# One Identity Safeguard for Privileged Sessions 6.0

# Release Notes

**04 February 2021, 11:17**

These release notes provide information about the One Identity Safeguard for Privileged Sessions 6.0 release.

# About this release

One Identity Safeguard for Privileged Sessions Version 6.0 is a long-term supportedfeature release with new features and resolved issues. For details, see:

- New features
- Resolved issues

NOTE:

For a full list of key features in One Identity Safeguard for Privileged Sessions, see Administration Guide.

# About the Safeguard product line

The One Identity Safeguard Appliance is built specifically for use only with the Safeguard privileged management software, which is pre-installed and ready for immediate use. The appliance is hardened to ensure the system is secured at the hardware, operating system and software levels. The hardened appliance approach protects the privileged management software from attacks while simplifying deployment and ongoing management -- and shortening the timeframe to value.

## Safeguard privileged management software suite

Safeguard privileged management software is used to control, monitor, and govern privileged user accounts and activities to identify possible malicious activities, detect entitlement risks, and provide tamper proof evidence. The Safeguard products also aid incident investigation, forensics work, and compliance efforts.

The Safeguard products' unique strengths are:

- One-stop solution for all privileged access management needs
- Easy to deploy and integrate
- Unparalleled depth of recording
- Comprehensive risk analysis of entitlements and activities
- Thorough Governance for privileged account

The suite includes the following modules:

- **One Identity Safeguard for Privileged Passwords** automates, controls and secures the process of granting privileged credentials with role-based access management and automated workflows. Deployed on a hardened appliance, Safeguard for Privileged Passwords eliminates concerns about secured access to the solution itself, which helps to speed integration with your systems and IT strategies. Plus, its user-centered design means a small learning curve and the ability to manage passwords from anywhere and using nearly any device. The result is a solution that secures your enterprise and enables your privileged users with a new level of freedom and functionality.
- **One Identity Safeguard for Privileged Sessions** is part of One Identity's Privileged Access Management portfolio. Addressing large enterprise needs, Safeguard for Privileged Sessions is a privileged session management solution, which provides industry-leading access control, as well as session monitoring and recording to prevent privileged account misuse, facilitate compliance, and accelerate forensics investigations.

  Safeguard for Privileged Sessions is a quickly deployable enterprise appliance, 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 forensics investigations.
- **One Identity Safeguard for Privileged Analytics** integrates data from Safeguard for Privileged Sessions to use as the basis of privileged user behavior analysis. Safeguard for Privileged Analytics uses machine learning algorithms to scrutinize behavioral characteristics and generates user behavior profiles for each individual privileged user. Safeguard for Privileged Analytics compares actual user activity to user profiles in real time and profiles are continually adjusted using machine learning. Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action - and ultimately prevent data breaches.

# New features

### New features and improvements in SPS 6.0.8:

- SPS is certified for the Citrix Virtual Desktops 19.12. in 6 LTS and the documentation has also been updated.
- Section Configuring the IPMI from the console has been extended with information about encryption methods and security extensions in the IPMI. For more information, see Administration Guide.

### New features in SPS 6.0.7:

### RDP login screen enhancements

The RDP login screen now allows you to paste text-based clipboard contents. It also provides a warning if Caps Lock is on.

### New features in SPS 6.0.4:

### Value range of Disk space fill-up prevention is now limited

The value range of **Disconnect clients when disks are: x percent used** field in **Basic Settings > Management > Disk space fill up prevention** is now limited to 50-98 percent.

For more information, see Preventing disk space fill-up.

### REST API improvements

- You can now check the synchronization status of cluster nodes. The value of the `sync_status` field displays whether the configuration of the SPS cluster node is synchronized with the configuration of the Central-Management node.

  In addition to the REST API, the following has changed on the SPS UI:

  **NOT FETCHED** has been added as a new status to **Basic Settings > Cluster management > Cluster management status**.

### Other improvements

- Starting from SPS versions 6.0.4 and 6.5.0, certificates with SHA1-based signatures are no longer trusted for Active Directory or LDAP authentication.

## New features in SPS 6.0:

### Search interface

The classic search interface of SPS is deprecated. If you have not used the new search interface before, read about its main changes compared to the classic search.

To search in the contents of a single session, you cannot use the **details > contents** tab of the Search interface anymore (except for sessions recorded before the upgrade). For new sessions, download the audit trail and use the search in the Safeguard Desktop Player application. Note that you can search in the contents of audit trails from the web interface, just not for specifics within a single session.

### Support for new hardware appliances

Version 6.0.9 supports the new Safeguard Sessions Appliance 3000 and 3500 appliances. For the technical details of these appliances, see "Hardware specifications" in the Installation Guide.

### LDAP

LDAP and Active Directory policies can be configured more flexibly to check group memberships. Also, to help troubleshoot LDAP-related issues, detailed documentation about how SPS resolves user IDs and group memberships has been added to the documentation.

### Plugins

Old credential store and authentication plugins are deprecated and will not be supported in upcoming releases. For details on updating your plugins, see Upgrading plugins for One Identity Safeguard for Privileged Sessions version 6.0.

If you want to write a new plugin for One Identity Safeguard for Privileged Sessions, you can use the new Plugin SDK for Safeguard for Privileged Sessions (SPS). For details, see the Plugin SDK for Safeguard for Privileged Sessions (SPS) documentation.

A new plugin is available for RADIUS multi-factor authentication. For details, see RADIUS Multi-Factor Authentication - Overview and RADIUS Multi-Factor Authentication - Tutorial.

### Join SPS to SPP

You can join your One Identity Safeguard for Privileged Sessions (SPS) deployment to your One Identity Safeguard for Privileged Passwords (SPP) deployment using the SPS web interface. For details, see "Joining SPS to SPP" in the Administration Guide.

### New Splunk application

To better integrate SPS with Splunk, a new Splunk app and addon is available. For details, see Using Splunk with One Identity Safeguard for Privileged Sessions.

### Installing support hotfixes

To solve problems you might encounter when using SPS faster and easier, it is now possible to upload individual hotfix packages to SPS if needed. For details, see "Support hotfixes" in the Administration Guide.

### Desktop Player

For audit trails of graphical session created and indexed with SPS 6.0, you can use the Safeguard Desktop Player application to search in the contents of the audit trail. For details, see Safeguard Desktop Player User Guide.

### REST API

- Health information about standalone SPS nodes is available on the `/api/health-status` endpoint.

### Changes in the external indexer

NOTE:

Due to legal reasons, installation packages of the external indexer application will be available only from the SPS web interface. After SPS versions 6.4 and 6.0.3 are released, the installation packages will be removed from our website.

### Enhancements

- The verbosity level of the audited sessions can be set separately for each Connection Policy. For details, see "Changing log verbosity level of One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
- DSA keys are not supported anymore.
- X.509 certificates are not supported for SSH authentication anymore.
- Log ingestion is not supported anymore.
- Lieberman ERPM is not supported natively anymore.

# New features between SPS 5.1 and 5.11

The following sections describe the main new features introduced between SPS versions 5.1 and 5.11.

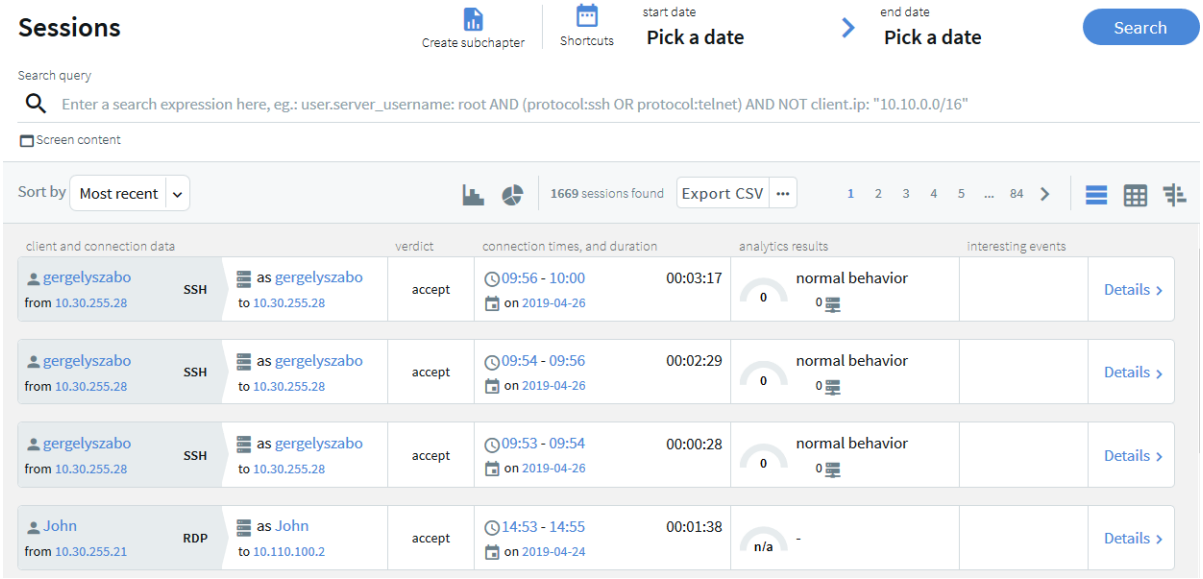
# New features between SPS 5.1 and 5.11 - search

## New Search interface

SPS's new search interface is built on a more modern technology stack and comes with a lean design and an easy-to-use interface. Our goal in overhauling the old search functionality was to better serve user needs and improve alignment with possible use cases. The result is a new search interface that offers ways to perform more complex searches in a more flexible way, often with improved speed.

Instead of simple tables, you can now display session information in a more visual view that allows you to get a faster overview about the important information of the sessions. For ongoing sessions, the Search interface is updated in real-time to always show the most up-to-date information. For more information on the new Search interface, see "Using the Search interface" in the Administration Guide.

**Figure 1: Search interface improvements**

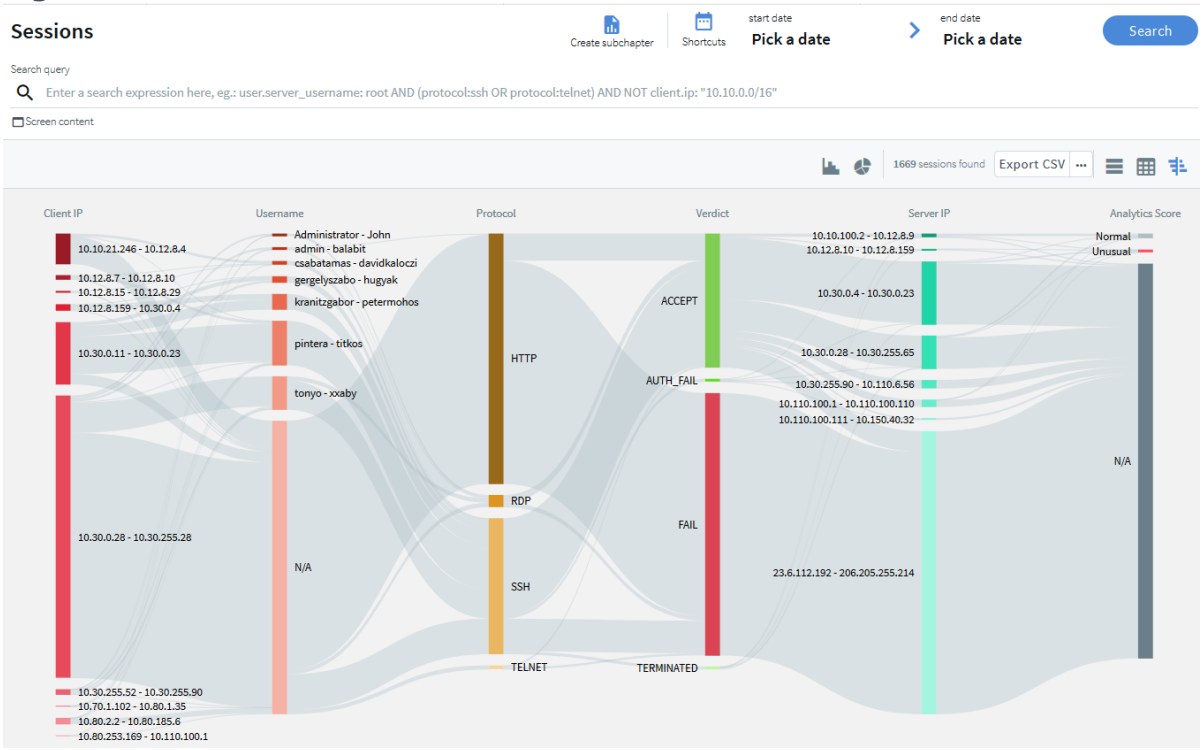



## Quick session analytics

The Search interface can now display an interactive visual overview of search results to quickly visualize their distribution along multiple attributes, such as client and target IP addresses, protocol, or usernames. It can be used to identify patterns in user behavior and drill down fast to the most relevant sessions.

For details, see "Searching audit trails: the One Identity Safeguard for Privileged Sessions (SPS) connection database" in the Administration Guide.

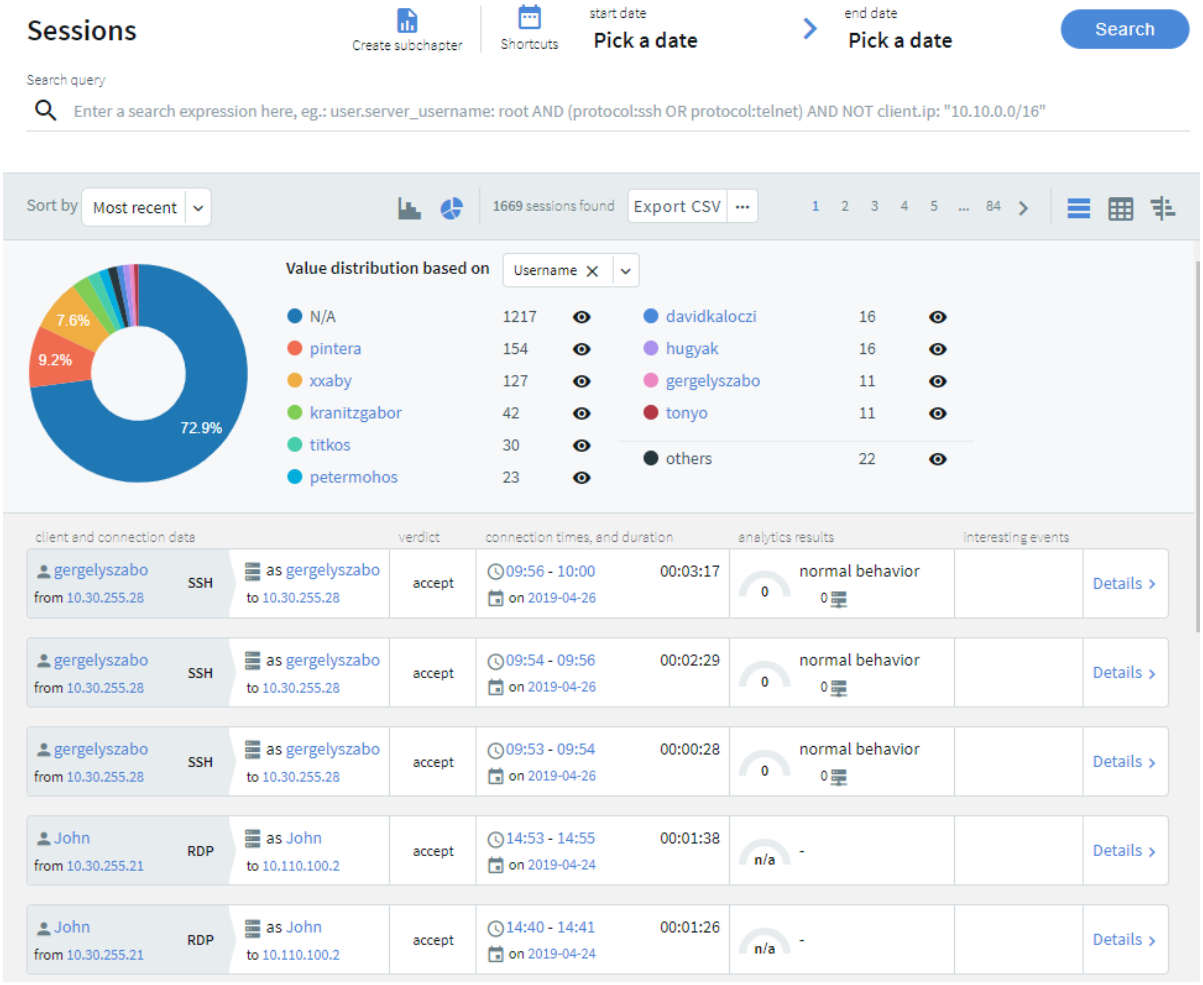
**Figure 2: Search — Flow view**




## Quick statistics and timeline from search results

The Search interface can now display a timeline showing the search results. Also, you can quickly sort and visualize the distribution of the sessions based on their various metadata, for example, username, server address, and so on.

