One Identity Safeguard Privilege Manager for Windows 4.7

User Guide

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.

Safeguard Privilege Manager for Windows User Guide
Updated - 30 May 2024, 20:26

For the most recent documents and product information, see Online product documentation.

Contents

1

About this guide

Welcome to the *Privilege Manager for Windows User Guide*. This guide provides you with instructions on using the Safeguard Privilege Manager for Windows software that has been installed on your computer.

This document is structured as follows:

- What is Safeguard Privilege Manager for Windows?: An introduction to Safeguard Privilege Manager for Windows software.
- Displaying the Client icon: Instructions on how to display the Client icon.
- Using Self-Service Elevation: Instructions on how to use a Self-Service Elevation Request Form or Prompt to request permission to launch applications.
- Using Instant Elevation: Instructions on how to use Instant Elevation to automatically launch applications.
- Viewing rules: Instructions on how to view rules that are deployed to your computer or user account.
- Viewing the status of advanced features: Instructions on how to view the status of the advanced features that are deployed on your computer or user account.

System administrators can refer to these additional resources:

- *Safeguard Privilege Manager for Windows Quick Start Guide*: Learn how to set up Safeguard Privilege Manager for Windows.
- *Safeguard Privilege Manager for Windows Administrator Guide*: Learn how to use Safeguard Privilege Manager for Windows.

What is Safeguard Privilege Manager for Windows?

Safeguard Privilege Manager for Windows is a software that lets you update your own computer without calling your system administrator. Some applications require full administrative privileges to run or to be installed. In most cases, you do not have administrative privileges that allow you to update everything. However, you can use Safeguard Privilege Manager for Windows to request elevated privileges for specific applications, using features of the program called Self-Service and Instant Elevation. For more information, see Using Self-Service Elevation and Using Instant Elevation.

Displaying the Client icon

If you see the icon below in the notification area of the task bar at the bottom of your computer screen, your system administrator has installed the Safeguard Privilege Manager for Windows Client software on your computer:

To display the Client icon if you do not see it on your task bar even though Safeguard Privilege Manager for Windows has been installed

1. Click the small triangle (**Show hidden icons**) in the Windows system tray on the task bar to the left of your date/time display, and select the **Customize...** link.

   The **Notification Area Icons** dialog appears.
2. Scroll down the list of programs and locate the **Privilege Manager for Windows** icon in the list.
3. Select **Show icon and notifications** from the **Behaviors** drop-down list.

Using Self-Service Elevation

If your system administrator has set up Self-Service Elevation features for your computer, you will be able to use a **Self-Service Elevation Request** prompt or form to request permission to launch applications.

A **Self-Service Elevation Request** prompt or form may display when you try to launch an application without entering the administrator **User Name** and **Password** when prompted.

For more information about your permissions, contact your system administrator.

Using the Self-Service Elevation Request Prompt

NOTE: Using the prompt is the only way to ask for permission to download an ActiveX control through Safeguard Privilege Manager for Windows. An ActiveX control is a small program or add-on that you can download from your web browser.

To request permission to launch an application that requires administrative rights

1. Visit the site from which you want to download the application and click the installation button. For example, to download the Adobe Shockwave Player, visit http://get.adobe.com/shockwave/ and click **Download now**.
2. If prompted, enter the administrator **User name** and **Password**. If you do not know the administrator **User name** and **Password**, click **No**.
3. Request permission to launch the application in the **Self-Service Elevation Request** prompt that appears.

   NOTE: Consider the following:

   - If the prompt does not display for an ActiveX installation, ensure that the **Self-Service Elevation Request (ActiveX installations)** feature is

enabled in the Viewing the status of advanced features window.

- If the prompt does not display for an application that is not an ActiveX installation, ensure that the **Self-Service Elevation Request** feature is enabled in the Viewing the status of advanced features window.
- Contact your administrator if neither features are enabled.

