

One Identity Safeguard for Privileged Passwords 2.5

Release Notes

December 2018

These release notes provide information about the One Identity Safeguard for Privileged Passwords 2.5 release.

About the Safeguard product line

The One Identity Safeguard for Privileged Passwords Appliance is built specifically for use only with the Safeguard for Privileged Passwords 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.

The privileged management software provided with One Identity Safeguard for Privileged Passwords consists of 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 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.

One Identity Safeguard for Privileged Passwords Version 2.5 is a major release with new features and functionality in addition to numerous bug fixes. In this release you will find custom platforms, authentication options, and Safeguard Sessions Appliance join. See [New features](#).

i **NOTE:** For a full list of key features in One Identity Safeguard for Privileged Passwords, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

New features

Directory based user discovery (713614 and 761638)

When adding a new directory based user group, the Authorizer Administrator or the User Administrator now have the option to:

- Configure primary and secondary authentication providers and
- Set administrator permissions on the imported or updated Safeguard for Privileged Passwords users.

In addition, any managed directory accounts that exist in Safeguard for Privileged Passwords at the time of the import process (or during the background synchronization of the directory), can automatically be assigned to a Safeguard user as a linked account. That association will be dependent upon the value of an attribute from the directory (such as "managedObjects" or "directoryReports" in Active Directory or "seeAlso" in OpenLDAP 2.4).

Offline Workflow (782735)

To ensure password consistency and individual accountability for privileged accounts, when an appliance loses consensus in the cluster access requests are disabled. In the event of an extended network partition, the Appliance Administrator can manually place an appliance in Offline Workflow mode to run access request workflow on that appliance in isolation from the rest of the cluster. When the network issues are resolved and connectivity is reestablished, the Appliance Administrator can manually resume online operations to merge audit logs, drop any in flight access requests, and return the appliance to full participation in the cluster.

It is recommended that no changes to cluster membership are made while an appliance is in Offline Workflow mode. The Appliance Administrator must manually restore the online operations before adding other nodes to ensure the appliance can seamlessly reintegrate with the cluster.

See also:

- [Resolved issues](#) on page 3

Resolved issues

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

Table 1: General resolved issues

Resolved Issue	Issue ID
Cluster failover not available in UI when Primary is down.	792849
Update Task on Password Change (UpdateDependentSystem) fails with Transport reported error	791794
AD User Group update fails with MySQL Transaction Cancelled Error	791479
DC Selection Algorithm Selects no DC when all weights are 0 (error: Selected Server '')	787824
Domain name not visible when requesting Active Directory account	787431
UI doesn't use fields with GET/Me/Entitlements which can result in huge responses	773876 and 793564
Chinese Simplified has been depreciated. The plan is to remove Chinese Simplified from Safeguard for Privileged Password in a future release yet to be determined.	NA

Known issues

The following is a list of issues known to exist at the time of release.

Table 2: Known issues

Known Issue	Issue ID
Update from 2.4.0 with managed Network settings to 2.5.0 may lose the defined appliance per network setting.	794771
Updating BMC firmware is not recommended. Changes to the BIOS may have unexpected results.	792851
AIX check password fails if salt is ".." Detail: If during an ChangePassword on AIX (and perhaps other Unix systems) the DES Encryption randomly selects ".." as the salt to use during the encryption process, Safeguard will fail when trying to check the password later. Workaround: Run ChangePassword again and create a new password, hopefully without a ".." salt. The odds of hitting this condition are 1 in 4096.	792411
Patching the appliance takes longer based on the number of assets. It is estimated that 1000 assets may take 20 minutes.	782908

System requirements

One Identity Safeguard for Privileged Passwords has two graphical user interfaces that allow you to manage access requests, approvals and reviews for your managed accounts and systems. Ensure that your system meets the following minimum hardware and software requirements for these clients.

Windows desktop client requirements

The desktop client is a native Windows application suitable for use on end-user machines. The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions.

