Safeguard Privilege Manager for Windows 4.5

Release Notes

22 February 2023, 16:38

These release notes provide information about the Safeguard Privilege Manager for Windows release. For the most recent documents and product information, see the online product documentation.

About this release

Giving users administrator rights creates security risks but must be weighed against constant help desk calls for basic operations like updating Adobe Reader, Java, or simply changing the time zone on desktops.

Safeguard Privilege Manager for Windows lets you grant selected privileges to users so they can update their own computers, reducing help desk calls while maintaining a secure network. By automating user privilege settings, Safeguard Privilege Manager for Windows keeps users working. This allows you to focus on higher priority tasks, for exceptional resource and time savings.

As a system administrator, you can use Safeguard Privilege Manager for Windows to elevate and manage user rights quickly and precisely with validation logic targeting technology. This provides administrators the ability to create rules that allow administrator-level access to specific applications for specifics users. You can also enable your end users to request elevated privileges for specific applications through Self-Service and Instant Elevation.

> NOTE: Customers upgrading from previous versions of Safeguard Privilege Manager for Windows (such as 3.x and earlier) are required to obtain a new license file. For additional information, see Product licensing.

> NOTE: The security status of the installation file can become "blocked" after download, inhibiting the ability of the product to be properly installed. For information on detecting

and resolving this issue, see KB 4268094.

Enhancements

The following is a list of enhancements implemented in Safeguard Privilege Manager for Windows 4.5.

Table 1: General enhancements

Enhancement	Issue ID
Improved the coherency of check boxes used for the validation logics of operating systems.	393552

Table 2: Console enhancements

Enhancement	Issue ID
Added support for Safeguard Privilege Manager for Windows Console to target existing MS SQL Server 2019 for database.	932
Added support to install Safeguard Privilege Manager for Windows on MS Windows Server 2019.	930

Table 3: Client enhancements

Enhancement	Issue ID
Added support to manage Windows Server 2019 as a Safeguard Privilege Manager for Windows Client.	931
Added a menu option to run gpupdate from the client's system tray menu.	322459

Resolved issues

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

Table 4: General resolved issues

Resolved Issue	Issue ID
Some menu items in the client system tray (for example, **Temporary**	SR Number:

Resolved Issue	Issue ID
Session Elevation) occasionally appeared more than once. This issue has been fixed in version 4.5.	4517221-1
Fixed a potential severe client computer performance degradation that could occur when a user was logging on.	SR Number: 01852116
Previously, the Client icon of Safeguard Privilege Manager for Windows occasionally showed incorrect wording if the Windows Display Language was set to a language other than English. This issue is now fixed.	904

Table 5: Resolved issues – Reporting

Resolved Issue	Issue ID
Previously, under complex conditions, the following error could appear in the Safeguard Privilege Manager for Windows Console log (`PAConsole_Log.txt` or `PAReporting_log.ldf`): `System.Data.SqlClient.SqlException: Cannot create file 'c:\Program Files\Microsoft SQL Server-\MSSQL12.PAREPORTING\MSSQL\DATA\PAReporting.mdf' because it already exists. Change the file path or the file name, and retry the operation.` This issue occurred due to a reporting configuration failure, and has been fixed by ensuring that Safeguard Privilege Manager for Windows can handle file duplication properly.	665

Table 6: Resolved issues – Privileged Application Discovery

Resolved Issue	Issue ID
Previously, when using the Privileged Application Discovery Rules Generation Wizard, grouping the results on the **Review** panel for a specific column and attempting to view the details of a grouped rule could result in an exception error. This issue has been fixed by ensuring that the Safeguard Privilege Manager for Windows rules generation wizard can manage grouping correctly.	1967

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 7: General known issues

Known Issue	Issue ID
Some log files are still being created and maintained on the system drive even when Safeguard Privilege Manager for Windows has been installed to a non-system drive.	618
Some duplicate records exist in the database and could be optimized.	624
`Error 1920` encountered during a PM Client installation repair (initiated from **Add/Remove Programs**), if the PM Client was manually installed. Workaround: Instead of performing a repair, manually uninstall, then reinstall the Client.	721
`CSEHostEngine.log` grows quickly.	824

