Safeguard Privilege Manager for Windows 4.8

Administration 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 Administration Guide
Updated - 25 November 2024, 10:16

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

Contents

1

About this guide

The Safeguard Privilege Manager for Windows Administration Guide is intended for system administrators and describes how to use Safeguard Privilege Manager for Windows. The document contains detailed instructions on how to:

- Prepare your environment for least privileged use.
- Maintain a least privileged environment.
- Run reports.
- Interface with Microsoft tools.

For more information on how to configure and deploy the product, and how to use it by end users, see the following resources.

For system administrators

- **Safeguard Privilege Manager for Windows Quick Start Guide**: This document lists the system requirements of the product, and also provides instructions on how to set up the Safeguard Privilege Manager for Windows Console, Server, and Client components. The document also provides an overview of the key product features and the wizards that will help you use them.
- **Safeguard Privilege Manager for Windows Console**: To find additional information within the Console, navigate to the **Additional Resources** > **Getting Started** tab.

For end users with Safeguard Privilege Manager for Windows Client installed on their computers

- **Safeguard Privilege Manager for Windows User Guide**: Learn the basics of using the Safeguard Privilege Manager for Windows Client, including how to use the Self-Service Elevation and Instant Elevation features, and how to view rules.

What is Safeguard Privilege Manager for Windows?

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.

Editions

Components

Editions

Safeguard Privilege Manager for Windows is available in the following editions:

- **Privilege Manager Community Edition**: This edition is free and does not require a license. You can collaborate, brainstorm new Elevation rules, share rules with other users, and provide bug reports and enhancement requests to One Identity.
- **Privilege Manager Professional Edition**: This edition requires a paid license and includes additional security, discovery, and reporting capabilities, as well as technical support from One Identity.
- **Safeguard Privilege Manager for Windows Professional Evaluation**: This edition is the free 30-day trial of Safeguard Privilege Manager for Windows Professional Edition. If you do not buy a license after 30 days, the software will revert to the lesser-featured Community Edition. As such, you cannot keep the features of the Professional Edition, but you can continue using the Community Edition.

  When reverting back to the Community edition, you will need to re-save all computer-based Group Policy object (GPO) rules as user-based. Computer-based rules will no longer work on the client-side once the trial expires.

Components

There are three software components included with Safeguard Privilege Manager for Windows:

- the Console
- the Server
- the Client

Console

The Safeguard Privilege Manager for Windows Console, installed via `PAConsole_Pro.msi`, is a management application. It is installed on a domain computer (server or workstation) and is used to create and manage rules within the Group Policy. Any user who has permission to edit a GPO can use the Console to set privileges.

Server

The Safeguard Privilege Manager for Windows Server, installed through the Console, is a service which has several functions. It can deploy the Client, collect and report on data, and discover and process applications that require elevated privileges.

Client

The Safeguard Privilege Manager for Windows Client, installed through `PAClient.msi`, is a service that runs on each client computer. It applies the rules created in the Console by monitoring processes as they are launched on the Client and elevates or lowers the privileges for processes that are configured to be monitored. This is done by injecting an administrative token into the process or revoking it.

Microsoft Active Directory and Group Policy are used to distribute Safeguard Privilege Manager for Windows rules to client computers.

Privilege Manager can modify privileges only for a standard user account, not a guest account. Elevated privileges can be revoked even if the user is a local admin.

Installing Safeguard Privilege Manager for Windows

Detailed information about this topic

Deploying Safeguard Privilege Manager for Windows in your organization has three main steps:

- Installing the Safeguard Privilege Manager for Windows Console, as described in Installing the Console.
- Configuring the Safeguard Privilege Manager for Windows Server, as described in Configuring the Server.
- Installing the Safeguard Privilege Manager for Windows Client, as described in Installing the Client.

For more information on these product components, see Components.

NOTE: Before you begin installation, make sure that you meet the minimum hardware, software, network and permission requirements of the product. For more information, see *System Requirements* in the *Safeguard Privilege Manager for Windows Release Notes*.

After installing these components, you can start using the product based on your Windows rights within the Group Policy Management Console. If you do not have sufficient rights to an object, you will receive an access denied prompt.

Installing the Console

Detailed information about this topic

The Console must be installed on a computer that is joined to the domain and run under a user account that has the rights to change at least one GPO. The Console displays GPOs based on the security context of the user that is logged on.

Using the Console Windows Installer file

The Console must be installed on a computer that is joined to the domain and run under a user account that has the rights to change at least one GPO. The Console displays GPOs based on the security context of the user that is logged on.

