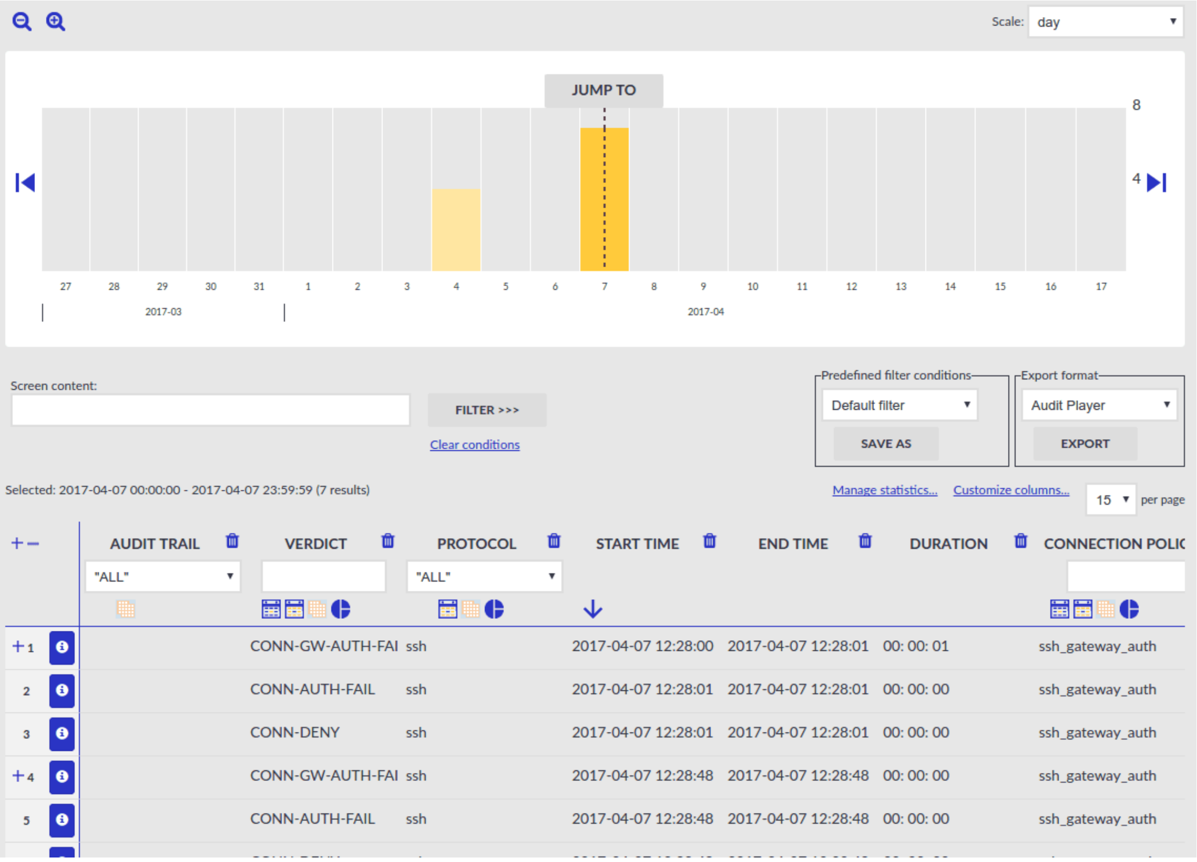
New features

Changes since SPS 4 F4

New user interface design

The user interface has received a facelift and now has a more modern look-and-feel.

Figure 1. The Search page after the facelift



Screen content:

Predefined filter conditions: Default filter

Export format: Audit Player

Selected: 2017-04-07 00:00:00 - 2017-04-07 23:59:59 (7 results)