Table 3: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6
Windows platforms	64-bit editions of:

Component	Requirements
	<ul style="list-style-type: none"> Windows 7 Windows 8.1 Windows 10 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 <p>i NOTE: Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the Internet Options dialog (In Internet Explorer, go to Tools Internet Options Advanced tab).</p> <p>i NOTE: If the appliance setting, TLS 1.2 Only is enabled, (Administrative Tools Settings Appliance Appliance Information), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard for Privileged Passwords.</p>
Safeguard for Privileged Passwords Desktop Player	The sessions player is only supported on 64-bit operating systems.

Web client requirements

The web client is functionally similar to the desktop client end-user view. It exposes the access request workflow functionality and is meant primarily for the non-Administrative user.

Table 4: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: <ul style="list-style-type: none"> Google Chrome 66 (or later) Microsoft Internet Explorer 11 and Edge Mozilla Firefox 52 (or later) Mobile device browsers:

Component	Requirements
	<ul style="list-style-type: none"> • Apple Safari iOS 10 (or later) • Google Chrome on Android <p>The web client is implemented for modern web browser technology, using:</p> <ul style="list-style-type: none"> • HTML5 • CSS • JavaScript <p>i NOTE: If your browser lacks these required technologies, then use the desktop client.</p>

Supported platforms

One Identity Safeguard for Privileged Passwords supports a variety of platforms.

i **NOTE:** The following table lists the platforms and versions that have been tested. Additional assets may be added to Safeguard for Privileged Passwords. If you do not see a particular platform listed when adding an asset, use the "Other" or "Other Linux" option on the **Management** tab of the **Asset** dialog. Custom platforms can be added. For more information, see [Custom Platform](#).

In addition, platforms that support RDP and SSH protocols are generally supported for sessions management.

Table 5: Supported platforms: Assets that can be managed

Platform	Version	Architecture
ACF2 - Mainframe	r14, r15	zSeries
ACF2 - Mainframe LDAP	r14, r15	zSeries
AIX	6.1, 7.1, 7.2	PPC
Amazon Web Services	1	
CentOS Linux	6	x86, x86_64
	7	x86_64
Cisco IOS	12.X, 15.X	
Cisco PIX	7.X, 8.X	
Debian GNU/Linux	6, 7, 8, 9	MIPS, PPC, x86, x86_64, zSeries

Platform	Version	Architecture
Dell iDRAC	7, 8	
F5 Big-IP	12.1.X, 13.0	
Facebook		
Fedora	21, 22, 23, 24, 25, 26	x86, x86_64
Fortinet FortiOS	5.2, 5.6	
FreeBSD	10.4, 11.1	x86, x86_64
HP iLO	iLO 2, 3, 4	x86
HP iLO MP	2, 3, 4	IA-64
HP-UX	11iv2 (B.11.23), 11iv3 (B.11.31)	IA-64, PA-RISC
IBM i	7.1, 7.2	PPC
Junos - Juniper Networks	12, 13, 14, 15	
MAC OS X	10.9, 10.10, 10.11, 10.12, 10.13	x86_64
MongoDB	3.4, 3.6	
MySQL	5.6, 5.7	
Oracle Database	11g Release 2, 12c Release 1	
Oracle Linux (OEL)	6 7	x86, x86_64 x86_64
PAN-OS	6.0, 7.0	
PostgreSQL	9.6.7, 10.2	
RACF - Mainframe	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries
RACF - Mainframe LDAP	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries
Red Hat Enterprise Linux (RHEL)	6 7	PPC, x86, x86_64, zSeries PPC, x86_64, zSeries

Platform	Version	Architecture
SAP HANA	2.0	Other
SAP Netweaver Application Server	7.3, 7.4	
Solaris	10	SPARC, x86, x86_64
	11	SPARC, x86_64
SonicOS	5.9, 6.2	
SonicWALL SMA or CMS	11.3.0	
SQL Server	2012, 2014, 2016	
SUSE Linux Enterprise Server (SLES)	11	IA-64, PPC, x86, x86_64, zSeries
	12	PPC, x86_64, zSeries
Sybase (Adaptive Server Enterprise)	15.7, 16	
Top Secret - Mainframe	r14, r15	zSeries
Top Secret - Mainframe LDAP	r14, r15	zSeries
Twitter		
Ubuntu	14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04	x86, x86_64
VMware ESXi	5.5, 6.0, 6.5	
Windows	Vista, 7, 8, 8.1, 10	
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016	

Table 6: Supported platforms: Directories that can be searched

Platform	Version
Microsoft Active Directory	Windows 2008+ DFL/FFL
OpenLDAP	2.4

Appliance specifications

The Safeguard for Privileged Passwords Appliance is built specifically for use only with the Safeguard for Privileged Passwords privileged management 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.