To complete the Console installation, follow the Windows Installer through a series of dialogs

1. Run the Privilege Manager setup file, `PAConsole_Pro.msi`.

   The installer checks to see if your system is missing any of the required components.
2. Review the system requirements for Privilege Manager. A window appears, allowing you to install any of the missing components.
3. Complete one of the following steps:
   - Click **Yes** to download and install a single missing component. A new notification window will display to install others, if necessary.
   - Click **Yes** to all to download and install all the missing components with a single click.
   - Click **No** to manually download the missing components. A dialog will follow, displaying the download links for the missing components. Install the components and resume the installation.
4. Click the link and download the component.
5. Close the Console setup notification window with the download link to .Net 4.0 Framework.
6. Install the component.

7. The initial dialog is the installation Welcome. Click **Next**.
8. The **License Agreement** dialog displays. Select **I accept the terms in the License Agreement** and click **Next**. For more information on applying a license, see the *Safeguard Privilege Manager for Windows Administrator Guide*.
9. In the **Destination Directory** dialog, select a destination folder. The installation path depends on the system architecture and defaults to `%PROGRAMFILES%\Quest` or `%ProgramFiles(x86)%\Quest`. Click **Browse** to select a different installation path, however, accepting the default values is recommended. Click **Next**.
10. Click **Install** on the final installation dialog. Once the installation is complete, click **Finish**.

Opening the Console

After installation, you can start the Safeguard Privilege Manager for Windows Console from the Windows start menu or the default shortcut.

To start the Safeguard Privilege Manager for Windows Console on the host, do one of the following:

- Go to **Start** > **All Programs** > **One Identity** > **Safeguard Privilege Manager for Windows**.
- Select the Safeguard Privilege Manager for Windows shortcut icon on the **Start menu**.

Applying a license

You can apply a license upon initial start-up or later. Otherwise, if your trial has expired, you'll only be able to access the Community edition.

NOTE: Supported license files have the `.dlv` extension.

To apply a license when you start the Console for the first time

1. A window appears, asking you to apply a license.
    - If you are going to apply a Safeguard Privilege Manager for Windows Professional Edition or Professional Evaluation Edition license, click **Yes**. Then, browse to the license file and click **Open**.
    - To access the Privilege Manager Community Edition that does not require a license, click **No**.

You can also apply a license later.

To apply a license in the Console after initial start-up

1. Click **Help** > **About** in the menu.
2. Navigate to the **License** tab.
3. Click **Apply License File**.
4. Browse the license file, and click **Open**.
5. If you are upgrading, you may need to follow the additional steps detailed in the Upgrading section.

Viewing GPOs

To view the GPOs that you have access to

- Switch from the **Setup Tasks** > **Getting Started** window to the **Group Policy Settings** > **All GPOs** window.

NOTE: If you do not see the domain tree when the **Group Policy Settings** section is selected, check that the default domain is selected in the **Setup Tasks** > **Select Target Domains** window.

Selecting target domains

The Safeguard Privilege Manager for Windows is initially configured to allow you to manage the privilege Elevation settings for the domain to which the local computer belongs. In addition, the Console also allows you to manage other domains in your forest.

For Safeguard Privilege Manager for Windows to work across multiple domains within a single forest, the appropriate domain permissions must be configured and an Enterprise Admin Active Directory account must be used with the Safeguard Privilege Manager for Windows Console. The Windows user account must include the following:

- SQL Server System Administrators role
- **`db_owner`** access to the master database
- **`db_owner`** access to the **PAReporting database** (required for upgrades)

  For complete information about the database space requirements, see Database Planning.

  NOTE: The recommendation for multiple domains in a single forest is for each domain within the forest to host a completely separate installation of Safeguard Privilege Manager for Windows.

To customize the number of your forest's domains available in the Group Policy Settings pane

1. In the **Getting Started** section of the navigation pane, select **Setup Tasks**, then click **Select Target Domains** in the right pane.
2. In the window that appears, specify the domain names, as applicable.
3. (Optional) To open the **Select Domain Controller** dialog, click **Select DC**. Specify the exact domain controller that the Console will communicate with.

   The list of the domains and GPOs change accordingly.

   NOTE: You can create the GPO rules only on a domain where you have write permissions for the GPOs.

Installing a second Console

To manage Safeguard Privilege Manager for Windows Group Policies (GPOs) from a Microsoft Windows 10 machine that does not host the Safeguard Privilege Manager for Windows Console or Server, install a second Safeguard Privilege Manager for Windows Console instance.

NOTE: There is no GPO locking mechanism so ensure that the same GPO is not edited at the same time from different consoles. Changes can be lost when multiple saves occur.

