One Identity Safeguard for Privileged Passwords 2.8

Release Notes

July 2019

These release notes provide information about the One Identity Safeguard for Privileged Passwords 2.8 release.

About this release

One Identity Safeguard for Privileged Passwords Version 2.8 is a minor release with new features and resolved issues. The new features include:

- Virtual appliance and web management console (770749, 781091, 798013, 798014, 798527)
- Application to Application (A2A) enhancement: API visible to certificate user (794148)
- Custom platforms: Telnet and HTTP support (799699, 787583)
- Advanced password complexity rules (780274)
- Job scheduler enhancements (753203)
- Safeguard for Privileged Sessions (SPS) initiated session (797262)
- Support for additional ServiceNow ticket types (793493)

For more detail, see:

- New features
- Resolved issues

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*.

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.

A Safeguard for Privileged Passwords virtual appliance is also available.

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 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

Virtual appliance and web management console (770749, 781091, 798013, 798014, 798527)

The Appliance Administrator responsible for racking and initial configuration of the appliance can create the virtual appliance, launch the Safeguard web management console, and select one of the following wizards.

- **Initial Setup**: Used to set up the virtual appliance for the first time including naming, OS licensing, and networking.
- **Setup**: After the first setup, Safeguard for Privileged Passwords updates and networking changes can be made via the web management console, **Setup**.
- **Support Kiosk**: The **Support Kiosk** is used to diagnose and resolve issues with Safeguard for Privileged Passwords. Any user able to access the kiosk can perform low-risk support operations including appliance restart or shutdown and support bundle creation. In order to reset the admin password, the user must obtain a challenge response token from One Identity support.

Security and backups

To maximize security in the absence of a hardened appliance, restrict the access to the Safeguard virtual disks, the web management console, and the MGMT interface to as few users as possible. Recommendations:

- X0 hosts the public API and is network adapter 1 in the virtual machine settings. Connect this to your internal network.
- MGMT hosts the web management console and is network adapter 2 in the virtual machine settings. This interface always has the IP address of 192.168.1.105. Connect this to a private, restricted network accessible to administrators only or disconnect it from the network to restrict unauthenticated actions such as rebooting or shutting down the appliance. The web management console is also available via the VMware console.

Once setup is completed, you can verify which of your NICs is MGMT and X0 by referring to the MAC address information found in **Support Kiosk** | **Appliance Information** | **Networking** for X0 and MGMT.

To protect the security posture of the Safeguard hardware appliance, Safeguard hardware appliances cannot be clustered with Safeguard virtual appliances. Additionally, to ensure the security of the hardware appliance, backups taken from a hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

Application to Application (A2A) enhancement: API visible to certificate user (794148)

When registering a third-party application configured for credential retrieval, the Policy Administrator can make the registration, including the API keys, visible to the certificate user that is configured for the A2A registration. The third-party application can discover the API key and other information needed. The **Visible to certificate user** check box can be selected when adding an application registration via **Administrative Tools** | **Settings** | **External Integration** | **Application to Application**.

Custom platform: Telnet and HTTP support (799699, 787583)

Custom HTTP, SSH, Telnet, and TN3270 transports are available. For more information, see *Safeguard for Privileged Passwords Administration Guide*,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 scripts 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.

Advanced password complexity rules (780274)

Separate password complexity rules can be set for local users and managed accounts. Password rules can be finely managed.

- Set the allowable password length in a range from 3 to 225 characters.
- Set first characters type and last character type.
- Allow uppercase letters, lowercase letters, numbers, and/or printable ASCII symbols along with the minimum amounts of each.
- Identify excluded uppercase letters, lowercase letters, numbers, and symbols.
- Identify if consecutive letters, numbers, and/or symbols can be repeated sequentially and, if allowed, set the maximum repetitions allowed.

Passwords are validated against the password rules before they are saved.

Job scheduler enhancements (753203)

An Appliance Administrator can finely tune backup and password check and change job schedules including the ability to ensure changes occur after hours. The administrator can create time windows including start and end times, days of the week, and days in a month by a static day of month or the first through fourth day of the month.

Safeguard for Privileged Sessions (SPS) initiated session (797262)

CAUTION: This functionality supports a future release of Safeguard for Privileged Sessions (SPS). For information on feature availability and use, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Once the future release of SPS is joined to SPP, the Safeguard for Privileged Passwords (SPP) Asset Administrator can enable an SPS initiated session to get the session credentials from SPP.

- The administrator will navigate to **Administrative Tools** | **Settings** | **External Integration** | **Sessions Management** and set the **Session Module Password Access Enabled** toggle on or off. When the toggle is on (), SPS will create an access request and check out a password from SPP on behalf of another user. When the toggle is switched off (), this ability is revoked. (The toggle displays in SPP 2.8 but has no impact.)

  CAUTION: On the Session Settings tab, SPS Connection Policy, do not select `Sps initiated`. This is reserved for a future release of SPS if an access policy is used by SPS to create an SPS initiated access request.

Support for additional ServiceNow ticket types (793493)

System integrators designing privileged account access based on ServiceNow tickets can include ticket types for validation during access request workflow. The following tickets types are supported in addition to INC tickets:

- PRB (problem) tickets
- CHG (change) tickets
- RITM (request) tickets

If the ticket number is found in any of the ServiceNow tables searched (INC, CHG, RITM, or PRB) and the ServiceNow API property for the ticket is "Active", the user can make the access request.