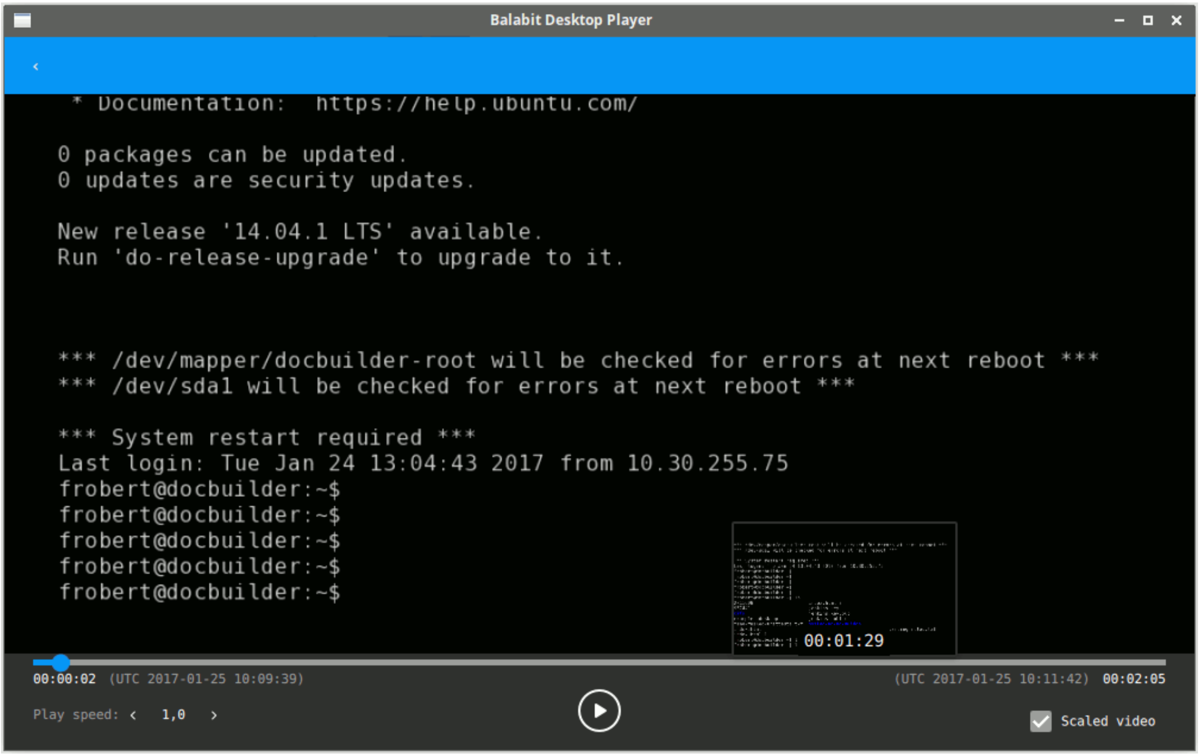
15 per page

	AUDIT TRAIL	VERDICT	PROTOCOL	START TIME	END TIME	DURATION	CONNECTION POLIC
	"ALL"		"ALL"				
+1		CONN-GW-AUTH-FAI	ssh	2017-04-07 12:28:00	2017-04-07 12:28:01	00: 00: 01	ssh_gateway_auth
2		CONN-AUTH-FAIL	ssh	2017-04-07 12:28:01	2017-04-07 12:28:01	00: 00: 00	ssh_gateway_auth
3		CONN-DENY	ssh	2017-04-07 12:28:01	2017-04-07 12:28:01	00: 00: 00	ssh_gateway_auth
+4		CONN-GW-AUTH-FAI	ssh	2017-04-07 12:28:48	2017-04-07 12:28:48	00: 00: 00	ssh_gateway_auth
5		CONN-AUTH-FAIL	ssh	2017-04-07 12:28:48	2017-04-07 12:28:48	00: 00: 00	ssh_gateway_auth

New One Identity Desktop Player

You can use the One Identity Desktop Player application to replay audit trail files that you have downloaded from the One Identity Safeguard for Privileged Sessions.

Figure 2. One Identity Desktop Player



Balabit Desktop Player
00:01:29
00:00:02 (UTC 2017-01-25 10:09:39)
(UTC 2017-01-25 10:11:42) 00:02:05
Play speed: ‹ 1,0 ›
Scaled video

```
  * Documentation:  https://help.ubuntu.com/

 0 packages can be updated.
 0 updates are security updates.

 New release '14.04.1 LTS' available.
 Run 'do-release-upgrade' to upgrade to it.



 *** /dev/mapper/docbuilder-root will be checked for errors at next reboot ***
 *** /dev/sda1 will be checked for errors at next reboot ***

 *** System restart required ***
 Last login: Tue Jan 24 13:04:43 2017 from 10.30.255.75
 frobert@docbuilder:~$
 frobert@docbuilder:~$
 frobert@docbuilder:~$
 frobert@docbuilder:~$
 frobert@docbuilder:~$
```

For further details on the One Identity Desktop Player application, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Modifying the disk size of a SPS virtual appliance

Newly installed SPS 5 LTS virtual instances come with a simplified filesystem structure, making online disk resizing possible. That way, you can more easily accommodate the disk requirements of your stored audit trails. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Backup and archiving improvements

SPS now fully supports backups and archiving using the NFSv4 protocol. NetApp devices are also supported.

API changes in the AA plugin

There were API changes in the AA plugin, therefore the old plugins require an update.

- The authorize hook is now mandatory, and it must return at least an ACCEPT verdict.
- The gateway_user is now a separate argument and not a value in key-value pairs.

Changes in the ticketing plugin

SPS 4 F3 and 4 F4 included a ticketing plugin framework to integrate SPS to ticketings systems, for example, to request a valid ticket ID from the user to authorize the connection. In SPS 5 LTS and later, this functionality is available using the Authentication and Authorization (AA) plugin.

You cannot use ticketing plugins in SPS 5 LTS, they must be reimplemented as AA plugins. Contact the vendor who created the ticketing plugin for you for details on updating the ticketing plugins to AA plugins. If you received the ticketing plugin from One Identity contact your service delivery partner, or contact our Support Team.

REST API changes

The following new details are available about the recorded sessions when you access the *api/audit/sessions/<connection-key>* endpoint. For details on these fields, see One Identity Safeguard for Privileged Sessions - Technical Documentation: *_connection_id*, *alerts*, *archived*, *auth_method*, *command_extracted*, *events*, *index_status*, *network_id*, *window_title_extracted*. Also, note that the *connection_policy* field now contains the name of the Connection Policy that handled the session (in earlier version it contained the key of the session, which is now available in the *connection_policy_id* field).

The timestamps returned in the REST API now use the ISO 8601 format instead of UNIX timestamp.

The events of a session and the alerts triggered by such events is available in the *api/audit/sessions/<connection-key>/events* and *api/audit/sessions/<connection-key>/alerts* endpoints. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation and One Identity Safeguard for Privileged Sessions - Technical Documentation.

From now on, you can search in metadata and session content at the same time, for example: **api/audit/sessions?q=protocol:ssh&content=sudo**"

The REST API now supports X.509 certificate based authentication as well.

Unsupported browsers and operating systems

Support for the following browsers and operating systems is discontinued starting from SPS 5 LTS:

- Browsers: Internet Explorer 10

- Operating systems: Windows 2003 Server, Windows Vista

Extended support period for SPS 4 F3

Version 4 F3 has extended support period, and will be supported for 6 months after SPS 5 LTS is released.