Requirements

To install a second Console, you must meet the following requirements:

- Use same license as for the first Console.
- Use same version of PM Console as the first Console.
- Permissions: User running the remote Console must be a member of the super user group specified during the setup of the first Safeguard Privilege Manager for Windows Console or Server. User must also have permissions to edit GPOs.

To install a second Console

1. Install the second Console on another machine.
2. Apply the same license that is used on the first Console.
3. Open the **Console** and go to **Setup Tasks** > **Configure a server**.
4. Click **Browse** to choose an existing Safeguard Privilege Manager for Windows Server. In the box at the bottom, type the name of the Server.
5. To close the dialog, click **OK**, then click **Test** to ensure a successful connection.
6. Click **OK** to finish.
7. (Optional) If using Temporary Session Elevation passcodes:

a. On the original Safeguard Privilege Manager for Windows Server, locate and copy this file: `C:\Program Files (x86)\One Identity\Safeguard Privilege Manager for Windows\Console\pmtse.ske`.

b. On the second Console, locate the same file in same location.

c. Rename it to `pmtse.ske.old`.

d. Copy the `pmtse.ske` file from the original Safeguard Privilege Manager for Windows Server to the second Console.

e. Close and re-open the second Console.

Configuring the Server

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

After installing the Console, a Server must be configured. Configuring the Server sets up the back-end services needed to automatically deploy the Client, as well as enable reporting, discovery and remediation.

Using the Server Configuration Wizard

NOTE: This feature is available only in Professional and Professional Evaluation editions.

After installing the Console, you must configure a Server. Configuring the Server sets up the backend services needed to automatically deploy the Client, as well as enabling reporting, discovery and remediation.

To use the Privilege Manager for Windows Server Configuration Wizard to set up the Server

1. Start the Privilege Manager for Windows Server Configuration Wizard.
    a. Open the Console.
    b. Under the **Getting Started** section of the left navigation menu, click **Setup Tasks**.
    c. Select the **Configure a server** icon in the **Basic Setup** right pane.
2. The **Privilege Manager for Windows Server Configuration** screen appears.
    a. Click **Browse** to locate a Server through Active Directory.
    b. Click **Test** to verify the connection of the selected Server to the ScriptLogic PA Reporting Service. If the test fails, check to see if there are network or firewall problems.
    c. Click the **Clear the server name** link if you want to configure another Server. The displayed service remains installed.

3. Click **Setup/configure the Privilege Manager Server on this computer** to install a new Server or configure one on the local computer.
4. In the **Privilege Manager for Windows Server Setup Wizard** that appears, set the port for the web service.
    a. Click **Reset** to set the **Port Number** to its default. The ScriptLogic PA Reporting data collection web service listens for incoming data from the clients on port **`8003`**, by default. The firewall must be configured to allow communication over any port you select.
    b. Select the **Add an application exception to the firewall for this service** option to automatically add UDP and TCP rules (named ScriptLogic PA Reporting Svc) to the Windows Firewall exceptions list to allow inbound traffic for the service on the local computer.
5. Under the optional **Server Email Notification Configuration** section, select the Server to use for email notifications of Self-Service requests and scheduled reports.

    Configure the following fields:

    a. **Host Name**: Enter the SMTP Server name of the email account from which you are going to send your emails.
    b. **SMTP Port**: Enter the port number.
    c. **SMTP User Name and Password**: If necessary, enter the authentication information and check the SSL check box.
    d. **From Email**: Enter the corresponding email.

    NOTE: You must enter the SMTP Password each time you configure the Server or an error is received.
6. Click **Send Test Email** to send an email to the account specified in the **From Email** field.
    a. If Privilege Manager succeeds in sending the email, the corresponding message appears.
    b. Log into an email program with the corresponding account and locate the sent email folder, with **`Privilege Manager Test Email`** in the subject.
7. Click **Next**.
8. Select an SQL Server instance to use for the PA Reporting database.
    a. Select **Download** and install a local instance of SQL Server 2022 Express to be used by the server wizard. Then, click **Next**.

        NOTE: By default, the SQL Server installed via the Console uses Windows authentication.
9. To connect to an existing local or remote SQL instance, select **Use an existing SQL Server instance** (requires at least Microsoft SQL Server 2014), and click **Next**.

To use the Privilege Manager for Windows Server Configuration Wizard to set up the Server when using a remote SQL database

1. Enable TCP/IP protocol for the selected SQL Server instance.
2. Enable the Console host to address the remote SQL Server.
3. Allow the firewall to communicate between the SQL database and the Console host on the port that the remote SQL Server is configured to listen on.

