One Identity Safeguard for Privileged Passwords 2.7

Release Notes

May 2019

These release notes provide information about the One Identity Safeguard for Privileged Passwords 2.7 release.

About this release

One Identity Safeguard for Privileged Passwords Version 2.7 is a minor release with new features and resolved issues. The new features include:

- Account discovery enhancements
- Activity Center enhancements
- Allow Oracle SYS account as a service account
- Asset discovery enhancements
- Custom platform: TN3270
- Separate identity and management for directories for fine grained management
- Microsoft SQL Server TCP/IP support
- Multiple directory account session support with access request policy
- Sessions Appliance join
- Radius enhancements

For more detail, see:

- New features
- Enhancements
- 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.

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

Sessions Appliance join (792394)

CAUTION: The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.

Managing sessions via the Safeguard Sessions Appliance is now available for use in production. For this release, the embedded sessions module for Safeguard for Privileged Passwords is still available.

The Asset Administrator can join a Safeguard for Privileged Sessions (SPS) cluster to a Safeguard for Privileged Password (SPP) cluster of one appliance or more for session recording and auditing. The actual join must be between the SPP primary and the SPS cluster master. This means that the Safeguard for Privileged Sessions (SPS) cluster is aware of each node in an SPP cluster and vice-versa.

Once joined, all sessions are initiated by the SPP appliance via an access request and managed by the SPS appliance and sessions are recorded via the Sessions Appliance.

Session recording, playback, and storage

- Sessions recorded after the join are playable through SPP and are stored on the SPS appliance. An archive server can be set up through SPS.
- Sessions recorded prior to joining the Safeguard Sessions Appliances are not migrated to the SPS appliance. For that reason, it is recommended that the SPP sessions be migrated to an archive server prior to the join.

Safeguard for Privileged Passwords join guidance

Before initiating the join, review the steps and considerations in the join guidance. For more information, see *Safeguard for Privileged Passwords Administration Guide*, Appendix C: SPP and SPS sessions appliance join guidance.

Safeguard for Privileged Sessions join steps and troubleshooting

The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Separate identity and management for directories for fine grained management (773267)

The following information summarizes the changes at a high level. For more information specific for your initial deployment of Safeguard for Privileged Passwords 2.7, see the *Safeguard for Privileged Passwords Administration Guide*, Appendix B: SPP 2.7 Migration guidance.

Overview

Safeguard for Privileged Passwords version 2.7, has been simplified to allow for a separation of duties based only on identity management, asset management, access policy configuration, and appliance maintenance. In the migration to version 2.7, greater flexibility is realized through these high-level assignments:

- Directories are migrated to assets.
- Accounts include both directory accounts and asset accounts.
- Each directory is assigned its own partition in the migration to version 2.7.

The following information details the changes from version 2.6 to version 2.7. The same information is generally true if you are upgrading from version 2.1 forward to version 2.7.

Administrators

- The Directory Administrator role is removed and users with Directory Administrator permission are assigned as partition owners for directories that are migrated to assets. This role does not include the ability to manage identity providers.
- An Authorizer administrator can now add an Active Directory forest only for identity to use as an unprivileged service account for connection.
- An Asset administrator can now:
    - Use service accounts to manage Active Directory. The service accounts can have limited permissions within a single domain.
    - Use multiple service accounts for managing the same Active Directory domain with different limited permissions within the domain. For example, the administrator can add the domain as a managed asset multiple times with different service accounts.
    - Use a service account from Active Directory to manage an asset from a different partition so that the administrator does not have to add that Active Directory to each of the administrator's partitions.

- Set up a dependent system for a service running as an Active Directory account that isn't in the administrator's partition. This avoids having to add the Active Directory asset or the account to the partition.
- Add Active Directory for authentication to Safeguard for Privileged Passwords without managing any of the accounts in Active Directory.
- Set up multiple assets for the same domain.

Identity

During the migration to version 2.7, directories are migrated as an asset with the appropriate identity provider and associated users.

Management

Directories can be subdivided so administrators can be assigned to manage portions of a directory. For example, Admin A might only manage objects in the Finance organizational unit (OU) of the directory and Admin B might only manage objects in the Engineering OU of the directory. This is possible via the settings on Assets including the asset **Name**, **Domain Name**, and whether to **Manage Forest**. This way, multiple assets can govern the same domain.

Directory accounts can be service accounts to other assets to run windows services/tasks on assets to keep password changes in sync.

Accounts

- You can select a directory account and view the assets that have a dependency on the account.
- You can sync passwords between a directory account and an asset account.