Table 8: Installation and Upgrade known issues

Known Issue	Issue ID
There is an issue with sending data from clients to the database installed with the Safeguard Privilege Manager for Windows Console if there is an older Privilege Authority or Safeguard Privilege Manager for Windows Client running on the network. Workaround: Ensure the following: • The **Client Data Collection Settings** in the **Advanced Policy Settings** for the relevant Group Policy Object (GPO) are enabled. • The Safeguard Privilege Manager for Windows Server information is correct. • The Privilege Authority clients are upgraded to the current version.	1568
Some files may still exist on your computer even after the Console or Client are uninstalled.	1837
After uninstalling the Safeguard Privilege Manager for Windows Console from a computer that also has the Safeguard Privilege Manager for Windows Client installed, the **Start** menu shortcut to the *Safeguard Privilege Manager for Windows User Guide* will fail to open the guide. Instead, the shortcut prompts the user for the location of the `PAClient.msi` file. Workaround: Uninstall and re-install the Client. Alternatively, reinstall the Console.	1960

Table 9: Licensing known issues

Known Issue	Issue ID
Applying a Professional license fails to prevent a rule with an expiration date from expiring. Workaround: After you apply the license, open a rule that is going to expire, make your changes, and save the rule.	932
Applying a Professional license to an installation with an expired trial license can result in the loss of previously saved policies.	535

Table 10: Server known issues

Known Issue	Issue ID
Sometimes when configuring the reporting feature, the connection to the web service fails on the last step of the wizard. Workaround: Try again (click **Previous** and **Next** again).	834
If you select a remote Safeguard Privilege Manager for Windows Server on a computer with a firewall enabled, you may encounter a `Database Connection` error when using the Reporting or Discovery and Remediation functions. Workaround: Add the following firewall exceptions to the remote Safeguard Privilege Manager for Windows Server: • SQL Server Browser Service: `%ProgramFiles(x86)%\Microsoft SQL Server\90\Shared\sqlbrowser.exe` • SQL Server <ServerName>: `%ProgramFiles%\Microsoft SQL Server\MSSQL10.PAREPORTING\MSSQL\Binn\sqlservr.exe`	1105
If Windows Firewall is configured to deny connections (the **Don't allow exceptions** and **Block all connections** options are chosen in all other operating systems), Safeguard Privilege Manager for Windows does not automatically override the settings when configuring firewall exceptions during the Safeguard Privilege Manager for Windows Server setup. Workaround: Add an exception to the firewall manually for `%ProgramFiles (x86)%\One Identity\Safeguard Privilege Manager for Windows\Console\Data Collection Service\PADataCollectionWinSvc.exe.`	1657
If the administrator is prompted to reboot the computer after installing a prerequisite while using the Privilege Manager Server Setup wizard: Once the computer is rebooted and setup wizard continues, the administrator must click the **Back** button to reenter any of the **Server Email Notification Configuration** settings they entered prior to the reboot.	1980
If the administrator is changing the selected Safeguard Privilege Manager for Windows Server that the Console points to by setting up a Server on the local	1981

Known Issue	Issue ID
computer: After the wizard and Safeguard Privilege Manager for Windows Server Configuration are closed, the administrator may have to reopen the dialog. If the reporting screens still appear to be pulling data from the previously selected server, the administrator has to make sure the newly configured Safeguard Privilege Manager for Windows Server is the currently selected server.	

Table 11: Self-Service Elevation known issues

Known Issue	Issue ID
The **Self-Service Elevation Request Prompt** does not display for a MSI Windows Installer file. Workaround: Launch the **Self-Service Elevation Request Form** via the **Elevate!** button. You must configure the corresponding **Self-Service Elevation Request** settings.	1311
Some processes do not trigger the **Self-Service Elevation Request Prompt** even though they trigger User Account Control (UAC).	1674
On Windows 8.1 and Windows Server 2012 R2, if your client is running on a system with UAC turned off: When you right-click the Safeguard Privilege Manager for Windows icon in the Windows system tray and select the **View status of advanced features** dialog, the **Self-Service Elevation Request** and **Self-Service Elevation Request (ActiveX installations)** options should display as **N/A** (Not Applicable). Instead, it will incorrectly display an **Enabled** status.	1865

Table 12: Rules known issues

Known Issue	Issue ID
A login failure occurs when connecting to the database and web service if you are using a SQL Server from an untrusted domain. Workaround: Use the database server on the same trusted domain network environment.	698
When configuring reporting to use an existing SQL Server, clicking **Previous** in the **Configure Database and Services** step navigates you to an incorrect wizard step. **Workaround** To navigate to the **Select an Existing SQL Server** step, click **Next**.	832
Sometimes changing settings on the **Advanced Policy Settings** tab of a	1671