Administrators can search by a ticket number in the Activity Center to find the access request.

See also:

- Resolved issues on page 6

Resolved issues

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

Table 1: General resolved issues

Resolved Issue	Issue ID
It is now possible to enable and disable accounts from the Accounts view.	796079
Submitting a request through the web client when a policy expiration date is set now works as intended.	796866

Resolved Issue	Issue ID
Support bundles now include rSMS service logs.	797504
Increased the amount of time that the primary will wait for replicas to finish patching during a cluster patch.	800031
The user interface no longer reports an error with large backup archives even when the archive operation is successful.	800419
Clicking the Template Assistant link when importing assets no longer causes an error.	800524
In the discovery user interface, the partition is now more apparent in the discovered accounts and discovered services tiles.	800565
Unsent emails no longer cause the patch to stall.	800727
During a cluster patch, the scope of the repair operation on the replica has been reduced to prevent timeouts.	801035
Fixed a rare internal crash which could lead to quarantine.	801421, 802063
It is now possible to map Active Directory attributes from auxiliary classes.	801532
Profile names have been limited to 50 characters as intended.	801560
Editing account discovery jobs when more than 500 assets are present no longer causes an error.	802033
The option for **User Supplied** credentials now appears in access requests as intended.	802119
The account discovery tab on assets no longer shows account discovery details from the profile if the asset does not support account discovery.	802123, 802182
CheckPassword succeeds on a managed SYS account when a non-SYSDBA service account is used.	802173
Safeguard sends Syslog events to ArcSight in an RFC3164 or CEF compatible format.	802288
Acknowledging expired or revoked access requests after upgrading now works as intended.	802310
Safeguard for Privileged Passwords (SPP) now correctly locates the Safeguard for Privileged Sessions (SPS) Player executable.	802402

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
Do not preconfigure session policies unless you have a virtual machine (VM) join. Safeguard for Privileged Sessions (SPS) initiated session functionality supports an SPS feature available in a future release. For information on feature availability and use, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.	797262 (feature)
When using a VMWare virtual machine with Safeguard for Privileged Passwords for on initial setup, you cannot copy and paste. The copy and paste pop-ups display but no data is copied or pasted. A support request related to this kiosk app issue is pending with Microsoft (Microsoft support case 119041825001627).	800191
After restoring a backup, a joined SPS is no longer accessible from SPP. If you try to activate the appliance, this message will display: `Invalid policies detected`. The workaround for this issue is to soft delete the session connection in SPP and then rejoin SPS to SPP. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, "Sessions management with SPS joined" in the section "Connection deletion: soft delete versus hard delete".	802696
After restoring a backup, deleting a joined SPS session connection causes an incorrect error to display in the user interface: Cannot remove built-in certificate authorities. However, the session connection is still deleted and the user is still able to rejoin SPS to SPP.	802697

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. This number is 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. 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.

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
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

Platform	Version	Architecture
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
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

Platform	Version	Architecture
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.

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.

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 8: 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

Safeguard for Privileged Passwords 2000	Feature / Specification
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 9: 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.

- ✔ Green check mark button: 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.

  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.

- Red X button: 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.

  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.

- Down, up, left and right arrow buttons: When the appliance is running, the LCD home screen displays: `Safeguard for Privileged Passwords <version number>`. Use the arrow buttons to scroll through the following details:
  - Serial: <appliance serial number>
  - X0: <appliance IP address>
  - X1: <IP address of the sessions module interface>

    If one or more Safeguard Sessions Appliances are joined to Safeguard for Privileged Passwords, X1 is not available in Safeguard for Privileged Passwords.
  - MGMT: <management IP address>
  - MGMT MAC: <media access control address>
  - IPMI: <IP address for IPMI>

Table 10: Appliance LCD and controls

Control	Description
Green check mark button	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. **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.**
Red X button	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. **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.**

Control	Description
Down, up, left and right arrow buttons	When the appliance is running, the LCD home screen displays: • Safeguard for Privileged Passwords <version number> Use the arrow buttons to scroll through the following details: • Serial: <appliance serial number> • X0: <appliance IP address> • X1: <IP address of the sessions module interface> If one or more Safeguard Sessions Appliances are joined to Safeguard for Privileged Passwords, X1 is not available in Safeguard for Privileged Passwords. • MGMT: <management IP address> • 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 2.8 patch.
- **Clustered environment**: Please see the *Patching cluster members* section in the *One Identity Safeguard for Privileged PasswordsAdministration 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: The install also includes: 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.

Installing the Desktop Player

CAUTION: If the Desktop Player is not installed and a user tries to play back a session from the Activity Center, a message like the following will display: `No Desktop Player. The Safeguard Desktop Player is not installed. Would you like to install it now?` **The user will need to click Yes to go to the download page to install the player following step 2 below.**

1. Once the Safeguard for Privileged Passwords installation is complete, go to the Windows **Start** menu, **Safeguard** folder and click **Download Safeguard Player** to be taken to the One Identity Safeguard for Privileged Sessions - Download Software web page.
2. Follow the *Install Safeguard Desktop Player* section of the player user guide found here:
   a. Click this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.
   b. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.

New Desktop Player versions

When you have installed a version of the Safeguard Desktop Player application, you will need to uninstall the previous version to upgrade to a newer player version.

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 Communities: https://www.quest.com/community/one-identity/
- Knowledge Base: https://support.oneidentity.com/one-identity-safeguard/kb

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 (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

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.