**Figure 3: Search — Displaying statistics and timeline**




## Screen content search improvements

- You can now combine content search queries arbitrarily with other search queries. As a result, flow view and quick statistics charts on the Search interface can handle content searches.
- Screen content search is now available in search clusters.
- Screen content hits are no longer limited to 3000 per query.

## Search queries and statistics as custom report subchapters

It is now possible to turn any search query or statistics into a subchapter that can be included in reports. You can define reports about the monitored traffic in a more flexible and easy-to-use way than was possible before. Reporting subchapters can also include reports about specific content search queries (Reporting > Search subchapters). For details, see "Creating search-based report subchapters from scratch" in the Administration Guide.

# New features between SPS 5.1 and 5.11 - clustering

## Central configuration management

It is now possible to join multiple SPS nodes into a cluster, monitor their status, and update their configuration from a central location. Note that this feature is currently in an experimental status: consult your Support representative before enabling it.

For details, see "Managing Safeguard for Privileged Sessions (SPS) clusters" in the Administration Guide and "Manage Safeguard for Privileged Sessions clusters" in the REST API Reference Guide.

## Improvements to central configuration management

Starting with version 5 F6, it became possible to join multiple SPS nodes into a cluster, monitor their status, and update their configuration from a central location. In this new version, this feature was improved in a number of ways:

- You can now promote a node to become the Central Management node and join additional nodes to the cluster using the web interface of One Identity Safeguard for Privileged Sessions. Previously, building a cluster was only possible through the REST API.
- When building a cluster, using the REST API, you can now query the join status of nodes to find out whether or not particular nodes have been joined to a cluster.
- When using a configuration synchronization plugin, it is now possible to enable the plugin through the web interface. Previously, this was also only possible through the REST API.
- SPS now also provides information about the status of configuration synchronization.
- When you want to create a backup or archive policy on SPS instances that are nodes in a cluster, you can choose to include the node ID in the path to the relevant directory name to prevent cluster nodes from backing up data to the same location, and so overwriting each other's data. For details, see "Data and configuration backups" in the Administration Guide and "Archiving or cleaning up the collected data" in the Administration Guide.
- When querying the status of all nodes or one particular node using the `/api/cluster/status` endpoint, the response now contains the hash of the latest downloaded configuration file (`downloaded_xml_hash`) that the nodes used for configuration synchronization.

Note that the cluster management feature is currently in an experimental status: consult your Support representative before enabling it.

For details, see "Assigning roles to nodes in your cluster" in the Administration Guide and "Manage Safeguard for Privileged Sessions clusters" in the REST API Reference Guide.

### Central search across clusters

Starting with SPS version 5 F6, it became possible to join multiple SPS nodes into a cluster, monitor their status, and update their configuration from a central location. Starting with this version, 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. Consult with the Support Team to learn more about network and capacity requirements.

For more information, see "Searching session data on a central node in a cluster" in the Administration Guide.

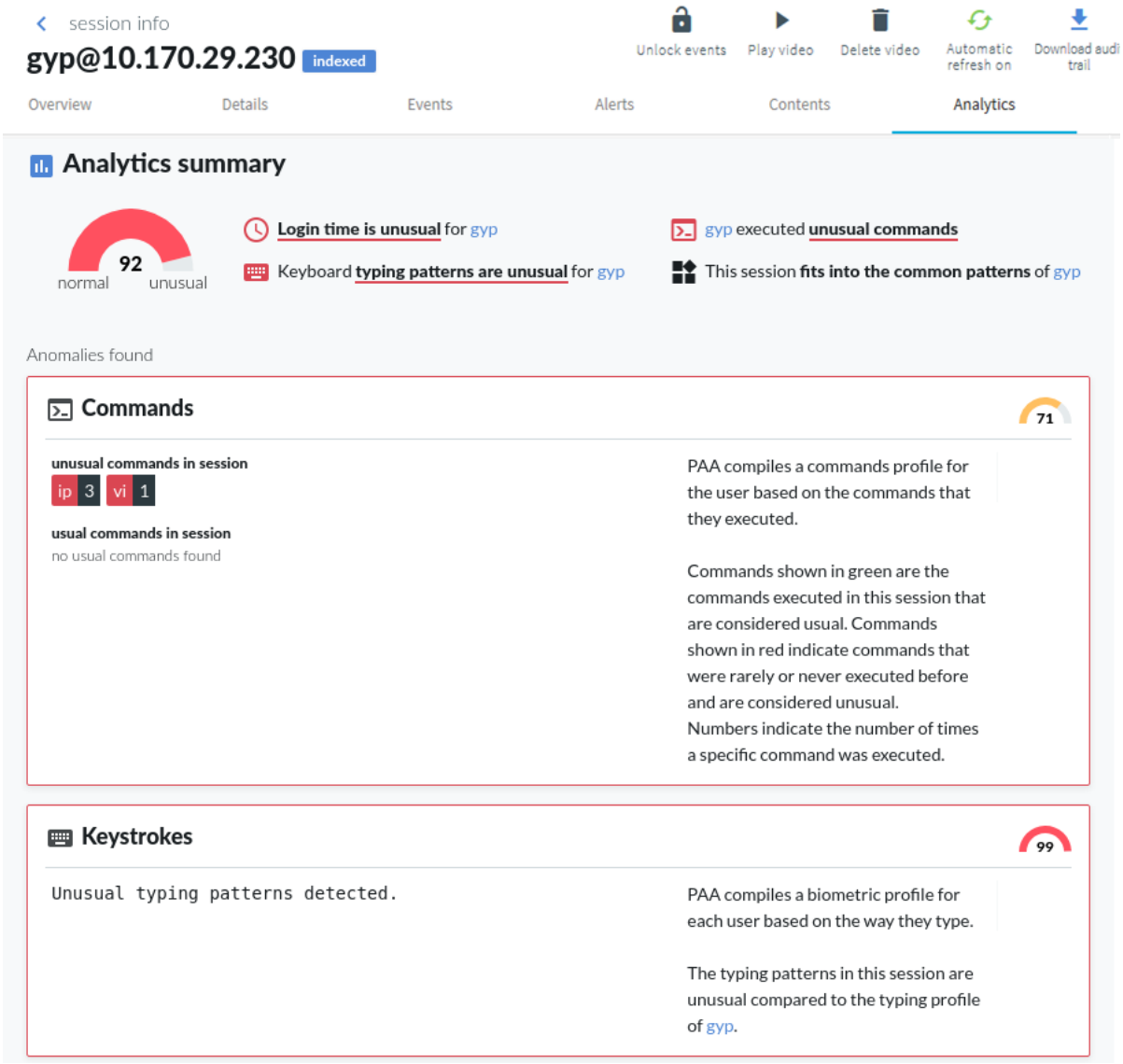
# New features between SPS 5.1 and 5.11 - analytics

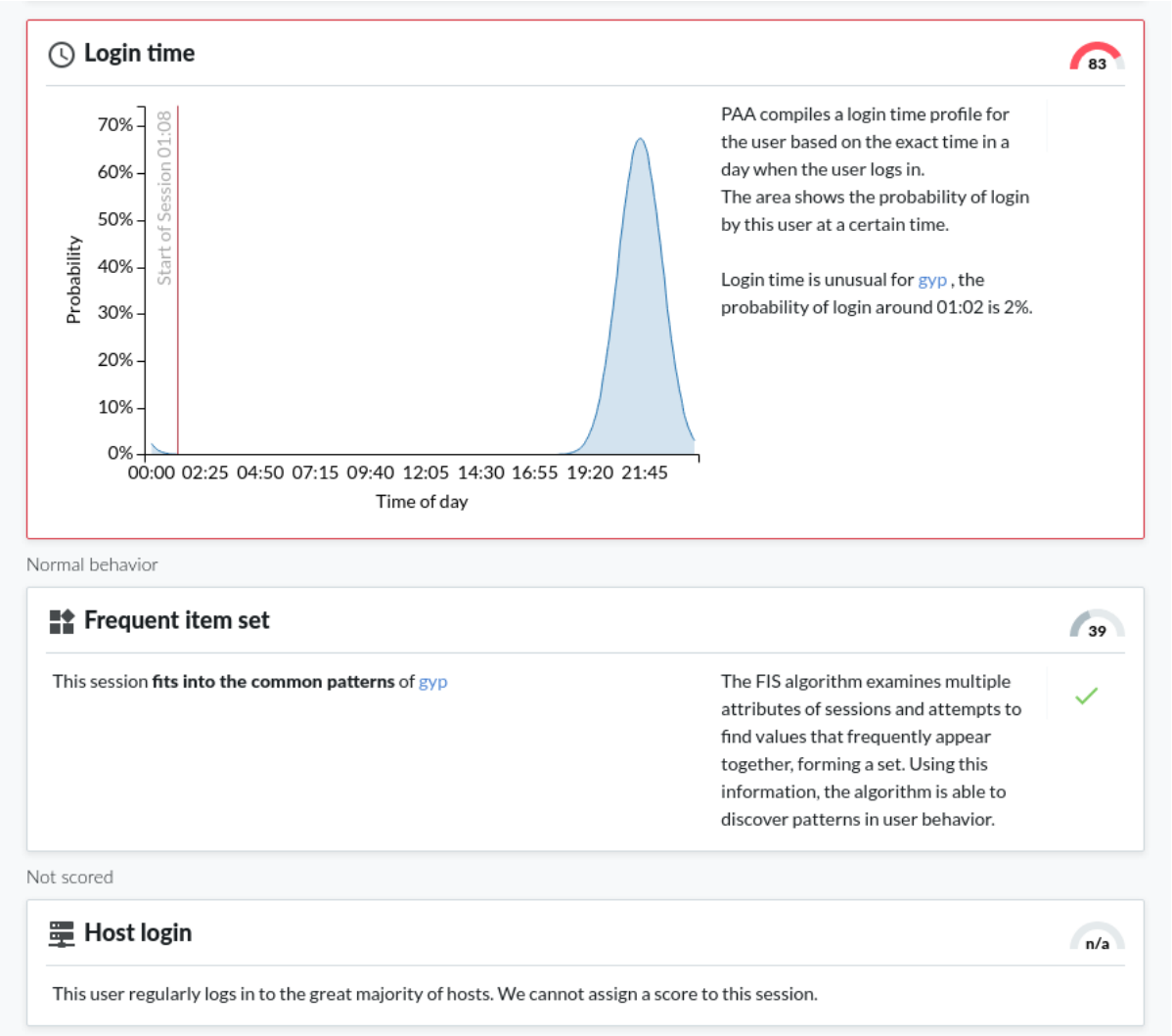
### One Identity Safeguard for Privileged Analytics on SPS

You can now run One Identity Safeguard for Privileged Analytics directly on SPS, to get insight about your privileged users, prevent identity theft, and more. To enable One Identity Safeguard for Privileged Analytics and analyze the behavior of your users, SPS requires a special license. Also, depending on the number of your users and sessions, the performance and sizing of SPS must be considered. If you are interested in One Identity Safeguard for Privileged Analytics, contact your One Identity representative, or directly contact our Sales Team.

If you are using One Identity Safeguard for Privileged Analytics, you can configure your indexer policies to extract biometric data from the recorded sessions for keystroke and pointing-device analytics.

**Figure 4: One Identity Safeguard for Privileged Analytics**






## Detecting script usage with One Identity Safeguard for Privileged Analytics

Through enabling the Safeguard for Privileged Analytics module (licensed separately but can be enabled free for a 2-month trial), it is now possible to detect user accounts that show highly periodic and repetitive behavior that is likely the result of scripted activity.

For more information, see Safeguard for Privileged Analytics Configuration Guide.

## Gapminder algorithm

The *gapminder algorithm* is able to detect scripted sessions based on the time gaps between the sessions that belong to a given account. When the time gaps between sessions have typical, repeating values, then that suggests unnatural periodic behavior.

### Improvements to command algorithm

The command algorithm of One Identity Safeguard for Privileged Analytics has been improved significantly. Previously, the algorithm only analyzed users' activities separately for each user. Starting with this version, we also check if a command is issued frequently on the given server or globally by the majority of the users to improve the false positive rate.

### New analytics algorithms

The window title algorithm analyzes window titles in graphical protocol sessions to uncover unusual user behavior. It identifies users based on what window titles they usually have on their screen. It is currently an experimental algorithm and is disabled by default.

The host login algorithm analyzes how likely it is for a user to log in to a given host. Peer groups are taken into consideration: when users log in to hosts that are unusual for them but frequently used by their peers, such sessions are scored low.

The frequent item set (FIS) algorithm examines multiple attributes of sessions and attempts to find values that frequently appear together, forming a set. Using this information, the algorithm is able to discover patterns in user behavior.

### Fine-tune SPA configuration:

You can now configure which analytics algorithms to execute separately for every Connection Policy using **Analytics Policies**.

### Self-evaluation of algorithms:

It is now possible to run a self-evaluation tool on all algorithms to get feedback about how well they perform in a given environment. Using the results of the evaluation, it is possible to fine-tune your algorithms where necessary.

For details, see Safeguard for Privileged Analytics Configuration Guide.

### Free 2-month trial of One Identity Safeguard for Privileged Analytics available for all users

You can enable One Identity Safeguard for Privileged Analytics for free for 60 days on your SPS host to gain insight into what your users are doing, and how risky their actions are.