Known Issue	Issue ID
Group Policy Settings page results in the `Network path was not found` error once you save the changes to the Group Policy Object (GPO). Workarounds: - Restart the Safeguard Privilege Manager for Windows Console. - Check that the changes you made on the **Advanced Policy Settings** tab of the **Group Policy Settings** page have been saved. If not, re-apply your changes and save the GPO.	
Currently, Safeguard Privilege Manager for Windows displays no feedback message when a user is denied run privileges due to a **Blacklist** setting.	124
The **Rule Type** filter on the Instant Elevation Report mistakenly contains Privilege Authority v 2.7-related values. An Instant Elevation Report generated based on these values contains no data. As a workaround, only use the following filters: - **file** - **ActiveX** - **Windows Installer** - **script file**	1743

Table 13: Reporting known issues

Known Issue	Issue ID
The Elevation Activity Report does not display correctly when exported to an `.rtf` file. Workaround: Export your Elevation Activity Reports to different file formats.	728
The Console report shows the event time according to the current local time zone.	948
Some reports exported in Excel contain columns that do not display on the generated report page in the Safeguard Privilege Manager for Windows Console.	1738
Resultant Set of Policy (RSoP) output is empty or blank. ***For a workaround if the client is installed on your computer and RSoP is failing*** 1. Install .NET 3.5 Service Pack 1 (SP1). 2. Install GPMC, which is part of the Remote Server Administration Tools for Windows 8.1.	1881

Known Issue	Issue ID
3. Open a command prompt and change the directory to where the client files are installed, such as the following on an x64 computer: `C:\Program Files (x86)\Common Files\One Identity\Safeguard Privilege Manager for Windows\Client` 4. Run the following command: `%WINDIR%\Microsoft.NET\Framework\v2.0.50727\regasm.exe" "PrivilegeManager.Reporters.dll" /tlb /nologo /codebase` RSoP should now work for Safeguard Privilege Manager for Windows.	

System requirements

Before installing Safeguard Privilege Manager for Windows 4.5, ensure that your system meets the following minimum hardware and software requirements.

> NOTE: The security status of the installation file can become "blocked" after download, inhibiting the ability of the product to be properly installed. For information on detecting and resolving this issue, see KB 4268094.

Hardware, software, and operating system requirements

Table 14: Hardware, software and operating system requirements

Component	Hardware	Software	Operating system
Console and Server	• Processor: 2.0 GHz, dual core equivalent • Memory: 4 GB • Disk space: 100 MB (Console) NOTE: Additional space is required for the Privilege Manager database. For more information, see *Database Planning* in the	• .NET Framework 4.0 • Microsoft Group Policy Management Console • PDF reader to open the product documents	• Microsoft Windows 11 • Microsoft Windows 10 • Microsoft Windows 8.1 • Microsoft Windows Server 2022 • Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows

Component	Hardware	Software	Operating system
	Administration Guide. - Screen resolution: 1024x768 or higher		Server 2012 Standard/Enterprise NOTE: One Identity recommends using the product with 64-bit operating systems.
Client	As recommended for your operating system.	N/A	- Microsoft Windows 11 - Microsoft Windows 10 - Microsoft Windows 8.1 - Microsoft Windows Server 2022 - Microsoft Windows Server 2019 - Microsoft Windows Server 2016 - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2012 Standard/Enterprise NOTE: One Identity recommends using the product with a 64-bit operating system.

Network requirements

The Safeguard Privilege Manager for Windows Console and Client must be installed on a computer within the Active Directory domain.

Required permissions

- Local administrator rights to start the Console.
- Write permissions for Group Policy objects (GPOs) to be configured.

Reporting database requirements

The Safeguard Privilege Manager for Windows Server component requires, Microsoft SQL Server hosted either locally on the machine running the product, or remotely.

The product supports Microsoft SQL Server 2014 to Microsoft SQL Server 2019. Safeguard Privilege Manager for Windows can optionally install SQL Server 2014 SP2 Express.

Product licensing

For more information on the available product editions and applying a license, refer to the *Safeguard Privilege Manager for Windows Administration Guide*.

Safeguard Privilege Manager for Windows licenses are compatible with only a single major version of the product (for example, 3.x or 4.x). Therefore, when upgrading to new major product version, you need to renew your existing license. To obtain a new license file and properly register the product after upgrade, use the License Assistance portal.

> NOTE: Safeguard Privilege Manager for Windows does not phone home for product licensing.

Upgrade and installation instructions

For detailed information about upgrade information, refer to the *Safeguard Privilege Manager for Windows Administration Guide*.

For detailed information about installing the Console, configuring the Server, and installing the Client, refer to the *Safeguard Privilege Manager for Windows Quick Start Guide*.

More resources

Additional information is available from the following:

- Online product documentation

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.

In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options.

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.

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

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

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.**