Assets

- Directories are migrated to assets with the appropriate provider assignment.
- Directories are still synced with Safeguard.
- Migrated directory assets reflect the account dependencies.
- You can select whether a directory asset manages the forest or a subset of the forest. Multiple assets be assigned against the same forest.
- Migrated directory assets are available for access discovery jobs beyond partition boundaries.
- Each migrated directory asset is assigned to its own partition and includes the Account Discovery schedules, the check and change schedules, account password rules, password sync groups, and related functions.
- A directory is a member of an asset partition so that ownership of different parts of the directory can be delegated.
- During import, entities imported from a directory must be unique across all partitions (for example, you cannot import Admin C account into multiple asset partitions).
- When you add an asset, the Account Discovery schedule for the partition is displayed and can be changed.

Discovery schedules

- Account discovery includes the option for discovered accounts: enable password requests, enable session requests, and make the discovered accounts available for use across all partitions.
- Account discovery can be configured as Unix based, Windows based, or Directory based, each with its own schedule.

Account discovery enhancements (788930)

Asset Administrators and delegated partition owners can create account discovery jobs to perform the functions in the following list:

- Set the default password of a discovered account to configure the environment initially and incrementally.
- Add a discovered account to a sync group to configure the environment initially and incrementally.
- Immediately check and change the password of discovered accounts that are set to be automatically managed. This places the account under immediate management rather than waiting for the schedule to execute.

  NOTE: In **Settings** | **Profile**, the partition profile's **Change Password Schedule** and **Check Password Schedule** must both be set to a value other than **Never**.

Activity Center enhancements (799288, 799308, 799307)

From the Activity Center, you have the option to choose All entities (such as users, assets, and accounts) without picking all of them. You can export the report without first previewing the report.

Allow Oracle SYS account as a service account (799993, 800128)

An Asset Administrator responsible for Oracle database servers can use the SYS account with either SYSDBA or SYSOPER system privileges as a service account.

The SYS account is automatically created when the administrator installs Oracle and has the necessary privileges. See the Oracle document, About Administrative Accounts and Privileges, for more information. The SYS user is automatically granted the SYSDBA privilege on installation and can be SYSOPER. For more details, see the Oracle document, SYSDBA and SYSOPER System Privileges.

This is set via setting the Service Name when you add or edit an asset. Navigate to **Administrative Tools** | **Assets** | **Connection** tab.

Asset discovery enhancements (782848)

Asset Administrators are now given:

- Expanded connection options when setting up the connection template to discovered assets to automatically manage discovered assets and service accounts.
- The ability to set a platform type in the asset discovery rules.
- The ability to assign a different profile to service accounts in the asset discovery rules so that the service account is assigned a profile other than default asset profile inherited by other accounts discovered on the asset.

In addition, SSH keys are now auto-accepted for supported platforms.

Custom platform: TN3270 (798892)

An Asset Administrator responsible for an AS400 and mainframe infrastructure (such as ACF2 or RACF) can manage servers customized log in screens and connection strings.

A custom platform author can create a customer platform script to check and change passwords against servers where the login screens and connection strings have been customized.

Microsoft SQL Server TCP/IP support (798894, 799577)

An Asset Administrator responsible for Microsoft SQL Server can have Safeguard for Privileged Passwords connect to the databases using TCP/IP rather than named pipes.

Multiple directory account session support with access request policy (792426)

A Policy Administrator can add multiple directory accounts to a single access request policy. For example, you can grant access to a Windows asset via RDP using one of multiple directory accounts. Accounts are added when you create or edit an access request policy via the **Administrative Tools** | **Entitlements** | **Access Request Policies** | **Directory Account** option.

Radius enhancements (798896)

The User Administrator is offered two new configuration controls on **Settings** | **External Integration** | **Identity and Authentication** when Radius is selected as the provider.

- The User Administrator can choose to mask the Radius secondary authentication response entered by users by selecting the **Always Mask User Input** check box. If selected, the text box that the user enters their one-time password, or other

challenge required by the Radius server, will always be a password style text box in which the user's input is masked and appears as a series of dots, not as clear text. This may be desired when the challenge is not just a one-time password, but also contains the user's PIN. This will prevent any passer-by from seeing the private information. Note, however, that when this setting is enabled, it will also override the Prompt attribute of the Radius server's Access-Challenge response, such that the user's input will always be masked.

- The User Administrator can choose to have the Radius secondary authentication pre-submit an Access-Request message to the Radius server in order to initiate a challenge/response cycle before the user sees or enters any information. The **PreAuthenticate for Challenge/Response** check box is used to indicate whether an Access-Request call containing only the User-Name should be sent to the Radius server prior to the user's authentication attempt. This is done to inform the Radius server of the user's identity so the server can possibly begin the authentication process by starting a challenge/response cycle. This may be required to seed the user's state data. In addition, the Radius server's response may include a login message that is to be displayed, which is specific to that user. Note, if the Radius server is not configured to respond with an Access-Challenge, then this will cause the log in to fail and the user will be unable to proceed.