For more information, see Safeguard for Privileged Analytics Configuration Guide.

# New features between SPS 5.1 and 5.11 - integration and plugins

### Join to Starling

You can now join SPS to One Identity Starling. One Identity Starling helps to combine products from the One Identity line to create a secure and customizable cloud service. For details on One Identity Starling, see Starling - Technical Documentation.

For more information, see "Joining to One Identity Starling" in the Administration Guide.

### SIEM forwarder

You can now forward the log messages and events related to what happens in the privileged sessions to an external SIEM, such as Splunk or Arcsight, or other third-party systems that enable you to search, analyze, and visualize the forwarded data. SPS can send these events as industry-standard RFC3164 syslog messages, with the data formatted either as JSON or in Common Event Format (CEF).

For more information, see "Using the universal SIEM forwarder" in the Administration Guide.

### Enhancements to Credential Store plugin for One Identity Safeguard for Privileged Passwords

The Credential Store plugin for One Identity Safeguard for Privileged Passwords now supports connecting to a cluster of One Identity Safeguard servers. In addition, it is now possible to resolve the IP addresses of target servers to hostnames, and to expand domain names to full domain names when not provided in their FQDN form. For details, see How to connect One Identity Safeguard for Privileged Passwords with One Identity Safeguard for Privileged Sessions.

### Integrate with One Identity Total Privileged Access Management (TPAM)

An official plugin is now available that allows using TPAM as an external credential store.

For more information, see DEPRECATED How to connect One Identity TPAM with One Identity Safeguard for Privileged Sessions.

- The Duo Multi-Factor Authentication plugin has been updated for Duo Client version 3.3.0.
- A new Credential Store plugin is available for Safeguard for Privileged Passwords.
- A new Log Adapter plugin is available for SSHD application logs.

### Improved Splunk integration

Forwarding data from SPS to Splunk has been greatly simplified, now you can configure SPS on the web interface to do so. Also, the amount of data forwarded to Splunk has been

optimized. For details, "Using the Splunk forwarder" in the Administration Guide.

**Figure 5: Basic Settings > Management > Splunk forwarder — Sending session data to Splunk**

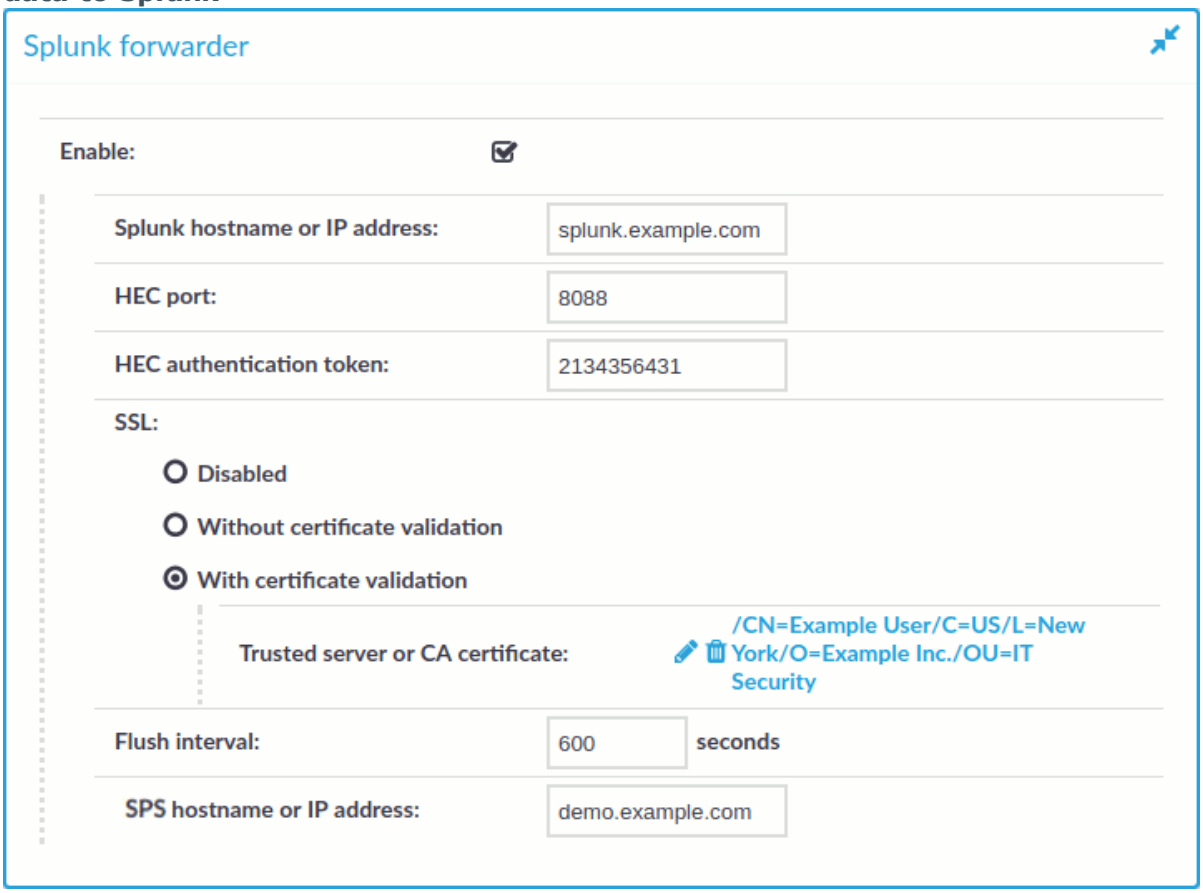
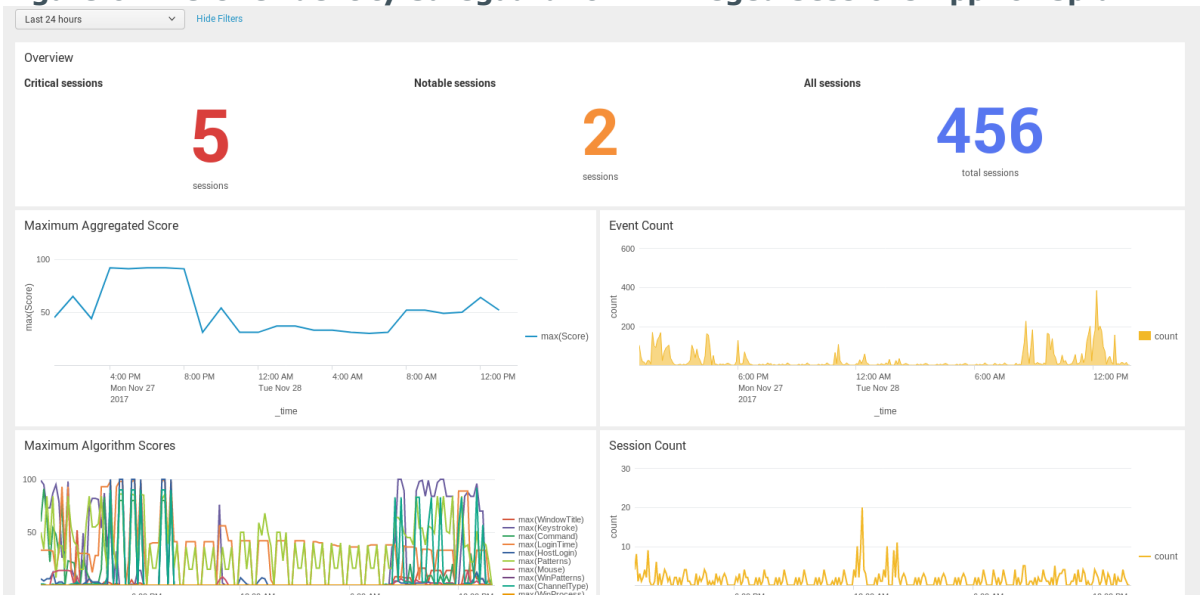



**Figure 6: The One Identity Safeguard for Privileged Sessions App for Splunk**



## New Authentication and Authorization plugins

SPS acts as a central authentication gateway, enforcing strong authentication before users access sensitive IT assets. SPS can integrate with remote user directories to resolve the group memberships of users who access nonpublic information. Credentials for accessing information systems can be retrieved transparently from SPS's local credential store or a third-party password management system. This method protects the confidentiality of passwords as users can never access them. When used together with a multi-factor authentication provider, SPS directs all connections to the authentication tool, and upon successful authentication, it permits the user to access the information system.

SPS can interact with your third-party multi-factor authentication account and can automatically request strong multi-factor authentication for your privileged users who are accessing the servers and services protected by PSM. When used together with a third-party multi-factor authentication, SPS directs all connections to the tool, and upon successful authentication, it permits the user to access the information system.

The integration adds an additional security layer to the gateway authentication performed on SPS.

Multi-factor authentication plugins are available for the following products:

- *Duo*

  For an overview, see: Duo Multi-Factor Authentication - Overview

  For detailed tutorial and configuration instructions, see: Duo Multi-Factor Authentication - Tutorial
- *inWebo*

  For an overview, see: inWebo Multi-Factor Authentication - Overview

  For detailed tutorial and configuration instructions, see: inWebo Multi-Factor Authentication - Tutorial
- *Okta*

  For an overview, see: Okta Multi-Factor Authentication - Overview

  For detailed tutorial and configuration instructions, see: Okta Multi-Factor Authentication - Tutorial
- *RSA*

  For an overview, see: RSA Multi-Factor Authentication - Overview

  For detailed tutorial and configuration instructions, see: DEPRECATED RSA Multi-Factor Authentication - Tutorial
- *Starling*

  For an overview, see: Starling Two-Factor Authentication - Overview

  For detailed tutorial and configuration instructions, see: Starling Two-Factor Authentication- Tutorial
- *YubiKey*

  For an overview, see: YubiKey Multi-Factor Authentication - Overview

For detailed tutorial and configuration instructions, see: YubiKey Multi-Factor Authentication - Tutorial

### Other changes

- *Plugin configuration files in debug bundle:* When creating debug bundles for troubleshooting purposes (for details, see "Collecting logs and system information for error reporting" in the Administration Guide), SPS now includes the configuration files of any plugins installed. Note that depending on the plugin, these configuration files can contain sensitive information, such as passwords or API keys. In this case, edit the plugin-related files in the `plugins` directory of the debug bundle and delete the sensitive information.

### New documents

- The Creating custom Authentication and Authorization plugins document is now publicly available. This document describes how to create custom Authentication and Authorization plugins.
- The Creating custom Credential Store plugins document is now publicly available. This document describes how to create custom Credential Store plugins.
- The documentation of the Safeguard for Privileged Sessions Plugin Software Development Kit (Plugin SDK) is now publicly available at https://oneidentity.github.io/safeguard-sessions-plugin-sdk/. The Plugin SDK provides base classes and services to enable rapid development of Python 3 plugins for the Safeguard for Privileged Sessions (SPS) product. SPS plugins released in the future will use this SDK.

# New features between SPS 5.1 and 5.11 - indexing

### Indexing sessions in near real-time

You now have the option to configure connection policies with near real-time indexing priority, meaning that you can start indexing sessions while they are still ongoing. This requires that you configure your indexers with the appropriate settings and capabilities. For details, see "Configuring the internal indexer" in the Administration Guide and "Configuring the external indexer" in the Administration Guide.

### HSM support in external indexers

The external indexers now support using Hardware Security Modules to process encrypted audit trails. For details, see "Configuring a hardware security module (HSM) or smart card to integrate with external indexer" in the Administration Guide.

### Lightweight indexing

One Identity Safeguard for Privileged Sessions is capable of analyzing the contents of the sessions it monitors to provide help analytics and speed up forensics investigations. This process is called indexing.

You can now select the depth of indexing: lightweight and full indexing.

Lightweight indexing is now enabled by default in case of a newly installed SPS or when you add new connection policies. If indexing was enabled for a connection policy it is converted to full indexing automatically during the upgrade.

Lightweight indexing is significantly faster than full indexing, but it extracts only the executed commands and the window titles 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).

For more information, see "Configuring the internal indexer" in the Administration Guide.

### Performance improvements in indexing graphical sessions

To make the text displayed in graphical sessions (for example, RDP) SPS uses optical character recognition. The way this is done has been greatly optimized. Depending on the exact scenario and the contents of the session, this can significantly decrease the time required to index the audit trails.

### Other changes

- When using a hardware security module (HSM) or smart card to integrate with an external indexer, the chroot is not used anymore, the solutions provided by RedHat/CentOS can be used. For more information, see "Configuring a hardware security module (HSM) or smart card to integrate with external indexer" in the Administration Guide.
- It is now possible to change the accuracy level of the Optical Character Recognition (OCR) analysis of graphical sessions. The accuracy level remains unchanged for existing indexer policies but the new default is the "balanced" setting that offers much improved performance with a minimal trade-off in accuracy.

  For details, see "Configuring the internal indexer" in the Administration Guide.

# New features between SPS 5.1 and 5.11 - Safeguard Desktop Player

### Safeguard Desktop Player replays audit trails of X11 sessions

The Safeguard Desktop Player application can now replay audit trails that contain graphical X11 sessions (the contents of the *X11 Forward* channel of the SSH protocol).

For further details, see "Replay X11 sessions" in the Safeguard Desktop Player User Guide.

### Install the Safeguard Desktop Player application on Mac

It is now possible to install the Safeguard Desktop Player application on Mac.

For more information, see "Install Safeguard Desktop Player on Mac" in the Safeguard Desktop Player User Guide.

### Follow active connections in Safeguard Desktop Player

It is now possible to follow active connections in semi-real time using Safeguard Desktop Player. In case you notice some user action that poses a security risk, you have the option to terminate the session you are monitoring. For detailed information, see "Replay audit files in follow mode" in the Safeguard Desktop Player User Guide

### Audit trail encryption improvements

**CAUTION:**

**One Identity Safeguard for Privileged Sessions (SPS) 5 F4 and later versions use a new encryption algorithm to encrypt the recorded audit trails (AES128-GCM). This change has the following effects:**

- **If you are using external indexers to index your audit trails, you must upgrade them to the latest version. Earlier versions will not be able to index encrypted audit trails recorded with SPS 5 F4 and later.**
- **To replay an encrypted audit trail recorded with SPS 5 F4 or later, you can use the latest version of the Safeguard Desktop Player application, or the browser-based player of SPS. You cannot replay such audit trails using earlier versions of Safeguard Desktop Player, nor any version of the Audit Player application.**

You can now manually re-encrypt your audit trails with a new encryption key. This is useful if you want to share encrypted audit trails with third parties — the data remains encrypted, but you do not have to share your encryption keys. For details, see "Sharing an encrypted audit trail" in the Safeguard Desktop Player User Guide.

# New features between SPS 5.1 and 5.11 - Protocols

### Security settings of TLS sessions

You can now uniformly set the TLS security settings of HTTP, RDP, Telnet, and VNC connections, including the permitted ciphers and TLS versions on the **<Protocol> Control > Settings** pages.

To ensure the security of your sessions, SSL encryption is not supported anymore, only TLS 1.0 and later.