4. Enter the reason you need the application along with an email address (if this feature is enabled) where the system administrator can respond to your request.
5. If it displays, check the In the future, don't show me this when I try to run applications that need approval check box if you do not want the **Self-Service Elevation Request** prompt to display automatically every time you do not have the administrator's credentials. To set the prompt to display again, follow the instructions for Displaying the Self-Service Elevation Request Prompt.
6. Click **Submit** to send your request to the system administrator.
7. The system administrator reviews your request and sends you the final decision.
8. If the system administrator confirms your request, a new privilege Elevation rule is created, allowing you to launch the application when you login into your computer. For more information, see Viewing rules.

Displaying the Self-Service Elevation Request Prompt

A **Self-Service Elevation Request** prompt may display when you try to launch an application without entering the administrator **User Name** and **Password** when prompted.

If the prompt does not display, you may be able to reset it to display so that you can request permission to launch the application.

To reset the Self-Service Elevation Request Prompt to display:

1. Right-click the **Client** icon in the notification area of the taskbar at the bottom of your computer screen.

2. Select **Display Self-Service Prompts** on the pop-up menu.

Using the Elevate! button and Self-Service Elevation Request Form

If you do not have administrative rights to launch an application, you can use the **Elevate!** button to open the **Self-Service Elevation Request Form** and request permission from your system administrator.

You can use the **Elevate!** button if the file name extension, the suffix after the dot '.' in the file name, for the application you need to install is `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs`.

To request permission to launch an application that requires administrative rights:

1. On your list of files in Windows Explorer, right-click the name of the application that you cannot start because you do not have sufficient privileges.
2. Select **Elevate!** on the pop-up menu that appears.
3. A **Self-Service Elevation Request Form** appears, allowing you to request permission to launch the application.

   If the form does not display, ensure that the **Self-Service Elevation Request (Elevate! context menu button)** feature is enabled in the Viewing the status of advanced features window.
4. Enter the reason you need the application along with an email address (if this feature is enabled) where the system administrator can respond to your request.
5. Click **Submit** to send your request to the system administrator.
6. The system administrator reviews your request and sends you the final decision.
7. If the system administrator confirms your request, a new privilege Elevation rule is created, allowing you to launch the application when you login into your computer. For more information, see Viewing rules.

5

Using Instant Elevation

You may be able to use the **Elevate!** button to automatically launch programs, if your system administrator set up the Instant Elevation feature for your computer. For more information about your permissions, contact your system administrator.

You can use the **Elevate!** button if the file name extension, the suffix after the dot '.' in the file name, for the application you need to install is `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs`.

To automatically launch a program using Instant Elevation

1. On your list of files in Windows Explorer, right-click the name of the application that you cannot start because you do not have sufficient privileges.
2. Select **Elevate!** on the pop-up menu that appears.

To launch a program if the Elevate! button does not appear when you try to launch a program

1. Ensure that the Instant Elevation feature is enabled in the Viewing the status of advanced features window.
2. Ensure that the file name extension for the application is `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs`.
3. Contact your system administrator to confirm that your account has sufficient permissions to elevate privileges on your computer.

Using Temporary Session Elevation

If your system administrator has provided you with a TSE (Temporary Session Elevation) passcode for your computer, you can temporarily use the **Elevate!** button to automatically launch programs that require elevated privileges.

1. From the System Tray, right-click the Privilege Manager Server and select **Temporary session elevation**.

   The **TSE Client Request** dialog appears.

2. If your Administrator already supplied you with a passcode, **Load passcode from file** can be selected. If you do not have a passcode click **If you don't have a passcode you can request one...**

   The request for Elevation passcode dialog appears.

3. Complete the request form and click **Submit**.

4. When the passcode is entered, a notification appears, showing the time remaining before the Elevation expires. A notification is displayed when the passcode expires. If you specified the passcode more times than allowed, you receive an alert.

   Once a passcode is active, you can use the right-click **Elevate!** button if the file name extension, the suffix after the dot in the file name, for your application you need to install `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs`.

To automatically launch a program while a passcode is active:

1. On your list of files in Windows Explorer, right-click the application that you cannot start because you do not have sufficient privileges.
2. Click **Elevate!** in the pop-up menu that appears.

If the Elevate! button does not appear when you try to launch a program:

1. Ensure that the **Temporary Session Elevation** feature is enabled.
2. Ensure that the file name extension for the application is `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs`.
3. Contact your system administrator to confirm that your account has permission to elevate privileges on your computer.

