

Safeguard Privilege Manager for Windows

Release Notes

Version 4.8

25 November 2024, 10:17

These release notes provide information about the Safeguard Privilege Manager for Windows release. For the most recent documents and product information, see [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 specific 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 [KB4268094](#).

Enhancements

The following is a list of enhancements implemented in Safeguard Privilege Manager for Windows 4.8.

Table 1: General enhancements

Enhancement	Issue ID
General security improvements.	459211

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 2: 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 3: 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	1568

Known Issue	Issue ID
<p>Privilege Authority or Safeguard Privilege Manager for Windows Client running on the network.</p> <p>Workaround: Ensure the following:</p> <ul style="list-style-type: none"> • 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. 	
<p>Some files may still exist on your computer even after the Console or Client are uninstalled.</p>	1837
<p>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 <i>Safeguard Privilege Manager for Windows User Guide</i> will fail to open the guide. Instead, the shortcut prompts the user for the location of the PAClient.msi file.</p> <p>Workaround: Uninstall and re-install the Client. Alternatively, reinstall the Console.</p>	1960

Table 4: Licensing known issues

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

Table 5: Server known issues

Known Issue	Issue ID
<p>Sometimes when configuring the reporting feature, the connection to the web service fails on the last step of the wizard.</p> <p>Workaround</p> <p>Try again by clicking Previous, then Next again.</p>	834
<p>If you select a remote Safeguard Privilege Manager for Windows Server on a computer with a firewall enabled, you may encounter a Database Connection</p>	1105

Known Issue	Issue ID
<p>error when using the Reporting or Discovery and Remediation functions.</p> <p>Workaround: Add the following firewall exceptions to the remote Safeguard Privilege Manager for Windows Server:</p> <ul style="list-style-type: none"> • 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 	
<p>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.</p> <p>Workaround: Add an exception to the firewall manually for %ProgramFiles(x86)%\One Identity\Safeguard Privilege Manager for Windows\Console\Data Collection Service\PADataCollectionWinSvc.exe.</p>	1657
<p>If the administrator is prompted to reboot the computer after installing a prerequisite while using the Privilege Manager Server Setup wizard:</p> <p>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.</p>	1980
<p>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 computer:</p> <p>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.</p>	1981

Table 6: Self-Service Elevation known issues

Known Issue	Issue ID
<p>The Self-Service Elevation Request Prompt does not appear for an MSI Windows installer file.</p> <p>Workaround: Launch the Self-Service Elevation Request Form via the Elevate! button. You must configure the corresponding Self-Service Elevation Request settings.</p>	1311
<p>Some processes do not trigger the Self-Service Elevation Request Prompt even though they trigger User Account Control (UAC).</p>	1674

Known Issue	Issue ID
<p>On Windows Server 2012 R2, if your client is running on a system with UAC turned off:</p> <p>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.</p>	1865

Table 7: Rules known issues

Known Issue	Issue ID
<p>A login failure occurs when connecting to the database and web service if you are using a SQL Server from an untrusted domain.</p> <p>Workaround: Use the database server on the same trusted domain network environment.</p>	698
<p>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.</p> <p>Workaround</p> <p>To navigate to the Select an Existing SQL Server step, click Next.</p>	832
<p>Sometimes changing settings on the Advanced Policy Settings tab of a Group Policy Settings page results in the Network path was not found error once you save the changes to the Group Policy Object (GPO).</p> <p>Workarounds:</p> <ul style="list-style-type: none"> 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. 	1671
<p>Currently, Safeguard Privilege Manager for Windows displays no feedback message when a user is denied run privileges due to a Blacklist setting.</p>	124

Table 8: Reporting known issues

Known Issue	Issue ID
<p>The Elevation Activity Report does not display correctly when exported to an .rtf file.</p> <p>Workaround: Export your Elevation Activity Reports to different file formats.</p>	728

Known Issue	Issue ID
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.	1881

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.
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 4.8, 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 [KB4268094](#).

Hardware, software, and operating system requirements

Table 9: Hardware, software and operating system requirements

Component	Hardware	Software	Operating system
Console and Server	<ul style="list-style-type: none"> • Processor: 2.0 GHz, dual core equivalent • Memory: 4 GB 	<ul style="list-style-type: none"> • .NET Framework 4.0 • Microsoft 	<ul style="list-style-type: none"> • Microsoft Windows 11 • Microsoft

Component	Hardware	Software	Operating system
	<ul style="list-style-type: none"> Disk space: 100 MB (Console) <p>NOTE: Additional space is required for the Privilege Manager database. For more information, see <i>Database Planning</i> in the <i>Administration Guide</i>.</p> <ul style="list-style-type: none"> Screen resolution: 1024x768 or higher 	<ul style="list-style-type: none"> Group Policy Management Console PDF reader to open the product documents 	<ul style="list-style-type: none"> Windows 10 Microsoft Windows Server 2022 Microsoft Windows Server 2019 Microsoft Windows Server 2016 Microsoft Windows Server 2012 R2 Microsoft Windows Server 2012 <p>NOTE: One Identity recommends using the product with 64-bit operating systems.</p>
Client	As recommended for your operating system.	N/A	<ul style="list-style-type: none"> Microsoft Windows 11 Microsoft Windows 10 Microsoft Windows Server 2022 Microsoft Windows

Component	Hardware	Software	Operating system
			<p>Server 2019</p> <ul style="list-style-type: none"> • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 <p>NOTE: One Identity recommends using the product with a 64-bit operating system.</p>

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 2022. Safeguard Privilege Manager for Windows can optionally install SQL Server 2022 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 transmit license data automatically to One Identity. Instead, you must update the product license manually.

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

Third-party contributions

This product contains some third-party components (listed below). Copies of their licenses may be found at referencing <https://www.oneidentity.com/legal/license-agreements.aspx>. Source code for components marked with an asterisk (*) is available at <http://opensource.quest.com>.

Table 10: List of Third-Party Contributions

Component	License or Acknowledgement
Boost 1.53	Copyright © Beman Dawes, David Abrahams, 1998-2005. Copyright © Rene Rivera 2004-2005. Distributed under the Boost Software License, Version 1.0 .
stdole 7.00	Copyright © The Microsoft Corporation Licensed under the Microsoft Visual Studio Tools, Add-ons and Extensions 2017 license.
ZLib 1.2.13	Copyright © 1995-2005 Jean-loup Gailly and Mark Adler Licensed under the zlib/libpng License .

Copyright 2024 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

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 website (<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.