New SNMP/email alert when a service fails

There is a new SNMP/email alert, which is triggered when a service fails. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

New authentication protocol options when authenticating users to a RADIUS server

When authenticating users to a RADIUS server, you can now specify authentication protocol options Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). For more information, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Export/import the configuration of SPS using the console

You can now export/import the configuration of SPS from the console using a script. For further details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Improved search in reports created from audit trail content

The character limit on search words when looking for specific search expressions in content subchapters has been raised from 150 to 255 characters. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Changes between SPS 4 LTS and 4 F4

Installation and upgrade-related improvements

Installing One Identity Safeguard for Privileged Sessions as a Kernel-based Virtual Machine

You can deploy SPS as a virtual appliance using the Kernel-based Virtual Machine (KVM) solution. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

SPS in Azure Marketplace

You can deploy SPS from the Microsoft Azure Marketplace, with a bring-your-own-license model. For details, see the One Identity Safeguard for Privileged Sessions virtual machine page.

When deployed from the Azure Marketplace, you can use Azure File storage shares in your for Backup and Archive Policies. This is very useful as the quota for the files storage can be changed dynamically, so the cumulative size of the audit trails is not limited to the OS disk size. You can set up this share as a normal SMB shares in your Backup and Archive policies. The parameters for the policy can be obtained from the Azure portal.

SPS in Azure Cloud

You can deploy SPS as a virtual machine in the Microsoft Azure cloud computing platform. This allows you to conveniently audit access to your entire virtualized infrastructure.

Simplified, more robust upgrade process

SPS 4 F1 offers a more robust upgrade process that allows you to test upgrading your configuration and correct any problems that are not compatible with version 4 F1. Also, firmware upgrading has been simplified: instead of uploading the boot and core firmwares separately, you only have to upload a single ISO file, and SPS extract the firmwares on the box.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation and One Identity Safeguard for Privileged Sessions - Technical Documentation.

Protocol-related improvements

Credential store fallback

Until now, if you have configured SPS to use a credential store, but accessing the password or the credential store failed for some reason, SPS rejected the session. From now on, SPS automatically requests a password from the user in such scenario, so your users can access the target server. This fallback is supported in the RDP, SSH, and Telnet protocols.

Inband destination selection improvements in RDP

Using inband destination selection in RDP connections without a Terminal Services Gateway was difficult and limited, because Windows RDP clients often send only the first 9 characters of the username to the server. SPS now supports parsing key-value pairs from the username, making it possible to encode the address and port of the target server into the username of the client.

Plugin framework for authentication and authorization (AAPlugin)

SPS now includes a new plugin framework that allows you to integrate with external third-party tools to request authentication or authorization for connections that SPS monitors. As a first step, AAPlugins are supported only in RDP connections.

Such plugins allow you, for example, to request additional challenge-response information from the user or an external system (for example, LDAP or Active Directory), and permit or deny the connection based on this information. For details, contact the One Identity Support Team.

Windows 10 support and new client applications

SPS now supports the Remote Desktop client of Windows 10.

In addition, the Royal TSX client application running on OS X, and the WinFIOL SSH client are also supported.

Network Level Authentication in RDP without domain

membership

There are scenarios when you want to use SPS to monitor RDP access to servers that accept only Network Level Authentication (NLA, also called CredSSP), but SPS is not a member of the same domain (or of a trusted domain) as the RDP server. For example, you cannot add SPS to that domain for some reason, or the RDP server is a standalone server that is not part of a domain. Now SPS support such scenarios as well.

Authentication improvements in HTTP

SPS now supports the following inband authentication methods for the HTTP protocol: Basic Access Authentication (according to RFC2617), and the NTLM authentication method commonly used by Microsoft browsers, proxies, and servers. This allows SPS to identify HTTP sessions better, and also makes it possible to match authorized sessions to real users.

Furthermore, for authenticated sessions, SPS can perform group-based user authorization that allows you to finetune access to your servers and services: you can now set the required group membership in the Channel policy of the HTTP connection.

Integrating ticketing systems for RDP connections

SPS provides a plugin framework to integrate SPS to external ticketing (or issue tracking) systems, allowing you to request a ticket ID from the user before authenticating on the target server. That way, SPS can verify that the user has a valid reason to access the server — and optionally terminate the connection if he does not. In addition SSH and Telnet, SPS 4 F1 adds ticketing support for the Remote Desktop (RDP) protocol.

To request a plugin that interoperates with your ticketing system, contact our Support Team. For details on configuring SPS to use a plugin, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Telnet improvements

SPS 4 F1 supports the Telnet 5250 terminal protocol, as described in RFC2877. Extracting usernames from TN5250 connections is not supported.

SPS 4 F1 can properly replay TN3270 audit trails without the upstream encryption key.

Audit trails and indexing

Audit Player indexer service EOL

The Audit Player indexer service has been deprecated and is not supported in SPS 4 F4. Before upgrading, you must configure SPS to use the Indexer service running on SPS, and install and configure external indexers. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation and One Identity Safeguard for Privileged Sessions - Technical Documentation.

If you need help to estimate the required number and resources of the external indexers, contact the One Identity Support Team.

⚠ **CAUTION:**

Enabling the indexer without any previous estimations is dangerous and might result in overloading the box.

The indexer does not support USB Hardware security modules (HSMs). If your audit trails are encrypted and the related private keys are stored on a HSM, DO NOT UPGRADE to SPS 4 F4 or later.

Indexing improvements in graphical protocols

To optimize indexing resources and improve the speed and performance of Optical Character Recognition in graphical protocols, you can now configure **Indexer policies** for every Connection policy to specify the languages typically used in these connections. For example, if you know that your users use only a few languages in their connections (for example, because they use the Remote Desktop Protocol (RDP) to access only English and French software), then setting these languages in the Indexer policy improves accuracy and reduces the time required to perform character recognition.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Indexing Arabic text in graphical protocols

To make the audit trails of graphical protocols easier to review and manage in forensic situations, SPS 4 F3 adds support for Optical Character Recognition for languages that use Arabic characters. That way your auditors can search in the content of the graphical protocols, for example, in the texts typed or seen by a user in RDP, even if the text is Arabic.