The One Identity Safeguard for Privileged Passwords 2000 Appliance specifications and power requirements are as follows.

Table 7: Safeguard 2000 Appliance: Feature specifications

Safeguard for Privileged Passwords 2000	Feature / Specification
Processor	Intel Xeon E3-1275v5 3.60 GHz
# of Processors	1
# of Cores per Processor	4
L2/L3 Cache	4 x 256KB L2, 8MB L3 SmartCache
Chipset	Intel C236 Chipset
DIMMs	DDR4-2400 ECC Unbuffered DIMMs
RAM	32GB
Internal HD Controller	LSI MegaRAID SAS 9391-4i 12Gbps SAS3
Disk	4 x Seagate EC2.5 1TB SAS 512e
Availability	TPM 2.0, EEC Memory, Redundant PSU
I/O Slots	x16 PCIe 3.0, x8 PCIe 3.0
RAID	RAID10
NIC/LOM	3 x Intel i210-AT GbE
Power Supplies	Redundant, 700W, Auto Ranging (100v~240V), ACPI compatible
Fans	4 x 40mm Counter-rotating, Non-hot-swappable
Chassis	1U Rack
Dimensions (HxWxD)	43 x 437.0 x 597.0 (mm) 1.7 x 17.2 x 23.5 (in)
Weight	Max: 46 lbs (20.9 Kg)
Miscellaneous	FIPS Compliant Chassis

Table 8: Safeguard 2000 Appliance: Power requirements

Input Voltage	100-240 Vac
---------------	-------------

Frequency	50-60Hz
Power Consumption (Watts)	170.9
BTU	583

Appliance LCD and controls

The front panel of the One Identity Safeguard for Privileged Passwords 2000 Appliance contains the following controls for powering on, powering off, and scrolling through the LCD display.

Table 9: Appliance LCD and controls

Control	Description
Green check mark button	<p>Use the Green check mark button to start the appliance. Press the Green check mark button for NO more than one second to power on the appliance.</p> <p>⚠ CAUTION: Once the Safeguard for Privileged Passwords Appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.</p>
Red X button	<p>Use the Red X button to shut down the appliance. Press and hold the Red X button for four seconds until the LCD displays POWER OFF.</p> <p>⚠ CAUTION: Once the Safeguard for Privileged Passwords Appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.</p>
Down, up, left and right arrow buttons	<p>When the appliance is running, the LCD home screen displays:</p> <ul style="list-style-type: none"> • Safeguard for Privileged Passwords <version number> <p>Use the arrow buttons to scroll through the following details:</p> <ul style="list-style-type: none"> • Serial: <appliance serial number> • X0: <appliance IP address> • X1: <IP address of the sessions module interface> <p>If one or more Safeguard Sessions Appliances are joined to Safeguard for Privileged Passwords, X1 is not available in Safeguard for Privileged Passwords.</p> <ul style="list-style-type: none"> • MGMT: <management IP address>

Control	Description
	<ul style="list-style-type: none"> • MGMT MAC: <media access control address> • IPMI: <IP address for IPMI>

Product licensing

The One Identity Safeguard for Privileged Passwords 2000 Appliance ships with the following modules, each requiring a valid license to enable functionality:

- One Identity Safeguard for Privileged Passwords
- One Identity Safeguard for Privileged Sessions

To add a Safeguard for Privileged Passwords module license

The first time you log into the Safeguard for Privileged Passwords desktop client as the Appliance Administrator, it prompts you to add a license. In addition, you can add additional Safeguard for Privileged Passwords module licenses.

1. Navigate to **Administrative Tools | Settings | Appliance | Licensing** in the desktop client.
2. Click **+**.
3. **Browse** to select the license file.

Once you add a license, Safeguard for Privileged Passwords displays the current license information and additional links that allow you to update the license.

