Safeguard for Privileged Passwords 2.11.1

Patch Release Notes

March 2020

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 a issue. The minimum version required for installing this patch is 2.1.0.5687.

Resolved issues

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

Table 1: Resolved issues

Resolved issue	Issue ID
Users can play back a session recorded while Safeguard for Privileged Passwords was in Offline Workflow mode. Users can play sessions from a system in Offline Workflow mode without connecting to the CM.	227143
Assets keep valid SSH keys.	226052
Session connection policy works as designed when SPS Central Management	225962

Resolved issue	Issue ID
Node is also Search Master.	
SPS initiated SSH sessions works from AA plugin after SPP upgrade from 2.10 to 2.11.	225960
Users can save favorites and access request for Request Type: RDP with own credentials.	225580
Session request from web client is working.	224694
Scheduler and directory syncing works with appropriate accounts updated.	224664
Sessions can be reviewed as new and after several days.	224578
Safeguard for Privileged Passwords (SPP) can use available Safeguard for Privileged Sessions (SPS) nodes whether SPP is in offline workflow mode or not. SPS nodes must be set up correctly.	224121 226219
Initiated sessions process, including Active Directory forests with multiple subdomains and authenticating via federation (Okta) with AD identity information.	223911
Account Discovery on Linux systems will find accounts with unique usernames, even if the UID is shared with other users.	223893
2.11.0 patch distribution succeeds.	223809
Single and multiple requests to an access rule succeed.	223430
Favorites can be saved.	221812
Protection was added for both the Safeguard 2000 Appliance (hardware) and the virtual machine (VM). The patch relates to a Microsoft Windows update that resolved a defect in the verification of signatures using elliptic curve cryptography. For more information, see: • One Identity Support Knowledge Base: KB article 311852 • Microsoft: CVE-2020-0601, Windows CryptoAPI Spoofing Vulnerability. Only the second issue is pertinent, which relates to man-in-the-middle attacks and confidential information decryption on connections relying on TLS for security, for example, HTTPS, LDAPS, TN3270, and so on (not SSH or Windows).	219093
Azure virtual machine (VM) works as expected during a cluster reset.	215793

Known issues

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

Known issue	Issue ID
For versions 2.11.1 and 2.11, the web UI shows a launch button for both RDP and SSH sessions. • If you have an application registered (`rdp://` for RDP sessions), you can click the ▶ **Launch** button to the right of the asset name then click **Connect** . See KB 313918 for details on application registration. A password must be entered and we recommend `sg`. A blank password will cause the session to fail. • If you do not have an application registered, download the RDP launch file instead of using the ▶**Launch** button. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.	227292

Applicability of this patch

Table 2: Products affected by this patch

Product name	Version
Safeguard for Privileged Passwords	2.11.0.11444

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).

Always back up your appliance before you install an update file. Once you install an update file, you cannot uninstall it.

If you are using a clustered environment, 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.

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 in to 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.
   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 Appliance.

To verify the uploaded patch was installed

1. Log in to 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 a patch file, you cannot uninstall it.

System requirements

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

It is recommended that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500 milliseconds. 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 are any further questions, please check with your Network Administration team.

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 later)
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. Considerations: • 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). • To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard.
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 requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 77 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 69 (or later) NOTE: To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard. Mobile device browsers: • Apple iOS 13 (or later) • Google Chrome on Android version 77 (or later) 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 77 (or later) • Microsoft Internet Explorer 11 and Edge

Component	Requirements
	• Mozilla Firefox 69 (or later) NOTE: To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard. The web management console is implemented for modern web browser technology, using: • HTML5 • CSS • JavaScript

Supported platforms

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

Safeguard for Privileged Passwords tested platforms

The following table lists the platforms and versions that have been tested for Safeguard for Privileged Passwords (SPP). 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**, **Other Managed**, or **Other Linux** selection on the **Management** tab of the **Asset** dialog. For more information, see Management tab.

SPP joined to SPS: Sessions platforms

When Safeguard for Privileged Passwords (SPP) is joined with a Safeguard for Privileged Sessions (SPS) appliance, platforms are supported that use one of these protocols:

• SPP 2.8 or lower: RDP, SSH

• SPP 2.9 or higher: RDP, SSH, or Telnet

Some platforms may support more than one protocol. For example, a Linux (or Linux variation) platform supports both SSH and Telnet protocols.

