One Identity Safeguard for Privileged Passwords 2.8.1.10618

Patch Release Notes

September 2019

This patch includes the changes listed in the following sections. One Identity may generate additional patches for future releases of the product.

About this patch

This patch addresses issues involving account discovery, memory release, cluster connectivity validation, notification service reporting, password check and change process, and overall efficiencies.

The minimum version required for installing this patch is Safeguard for Privileged Passwords 2.1.0.5687.

NOTE: Safeguard for Privileged Passwords version 2.8.1 does not include any virtual machine (VM) patch or deployment.

Resolved issues

The following is a list of issues resolved in this patch.

Table 1: Resolved issues

Resolved issue	Issue ID
Favorites load promptly.	802741
Dynamic account groups and tagging are updated properly and efficiently.	803043
All tags are displayed.	803286
NTP monitor behaves as planned.	803849
Resolved the Tinc repeated restart on a replica issue.	804110
Resolved issues related to the internal server error which prevented successful password requests on the replica. Password requests process as expected.	804115
Able to select a directory from the Asset Discovery job dialog with 20k assets added to appliance.	804133

Applicability of this patch

Table 2: Products affected by this patch

Product name	Version
One Identity Safeguard for Privileged Passwords	2.8.0.10133

Installing this patch

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

NOTE: **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.

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**.

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.

Removing this patch

Once you install an update file, you cannot uninstall it.

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.

Bandwidth

We recommend that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500ms. If you are using traffic shaping, you must allow sufficient bandwidth and priority to port 655 UDP/TCP in the shaping profile. These numbers are offered as a guideline only in that other factors could require additional network tuning. These factors include but are not limited to: jitter, packet loss, response time, usage, and network saturation. If there is any questions please contact One Identity Technical Support.

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 (or greater)
Windows platforms	64-bit editions of: • Windows 7 • Windows 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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.

Component	Requirements
	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).
Desktop Player	See *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide* available at: One Identity Safeguard for Privileged Sessions - Technical Documentation, **User Guide**.

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: • Google Chrome 66 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) Mobile device browsers: • Apple Safari iOS 10 (or later) • Google Chrome on Android The web client is implemented for modern web browser technology, using: • HTML5 • CSS • JavaScript NOTE: If your browser lacks these required technologies, then use the desktop client.

Web kiosk requirements

The web kiosk is functionally similar to the desktop client end-user view. The web kiosk consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions.

Table 5: Web kiosk requirements

Component	Requirements
Web management console	Desktop browsers: • Google Chrome 66 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) The web management console is implemented for modern web browser technology, using: • HTML5 • CSS • JavaScript

Supported platforms

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

Tested platforms

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. For more information, see Management tab.

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

Table 6: 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

Platform	Version	Architecture
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
Dell iDRAC	7, 8	
F5 Big-IP	12.1.X, 13.0	
Facebook (deprecated)		
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	x86, x86_64
	7	x86_64
PAN-OS	6.0, 7.0	
PostgreSQL	9.6.7, 10.2	
RACF - Mainframe	z/OS V2.1 Security Server,	zSeries

Platform	Version	Architecture
	z/OS V2.2 Security Server	
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
SAP HANA	2.0	Other
SAP Netweaver Application Server	7.3, 7.4	
Solaris	10 11	SPARC, x86, x86_64 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 12	IA-64, PPC, x86, x86_64, zSeries 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 (deprecated)		
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, 2019	

Table 7: Supported platforms: Directories that can be searched

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

Custom platforms

The following example platform scripts are available:

- Custom HTTP
- Linux SSH
- Telnet
- TN3270 transports are available

For more information, see *Safeguard for Privileged Passwords Administration Guide*, Custom Platforms and Creating a custom platform script. Custom Platforms and Creating a custom platform script.

CAUTION: Facebook and Twitter functionality has been deprecated. Refer to the custom platform open source script provided on GitHub. Facebook and Twitter platforms will be remove in a future release.

Sample custom platform scripts and command details are available at the following links available from the Safeguard Custom Platform Home wiki on GitHub:

- Command-Reference:

  https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference

- Writing a custom platform script:

  https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript

- Example platform scripts are available at this location:

  https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts

CAUTION: Example scripts are provided for information only. Updates, error checking, and testing are required before using them in production. Safeguard for Privileged Passwords checks to ensure the values match the type of the property which include: a string, boolean, integer, or password (which is called secret in the API scripts). Safeguard for Privileged Passwords cannot check the validity or system impact of values entered for custom platforms.

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.

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

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.