4. To add another module license, click **Add Another License** from the **Success** dialog.

NOTE: To avoid disruptions in the use of Safeguard for Privileged Passwords, the Appliance Administrator must configure the SMTP server, and define email templates for the *License Expired* and the *License Expiring Soon* event types. This ensures you will be notified of an approaching expiration date.

Update and installation instructions

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

To setup a new One Identity Safeguard for Privileged Passwords 2000 Appliance

If this is a new One Identity Safeguard for Privileged Passwords 2000 Appliance, see the *One Identity Safeguard for Privileged Passwords Appliance Setup Guide* that was included in the package with your appliance. You can also find this guide on the One Identity Support Portal: <https://support.oneidentity.com/one-identity-safeguard/2.1/technical-documents>.

To update an existing Safeguard for Privileged Passwords 2000 Appliance with this patch

It is the responsibility of the Appliance Administrator to upgrade One Identity Safeguard for Privileged Passwords by installing an update file (patch). Consider the following:

- **Minimum patch version:** 2.0.1.5037. If you are running an earlier version of the Safeguard for Privileged Passwords Appliance, you must upgrade to this version before applying the 2.5 patch.
- **Clustered environment:** Please see the *Patching cluster members* section in the *One Identity Safeguard for Privileged Passwords Administration Guide* for instructions on how to deploy a patch so all appliances in the cluster are on the same version.

IMPORTANT: Always back up your appliance before you install an update file. Once you install an update file, you cannot uninstall it. For more information, see the *One Identity Safeguard for Privileged Passwords Administration Guide*.

Download the latest update from the One Identity Support Portal:

<https://support.oneidentity.com/one-identity-safeguard/>

To install the software patch

1. As an Appliance Administrator, log into the Safeguard for Privileged Passwords desktop client.
2. From the **Home** page, select **Administrative Tools**.
3. Select **Settings | Appliance | Updates**.
The current appliance and client versions are displayed.
4. Click **Upload a File** and browse to select the update file you downloaded from the One Identity support web site.

NOTE: When you select a file, Safeguard for Privileged Passwords uploads it to the server, but does not install it.

5. Once the file has successfully uploaded, click **Install Now**.

To install the Safeguard for Privileged Passwords desktop client

To define and enforce security policy for your enterprise, install the Windows desktop client application which gives you access to the Administrative Tools. You install the Windows desktop client by means of an MSI package which can be downloaded from the appliance

web client portal. You do not need administrator privileges to install the One Identity Safeguard for Privileged Passwords desktop client.

NOTE: When you install the Windows desktop client, the following components are also installed:

- Safeguard for Privileged Passwords Desktop Player which is used to replay recorded sessions.
- Safeguard for Privileged Passwords PuTTY which is used to launch the SSH client for SSH session requests.

Installing the Safeguard for Privileged Passwords desktop client application

1. To download the Safeguard for Privileged Passwords desktop client Windows installer .msi file, open a browser and navigate to:
`https://<Appliance IP>/Safeguard.msi`
Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.
4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.

Verify successful installation

You can verify that the correct version has been successfully installed from the Safeguard for Privileged Passwords desktop client or the LCD on the Safeguard for Privileged Passwords 2000 Appliance.

To verify the uploaded patch was installed

1. Log into the Safeguard for Privileged Passwords desktop client as an Operations Administrator or an Appliance Administrator.
2. Select **✕ Administrative Tools**.
3. Select **Settings | Appliance | Appliance Information**.
4. Verify the correct appliance version is displayed in the appliance properties pane.

In addition, when the appliance is running, the LCD home screen on the front panel of the appliance displays **Safeguard for Privileged Passwords** <version number>. Therefore, you can verify the correct appliance version is running from there as well.

More resources

Additional information is available from the following:

- Online product documentation: <https://support.oneidentity.com/one-identity-safeguard/technical-documents>
- One Identity Community: <https://www.quest.com/community/products/one-identity/>

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. It supports simultaneous operation with multilingual data. 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).

The release is localized to the following languages: Arabic (Saudi Arabia), Chinese (Simplified), Chinese (Traditional), Dutch, French, German, Italian, Japanese, Korean, Russian, Spanish.

About us

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

Contacting us

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

Technical support resources

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

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

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

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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




Patents

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

Trademarks

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

Legend

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