### Using GSSAPI in SSH connections

You can now use an Authentication Policy with GSSAPI and a Usermapping Policy in SSH connections. When an SSH Connection Policy uses an Authentication Policy with GSSAPI, and a Usermapping Policy, then SPS stores the user principal as the **Gateway username**, and the username used on the target as the **Server username**.

Note that this change has the following side effect: when using an Authentication Policy with GSSAPI, earlier versions of SPS used the `client-username@REALM` username to authenticate on the target server. Starting with version 5.9.0, it uses the `client-username` as username. Configure your servers accordingly, or configure a Usermapping Policy for your SSH connections in SPS.

### Session cookies in HTTP auditing

SPS can now distinguish the audited HTTP requests and responses based on the session cookies of web applications. For details, see "Creating and editing protocol-level HTTP settings" in the Administration Guide.

### Authenticate HTTP/HTTPS connections on the SPS gateway

SPS now provides a way to authenticate non-transparent HTTP/HTTPS connections on SPS to local and external backends (LDAP, Microsoft Active Directory, RADIUS). The client must support proxy authentication.

For more information, see "Creating a new HTTP authentication policy" in the Administration Guide.

### Credential store support for TN3270 protocol

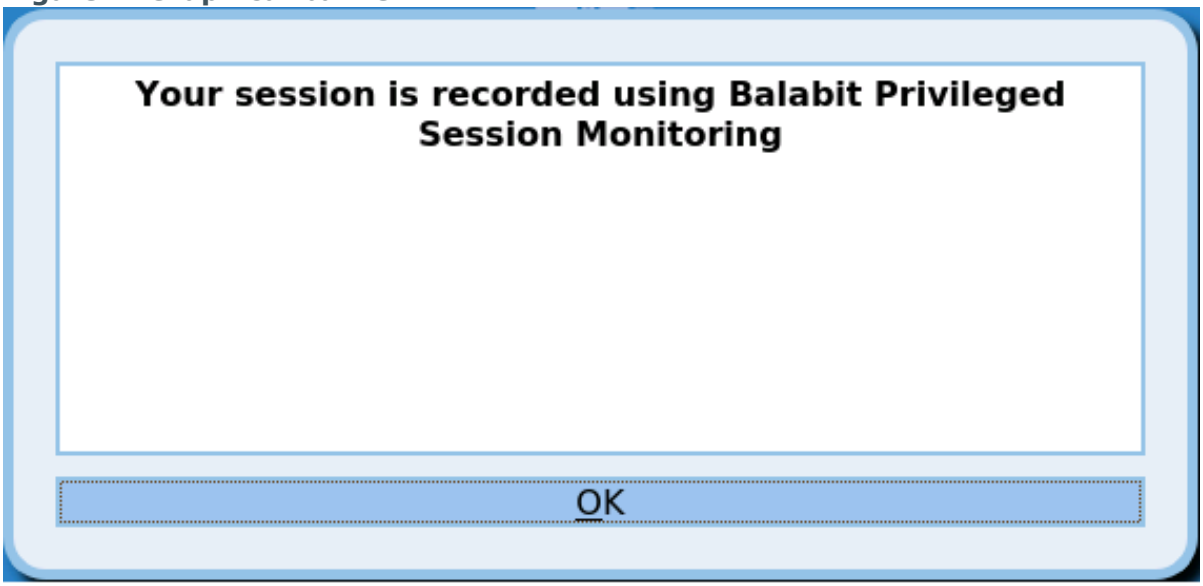
SPS can now be configured to check out passwords from the built-in or external credential stores, such as One Identity Safeguard for Privileged Passwords, and play them in during a connection using the TN3270 protocol.

## New features between SPS 5.1 and 5.11 - RDP

### RDP improvements

You can now display a banner to your clients in RDP sessions. For example, this banner can inform the users that the connection is audited. For details, see "Creating and editing protocol-level RDP settings" in the Administration Guide.

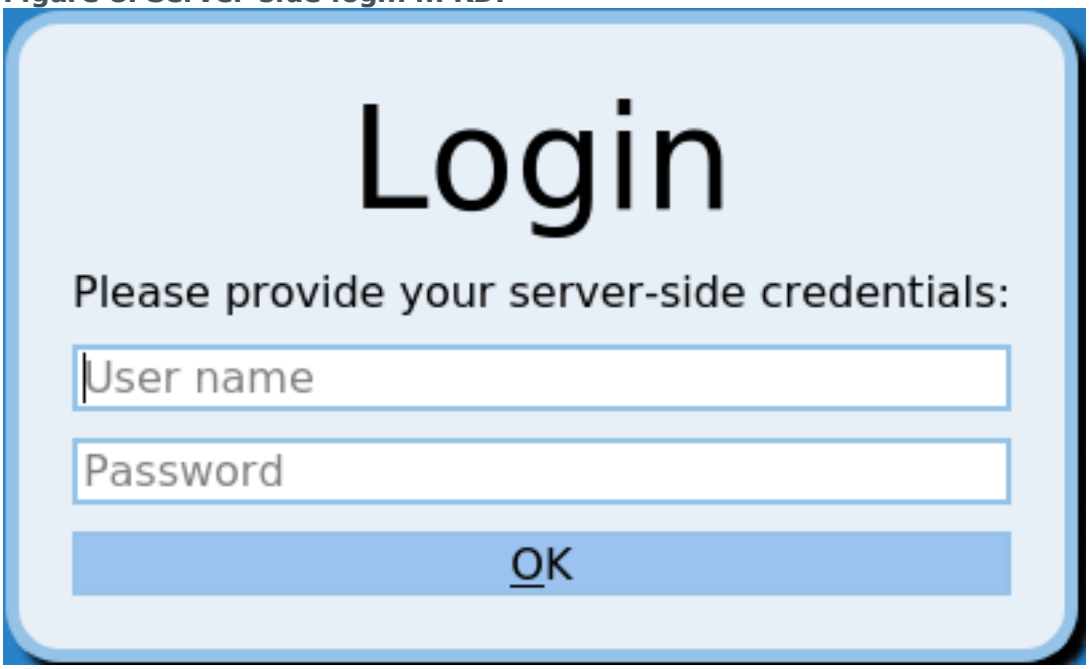
**Figure 7: Graphical banner in RDP**




The Authentication and Authorization plugins now can request information interactively from the user in a graphical window, for example, a ticket ID, or a one-type password. To request a plugin that interoperates with your authentication or authorization system, contact our Support Team.

If the server requires Network Level Authentication and the **Allow me to save credentials** option is not selected in the RDP client, SPS now automatically displays a graphical prompt where the users can enter their usernames and passwords.

**Figure 8: Server-side login in RDP**



### Interactive RDP improvements

When using inband destination selection, your users now do not have to encode any data in the username: SPS can display an interactive prompt in the RDP connection to request the address of the destination server, username, and other required information. For details, see "Inband destination selection in RDP connections" in the Administration Guide.

As a smaller improvement, SPS now supports using certificate chains in the signing CA used for RDP connections.

### TLS-encryption for RDP connections

Enabling TLS-encryption in an RDP connection policy has been simplified. When the connection is encrypted, SPS has to show a certificate to the peer. You can define the type of certificate to show to the peers.

In case of compatibility issues, you also have the option to allow fallback to legacy RDP Security Layer (also known as: Standard RDP Security). However, it is not advised due to security reasons.

For more information, see "Enabling TLS-encryption for RDP connections" in the Administration Guide.

### Windows 2019 Server support

SPS now supports Windows 2019 Server as a client and server in RDP sessions.

### Certificate Revocation Lists (CRLs) in signing CAs

It is now possible to configure the CRL that you generated using your Certificate Authority (CA) in your Public Key Infrastructure (PKI) solution. This is the CRL information that will be shown to clients connecting to SPS. For more information, see "Signing certificates on-the-fly" in the Administration Guide.

# New features between SPS 5.1 and 5.11 - web interface

### Required minimum version of encrypted protocol

You can now configure the required minimum version of the default web listener.

The default setting is TLS 1.2. You can configure SPS to use TLS 1.0, but it is not advised, because there are known serious attacks against TLS (for details, see: https://tools.ietf.org/html/rfc7457).

For more information, see "Configuring user and administrator login addresses" in the Administration Guide.

### Boot messages and upgrade logs displayed on web interface

In addition to displaying upgrade logs and boot messages on the local console, SPS now shows information about the upgrade and reboot processes on the web interface, too. The information displayed in the browser and on the console is the same. For details, see "Controlling One Identity Safeguard for Privileged Sessions (SPS): reboot, shutdown" in the Administration Guide and "Upgrade checklist" in the Administration Guide.

NOTE:

This feature is enabled after the first boot to version 5 F2 or later. So during the upgrade from 5.0 to version 6.0, you will not be able to see any upgrade logs on the web interface.

### Maximum Transmission Unit (MTU) for network interfaces

To support deployment in more complex networking environments, it is now possible to set the MTU for each network interface individually. For details, see "Network settings" in the Administration Guide and "Managing logical interfaces" in the Administration Guide.

### Other changes

- When using X.509 certificates to authenticate on the SPS web interface, SPS can now extract the name of the user from the UserPrincipalName field of the certificate. For details, see "Authenticating users with X.509 certificates" in the Administration Guide.
- Command detection and window title detection in content policies have changed and they are case-insensitive as of SPS version 5.8.0. In earlier versions, both used to be case-sensitive. For more information, see "Creating a new content policy" in the Administration Guide.
- The **Indexing history** section on the **Indexer > Indexer status** page has been removed and it is now possible to search for indexing details. For more information about the indexing search filters that you can use, see "List of available search filters" in the Administration Guide.
- Alerts defined in Content Policies are now only sent out again if there is change in the matched screen contents to avoid flooding security administrators with alerts.
- The script used for exporting and importing the configuration of SPS through the console has changed, it is now: `/opt/scb/bin/configbundle.py`. As a result, the required commands have changed, too. For details, see "Exporting and importing the configuration of SPS using the console" in the Administration Guide.
- It is now possible to upload a certificate chain when configuring a remote syslog server to send system log messages to. This is handled both on the web interface and the REST API of SPS. For details, see "Configuring system logging" in the Administration Guide.
- It is now possible to specify the base DN of LDAP subtrees for users and for groups separately. Specifying a sufficiently narrow base for the LDAP subtrees can speed up

LDAP operations. For details, see "Managing One Identity Safeguard for Privileged Sessions (SPS) users from an LDAP database" in the Administration Guide and "Authenticating users to an LDAP server" in the Administration Guide.

- Backup policies can be configured to run more than once a day.
- You can now select which Server Message Block protocol version to use in the Archive and Backup policies if your server uses **SMB/CIFS**.

# New features between SPS 5.1 and 5.11 - REST API

### Sessions schema change in REST API

In order to better integrate SPS with One Identity Safeguard for Privileged Analytics, some architectural changes have been introduced. These changes have brought alterations for the sessions schema of the REST API. As a result, REST responses have changed in the case of the following endpoints:

- `/api/audit/sessions`
- `/api/audit/sessions/<session-id>`
- `/api/audit/sessions/<session-id>/content`
- `/api/audit/sessions/<session-id>/alerts`
- `/api/audit/sessions/<session-id>/events`
- **Search, download and index sessions section restructure**

  The Search, download and index sessions section has been restructured and updated in the SPS REST API.

  For more information, see "Search, download, and index sessions" in the REST API Reference Guide.
- **HTTP connection policies can now be configured through REST**

  The endpoint is now writable and allows create, update and delete.

  For more information, see "HTTP connections" in the REST API Reference Guide.
- **The user now has the same privileges on the web UI and REST API**

  For the user to have full access over the SPS REST API, they must have the **REST server** privilege. The user privileges on the web UI and REST API are now synchronized. For example, if the user has the **ICA Control / Connections** privilege then they can access this page on the web UI and also the `/api/configuration/ica/connections` endpoint on the REST API.

  For more information, see "Authenticate to the SPS REST API" in the REST API Reference Guide.
- **Changes to audit data access rules (ADAR) on REST**

The endpoint can only be queried and is not writable. It does not allow create, update, or delete.

For more information, see "Audit data access rules" in the REST API Reference Guide.

- When querying the `/api/info` endpoint, the response now contains the hash of the XML database (`config_hash`) running on a given SPS host.

  For details, see "Retrieve basic firmware and host information" in the REST API Reference Guide.

- It is now possible to change the settings for the RDP protocol using the `/api/configuration/rdp/settings_policies/` endpoint.

  For details, see "RDP settings policies" in the REST API Reference Guide.

- The `api/audit/sessions/stats` endpoint provides statistics about recorded sessions. For details, see "Session statistics" in the REST API Reference Guide.
- The `api/audit/sessions/histogram` endpoint provides a histogram about the recorded sessions. For details, see "Session histogram" in the REST API Reference Guide.
- You can now enable One Identity Safeguard for Privileged Analytics using the REST API. For details, see "Enable One Identity Safeguard for Privileged Analytics" in the REST API Reference Guide.
- The `api/configuration/policies/analytics` endpoint allows you to configure One Identity Safeguard for Privileged Analytics by adding and removing analytics policies. For details, see "Configure One Identity Safeguard for Privileged Analytics" in the REST API Reference Guide.
- You can now read and update the license of SPS. For details, see "Manage the SPS license" in the REST API Reference Guide.
- Changing the root and admin passwords of SPS has been documented. For details, see "Passwords stored on SPS" in the REST API Reference Guide.
- Configuring RDP connection policies using the REST API has been documented. For details, see "RDP connection policies" in the REST API Reference Guide.
- You can complete the Welcome Wizard using the API.
- You can now upload the SPS license file using the API.
- You can now change the password of local users, for example, the `admin`, and the `root` passwords.
- *New content endpoint:* A new endpoint, `/api/audit/sessions/<session-id>/content`, has been added, which enables you to search in the contents of individual connections. For details, see "Searching in connection content" in the REST API Reference Guide.
- *Filter events:* The filtering functionality previously only available under the `api/audit/sessions` endpoint is now added to the `api/audit/sessions/<session-id>/events` endpoint, too. This means that you can now search in the events of individual connections. For more information, see "Session events" in the REST API Reference Guide.

- Backup and archive policies can now be configured using the REST API.
- Health status information about the Central Management node and the cluster nodes is now available at the /api/cluster/status endpoint of the node.
- You can now download audit trails from SPS using the REST API. For details, see "Download audit trails" in the REST API Reference Guide.

# Enhancements

The following is a list of enhancements implemented in SPS 6.0.

**Table 1: General enhancements**

| Enhancement | Issue ID |
|---|---|
| Created PDF reports have been enhanced with the others label and others subsection, which indicate that more data is available but cannot be displayed in the report unless the search is further refined. | |
| The "Top X" predefined report subchapters now include the **others** label, which indicates that more data is available but cannot be displayed in the report unless the search is further refined. | |

# Deprecated features

The following is a list of features that are no longer supported starting with SPS 6.0.

- X.509 host certificates are not supported, the related options have been removed from the product. One Identity recommends using public keys instead.
- DSA keys are not supported, the related options have been removed from the product. One Identity recommends using RSA keys instead.
- The log ingestion feature of SPS has been removed from the product.

