Safeguard for Privileged Passwords Patch for version 6.7.1

Release Notes

16 November 2020, 12:12

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 an issue. The minimum version required for installing this patch is 6.0.

Resolved issues

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

Table 1: Resolved issues

Resolved issue	Issue ID
Fixed an issue where after updating to 6.7 SMTP Auth service repeatedly crashes causing quarantine.	256006

Applicability of this patch

Table 2: Product affected by this patch

Product name	Version
Safeguard for Privileged Passwords	6.7

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).

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

Installing the software patch

1. As an Appliance Administrator, log in to the Safeguard for Privileged Passwords desktop client.
2. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Updates**.
3. 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.
4. Once the file has successfully uploaded, click **Install Now**.

Verifying successful completion

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 determine if this patch is installed

1. Log in to the Safeguard for Privileged Passwords desktop client as an Operations Administrator or an Appliance Administrator.
2. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**.
3. 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 6.7.1. 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.

Product licensing

The Safeguard for Privileged Passwords 3000 Appliance and 2000 Appliance ship with the following modules, each requiring a valid license to enable functionality:

- One Identity Safeguard for Safeguard for Privileged Passwords (SPP)
- One Identity Safeguard for Privileged Sessions (SPS)
  SPS is a separate product. To update the SPS license, see the *Safeguard for Privileged Sessions Administration Guide*, Updating the SPS license.

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.

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

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 highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.