Scaling audit trail processing

If SPS audits lots of connections, processing and indexing the created audit trails requires significant computing resources, which may not be available in the SPS appliance. To decrease the load on the SPS appliance, you can install the indexer service on external Linux hosts. These external indexer hosts run the same indexer service as the SPS appliance, and can index audit trails, or generate screenshots and replayable video files from the audit trails as needed. The external indexers register on SPS, wait for SPS to send an audit trail to process, process the audit trail, then return the processed data to SPS. The external indexer hosts do not store any data, thus any sensitive data is available on the host while it is being processed.

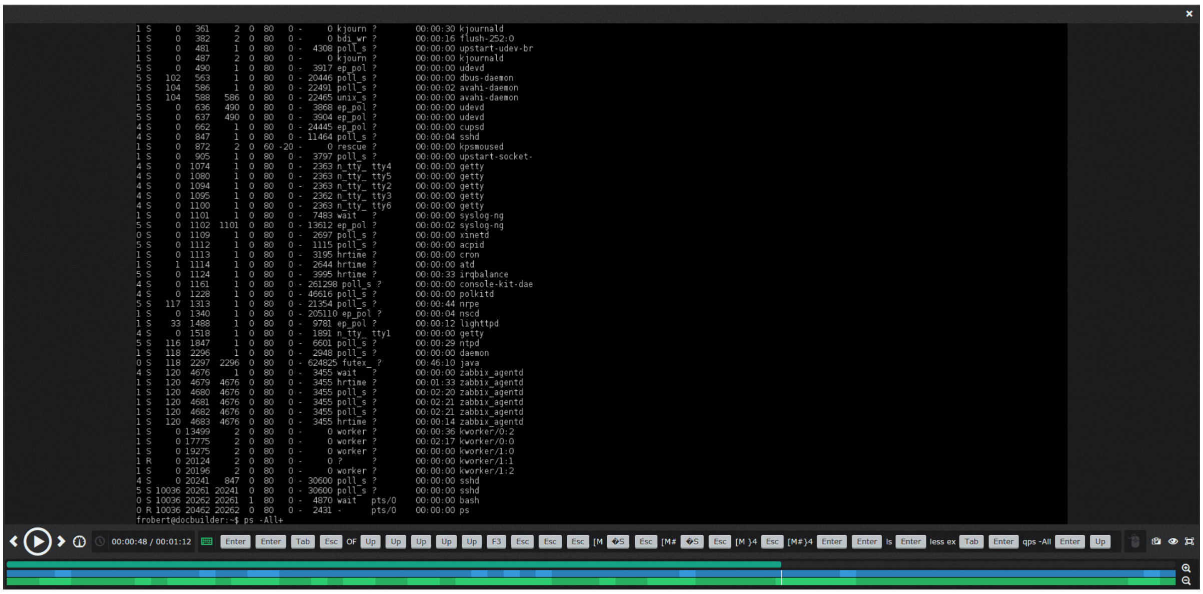
IPv6 support for the audited traffic

SPS now supports the auditing of IPv6 environments. You can audit IPv4 clients accessing IPv6 servers, IPv6 clients accessing IPv4 servers, and naturally, IPv6 clients accessing IPv6 servers. You can also use IPv6 addresses with inband destination selection.

Replaying audit trails in your browser

With SPS 4 F1, you can conveniently replay audit trails in your browser, without having to install extra software.