# Deprecated features between SPS 5.1 and SPS 5.11

The following is a list of features that are no longer supported starting with SPS 6.0.

**CAUTION:**

**Physical SPS appliances based on Pyramid hardware are not supported in 5 F1 and later releases. Do not upgrade to 5 F1 or later on a Pyramid-based hardware. The last supported release for this hardware is 5 LTS, which is a long-term supported release.**

**If you have purchased SPS before August, 2014 and have not received a replacement hardware since then, you have Pyramid hardware, so do not upgrade to SPS 5 F1 or later. If you have purchased SPS after August 2014, you can upgrade to 5 F1.**

**If you do not know the type of your hardware or when it was purchased, complete the following steps:**

1. **Login to SPS.**
2. **Navigate to Basic Settings > Troubleshooting > Create support bundle, click Create support bundle, and save the file.**
3. **Open a ticket at https://support.oneidentity.com/create-service-request/.**
4. **Upload the file you downloaded from SPS in Step 1.**
5. **We will check the type of your hardware and notify you.**

- Support for the Lieberman ERPM credential store has been deprecated, this feature will be removed from the upcoming One Identity Safeguard for Privileged Sessions (SPS) 6 LTS release. One Identity recommends to use Safeguard for Privileged Passwords instead. For details, contact our Sales Team.
- SSLv3 encryption is not supported in SPS version 5.10 and later. This has the following effects:
  - You cannot configure SPS if your browser does not support at least TLSv1.
  - If you are auditing HTTP, Telnet or VNC sessions that use TLS encryption, the client- and server applications must support at least TLSv1.
- Support for X.509 host certificates is deprecated. This feature will be removed from SPS version 6 LTS (6.0). One Identity recommends using public keys instead.
- Support for DSA keys is deprecated. This feature will be removed from SPS version 6 LTS (6.0). One Identity recommends using RSA keys instead.

### Shorter than 1024-bit SSH keys

Following the upgrade, support for less than 1024-bit SSH keys is lost.

You can now use an Authentication Policy with GSSAPI and a Usermapping Policy in SSH connections. When an SSH Connection Policy uses an Authentication Policy with GSSAPI, and a Usermapping Policy, then SPS stores the user principal as the **Gateway username**, and the username used on the target as the **Server username**.

Note that this change has the following side effect: when using an Authentication Policy with GSSAPI, earlier versions of SPS used the `client-username@REALM` username to

authenticate on the target server. Starting with version 5.9.0, it uses the `client-username` as username. Configure your servers accordingly, or configure a Usermapping Policy for your SSH connections in SPS.

### Minimum version of encryption protocol for the web UI

The **Basic Settings > Local Services > Required minimum version of encryption protocol** option has been removed. This option governed the encryption protocol required to access the SPS web interface.

Regardless of the TLS version you configured previously, SPS will uniformly use TLS version 1.2.

This change might have the effect that using old (likely unsupported) browsers, it will not be possible to access the web interface of SPS.

### Deprecation of RPC API

The RPC API is deprecated as of SPS 5 F7 and will be removed in an upcoming feature release. One Identity recommends using the REST API instead.

### Screen content search in sessions indexed by the old Audit Player

It is no longer possible to search for screen contents indexed by the old Audit Player on the new search UI and the REST interface. Searching in session metadata (such as IP addresses and usernames) and in extracted events (such as executed commands and window titles that appeared on the screen) remains possible.

As the old Audit Player was replaced and deprecated as an indexing tool during the 4.x versions, this should only affect very old sessions. Sessions that were processed by the new indexing service will work perfectly. If you wish to do screen content searches in historical sessions, contact our Support Team.

# Resolved issues

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

**Table 2: General resolved issues in release 6.0.9**

| Resolved Issue | Issue ID |
|---|---|
| When SNMP service was enabled in Local Services, disk-related information was not included<br>When SNMP service is enabled in Local Services, disk-related information such as free space and total capacity is now reported when the SNMP server is queried. | PAM-13741 |
| HTTP service aborts with "Fatal Python error: deallocating None" | PAM-13727 |

| Resolved Issue | Issue ID |
|---|---|
| Under certain circumstances the HTTP proxy on SPS printed "Fatal Python error: deallocating None" to the logs and aborted while generating a core dump.<br>The underlying reference counting issue has been fixed. | |
| Zorp RDP instance could crash and create a core dump.<br>Certain I/O patterns could trigger an assertion in the RDP proxy that led to a crash and a core dump file being written, terminating all currently active RDP connections.<br>This has been fixed. | PAM-13364 |
| SPS now supports certificate chains with keys other than RSA/DSA.<br>When a certificate chain is uploaded (for example, as the web server certificate), SPS verifies that the entire certificate chain is valid. A certificate chain is considered valid if it does not include weak certificates and a trust relationship exists between them.<br>Previously, certificate chain validation has worked only for certificates that had RSA and DSA public keys. Other chains have been rejected with a "No such digest method" error message. This issue is now fixed so that every certificate chain that can be verified by OpenSSL 1.1.1 is now accepted. | PAM-13154 |
| Fixed a potential "Permission denied" error on the Sessions > Details > Analytics tab.<br>Previously, if you have tried opening the Analytics tab of a session in Sessions > Details with a user that belonged to a user group with a specific set of permissions, you could receive a "Permission denied" error, preventing you to check the contents of the Analytics tab. This issue has been fixed so that the Analytics tab appears only if your user has the proper permissions to access it. | PAM-13014 |
| Fixed the Generate video (now known as Start rendering) button missing from the Search > Details page for SSH connections with a Session exec channel type.<br>Previously, when opening the Details page of an SSH session on the Search interface, the Generate video button has been missing for SSH sessions with a Session exec channel type. This has been now fixed, so that the button (now known as Start rendering) always appears for such channels if they have renderable content. | PAM-12927 |

**Table 3: General resolved issues in release 6.0.8**

| Resolved Issue | Issue ID |
|---|---|
| Permission denied error on the session details tab<br>You could get a Permission denied error on the session details tab if you created a group with special permissions. This has been fixed. | PAM-13014 |

| Resolved Issue | Issue ID |
|---|---|
| Administrator password cannot be changed over the REST API when user database is LDAP<br>The "admin" user is always authenticated locally, so even though changing the password of normal users is not supported when LDAP user database is configured, it should still be allowed for the administrator's password. | PAM-12706 |
| Application proxy and message queuing data collection improved.<br>By improving the data collection related to the internal application proxy and the message queuing subsystems, we allow our product experts to have a deeper insight in case of troubleshooting.<br>The collected data is not available on any user interface but is a part of the generated support bundle. | PAM-12686 |
| The firmware installation is extended with a rollback functionality.<br>The firmware installation is extended with a rollback functionality that restores the original state if the firmware installation fails on any node of an HA cluster that makes the installation process more fault-tolerant. | PAM-12681 |
| Title detection issue on Windows 10 with a high DPI scaling<br>Title detection on Windows 10 with high DPI scaling of 100-200% DPI did not work properly. This has been fixed. | PAM-12613 |
| OCR engine failure<br>In some cases, the OCR process reached an internal memory limit, which caused it to crash. This has been fixed and the internal memory limit was raised to meet the requirements of the new OCR engine. | PAM-12434 |
| Fixes an possible (harmless) error message that could occur when executing large archiving jobs concurrently.<br>When an archive job affected a large amount of the data it could happen that multiple archive processes worked on the same directory. In special cases a race condition could occur when the existence and the creation of given directories were handled in parallel and the second creation attempt caused an error message that was logged and (depending on the current configuration) also sent out as email or SNMP alert.<br>This fix makes the directory checking and creation more robust. | PAM-12344 |
| Changing RDP domain membership settings over REST API was not persisted<br>It is possible to configure RDP domain membership over the REST API, except for actually joining the domain.<br>When RDP domain membership was changed using the REST API, and the changes were committed, the configuration has been applied. However, it has not been persisted, which resulted in reverting to the previous RDP domain settings shortly thereafter, for example by committing changes on the web UI. | PAM-4827 |

| Resolved Issue | Issue ID |
|---|---|
| This has been fixed, changing RDP domain membership settings on the REST API is now properly persisted. Note that joining the domain using the REST API is still not supported. | |
| None<br>In advanced statistics, the tables were truncated when too many columns were used in a table. With CSS modification, all text in tables are wrapped now and the tables fit into the size of the generated pdf. | PAM-3364 |

**Table 4: General resolved issues in release 6.0.7**

| Resolved Issue | Issue ID |
|---|---|
| Introduces a new feature to ease the information collection for troubleshooting purposes.<br>A new directory (under /var/lib/support) has been created for files requested by support that will be automatically included by the support bundle.<br>These files are kept only for a limited time (for a week after creation) to prevent them filling the disk up on a long run.<br>The files bigger than 300MB are only listed in the bundle instead of having them to prevent to grow the bundles themselves over a manageable size. | PAM-12384 |
| Could not download a .zatx file larger than 1GB.<br>A .zatx file larger than 1GB could not be downloaded. This has been fixed. | PAM-12337 |
| Dedicated hot spare disk monitoring added to the RAID status monitoring and send alert from them.<br>Dedicated hot spare disk was not checked, because it was not part of the RAID array in term of the RAID controller, but it is a useful information to know the status of the dedicated hot spare disk. Now we check the status of the hot spare disk: send SNMP alert and show a RAID status warning about that. | PAM-11701 |
| Fixed unhandled invalid duration parameters<br>Some of the invalid duration values were not handled on the Search page in the advanced search query filter. Consequently, the user received internal server error. This has been fixed and the user now will receive informative error messages about the correct values. | PAM-11624 |
| Audit trail location was not retrieved correctly.<br>The exact location of an audit trail was not retrieved correctly in a cluster configuration. This has been fixed and now the audit trail location is retrieved correctly. | PAM-11153 |
| Cleanup left metadata on search local machine in case there was a search master | PAM- |

| Resolved Issue | Issue ID |
|---|---|
| in the cluster.<br>The bug has been fixed and all data will be deleted properly during a cleanup. | 11117 |
| Minor PCI-DSS report content changes<br>PCI-DSS report contained some misspellings, outdated links and old naming conventions that have been fixed. | PAM-11077 |
| Fixed mapping of 0 value in pie chart<br>When the Analytics score field was presented with a 0 value in the pie chart, the 'n/a' value was mapped in the report instead of 0 which is misleading. Now this problem is solved, so any field of a type 0 value is mapped to 0. | PAM-10066 |
| MD5 certificates may break the configuration<br>If a certificate chain was uploaded as a Server X.509 certificate, which contained a certificate that was signed using the MD5 algorithm, the web server was unable to start.<br>Since the MD5 signing algorithm is not considered as safe, such certificate chains are now rejected at all places at configuration time. This means that client or server certificate chains configured for any purpose (eg. for connecting to LDAP or mail server or configuring a Signing CA or a Timestamping Authority) are not accepted if any of the certificates in the chain (except the root) is signed using MD5. It is not possible to upgrade to this version of SPS if the current configuration contains such certificates or certificate chains. The only exception to this is the indexer / encryption "certificate", which is essentially just a container of a public key, therefore all the X.509 details are ignored for such certificates.<br>Note that the current error which blocks the upgrade contains unnecessary technical details on the UI (this is tracked as PAM-12447). The relevant error message is that the "md [is] too weak". | PAM-7758 |

**Table 5: General resolved issues in release 6.0.6**

| Resolved Issue | Issue ID |
|---|---|
| Window title detection fix for Windows 2012 R2.<br>Window title detection did not find window titles when the DPI was slightly higher than the default one on Windows 2012. | PAM-12328 |
| Linux desktop resizing issues with Citrix 1912 LTSR<br>When using a Citrix Linux VDA with Citrix 1912 LTSR, the desktop could not be resized properly. This has been fixed. | PAM-12255 |
| Missing validation for RDP connections when NLA is enabled but TLS is not. | PAM-12186 |

| Resolved Issue | Issue ID |
|---|---|
| When SPS was configured to use Network Level Authentication in an RDP connection, but Legacy RDP Security Layer was selected for that connection, then no connection could be established. A traceback was written to the system log.<br>This has been fixed, SPS now validates that a connection for which NLA is enabled also has TLS Transport Security selected. | |
| Having a mismatching host key stored on the appliance could make the host key configured in backup policies ignored.<br>If the root user visited the backup host via SSH, it was prompted whether to have the offered host key stored or not. If the administrator selected to have it, that key was used later when performing backup (configured with Rsync over SSH), regardless the one configured on the WebUI.<br>The fix ensures that the user provided host key will be compared to the one presented by the backup server. | PAM-12173 |
| SPS installation on Azure vm made the firmware tainted<br>The service walinuxagent, which is required to be run on azure instances, creates files at runtime and this made the firmware tainted. These files have been added to the tainted whitelist. | PAM-12090 |
| Fixed timestamp conversion in report generation<br>When the timezone of SPS was other than UTC, timestamps for recorded sessions got converted to local time twice accidentally.<br>This has been fixed and the user should see the timestamps in connection with recorded sessions in their local time in case local timezone is applied on the box. | PAM-12087 |
| Certificate chain upload might fail with cross-signed intermediates<br>When uploading a certificate chain, if any of the intermediate CA-s in the chain was also a publicly trusted root, the upload failed with an error message. This has been corrected. | PAM-12059 |
| RDP device redirection only works if the Sound channel is enabled<br>Because of restrictions in Windows RDP servers device redirection only works if the "Sound" channel is enabled. A warning has been added that warns the user if device redirection is configured in the channel policies without having the "Sound" channel enabled. | PAM-12051 |
| Core files are produced when stopping or restarting proxy services<br>The proxy service component could crash and write a core dump during shutdown when timestamping was enabled but the timestamping server was unreachable. | PAM-12016 |
| Empty MenuInfo block appears instead of login screen<br>Invalid browser cookies could be set that prevented the rendering of the normal SPS login page.This has been corrected. | PAM-11985 |

| Resolved Issue | Issue ID |
|---|---|
| Save hashed PSK value in support bundle<br>In order to diagnose clustering issues, it is important to verify that the cluster members share the same IPSec pre-shared keys, but this was impossible, because the values were masked out. Following this change, the generated PSK tokens of the configuration are replaced by their SHA256 hash value. This means that the comparison can be performed while the actual values still remain secret. | PAM-11976 |
| Traceroute: switch to ICMP<br>Traceroute utility traditionally defaults to UDP probe packets, but such packets are likely to be filtered out by firewalls, even between SPS cluster nodes. It is expected that ICMP probes are more tolerated on networks, thus Troubleshooting > Traceroute has been changed to use ICMP instead of UDP. | PAM-11755 |
| Starting up and shutting down logs are transferred from boot journal to core firmware logs<br>There were many cases when logs have not been transferred from boot journal store to core firmware. In that case, the network-related issues were not transferred. This has been corrected. Starting up and shutting down logs are transferred from boot journal to core firmware logs. This makes the investigation easier, because all the logs are in one place and these logs are stored for longer time. | PAM-11738 |
| Fixed protocol binding in REST-based subchapter configurations<br>In REST-based reporting subchapter configurations under the binding options, protocol was either missing or it's value was written in lower case.<br>However, protocol values in ElasticSearch are stored in upper case form and when reporting queried our REST with protocol filter, due to the casing mismatch, no data were retrieved or not exactly the right data was being retrieved in some situations. This has been corrected. | PAM-11708 |
| When an audit trail was missing from the SPS, all further archiving processes failed<br>When an audit trail was missing from SPS, all further archiving processes failed. This has been corrected and the archiving will continue to the next audit trail file, and SPS records the error in the local database. | PAM-11700 |
| The firmware manipulation via console (core-shell) with firmwarectl synchronizes the firmware to the HA pair node.<br>The firmwarectl console tool, which can be called on the core-shell, did not synchronize the firmware to the other HA node which caused firmware version mismatch in case of a failover.<br>From now firmwarectl synchronizes the firmware to the other HA node just like the Basic Settings > High Availability page on the web-ui does. | PAM-11642 |
| Configuration of remote timestamping fails if policy is not set | PAM- |

| Resolved Issue | Issue ID |
|---|---|
| When configuring remote timestamping on the protocol Global Settings page and the policy OID was not set, committing the change failed with a generic error message. (When using the REST API, the error type was InvalidPropertyError.) This has been corrected. | 11401 |
| Rename Balabit in email attachments<br>In email attachments, Balabit Shell Control Box, which is the legacy product name, was still used. This has now been changed to One Identity Safeguard for Privileged Sessions. | PAM-10911 |
| Unable to change network settings<br>In rare cases the appliance could boot with incomplete network configuration. This caused a configuration commit failure, on basic/networking page.<br>This issue has been fixed. | PAM-10498 |