For the embedded sessions module, platforms that support RDP and SSH protocols are generally supported.

Table 6: Supported platforms: Assets that can be managed

Platform	Version	Architecture (all versions unless noted)	SPP	SPS
ACF2 - Mainframe	r14, r15	zSeries	True	True

Platform	Version	Architecture (all versions unless noted)	SPP	SPS
ACF2 - Mainframe LDAP	r14, r15	zSeries	True	False
Active Directory			True	False
AIX	6.1, 7.1, 7.2	PPC	True	True
Amazon Linux	2	x86_64	True	True
Amazon Web Services (AWS)	1		True	False
CentOS Linux	6 7	(ver 6) x86, x86_64 (ver 7) x86_64	True	True
Cisco ASA	7.x, 8.x		True	True
Cisco IOS	12.X, 15.X		True	True
Debian GNU/Linux	6, 7, 8, 9	x86, x86_64, MIPS, PPC, zSeries	True	True
Dell iDRAC	7, 8		True	True
ESXi (VSphere)	5.5, 6.0, 6.5, 6.7		True	False
F5 Big-IP	12.1.2, 13.0, 14.0		True	True
Facebook (deprecated)			True	False
Fedora	21, 22, 23, 24, 25, 26, 27, 28, 29, 30	x86, x86_64	True	True
Fortinet FortiOS	5.2, 5.6		True	True
FreeBSD	10.4, 11.1, 11.2	x86, x86_64	True	True
HP iLO	2, 3, 4	x86	True	True
HP iLO MP	2, 3	IA-64	True	True
HP-UX	11iv2 (B.11.23), 11iv3 (B.11.31)	PA-RISC, IA-64	True	True
IBM i	7.1, 7.2, 7.3	PPC	True	True
Junos - Juniper Networks	12, 13, 14, 15		True	True

Platform	Version	Architecture (all versions unless noted)	SPP	SPS
macOS	10.9, 10.10, 10.11, 10.12, 10.13	x86_64	True	True
MongoDB	3.4, 3.6, 4.0		True	False
MySQL	5.6, 5.7		True	False
OpenLDAP	2.4		True	False
Oracle	11g Release 2, 12c Release 1		True	False
Oracle Linux (OEL)	6 7	(ver 6) x86, x86_64 (ver 7) x86_64	True	True
Other			False	False
Other Linux			True	True
Other Managed			True	False
PAN-OS	6.0, 7.0, 8.0, 8.1		True	True
PostgreSQL	9.6, 10.2, 10.3, 10.4, 10.5		True	False
RACF - Mainframe	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries	True	True
RACF - Mainframe LDAP	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries	True	False
Red Hat Enterprise Linux (RHEL)	6, 7, 8	(ver 6) x86, x86_64, PPC, zSeries (ver 7 and 8) x86, x86_64, PPC, zSeries	True	True
SAP HANA	2.0	Other	True	False
SAP Netweaver Application Server	7.3, 7.4, 7.5		True	False
Solaris	10, 11	(ver 10) SPARC, x86, x86_64 (ver 11) SPARC, x86_64	True	True
SonicOS	5.9, 6.2		True	False

Platform	Version	Architecture (all versions unless noted)	SPP	SPS
SonicWALL SMA or CMS	11.3.0		True	False
SQL Server	2012, 2014, 2016		True	False
SUSE Linux Enterprise Server (SLES)	11 12	(ver 11) x86, x86_64, PPC, zSeries, IA-64 (ver 12) x86_64, PPC, zSeries	True	True
Sybase (Adaptive Server Enterprise)	15.7, 16		True	False
Top Secret - Mainframe	r14, r15	zSeries	True	True
Top Secret - Mainframe LDAP	r14, r15	zSeries	True	False
Twitter (deprecated)			True	False
Ubuntu	14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18.04 LTS, 18.10, 19.04	x86, x86_64	True	True
Windows	Vista, 7, 8, 8.1, 10 Enterprise (including LTSC and IoT).		True	True
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016, 2019		True	True
Windows SSH	7, 8, 8.1, 10 Server 2008 R2, 2012, 2012 R2, 2016, 2019 Windows SSH Other		True	True

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

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

To add a Safeguard for Privileged Passwords module license

The first time you log in to 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.