Viewing rules

When the Safeguard Privilege Manager for Windows Client software is installed on your computer, the settings that your system administrator selects are applied to your account and/or computer. These settings are called "rules".

You may be able to view the list of rules that apply to you, if your system administrator sets up this feature.

In addition, a notification from Safeguard Privilege Manager for Windows may pop up on your desktop to inform you when a new rule is added to, or removed from, your computer or user account.

To view the rules on your computer or user account:

1. Right-click the Client icon in the notification area of the taskbar at the bottom of your computer screen.

   

2. Select **View current rules** on the pop-up menu.

   The **Current Rules** window will display the titles of the rules that are deployed on your computer and user account.

   For more information, contact your system administrator.

Viewing the status of advanced features

You may be able to view the status of the advanced features that are deployed on your computer or user account, if your system administrator has set up this feature. Advanced features include client data collection, privileged application discovery, Self-Service Elevation requests (with and without ActiveX installations and/or the **Elevate!** button), and Instant Elevation.

To view the status of advanced features:

1. Right-click the **Client** icon in the notification area of the taskbar at the bottom of your computer screen.

   

2. Select **View status of advanced features** on the pop-up menu.

   The **View status of advanced features** window will display the status of the advanced features that are deployed on your computer and user account.

3. Click **More Details** to display a notepad with more information about the status of a feature.

Troubleshooting

This section provides workaround information for issues you may encounter during installation.

Server configuration gets stuck

On rare occasions, server configuration gets stuck when installing prerequisites (CRL Types and Shared Management Objects).

Figure 1: Stuck prerequisite installation during server configuration

Workaround

1. In Windows, open **Control Panel** > **Programs** > **Programs and Features**.
2. Check if the CRL Types and Shared Management Objects dependencies are installed.
    - If both dependencies are installed, restart the computer, and run server configuration again.
    - If any of these dependencies are not installed, check if their installers are available in the following location:

      `%ProgramData%\One Identity\Safeguard Privilege Manager for Windows\Downloads`

      If the installers are available in the specified location, install them manually from there, then restart the computer, and run server configuration again.
    - If any of the dependency installers are missing from the above location, install them manually as described in the *Offline installation* section of the *Safeguard Privilege Manager for Windows Administration Guide*.

Error code 2356

If you encounter error code 2356 during installation, or the server configuration gets stuck while installing the prerequisites (CLR Types and Shared Management Objects), the

Windows Installer service can end up in an incorrect state.

Workaround

1. Close any in-progress installation.
2. Open the Windows Task Manager.
3. Search for the **Windows Installer** service under the **Services** tab (`msiserver`).
4. Stop the service.
5. Run the installer/process again.

Potential startup delay on Windows 10

If Data Collection is enabled, Safeguard Privilege Manager for Windows may start up with a delay on Windows 10 workstations, stuck on a `please wait...` screen for an extended period of time. This can occur if the workstation cannot resolve the DNS name of the configured Data Collection server.

Workaround

To solve the issue, replace the configured Data Collection server name with the IP address of the Data Collection server.

SQL Server 2014 Express installation fails

Occasionally, Safeguard Privilege Manager for Windows may fail to install SQL Server 2014 Express.

Workaround

1. If possible, use a remote database instead of a local SQL Server installation.
2. If using a remote database is not feasible, try to install SQL Server 2014 manually.
3. If the issue still persists, contact our Support Team. Make sure you provide the SQL Server 2014 installation logs for One Identity Support from the following location:

   ```
   %ProgramFiles%\Microsoft SQL Server\120\SetupBootstrap\Log
   ```

Match rule failure for certain processes

If a process is running from a Universal Naming Convention (UNC) or mapped drive, rules that specify the file version, file hash, product code, or publisher might fail to match the process. This can happen if the security permissions set on the network resource prevent the computer account on which the Safeguard Privilege Manager for Windows Client is running to access it.

Workaround

In the **Edit Rule Wizard**, set **User's context will be used to resolve system and resource access** for the rule. This setting allows the Safeguard Privilege Manager for Windows Client to access the network resource under the security context of the user running the process.

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