Figure 3. Replaying audit trails in your browser



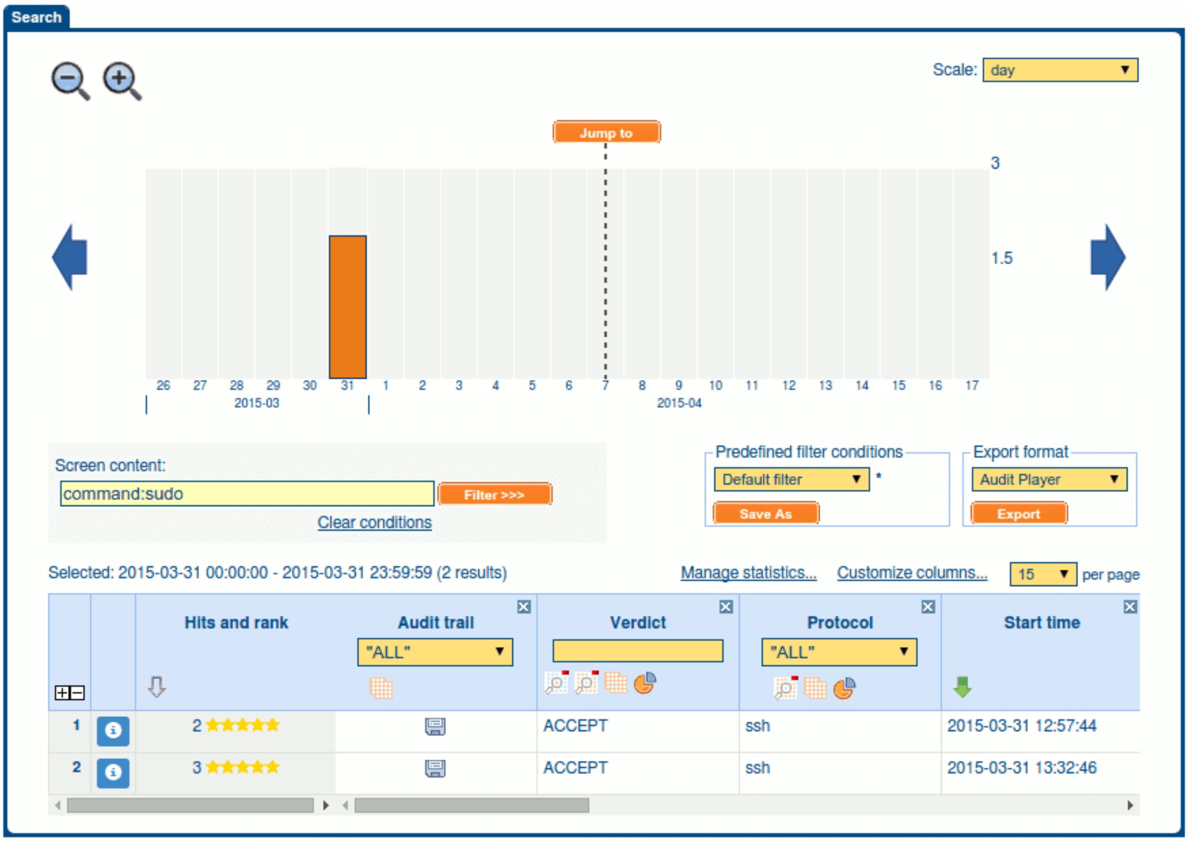
```
1 S     0   361     2  0  80   0 -     0 kjourn ?        00:00:30 kjournald
1 S     0   382     2  0  80   0 -     0 bdi_wr ?        00:00:16 flush-252:0
1 S     0   481     1  0  80   0 -  4308 poll_s ?        00:00:00 upstart-udev-br
1 S     0   487     2  0  80   0 -     0 kjourn ?        00:00:00 kjournald
5 S     0   490     1  0  80   0 -  3917 ep_pol ?        00:00:00 udevd
5 S   102   563     1  0  80   0 - 20446 poll_s ?        00:00:00 dbus-daemon
5 S   104   586     1  0  80   0 - 22491 poll_s ?        00:00:02 avahi-daemon
1 S   104   588   586  0  80   0 - 22465 unix_s ?        00:00:00 avahi-daemon
5 S     0   636   490  0  80   0 -  3868 ep_pol ?        00:00:00 udevd
5 S     0   637   490  0  80   0 -  3904 ep_pol ?        00:00:00 udevd
4 S     0   662     1  0  80   0 - 24445 ep_pol ?        00:00:00 cupsd
4 S     0   847     1  0  80   0 - 11464 poll_s ?        00:00:04 sshd
1 S     0   872     2  0  60 -20 -     0 rescue ?        00:00:00 kpsmoused
1 S     0   905     1  0  80   0 -  3797 poll_s ?        00:00:00 upstart-socket-
4 S     0  1074     1  0  80   0 -  2363 n_tty_ tty4     00:00:00 getty
4 S     0  1080     1  0  80   0 -  2363 n_tty_ tty5     00:00:00 getty
4 S     0  1094     1  0  80   0 -  2363 n_tty_ tty2     00:00:00 getty
4 S     0  1095     1  0  80   0 -  2362 n_tty_ tty3     00:00:00 getty
4 S     0  1100     1  0  80   0 -  2363 n_tty_ tty6     00:00:00 getty
1 S     0  1101     1  0  80   0 -  7483 wait   ?        00:00:00 syslog-ng
5 S     0  1102  1101  0  80   0 - 13612 ep_pol ?        00:00:02 syslog-ng
0 S     0  1109     1  0  80   0 -  2697 poll_s ?        00:00:00 xinetd
5 S     0  1112     1  0  80   0 -  1115 poll_s ?        00:00:00 acpid
1 S     0  1113     1  0  80   0 -  3195 hrtime ?        00:00:00 cron
1 S     1  1114     1  0  80   0 -  2644 hrtime ?        00:00:00 atd
5 S     0  1124     1  0  80   0 -  3995 hrtime ?        00:00:33 irqbalance
4 S     0  1161     1  0  80   0 - 261298 poll_s ?       00:00:00 console-kit-dae
4 S     0  1228     1  0  80   0 - 46616 poll_s ?        00:00:00 polkitd
5 S   117  1313     1  0  80   0 - 21354 poll_s ?        00:00:44 nrpe
1 S     0  1340     1  0  80   0 - 205110 ep_pol ?       00:00:04 nscd
1 S    33  1488     1  0  80   0 -  9781 ep_pol ?        00:00:12 lighttpd
4 S     0  1518     1  0  80   0 -  1891 n_tty_ tty1     00:00:00 getty
5 S   116  1847     1  0  80   0 -  6601 poll_s ?        00:00:29 ntpd
1 S   118  2296     1  0  80   0 -  2948 poll_s ?        00:00:00 daemon
0 S   118  2297  2296  0  80   0 - 624825 futex_ ?       00:46:10 java
4 S   120  4676     1  0  80   0 -  3455 wait   ?        00:00:00 zabbix_agentd
1 S   120  4679  4676  0  80   0 -  3455 hrtime ?        00:01:33 zabbix_agentd
1 S   120  4680  4676  0  80   0 -  3455 poll_s ?        00:02:20 zabbix_agentd
1 S   120  4681  4676  0  80   0 -  3455 poll_s ?        00:02:21 zabbix_agentd
1 S   120  4682  4676  0  80   0 -  3455 poll_s ?        00:02:21 zabbix_agentd
1 S   120  4683  4676  0  80   0 -  3455 hrtime ?        00:00:14 zabbix_agentd
1 S     0 13499     2  0  80   0 -     0 worker ?        00:00:36 kworker/0:2
1 S     0 17775     2  0  80   0 -     0 worker ?        00:02:17 kworker/0:0
1 S     0 19275     2  0  80   0 -     0 worker ?        00:00:00 kworker/1:0
1 R     0 20124     2  0  80   0 -     0 ?      ?        00:00:00 kworker/1:1
1 S     0 20196     2  0  80   0 -     0 worker ?        00:00:00 kworker/1:2
4 S     0 20241   847  0  80   0 - 30600 poll_s ?        00:00:00 sshd
5 S 10036 20261 20241  0  80   0 - 30600 poll_s ?        00:00:00 sshd
0 S 10036 20262 20261  1  80   0 -  4870 wait   pts/0    00:00:00 bash
0 R 10036 20462 20262  0  80   0 -  2431 -      pts/0    00:00:00 ps
frobert@docbuilder:~$ ps -All+
```