**Table 6: General resolved issues in release 6.0.5**

| Resolved Issue | Issue ID |
|---|---|
| Brackets were removed from around IPv6 addresses by the HTTP proxy in headers<br>The HTTP proxy removed the brackets from around IPv6 addresses in relayed HTTP headers, eg. "Host: [2001:db8::]" became "Host: 2001:db8::1", which caused problems on the server side. This has been fixed and such headers are now relayed properly. | PAM-11758 |
| Error messages appear in HTTP proxy logs when Authorization headers are not valid base64 encoded data<br>Our HTTP proxy tried to decode the Authorization header and if it could not, it logged an error because there was an error with the encoding. These log messages could be misleading as such headers happen frequently, so they were disabled. | PAM-11713 |
| Timestamps in upgrade logs are misleading<br>During the upgrade SPS produces log files which are separated from the standard syslog. Into these log files the timestamps of the log lines were added manually. These timestamps were not accurate. | PAM-11619 |
| When high amount of audit trails were stored on the disk, a process could cause performance issues during upgrade, HA takeover or boot.<br>After this fix this process will run only once. | PAM-11618 |
| Displaying the login page triggers General error (xcbError) SNMP or email alert<br>When the login page was loaded in a browser, then a background request | PAM-11597 |

| Resolved Issue | Issue ID |
|---|---|
| attempted to access a resource which mistakenly required an already authenticated user. If the General error (xcbError) alert was enabled on the Basic Settings / Alerting & Monitoring page, then this condition triggered sending SNMP or email alerts. This has been fixed. | |
| HTTP request URIs were sometimes forwarded incorrectly to the target server, with escaped URI parts not kept properly escaped.<br>The HTTP proxy in SPS improperly transformed URIs with escaped '/' characters. This has been fixed, and the requested URI is now passed intact to the target server. | PAM-11534 |
| In case of high amount of information, paginated data storage solution was implemented, but not used by the indexer tool.<br>To prevent overloading the database operations, data storage, for example, screen content storage during information collection from audit trail now works in an optimized way. | PAM-11523 |
| High memory consumption related to the indexer-jobgenerator service with sessions containing lots of channels<br>The jobgenerator service now handles channel related messages which are not required to store in memory anymore. | PAM-11513 |
| Assigning "All" privileges to a user group did not grant access to the Active Connections page<br>Assigning "All" (read and write/perform) privileges to a user group at the Users & Access Control / Appliance Access (formerly: AAA / Access Control) page did not grant access to the Active Connections page for the selected group. This has been fixed. | PAM-11392 |
| Multiple IPv4 addresses on the network interface which is assigned to clustering can break cluster node communication if other than the first one is used for clustering<br>Assigning multiple IPv4 addresses to the network interface which is used for clustering, and using other than the first one for secure communication between the cluster nodes results in a non-working configuration. Configuration validation has been extended with checks which prevent saving such configuration. | PAM-11047 |
| HA IP negotiation fails when more than two SPS hosts are accessible on the HA interface<br>When more than two SPS instances are accessible through the HA interface, the third host cannot obtain a valid HA IP address as the other two addresses are already taken. As this is not a supported way of working, a warning message is now shown to the user on the console. | PAM-10916 |
| Invalid software RAID-related events generated during one-shot checking (affects only MBX T1 hardware) | PAM-10771 |

| Resolved Issue | Issue ID |
|---|---|
| During the periodic checking of the software RAID array, DeviceDisappeared and NewDevice events were generated. These events were sent through SNMP or email, depending on the configuration.<br>This has now been fixed and these events are no longer generated. | |
| Unnecessary expiration warnings for indexer decryption key certificates<br>The decryption keys and the certificates that belong to them, used by the internal indexer to process encrypted audit trails, may still be needed in the configuration in order to access older audit data, long after the certificate itself is expired. Due to this, the expiration of these certificates will no longer trigger configuration validation warnings. | PAM-7653 |
| Commit Log Requirement settings did not take effect immediately in REST API configuration transactions<br>Changes in Commit Log Requirement settings did not take effect immediately in REST API configuration transactions. This has been fixed. Also, the response for {{GET /api/transaction}} requests now indicates if a commit message is required for saving configuration changes. | PAM-4957 |

**Table 7: General resolved issues in release 6.0.4**

| Resolved Issue | Issue ID |
|---|---|
| In case of high amount of information paginated data, storage solution was implemented but not used by the indexer tool.<br>To prevent overloading the database operations, data storage, for example, screen content storage during information collection from audit trail now works in an optimized way. | PAM-11523 |
| View log files > Tail window remains open even after the administrator has logged out.<br>The browser window displaying the live machine logs (Basic Settings > Troubleshooting > View log files > Tail) did not stop displaying new log messages after an administrator has logged out of their session. This has been corrected. Note that the window displaying the past log messages remains open even after logging out of the session. | PAM-11510 |
| Missing timestamps in audit trails and "Error connecting TSA" messages in the logs.<br>A bug in ICA proxy caused missing timestamps in audit trails and "Error connecting TSA" messages in the logs. This has been fixed. | PAM-11391 |
| Change in the trusted host keys did not trigger configuration synchronization in the SPS cluster. | PAM-11390 |

| Resolved Issue | Issue ID |
|---|---|
| Adding or removing a trusted host key now triggers configuration synchronization in the SPS cluster. | |
| Dynamic virtual channels in RDP proxy are not handled properly.<br>Some of the Dynamic virtual channels in RDP proxy were allowed even if they were not enabled in a Channel Policy. Now it has been fixed and must be explicitly added to the "Permitted channels" under the Dynamic virtual channels channel policy. | PAM-11319 |
| HA takeover issues after multi-step upgrades<br>If a system was upgraded in multiple steps (for example, from 5.11 to 6.0 to 6.3) without an HA takeover between the upgrades, a range of problems occurred while detecting the version of the firmware on the master and slave nodes. This issue has been fixed and these type of upgrades now work well. | PAM-11292 |
| From now on, Chrome on a newer version of macOS accepts the certificate generated by SPS.<br>The macOS has strictened its certificate policies, andthe generated certificate of SPS was not compliant with it. On Chrome, one could not turn off the warnings about the invalid certificate, rendering users unable to configure SPS for the first time.<br>During initial configuration (or later) one could upload a custom server certificate of course, but the browser did not allow the user to reach SPS to configure it.<br>The newly generated cert has the following additional properties:<br>• validity is 800 days long<br>• extendedKeyUsage has been specified<br>which makes it compliant with the recent Chrome+macOS combination. | PAM-11122 |
| On HA takeover, the IP address of SPS was not updated in other computer's ARP table in certain conditions.<br>SPS did not wait for the interface to be in the UP state, therefore sending the gratuitous ARP message was not successful when the interface didn't come up quickly. This has been fixed by waiting for the interface first. | PAM-10860 |
| Core files are generated for ICA sessions<br>In certain situations after the client has closed an ICA session, SPS generated a core file. This has been corrected. | PAM-10316 |
| A systemd service (proc-sys-fs-binfmt_misc.mount) failed to start at boot.<br>The proc-sys-fs-binfmt_misc.mount unit failed to start at boot. This generated alerts for the customer which resulted in SNMP trap or email, depending on the configuration. The service now starts at boot. | PAM-9935 |

**Table 8: General resolved issues in release 6.0.3**

| Resolved Issue | Issue ID |
|---|---|
| Overriding the global verbosity level in ICA connection policies had no effect<br>In order to help troubleshooting, the global log verbosity level can be overridden in connection policies. This setting was ignored in ICA connections. This has been fixed, ICA connection policies now also allow setting a per-connection verbosity level. | PAM-11251 |
| Password reuse always allowed when changing the password over REST<br>It is possible to configure SPS to prevent reusing previous passwords when changing the user password. This was not enforced when the password changed was performed through the REST API. It is now fixed and the restriction is enforced over the API, too. | PAM-11213 |
| Client unexpectedly closes RemoteApp sessions<br>In certain situations using RemoteApp connections, SPS sent an unneeded certificate to the client, causing the client to close the connection. This has been corrected, the unneeded certificate is not sent to the client. | PAM-11187 |
| RDP sessions shown as active even after client disconnects<br>In certain cases, SPS reported RDP sessions as active even after the client has disconnected. This has been corrected. | PAM-11168 |
| The SPS initiated workflow fails in case of SSH protocol.<br>Starting with Safeguard for Privileged Sessions version 6.2 it became possible to join Safeguard for Privileged Sessions and Safeguard for Privileged Passwords and make use of the full password approval workflow in SPP for sessions initiated through SPS. This feature was backported to the 6.0.2 maintenance release, but due to a problem with the backport, it did not work properly for SSH sessions. The problem is now fixed and SSH sessions can also be used in this scenario. | PAM-11139 |
| Improve the debug logging of ldapservice<br>The debug log messages of the ldapservice process now include a unique id to simplify troubleshooting of request-response pairs. | PAM-11135 |
| Sessions are terminated when using the credit-card detection and alerting features<br>In certain cases when the credit-card detection and alerting features were used, SPS terminated the affected sessions even when the Terminate action was not selected. This has been corrected. | PAM-11134 |
| Upgrading to SPS 6.0.2 fails if SPS is joined into SPP<br>Because of an error in the upgrade of Safeguard plugins, upgrade to SPS 6.0.2 failed if SPS was joined to SPP.<br>This has been corrected, in SPS 6.0.3 the upgrade works as expected. | PAM-11132 |

| Resolved Issue | Issue ID |
|---|---|
| Timeout in RDGW sessions causes core files on SPS<br>If a connection required for a Remote Desktop Gateway session could not be established within the expected timeout, the session failed and a core file appeared on SPS. This has been corrected, such timeout errors are now handled properly. | PAM-11123 |
| Traceback appears in the logs if the LDAP server is down<br>A traceback appeared in the logs if the LDAP server was unavailable and SPS tried to access this server. This has been corrected, the error is now properly handled. | PAM-11028 |
| Resizing the screen in ICA sessions to span multiple monitors did not work<br>If the number of relayed monitor screens was changed during an ICA session the change was not relayed by SPS properly which made such changes impossible. The problem is now fixed and it is possible to change the number of monitors during the session. | PAM-10988 |
| 'Analytics details are not available' warning appears on the UI<br>In some cases, the 'Analytics details are not available' warning was displayed even though the analytics scores were available for the session. | PAM-10886 |
| Traceback in the logs after rejecting a four-eyes authorization request<br>A traceback appeared in the logs after rejecting a four-eyes authorization request. This has been corrected, the event is now handled properly. | PAM-10881 |
| After upgrading a High Availability cluster, the Basic Settings > High Availability page displayed the Boot firmware version of the Other node incorrectly<br>After upgrading a High Availability cluster, the Basic Settings > High Availability page displayed the Boot firmware version of the Other node incorrectly, as if that node was still running the old firmware version. Despite the information displayed on the web user interface, both nodes were running the new firmware version. This has been fixed. | PAM-10413 |
| IPv6 routing table is missing from the support bundle<br>The IPv6 routing table was missing from the support bundle. This has been corrected. | PAM-10354 |
| Configuration changes not taking effect<br>In some cases, when the user modified system-related configuration settings of SPS, they did not take effect after committing the changes. This could happen for example when commiting networking changes, and restarting the networking service was very slow. This has been corrected, such errors are now handled properly. | PAM-10336 |
| Failed screenshots in content subchapter reports | PAM- |

| Resolved Issue | Issue ID |
|---|---|
| Using external-indexer or near real time indexing lead to failed screenshots in content subchapter reports, indicated by the following error message in the logs:<br>'Cannot retrieve image for screencontent'<br>This has been corrected, screenshots are now properly generated for the reports. | 10190 |
| Remote Desktop Gateway authentication fails for Windows 2012 R2 clients<br>Remote Desktop Gateway authentication failed for Windows 2012 R2 clients (Windows client version: Windows 2012 R2 , ver. 6.3.9600 Protocol 8.1). This has been corrected. | PAM-9967 |
| False data in achiving notice<br>After deleting a Connection Policy that had recorded sessions and creating a new policy with the same name, the number of archived files in the archiving notice was invalid. This has been corrected.<br>NOTE: It is not recommended to delete Connection Policies that were used in production systems, as this can prevent SPS from archiving the files and data related to these policies. We recommend disabling unneeded Connection Policies instead. | PAM-9615 |
| If completing the Welcome Wizard using the REST API fails, the appliance becomes unreachable<br>If completing the Welcome Wizard using the REST API failed, an internal error made the product unreachable: the IP address became 192.168.1.1 and the console access of the root user was disabled. From now on, the console access of the root user remains active, so it can be used to fix such situations. | PAM-7760 |