In addition, the timeout for log in is now configurable to more than 60 seconds.

See also:

- Resolved issues on page 9

Enhancements

The following is a list of enhancements implemented in Safeguard for Privileged Passwords 2.7.

Table 1: General enhancements

Enhancement	Issue ID
Add ability to set a profile on auto discovered accounts for directories.	789170
Would like to set a default known password for all auto discovered accounts.	789171
Custom platform sample script added for RACF mainframes.	798177
Increase valid time for factory reset keys from 24 to 48 hours.	799194
Allow customization of the SAP Client ID. Safeguard always uses Client ID 001.	799747
Add password check out reason to the access request activity report.	800084

Resolved issues

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

Table 2: General resolved issues

Resolved Issue	Issue ID
Archive server needs way to test connection/check system just like assets.	653394
RDP signing certificate fails with `A revocation check could not be performed for this certificate`.	763103
RACF platform tasks fail because logon command is wrong.	774792
In Top Secret Mainframe, the platform script doesn't work for different login screens.	782623
SQL accounts not manageable when Named pipes are disabled.	787919
If user changes from Certificate Authentication to Local Authentication, the parameter RequireCertificateAuthentication doesn't get changed back to false.	791699
Socket address already in use.	796623
Unable to set the BMC settings.	797146
Unable to generate asset entitlement report for all accounts.	798367, 798370
Unable to generate Password Management Activity Report.	798369
Clicking on a favorite for an access request that utilizes user supplied credentials returns an error message.	798739
Add TN3270 custom platform sample.	798892
Unable to manually generate all activity report.	798965
Approval Anywhere is not working if Active Directory is missing the country code.	798972
Right-click object selection issue.	798981
Client does not show any assets in Entitlement reports when **Browse** is clicked.	799188
UI times out waiting for password activity report to export.	799260
UI limits AuditLog export to 50,000 records instead of asking for the entire date range specified.	799261
UI should export directly from the Activity Center without actually running anything first.	799263
Oracle DB **Connection** tab properties shows the **Instance** field but this value is the **Service Name**.	799326

Resolved Issue	Issue ID
Scheduled reports are not working.	799448
Frequent reporting, looping AD Query in directory sync causes scheduler to consume too much memory and crash; Cassandra to exceed max memory usage.	799512
Oracle DB platform operations fail when using SYS as Service Account.	799575
Archiving does not work for 200 days or less with message `Batch too large` in Pangaea.Service.Core-20190326.log.	799636
Domain name of an account is not visible when requesting a session.	799676
Domain user **Require Certificate Authentication** selection does not save.	799748
Error received when running an entitlement report for an admin user.	799847
Replica goes to quarantine during join and this message displayed: `Failed to download policy data`.	799917
Manual backup fails. Messages include: `Aggregate exception caught` and `Value cannot be Null`.	799925
Administrator roles missing from CSV version of an entitlement report.	799955
Password activity report exported as JSON format opens as CSV format.	799956
BMC ILO reports an error when switching on / off or when trying to change the password.	800123
Allow Oracle SYS account as service account PBI.	800128
Add Oracle Privileges connection property.	800132
Password check in fails to cycle password on linked account when there is an open RDP request. Error: `You cannot access this account while another request is pending password reset (90010)`.	800242
Cannot reset SYS/SYSTEM with Oracle 11g.	800440
SSH key based authentication when adding archive server does not work.	800502
testConnection speed needs to be quicker.	800814

Known issues

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

Table 3: Known issues

Known Issue	Issue ID
This issue is applicable if you use the embedded sessions module. After a software patch, the SessionBannerText and and SessionSshHostKey may be lost. **Details and workaround:** Check the banner and host key in the user interface and update the information, as needed. • Navigate to **Administrative Tools** | **Settings** | **Sessions** | **SSH Banner**. • Navigate to **Administrative Tools** | **Settings** | **Sessions** | **SSH Host Key**. **CAUTION:The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.**	800520

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 4: 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 5: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 66 (or later)

Component	Requirements
	• 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.

Supported platforms

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

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 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

Platform	Version	Architecture
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		
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,	zSeries

Platform	Version	Architecture
	z/OS V2.2 Security Server	
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		
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

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
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.**
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 2.7 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: When you install the Windows desktop client, the following is also installed:

- 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 Community: https://www.quest.com/community/products/one-identity/
- Knowledge Base: https://support.oneidentity.com/one-identity-safeguard/kb?r=Category%3AVideos%2CSolution

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.