00:00:48 / 00:01:12
Enter Enter Tab Esc OF Up Up Up Up Up F3 Esc Esc Esc [M �S Esc [M# �S Esc [M }4 Esc [M#}4 Enter Enter ls Enter less ex Tab Enter qps -All Enter Up

Directly search for commands and window titles

When using the indexer service of SPS (that is, not the Audit Player application), you can directly search in the detected window titles or the commands of the audit trails. For example, the **`command:sudo`** search expression will return the relevant audit trails from terminal connections, while the **`title:properties`** search expression will return audit trails from graphical connections. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Figure 4. Searching for commands in terminal connections



Scale: day

Screen content: command:sudo

Predefined filter conditions: Default filter *

Export format: Audit Player

Selected: 2015-03-31 00:00:00 - 2015-03-31 23:59:59 (2 results)

15 per page

		Hits and rank	Audit trail	Verdict	Protocol	Start time
			"ALL"		"ALL"	
1	ⓘ	2 ★★★★★	🖫	ACCEPT	ssh	2015-03-31 12:57:44
2	ⓘ	3 ★★★★★	🖫	ACCEPT	ssh	2015-03-31 13:32:46

REST API

More SPS features accessible using the REST API

To make integrating SPS into various management systems easier and more complete, you can now use the following SPS features using the RESTful API:

Upload and update plugins using the API. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

The documentation of the REST API received a major update, including sections on several previously undocumented features, an index of the API parameters, and a reorganization of the reference chapter.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

More SPS features accessible using the REST API

To make integrating SPS into various management systems easier and more complete, you can now access the several SPS features using the RESTful API, including:

- One Identity Safeguard for Privileged Sessions - Technical Documentation
- One Identity Safeguard for Privileged Sessions - Technical Documentation
- One Identity Safeguard for Privileged Sessions - Technical Documentation
- One Identity Safeguard for Privileged Sessions - Technical Documentation

Other features will be available via the REST API in future releases.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Configuring SPS using a REST API

To make integrating SPS into various management systems possible, you can now access SPS using a RESTful API. Currently the API supports only the parts of the configuration that are changed most often at large enterprises, namely Channel policies.

Other features will be available via the REST API in future releases.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Compliance and awards

HPE Security ArcSight CEF Certification

SPS, formerly known as Shell Control Box has received the HPE Security ArcSight CEF Certification, and can send logs to the HPE ArcSight Data Platform via a syslog-ng relay (syslog-ng Premium Edition 5 F6 or syslog-ng Open Source Edition 3.8 and later).

Cybersecurity Excellence Awards

The SPS, formerly known as Shell Control Box, was a finalist of the 2016 Cybersecurity Excellence Awards in the Privileged Access Management category. Another One Identity product, the syslog-ng Store Box (SSB), won in the Forensics category. Cybersecurity Excellence Awards are rewarded each year to individuals, products and companies that demonstrate excellence, innovation and leadership in information security. Nominees are awarded based on the content of their nomination and the popular vote by the Information Security Community.

SPS, formerly known as Shell Control Box wins at SC Awards Europe

The One Identity Safeguard for Privileged Sessions has won the SC Awards Europe in Best Identity Management category.

FSTEK certification

SPS, formerly known as Shell Control Box has obtained the Federal Service for Technical and Export Control (FSTEK) certification, which is compulsory for information security products in Russia.

Reports and PCI DSS compliance

To help you comply with the regulations of the Payment Card Industry Data Security Standard (PCI DSS), SPS can generate reports on the compliance status of SPS. Note that this is not a fully-featured compliance report: it is a tool to enhance and complement your compliance report by providing information available in SPS. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

The charts in the general operational reports of SPS have been redesigned. In addition, you can replace the One Identity logo on the cover page of SPS reports with your own logo. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Other

New guides

Separate installation guide. To improve how information is organized in the documentation set and make it easier for users to find information relevant to their roles we have moved the chapters related to installing SPS to a separate installation guide For more information on the installation guide, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Getting your SPS ready for Blindspotter. Blindspotter is the real-time user behavior analytics tool developed by One Identity, that can monitor the behavior of your privileged users based on the data extracted from SPS sessions. One Identity Safeguard for Privileged Sessions - Technical Documentation collects the most important configuration tasks to prepare your SPS installation to integrate with Blindspotter.

Auto-assign option for web gateway authentication

The new auto-assign option simplifies using the web gateway authentication if your users have multiple connections. After you enable auto-assignment, your users can turn on auto-assigning for their connections on the web gateway authentication page. After that, your users do not need to access the SPS web interface to assign every connection individually, it will happen automatically after the initial login. Note that this feature is available only in SPS version 4.4.1 and later.

10Gbit interface support

The SPS T-10 appliance is equipped with a dual-port SFP+ interface card labeled A and B. You can use the 10Gbit interface both for proxy traffic and for local services. This means that these interfaces can be used for the same purposes as the other 3 physical interfaces. That way, you can use SPS without any additional changes even if your network devices support only 10Gbit, and you must connect SPS to a 10Gbit-only network.