**Table 9: General resolved issues in release 6.0.2**

| Resolved Issue | Issue ID |
|---|---|
| In some cases persisting indexer job status updates and command/title events made a big load on the database which caused big delays in opening new connections through SPS.<br>The way of persisting indexer events to the database was optimized in a way that it should not add delay on new connections. | PAM-10821 |
| Error in handling compressed ICA traffic causes the server to terminate the session<br>In some cases, SPS handled compressed ICA traffic incorrectly, causing the server to terminate the session. The following log message appeared in the system logs:<br>'Compression PD: Unable to expand slab'<br>This has been corrected, the traffic is now handled properly. | PAM-10781 |

| Resolved Issue | Issue ID |
|---|---|
| Ignore the actual result of the whoami request when checking the availability of an LDAP server<br>To check the availability of an LDAP server, SPS performs a "who am I" query against that server. If that query was disabled on the server, SPS treated the response as a sign of the server being down, even if it was handling other requests properly. This behavior has been changed and SPS now only checks if the server responds at all. | PAM-10729 |
| Low idle timeouts on LDAP servers not handled correctly<br>SPS did not correctly handle if an LDAP server closed idle sessions after less than 600 seconds. After this fix, idle timeout settings above 120s work correctly. | PAM-10674 |
| Connection data backup not available in the console menu<br>It is possible to manually initiate a backup process from the menu accessible via SSH or the appliance console. Due to a bug, only the system backup option was available there and the option to backup data associated with connection policies (such as audit trails) was not. This is now fixed and all backup options are available again. | PAM-10576 |
| Duplicate header appears on the ICA Control > Channel Policies page<br>While editing a new Channel Policy on the ICA Control > Channel Policies page, clicking on the Show details icon caused a new header and footer to appear. This has been corrected. | PAM-10575 |
| Login page can redirect to arbitrary external sites<br>To streamline the login process, SPS was able to redirect the user to the site they originally wanted to access after a successful login. However, this feature also redirected the user to any URL if the login page was accessed through a properly crafted link. This made phishing attacks against the administrators of SPS easier, so the login page now only redirects to URLs on SPS itself. | PAM-10560 |
| On an extremely overloaded machine, the OCR scanning (indexing) process could crash<br>When the machine was so overloaded that the connection between the process that controls the OCR scanning and indexing operation (indexerworker) and the process doing the computation (indexerservice) was lost, the worker process tried to abort the processing but crashed. The index job might be finished successfully later. The problem was fixed and the worker process now handles this outage correctly. | PAM-10547 |
| Disk fill-up prevention should always deny incoming connections when limit is reached<br>Disk fill-up prevention has not denied incoming connections in the following case: IP forwarding was enabled for the NIC where the connection was coming from | PAM-10510 |

| Resolved Issue | Issue ID |
|---|---|
| and a connection policy was configured to 'Use original target address of the client'. This issue has been fixed. All connections are now denied when disk fill-up limit is reached. Forwarded connections that do not match a connection policy, and therefore are not audited still pass trough the appliance even if disk fill-up limit is reached. | |
| Session verdict is 'auth-fail' after a failed gateway authentication attempt even if it succeeds after a retry<br>If the user enters a wrong password or the gateway authentication attempt failed for another reason, the "verdict" for that session on the search interface remained "auth-failed", even if a second attempt was offered for the user and that succeeded. This logic is now fixed and the final authentication decision is used to decide the verdict of the session. | PAM-10509 |
| Console menu does not timeout<br>As a side-effect of an unrelated change, the console menu did not log off idle users after a timeout. This is now fixed and idle sessions are properly terminated. | PAM-10441 |
| Transferring files over 4GB not possible over RDP disk redirection<br>Files over 4GB transfers via RDP disk redirection over SPS got corrupted. This is now fixed and both download and upload of larger files is possible. | PAM-10418 |
| indexer-service cannot be reloaded multiple times within a short time<br>Reloading indexer-service occasionally returned with a false error message, even though it was actually reloaded. However, if you attempted to reload it again within a short time (within in ~3 seconds), the reload failed. | PAM-10335 |
| Core files are generated for ICA sessions<br>In certain situations after the client has closed an ICA session, SPS generated a core file. This has been corrected. | PAM-10316 |
| RDP connection problems with certain client applications<br>If the client did not send a cookie when establishing the initial connection to SPS, SPS sent an invalid cookie to the target server, causing the server to terminate the connection. This has been corrected. | PAM-10284 |
| The /api/active-sessions endpoint responds with Internal Server Error (500)<br>The /api/active-sessions endpoint could respond only with Internal Server Error (500) in case of an error during DELETE. From now on the /api/active-sessions endpoint can respond with Not Found Error (404) if the given session id is not found in the list of active sessions. | PAM-10281 |
| Misspelled OK buttons on the web interface<br>Some OK buttons were spelled as 'Ok' on the web interface. These have been | PAM-10155 |

| Resolved Issue | Issue ID |
|---|---|
| corrected. | |
| Prevent joining SPS nodes running different firmware versions to a cluster<br>Configuration (and cluster state) synchronization may not work if the Central Management and other cluster nodes are running different versions of SPS. In order to avoid possible misconfiguration, product version compatibility will now be validated during joining nodes to an SPS cluster. | PAM-10020 |
| Improved error detection of Elasticsearch database for audit information<br>If the Elasticsearch instance that acts as a backend for the audit database failed to start for some reason, it kept retrying (and failing) and never notified the user about the problem. The problem has been fixed and such problems are properly escalated. | PAM-10018 |
| Inaccurate warning when upgrading external indexers<br>When upgrading an external indexer, an inaccurate warning was displayed about removing the directory that contained the configuration files of the old version of the indexer. This has been corrected. | PAM-9707 |
| Content search field does not handle the '<' character<br>Typing the '<' character followed by other characters in the screen content search field caused the query to disappear. This has been corrected, such queries are now handled properly. | PAM-9264 |
| OpenSSL encryption failure when changing the password of a permanent keystore<br>In some rare cases, when changing the password of a permanent keystore on the web interface, encrypting the keys failed with the following error message:<br>'Fatal error: escapeshellarg(): Input string contains NULL bytes in /opt/scb/lib/OpenSSL.php on line 62'<br>This has been corrected. | PAM-8345 |
| Stopping more data-producing processes when disk fillup prevention is triggered<br>The disk fillup prevention feature in SPS proactively stops traffic passing through if this usage reaches a predefined threshold to avoid more severe errors caused by the disk being filled up completely. Besides ongoing traffic there are several services that also produce data, which are now also stopped, providing further protection. | PAM-8012 |

**Table 10: General resolved issues in release 6.0.1**

| Resolved Issue | Issue ID |
|---|---|
| bind9: | |

| Resolved Issue | Issue ID |
| --- | --- |

- CVE-2018-5743
- CVE-2019-6471

bzip2:

- CVE-2019-12900

curl:

- CVE-2019-5346

db5.3:

- CVE-2019-8457

dbus:

- CVE-2019-12749

elfutils:

- CVE-2018-16062
- CVE-2018-16402
- CVE-2018-16403
- CVE-2018-18310
- CVE-2018-18520
- CVE-2018-18521
- CVE-2019-7149
- CVE-2019-7150
- CVE-2019-7665

expat:

- CVE-2018-20843

ffmpeg:

- CVE-2018-15822
- CVE-2019-9718
- CVE-2019-9721

glib2.0:

- CVE-2019-12450

gnutls28:

- CVE-2018-1084

- CVE-2018-10844
- CVE-2018-10845
- CVE-2018-10846
- CVE-2019-3829

isc-dhcp:

- CVE-2019-6470

jinja2:

- CVE-2019-10906

libpng1.6:

- CVE-2019-7317

libseccomp:

- CVE-2019-9893

linux:

- CVE-2017-5715
- CVE-2017-5753
- CVE-2017-5754
- CVE-2018-12126
- CVE-2018-12127
- CVE-2018-12130
- CVE-2018-16884
- CVE-2018-3620
- CVE-2018-3639
- CVE-2018-3646
- CVE-2019-11478
- CVE-2019-11479
- CVE-2019-3874
- CVE-2019-3882
- CVE-2019-9500
- CVE-2019-9503

mysql-5.7:

- CVE-2019-2566
- CVE-2019-2581
- CVE-2019-2592
- CVE-2019-2614
- CVE-2019-2627
- CVE-2019-2628
- CVE-2019-2632
- CVE-2019-2683

openjdk-8:

- CVE-2019-2422
- CVE-2019-2426
- CVE-2019-2602
- CVE-2019-2684
- CVE-2019-2698

php7.2:

- CVE-2019-11034
- CVE-2019-11035
- CVE-2019-11036
- CVE-2019-11039
- CVE-2019-11040
- CVE-2019-9637
- CVE-2019-9638
- CVE-2019-9639
- CVE-2019-9640
- CVE-2019-9641
- CVE-2019-9675

postgresql-10:

- CVE-2019-10130
- CVE-2019-10164

python-urllib3:

- CVE-2018-20060

| Resolved Issue | Issue ID |
| --- | --- |
| • CVE-2019-11236<br>• CVE-2019-11324<br>python2.7:<br>• CVE-2018-1000802<br>• CVE-2018-14647<br>qtbase-opensource-src:<br>• CVE-2018-15518<br>• CVE-2018-19870<br>• CVE-2018-19873<br>samba:<br>• CVE-2018-16860<br>sqlite3:<br>• CVE-2018-20346<br>• CVE-2018-20505<br>• CVE-2018-20506<br>• CVE-2019-8457<br>• CVE-2019-9936<br>• CVE-2019-9937<br>vim:<br>• CVE-2019-12735 | |
| Inconsistent merge behaviour in configuration sync<br>There were some cases, where a validation error occured during configuration synchronization. This has been fixed, and now System Backup is synchronized under Management, too. | PAM-9655 |
| Changing cluster roles may make the product tainted<br>When changing certain cluster roles, the firmware became tainted. This affected the upgrade process when the definition of a role changed between two releases, resulting in tainted firmware. Now this has been fixed. | PAM-9375 |
| Report generation can produce duplicate reports<br>If generating a report took more than 30 minutes, it was restarted, causing it to run twice and generate a duplicate report. This has been corrected, now report generation jobs cannot overlap to prevent processing them twice. | PAM-5477 |

| Resolved Issue | Issue ID |
| --- | --- |
| The default number of indexer workers was 16 on a newly installed SPS.<br>The default number of indexer workers was 16 on a newly installed SPS. This has been modified, and now the number of CPU cores of the machine is taken into account when deciding the default number of indexer workers. | PAM-3739 |
| Disk fill-up prevention should always deny incoming connections when limit is reached<br>Disk fill-up prevention has not denied incoming connections in the following case: IP forwarding was enabled for the NIC where the connection was coming from and a connection policy was configured to 'Use original target address of the client'. This issue has been fixed. All connections are now denied when disk fill-up limit is reached. Forwarded connections that do not match a connection policy, and therefore are not audited still pass trough the appliance even if disk fill-up limit is reached. | PAM-10039 |

**Table 11: General resolved issues in release 6.0**

| Resolved Issue | Issue ID |
| --- | --- |
| Security package updates<br>bind9:<br>• CVE-2018-5743<br>busybox:<br>• CVE-2011-5325<br>• CVE-2018-1000517<br>• CVE-2018-20679<br>• CVE-2019-5747<br>curl:<br>• CVE-2019-5346<br>ffmpeg:<br>• CVE-2018-15822<br>• CVE-2019-9718<br>• CVE-2019-9721<br>file:<br>• CVE-2019-8905<br>• CVE-2019-8906 | |

| Resolved Issue | Issue ID |
| --- | --- |

- CVE-2019-8907

isc-dhcp:

- CVE-2019-6470

ldb:

- CVE-2019-3824

libgd2:

- CVE-2019-6977
- CVE-2019-6978

libpng1.6:

- CVE-2019-7317

libxslt:

- CVE-2019-11068

linux:

- CVE-2017-5715
- CVE-2017-5753
- CVE-2017-5754
- CVE-2018-12126
- CVE-2018-12127
- CVE-2018-12130
- CVE-2018-14678
- CVE-2018-16884
- CVE-2018-18021
- CVE-2018-18397
- CVE-2018-19824
- CVE-2018-19854
- CVE-2018-3620
- CVE-2018-3639
- CVE-2018-3646
- CVE-2019-3459
- CVE-2019-3460

- CVE-2019-3874
- CVE-2019-3882
- CVE-2019-6133
- CVE-2019-6974
- CVE-2019-7221
- CVE-2019-7222
- CVE-2019-7308
- CVE-2019-8912
- CVE-2019-8980
- CVE-2019-9213
- CVE-2019-9500
- CVE-2019-9503

lua5.3:

- CVE-2019-6706

mysql-5.7:

- CVE-2019-2566
- CVE-2019-2581
- CVE-2019-2592
- CVE-2019-2614
- CVE-2019-2627
- CVE-2019-2628
- CVE-2019-2632
- CVE-2019-2683

nss:

- CVE-2018-18508

openjdk-8:

- CVE-2019-2422
- CVE-2019-2426
- CVE-2019-2602
- CVE-2019-2684
- CVE-2019-2698

| Resolved Issue | Issue ID |
| --- | --- |

openssh:

- CVE-2019-6109
- CVE-2019-6111

openssl1.0:

- CVE-2019-1559

php7.2:

- CVE-2019-11034
- CVE-2019-11035
- CVE-2019-9637
- CVE-2019-9638
- CVE-2019-9639
- CVE-2019-9640
- CVE-2019-9641
- CVE-2019-9675

python-urllib3:

- CVE-2018-20060
- CVE-2019-11236
- CVE-2019-11324

samba:

- CVE-2018-16860
- CVE-2019-3880

systemd:

- CVE-2019-3842

tiff:

- CVE-2018-10779
- CVE-2018-12900
- CVE-2018-17000
- CVE-2018-19210
- CVE-2019-6128
- CVE-2019-7663

| Resolved Issue | Issue ID |
| --- | --- |
| walinuxagent:<br>• CVE-2019-0804<br>wget:<br>• CVE-2018-20483<br>• CVE-2019-5953 | |
| Search interface not available after cluster upgrade on certain versions<br>When upgrading the cluster between certain versions, the search functionality was not available after the nodes rebooted. This has been fixed and the search backend starts up properly after a cluster upgrade. | PAM-9768 |
| Core file download button not visible for read-only users<br>Read-only access rights to the Basic Settings/Troubleshooting page allows the user to download all kinds of debug information, including core files. The "Download" button was not visible for users with read-only rights, even though they could download these files via the API. The button is now shown correctly. | PAM-9693 |
| Limited logging for Citrix ICA connections<br>Due to an internal error, system logging about Citrix ICA protocols did not work properly. Even though audit recording was unaffected, this made troubleshooting difficult. The problem was fixed and logging now works similarly to other protocols. | PAM-9671 |
| Rare crash when using Remote Desktop Gateway connections<br>Due to an unhandled race condition, the RDP proxy could crash in very rare cases when a large number of Remote Desktop Gateway connections were open in parallel. The problem was fixed. | PAM-9596 |
| Changes to SIEM forwarder setting not applied<br>Changes to the configuration of the SIEM forwarder except the initial setup were not applied until rebooting the machine or restarting the service. This is now fixed and all changes take effect immediately. | PAM-9499 |
| Stale RDP connections on the Active Connections page<br>Since version 5.6, stale RDP sessions can remain unclosed and displayed on the "Active Connections" page. This is now fixed and all RDP sessions are now closed properly. | PAM-9473 |
| Wrong IP address in autogenerated HTTPS certificates<br>Certificates generated for proxy mode HTTPS connections are using the IP address of SPS (the proxy) instead of the hostname/address of the target server. | PAM-9337 |
| AAA configuration (including root password) is not synchronized to the managed | PAM- |