Splunk integration

One Identity provides an add-on and an app for Splunk, integrating SPS logs into Splunk, and making SPS information available in other Splunk apps, for example, in the Splunk Enterprise Security app. The One Identity SPS Add-On for Splunk and the One Identity SPS App for Splunk are both available for free in the splunkbase.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

Integration with Blindspotter

SPS now supports the operation of Blindspotter, the real-time user behavior analytics solution of One Identity. Blindspotter is a monitoring tool that maps and profiles user behavior to reveal human risk, and can analyze user behavior using the data from the audit trails recorded by SPS. Learn more about Blindspotter

Flexible network configuration and VLAN support

To improve the networking flexibility of SPS and make it easier to integrate into complex environments, the networking configuration of SPS has been significantly changed. The most important improvements are as follows:

- The Bastion and Router modes of operation have been removed, and now you can use SPS in both transparent and non-transparent connections. SPS will automatically handle nontransparent (Bastion-mode) and transparent (Router-mode) connections simultaneously.
- Bridge mode has been removed from SPS.
- The network interfaces labeled as LAN1, LAN2, and LAN 3 (earlier labeled as external, internal, and management) of the appliance were dedicated to specific tasks, and you could not use them for other purposes. Now you can configure and use them any way you need to. For example, you can receive transparent connections on LAN1 and LAN2, and route them to LAN3.
- You can configure multiple logical interfaces for every physical interface. Each logical interface can belong to a different VLAN, and have multiple alias IP addresses.
- You can configure the services available on SPS (for example, remote SSH access to SPS, access to the web interface, and so on) to be available only on specific IP addresses and ports. You can also restrict access to these services based on the IP address or network of the clients.
- You can control how SPS routes unmanaged traffic (that is, traffic that passes SPS but is not inspected or audited) between its network interfaces. You can connect interface pairs, and SPS will route all unmanaged traffic between the specified interface pairs.

For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation and One Identity Safeguard for Privileged Sessions - Technical Documentation.

Resolved issues

The following is a list of issues addressed in this release.

Table 1: Issues resolved in version 5.0.9

Resolved issue	Issue ID
Local credential store finds the first host entry, not the most specific one If there were multiple entries in a local credential store that matched both the target username and the target host network, SPS always used the first hit. As the order of the entries can't be changed that made it difficult to configure such credential stores. This behavior is now changed and we always use the most specific match from the host specifications.	PAM-7967
Long-running backups can fail if indexing is in use If a backup process took too much time to complete and there were some indexing jobs that finished during that, we incorrectly thought that the indexer engine crashed and restarted it, which caused the backup to fail, too. We have improved the keepalive check to make sure backups are not treated as failures.	PAM-7764
In HA mode both nodes use the same MAC address When SPS is configured in HA, the primary and the secondary nodes used the same MAC address on the network. This has been removed from the software so from now each node will communicate using its own MAC address.	PAM-7609
Floating point values ending with .0 not accepted as thresholds on Alert & Monitoring The UI did not accept floating point numbers ending with .0 on the Basic Settings > Alert & Monitoring page as alerting thresholds. This has been corrected and it is now possible to specify any floating point values there.	PAM-7606
Wrong client IP address sent as NAS IP ADDRESS during RADIUS authentication If RADIUS was used for authentication, the appliance always sent the first IP address of the first physical interface as the NAS IP ADDRESS during RADIUS authentication, which could cause problems depending on the network configuration. This has been fixed and we always use the source IP address configured for the config UI.	PAM-7300
Unicity check of user/host pairs in local credential only performed for new entries To avoid confusion, the user-host pairs were verified to be unique in local credential stores. However, this check was only performed for new entries and not when existing entries were changed. We fixed this and now we check changed entries, too.	PAM-7140
Permission query fails for groups with special characters	PAM-

Resolved issue	Issue ID
Querying the permissions of groups that had non-Latin-2 characters in their name always returned empty results on the AAA/Permissions page. This is now fixed and we support the full UTF-8 character set here.	6699
Content index archiving fails if there are many of Connection Policies If there are lots of Connection Policies configured, and content search has been enabled for a long time, archiving some very old content index files could fail due to an internal error that spawned thousands of nested processes. This behavior is now fixed and such archiving should work properly.	PAM-6341
Some system alerts are not sent out Due to a problem in the underlying SNMP infrastructure, some alerts, including high system load alerts, were not sent out even if they were enabled. This included SNMP traps and email-based alerts, too. The problem is fixed and all alerts are sent out properly now.	PAM-6122
Show missing elements on the Channel Policies page in read-only mode Some elements were not visible on the Channel Policy pages in read-only mode, making it impossible to review the current settings. This is now fixed and all elements are properly displayed.	PAM-4352
Misleading message about time sync of the primary-secondary nodes When a user tries to sync the secondary node's time to the primary node on the UI with the Basic Settings > Date & Time > Timezone/NTP settings > Sync Slave to Master button, the popup message said: "Time synchronization with other node succeed", even though clicking that button merely starts the synchronization process and it will take some time to complete. We changed that message to avoid confusion.	PAM-384
Indexer jobs failed if the search indices were archived On version 5.0.8, indexer jobs failed with a " database(SEVERE): (23): Error while performing request;" error if some lucene indices were already archived.	PAM-8157

Table 2: Issues resolved in version 5.0.8

Resolved issue	Issue ID
Azure installations are incorrectly marked as "tainted" When SPS was installed in the Azure cloud, the appliance incorrectly detected that some files were changed on it and issued a "tainted" warning which made it difficult to perform upgrades. This has been corrected.	PAM-6851
Possible partition label collision makes some T1 appliances unbootable Due to a problem with the installer some T1 appliances could not boot after a fresh install. This has been corrected. The problem did not affect upgraded	PAM-6814