| Resolved Issue | Issue ID |
| --- | --- |
| hosts in an SPS cluster<br>The AAA configuration was blacklisted during the configuration synchronization between the central management and the managed host. This limitation is now solved, and AAA configuration is synchronized to the managed hosts.<br>The AAA configuration contains the local users (including admin), therefore we added the root password to the synchronized configuration data, too. | 9295 |
| Double check of group membership during public key-based gateway authentication in SSH<br>When using public-key-based gateway authentication in SSH, the group filtering was performed twice, which could have a significant performance penalty. This is now fixed and this check is done only once. | PAM-9268 |
| Indexing RDP sessions may fail with "Size out of range" errror<br>RDP sessions with multiple channels sometimes resulted in indexing errors ("Size out of range"). Such audit trails could not be opened in the Desktop Player. This has been fixed. | PAM-9267 |
| Audit trails of Citrix ICA sessions using XenApp and XenDesktop 7.15 cannot be replayed<br>Audit trails of Citrix ICA sessions using XenApp and XenDesktop 7.15 could not be properly replayed, and contained garbled screens. The error has been corrected, SPS 6.0 now properly record such sessions, so they can be properly replayed. | PAM-9232 |
| Report a more descriptive error message when firmware upload fails<br>When a firmware upload fails because of insufficient disk space, invalid file uploaded, or a similar error, now a more descriptive message is displayed instead of a generic error message. | PAM-9231 |
| Indexing certain archived sessions fails<br>Indexing jobs sometimes failed with the "No such file or directory" error message. This occurred when the audit trail of the session has already been archived and the remote archive was not mounted. Now the indexer automatically remounts such archives to complete the indexing. | PAM-9230 |
| Deleting keytabs failed when "Verbose system logs" (debug logging) was turned on<br>When "Verbose system logs" (debug logging) was turned on, then a server side error prevented deleting keytabs. This has been fixed. | PAM-9224 |
| None<br>The owner of the configuration lock was not reset within a browser session. As a result, if two different users logged in after each other in the same web browser, and the second user visited the Search > Search or Basic Settings > Cluster | PAM-9150 |

| Resolved Issue | Issue ID |
| --- | --- |
| management pages, then the System monitor showed that the configuration is locked by<br>REST@system<br>, and the user could not edit the configuration.<br>This problem has been fixed. | |
| SSH sessions disconnect if SPS cannot find the account in the Credential store<br>If a credential store was defined for a Connection Policy and SPS could not find an entry for the given target account in the store, it disconnected immediately instead of prompting the client to authenticate. This has been fixed, and now the fallback is triggered properly. | PAM-9128 |
| On an appliance with a Search minion role, generating daily/weekly/monthly reports results in several error e-mails<br>On an appliance with the Search minion role, when generating reports every Day / Week / Month, selecting "Send reports in e-mail", and attempting to inculde a Search subchapter in the report resulted in receiving several error e-mails from all Search minions that were configured in that cluster environment. The error message in the e-mails was:<br>"Unknown error: Error while fetching data via REST client, error: Error response got from REST client, status code: 500, reason: The search backend is unaccessible."<br>This has been corrected, no error messages will be sent.<br>If you want to include Search subchapters in your reports, generate them on the appliance with the Search master role. | PAM-9001 |
| Searching for audit trails that are not indexed is not working<br>In some cases if the connection database was big, searching for audit trails that are not indexed on the Search > Search (classic) page did not work properly. (Selecting the 'Not indexed' option in the "Channel's Indexing Status" column resulted in a search query that was never completed.) This has been fixed.<br>This has been corrected. | PAM-9000 |
| Failed SSH sessions can cause the System Monitor to show negative value as the number of active sessions<br>When certain incompatible configuration settings are used (for example, GSSAPI authentication with autologin), a failed SSH connection attempt could decrease the active session count, eventually pushing it below zero. This is now fixed and such failed connections don't change the number of active sessions. | PAM-8959 |
| Unnecessary health check warnings in the logs of the Search master node<br>In central search mode, the proxies are disabled on the Search master node. | PAM-8857 |

| Resolved Issue | Issue ID |
|---|---|
| However, the built-in health check processes still checked the status of the proxies and logged a warning message. This warning is now disabled for search master nodes. | |
| Generating certificates fails for long host and domain names<br>SPS generates several certificates internally, and it uses the configured hostname and domain name for the appliance in the Common Name (CN) of these certificates. If any of these were long, the CN could go beyond the 64-character limit of the underlying OpenSSL libraries and the certificate generation failed. The appliance now truncates the strings to make sure the CN stays below the 64-character limit. | PAM-8693 |
| Multiple processing issues fixed in terminal based protocols with CJK characters<br>The wide characters of CJK alphabets caused issues with command detection, video rendering, screenshot export in HTML, and the follow mode of the Safeguard Desktop Player. These are now fixed. | PAM-8611 |
| Session database upgrade fails for some ICA sessions<br>Some older versions of SPS saved the protocol information of ICA sessions differently, using the name "CGP" instead of "ICA". The session database upgrade process was not prepared to handle that and moving such sessions to the new database failed. Such sessions are now handled correctly by the upgrade process. | PAM-8465 |
| The RDP domain membership configuration is displayed even if the appliance was not a member of the domain<br>The RDP domain membership configuration was displayed even if the appliance was not a member of the currently configured domain. From now on, it is displayed only if the appliance is member of the currently configured domain. The status of the appliance (joined or not) is also displayed. | PAM-8372 |
| Insufficient error handling during external indexer initialization<br>If an indexer failed to start up for some reason, in some scenarios it asked for the password for the decryption key for the trails instead of recognizing and logging the error. This is now fixed and startup errors are handled properly. | PAM-8329 |
| No warnings about encrypted sessions on the new search interface<br>The Search > Search page did not warn the user if a session could not be played back because it was encrypted and the decryption key was not available in the keystore. This is now fixed and users get a warning that helps them solve the issue. | PAM-7585 |
| "Search subchapters" page only available to the "admin" user<br>The "Search subchapters" report configuration page was only accessible to the "admin" user. The permission handling of this page has been corrected and it can | PAM-7136 |

| Resolved Issue | Issue ID |
|---|---|
| be accessed by other users as well if they have the required Access Control rights. | |
| Configuration interface is unresponsive during session database upgrade<br>The System Monitor shows the status of the session database upgrade process. Unfortunately, the way it queryied the current status was highly inefficient, which could significantly slow down the entire web interface if the database being upgraded was large. The status check is now much more efficient and the UI remains responsive even during the upgrade. | PAM-6204 |

# System requirements

Before installing SPS 6.0, ensure that your system meets the following minimum hardware and software requirements.

The One Identity Safeguard for Privileged Sessions Appliance is built specifically for use only with the One Identity Safeguard for Privileged Sessions software that is already installed and ready for immediate use. It comes hardened to ensure the system is secure at the hardware, operating system, and software levels.

For the requirements about installing One Identity Safeguard for Privileged Sessions as a virtual appliance, see one of the following documents:

- Installation Guide
- Deployment from Azure Marketplace
- Deployment on Amazon Web Services

# Supported web browsers and operating systems

**CAUTION:**

**Since the official support of Internet Explorer 9 and 10 ended in January, 2016, they are not supported in One Identity Safeguard for Privileged Sessions (SPS) version 4 F3 and later.**

**CAUTION:**

**Even though the One Identity Safeguard for Privileged Sessions (SPS) web interface supports Internet Explorer and Microsoft Edge in general, to replay audit trails you need to use Internet Explorer 11, and install the Google WebM Video for Microsoft Internet Explorer plugin. If you cannot install Internet Explorer 11 or another supported browser on your computer, use the the Safeguard Desktop Player application. For details, see "Replaying audit trails in your browser" in the Administration Guide and Safeguard Desktop Player User Guide.**

NOTE:

SPS displays a warning message if your browser is not supported or JavaScript is disabled.

NOTE:

The minimum recommended screen resolution for viewing One Identity Safeguard for Privileged Sessions's (SPS's) web interface is 1366 x 768 pixels on a 14-inch widescreen (standard 16:9 ratio) laptop screen. Screen sizes and screen resolutions that are equal to or are above these values will guarantee an optimal display of the web interface.

### Supported browsers

The current version of Mozilla Firefox and Google Chrome, Microsoft Edge, and Microsoft Internet Explorer 11 or newer. The browser must support TLS-encrypted HTTPS connections, JavaScript, and cookies. Make sure that both JavaScript and cookies are enabled.

### Supported operating systems

Windows 2008 Server, Windows 7, Windows 2012 Server, Windows 2012 R2 Server, Windows 8, Windows 8.1, Windows 10, Windows 2016, and Linux.

The SPS web interface can be accessed only using TLS-encryption and strong cipher algorithms.

Opening the web interface in multiple browser windows or tabs is not supported.

# Safeguard Desktop Player system requirements

The Safeguard Desktop Player application supports the following platforms:

- **Microsoft Windows:**

  64-bit version of Windows 7 or newer. Install the appropriate driver for your graphic card.

- **Linux:**

  RHEL 6, CentOS 6, or newer. The Safeguard Desktop Player application will probably run on other distributions as well that have at least libc6 version 2.12 installed.

- **Mac:**

  macOS High Sierra 10.13, or newer.

Installing the Safeguard Desktop Player application requires about 120MB disk space, and a temporarily used disk space to store the audit trails that are replayed. The size of the temporary files depends on the size of the replayed audit trails.

You can install the Safeguard Desktop Player application with user privileges.

# Hardware specifications

The One Identity Safeguard for Privileged Sessions (SPS) appliances are built on high performance, energy efficient, and reliable hardware that are easily mounted into standard rack mounts.

The following sections provide detailed information of SPS appliances.

# 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

The One Identity Safeguard for Privileged Sessions appliance is built specifically for use only with the One Identity Safeguard for Privileged Sessions software that is already installed and ready for immediate use.

### To upgrade to One Identity Safeguard for Privileged Sessions 6.0

**CAUTION:**

**Due to a change in the underlying database, the upgrade process removes all risk scores generated earlier by One Identity Safeguard for Privileged Analytics. Sessions initiated after the upgrade will be scored again.**

For step-by-step instructions on upgrading to SPS 6.0, see Upgrade Guide.

NOTE:

Due to legal reasons, installation packages of the external indexer application will be available only from the SPS web interface. After SPS versions 6.4 and 6.0.3 are released, the installation packages will be removed from our website.

### About LTS releases

This is a long-term-supported (LTS) release, which means that it will be supported at least for 3 years after the release date.

For a full description of long-term-supported and feature releases, open the SPS product page on the Support Portal and navigate to **Product Life Cycle & Policies > Product Support Policies > Software Product Support Lifecycle Policy**.

### If you have a physical appliance based on MBX hardware

One Identity recommends you to upgrade to SPS 6.0, if you are not running SPS on Pyramid hardware and any of the following is true:

NOTE:

If you do not know the type of your hardware, see If you have a physical appliance based on Pyramid hardware.

- You wish to take advantage of any of the new features.
- You are running a previous feature release.
- You are running a previous long-term-supported release.

### If you have a physical appliance based on Pyramid hardware

Do NOT upgrade to SPS 6.0 if you are running SPS on Pyramid hardware:

**CAUTION:**

**Physical SPS appliances based on Pyramid hardware are not supported in 5 F1 and later releases. Do not upgrade to 5 F1 or later on a Pyramid-based hardware. The last supported release for this hardware is 5 LTS, which is a long-term supported release.**

**If you have purchased SPS before August, 2014 and have not received a replacement hardware since then, you have Pyramid hardware, so do not upgrade to SPS 5 F1 or later. If you have purchased SPS after August 2014, you can upgrade to 5 F1.**

**If you do not know the type of your hardware or when it was purchased, complete the following steps:**

1. **Login to SPS.**
2. **Navigate to Basic Settings > Troubleshooting > Create support bundle, click Create support bundle, and save the file.**
3. **Open a ticket at https://support.oneidentity.com/create-service-request/.**
4. **Upload the file you downloaded from SPS in Step 1.**
5. **We will check the type of your hardware and notify you.**

# Verify successful installation

Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 6.0 of the firmware. If not, it means that the upgrade process did not complete properly and SPS performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:

1. Navigate to **Basic Settings > Troubleshooting > Create support bundle** and click **Create support bundle**.
2. Save the resulting ZIP file.
3. contact our Support Team and send them the file. They will analyze its contents to determine why the upgrade was not completed and assist you in solving the problem.

# More resources

To obtain more information, read the technical documentation or consult the community:

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

# 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 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

# Third-party contributions

This appendix includes the open source licenses and attributions applicable to One Identity Safeguard for Privileged Sessions.

# GNU General Public License

Version 2, June 1991

1989, 1991 Free Software Foundation, Inc.

Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Version 2, June 1991

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software - to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps:

1. copyright the software, and
2. offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

# TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

## Section 0

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

## Section 1

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

## Section 2

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user

how to view a copy of this License. (Exception: If the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

### Section 3

You may copy and distribute the Program (or a work based on it, under Section 2 in object code or executable form under the terms of Section 1 and Section 2 above provided that you also do one of the following:

a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

### Section 4

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

### Section 5

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

### Section 6

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

### Section 7

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

### Section 8

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

### Section 9

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

### Section 10

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

### NO WARRANTY Section 11

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

### Section 12

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER

PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

## How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type "show w". This is free software, and you are welcome to redistribute it under certain conditions; type "show c" for details.

The hypothetical commands "show w" and "show c" should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than "show w" and "show c" ; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program "Gnomovision" (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

# GNU Lesser General Public License

Version 2.1, February 1999



Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor Boston, MA 02110-1301 USA



This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.

## Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method:

1. we copyright the library, and
2. we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the Lesser General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

# TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

## Section 0

This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

## Section 1

You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

## Section 2

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms ofSection 1 above, provided that you also meet all of these conditions:

a. The modified work must itself be a software library.

b. You must cause the files modified to carry prominent notices stating that you

changed the files and the date of any change.

c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

   (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

### Section 3

You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

### Section 4

You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Section 1 and Section 2 above provided that you accompany it with the complete corresponding machine-readable source code,

which must be distributed under the terms of Section 1 and Section 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

## Section 5

A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

## Section 6

As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be

distributed under Section 1 and Section 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

### Section 7

You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

## Section 8

You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

## Section 9

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

## Section 10

Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

## Section 11

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

### Section 12

If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

### Section 13

The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

### Section 14

If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

### NO WARRANTY Section 15

BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

### NO WARRANTY Section 16

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO

LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

### How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

## License attributions

### OpenSSL

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (https://www.openssl.org/). This product includes cryptographic software written

by Eric Young (eay@cryptsoft.com)

## Botan cryptographic library license

Botan http://botan.randombit.net/ is distributed under these terms:

Copyright

1999-2013,2014 Jack Lloyd

2001 Peter J Jones

2004-2007 Justin Karneges

2004 Vaclav Ovsik

2005 Matthew Gregan

2005-2006 Matt Johnston

2006 Luca Piccarreta

2007 Yves Jerschow

2007-2008 FlexSecure GmbH

2007-2008 Technische Universitat Darmstadt

2007-2008 Falko Strenzke

2007-2008 Martin Doering

2007 Manuel Hartl

2007 Christoph Ludwig

2007 Patrick Sona

2010 Olivier de Gaalon

2012 Vojtech Kral

2012-2014 Markus Wanner

2013 Joel Low

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

**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.**