Resolved issue	Issue ID
appliances.	
Domain join password is visible in debug logs If debug mode was enabled while the admin requested a domain join the password got logged into the system logs, which can be a serious security issue. We did a thorough overhaul of how we log actions that can involve credentials and other secrets and made sure that they don't end up in logs even when debug mode is turned on.	PAM-6444
Content subchapters in reports only contain the first hit for a session Even if there were multiple matches in a single session for a keyword defined for a content report subchapter, only the first hit was included in the report. This only affected reporting, all the hits could be found on the search interface.	PAM-6329
Upgrading the database of audit trail content can fail and break the entire upgrade process In some cases, upgrading the database that contains the results of the indexed screen contents for very old sessions (called Sphinx) could fail. This failure could cause the entire upgrade process to fail, and in some cases even the rollback to the previous version failed. We made the upgrade process more robust and the failure of upgrading this one component will not break the entire upgrade process.	PAM-6273
Incorrect access denied messages in Putty when gateway authentication is used in SSH If gateway authentication was used in SSH, the partial authentication flag was not set correctly throughout the process. This could cause some client applications, most notably Putty, to report an "access denied" failure to the user even though the connection could go on. This is now fixed and such connections are now handled well by all clients.	PAM-5582
Content-based alerting is now case-insensitive In some cases, window titles are recognized by OCR scanning when they have the wrong casing. From now on, content-based alerting will ignore the cases on command and screen-content events. This modification applies to all protocols, even if the extraction did not happen through OCR scan, such as in SSH.	PAM-4971

Table 3: Issues resolved in version 5.0.7

Resolved issue	Issue ID
Unnecessary NFS archive share remounts can cause problems with the archiving process Safeguard for Privileged Sessions checks the status of the archive targets and remounts the share as required. In case of NFS shares, this process did not work	PAM-6347

Resolved issue	Issue ID
properly and the share was remounted every time the check was performed even if the connection was working properly. This could cause problems with the archiving process. The problem did not affect SMB shares and has been fixed for NFS shares in this release.	
Upgrading from 4.4.x to the latest 5 LTS release is not allowed It was not possible to upgrade from any release in the 4.4.x branch to the latest 5.0.x release. It is now fixed and this upgrade path is possible.	PAM-6288
Upgrading the content index result database could fail and break the entire upgrade process In some cases, upgrading the database that contains the results of the indexed screen contents for very old sessions (called Sphinx) could fail and this failure could cause the entire upgrade process to fail and in some cases even the rollback to the previous version failed, too. We made the upgrade process more robust and the failure of upgrading this one component will not break the entire upgrade process.	PAM-6273
POST requests on the REST API are vulnerable against session fixation attacks The authentication endpoint accepts and reuses previously issued session ID cookies even if the authenticated session is expired, which can allow attackers to execute a session fixation attack if they can trick the requestor to execute specially crafted POST requests. This behavior was not present on GET requests. This issue has been fixed and session IDs are no longer reused after a new authentication.	PAM-6056
Password change notification in SPNEGO-enabled RDP connections In case a domain user's password is expired, the RDP server can "report" this by sending a TLS alert during the CredSSP setup. This was supported for plain NTLM authentications but not when SPNEGO was used. This is now fixed and password change notifications work properly when SPNEGO is in use.	PAM-6054
Large number of error messages in the logs for HTTP traffic For monitored HTTP sessions, a large number of error messages similar to "AttributeError: 'NoneType' object has no attribute 'startswith'" appeared in the logs even if connection passed through properly. This has been fixed and no such error messages appear in the logs anymore.	PAM-5802
SSH proxy crash if LDAP server is slow to respond Long response times of external LDAP servers that are accessed via STARTTLS could cause the SSH proxy to crash and consequently the termination of all ongoing SSH connections. This has been fixed and LDAP timeouts are now handled properly.	PAM-5610

Resolved issue	Issue ID
Invalid "Error storing XML database" alerts sent In different circumstances, while using the configuration interface, SPS sent out alerts notifying the administrator about an error "Error storing XML database". It was the result of an internal race condition and was not the signal of any actual problem. This has been corrected and no such messages are sent out anymore.	PAM-5266
Uploading TLS keys for syslog connections make the core firmware tainted Uploading TLS keys for syslog-ng into the syslog-ng/etc/ca.d directory made the core firmware tainted. The syslog-ng/etc/ca.d directory has been added to the tainted whitelist.	PAM-4543
When the web login IP address was changed on the UI, the user got locked out If the IP address of the web configuration interface is changed, the user needs to log in again on the new address. However, the configuration lock was not released before that, which meant that the user was temporarily prevented from accessing the configuration interface. This has been fixed and the configuration lock is now released automatically in this scenario.	PAM-2698
Large number of 'buffer too small to read octet string' error messages sent In different scenarios, SPS started sending out a large number of error alerts with the message 'buffer too small to read octet string'. This was not the signal of any actual problem with SPS rather only the result of a problem in the underlying net-snmp library used for self-monitoring. This has been fixed and no such alerts are sent out anymore.	PAM-1695
Invalid UTF-8 data received by a credential store plugin not handled properly If a credential store plugin was configured and one of the user-provided inputs (session cookie, username or the target host) contained an invalid UTF-8 character, it resulted in a hard-to-understand traceback in the logs and the termination of the session. Such problems are now detected in time, logged properly, and handled as normal authentication failures instead of an unexpected programming error in the plugin.	PAM-421

Product licensing

To enable a trial license

1. Visit the Download Trials page, and navigate to **One Identity Safeguard for Privileged Sessions > Download Free trial**.
2. Complete the registration form, and click **Download Trial**.
3. You will receive the details on how to access your license key and the download the ISO files in email.

To enable a purchased commercial license

1. Navigate to **My Account > My License Assets** on the support portal.
2. To access your license key, click **Retrieve Key** next to your product.
3. Once you have the license keys, navigate to **My Account > My Products** and click **Download** next to your product. The **Download Software** page is displayed.
4. Download the ISO image (install cdrom) of your product.

If you need help with accessing your license, navigate to the Licensing Assistance page, and follow the instructions on screen.

Upgrade and installation instructions

For details on upgrading to version 5.0.9, see One Identity Safeguard for Privileged Sessions 5 LTS Upgrade Guide in One Identity Safeguard for Privileged Sessions - Technical Documentation.

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

This release has the following known capabilities or limitations: OCR is limited to Nuance supported languages. No support for RTL languages.

About us

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

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.