   NOTE: If a domain controller hosts the Safeguard Privilege Manager for Windows Console, Microsoft does not recommend running a database on a domain controller computer. In this case, either connect to a remote SQL database instance or use another computer to install the Console and download SQL Server 2022 Express via the Privilege Manager for Windows Server Configuration Wizard.
4. Set up a Super User group, credentials for the Data Collection Web Service Account, and the database service account.
   a. Verify the default user group and user accounts will be granted administrative privileges in the Privilege Manager for Windows Reporting database. This group is configured as the Super User group. If a different group is required, click **Browse** to locate it using Active Directory.
   b. In the **Data Collection Web Service Account** section, enter the password of the account that is used to run the data collection service. This account requires local administrator rights.
   c. Use the **SQL Server Express Service Account** section to enter a new account for the SQL Server service, if you selected the option to download and install a local instance of SQL Server 2022 Express.
   d. Use the **SQL Server Administrator Password** section to supply a password for the SQL Server System Administrator (`sa`) account.

   NOTE: If you plan to use the configured server domain-wide, ensure the provided Database Super User Group includes every user account that may address the PAReporting database. Otherwise, a user that has no rights to the database will encounter an error. An example use-case is if you use the configured server from other consoles to run either by domain or organizational unit level admins.
5. To install a list of SQL Server Management Objects (SMOs) if the local computer is missing them, click **Next**. These prerequisites are required to connect to SQL Server instances on the network.
6. Select the existing SQL Server instance running remotely or locally, if you selected the option to use an existing SQL Server instance.
   a. In the **SQL Server Instance Name** field, specify the name in the following format:

      `SQLSERVER\INSTANCENAME.`
   b. To view the server instances available on your network, use the ▫ (**Browse**) button.

c. When using Windows authentication, ensure that the Windows account currently logged into the Console meets the following requirements:
    - It has the system administrator server role on the specified SQL Server instance.
    - It has `db_owner` role for the master database.
    - It has `db_owner` role for the PAReporting database, when you are upgrading a database previously created with the Privilege Manager for Windows Server Configuration Wizard.

NOTE: If you target a remote SQL database, it must use Windows authentication for runtime access to data. However, you can use SQL authentication to set up the database.

7. To install the prerequisites and launch the services, click **Next**.

   NOTE: During installation, a command prompt window may appear for a short period of time. This is normal.

8. To exit the Privilege Manager Server Setup Wizard, click **OK**, then **Finish**.
9. To ensure proper functioning of the Server, allow the following programs through the Windows firewall:
    a. On the client computer: `CSEHost.exe`.
    b. On the Server host: `PrivilegeAuthority.exe`, which is configured by default during Server configuration, provided that the firewall is turned on.

Modifying the Server

You must configure the settings for the Server on the Console where it was installed. However, any administrator with the rights to a specific GPO can update its data collection settings. Also, the administrator running the Console can view reports of data collected by any Server by selecting **Browse** and the preferred Server from the **Privilege Manager Server Configuration** screen (under **Setup Tasks** > **Configure a Server**).

To change the reporting database settings

1. Use the **Privilege Manager Server Configuration** screen to remove the Server.
2. Restart the wizard to reinstall the service and set the SQL database settings.

   NOTE: You may configure the following settings:
    - Connect to another instance.
    - Modify the authentication parameters.
    - Set up a new data collection service.

Removing the Server

If you do not want to use a Server, you can clear its settings and/or remove it from a host computer.

Removing the Server from the host computer

To remove the Server's settings or remove it from the host computer

1. Open the **Privilege Manager Server Configuration** screen (under **Setup Tasks** > **Configure a Server**).
2. To clear the settings which the Console uses to connect to reporting information, select **Clear the server name**. The locally running Server will not be stopped or disabled. This will not uninstall the Server.
3. To uninstall the Server from the local computer, click **Remove the Privilege Manager Server from this computer**. When you remove the Server:
    - You stop the web data collection service.
    - The shared folder with the Client file is no longer shared.
    - The database does not receive data sent by the corresponding Clients until a new Server is installed, provided that it is installed within the network timeout parameters.

Removing a Server running remotely

To remove a Server running remotely

1. Connect to the computer that hosts the Server.
2. Remove the Server using the **Privilege Manager Server Configuration** screen.

NOTE: If a domain administrator or the administrator of a nested Organizational Unit (OU) uninstalls the Server, they may render the reporting function unavailable on other Console computers or computers downstream from the parent OU. Also, if you have reinstalled the Server, report generation starts from the last installation.

Offline installation of the Server and Data Collection service

Safeguard Privilege Manager for Windows does not directly support offline installation. However, you can set up the Server and Data Collection service of the Console if you install some dependencies manually beforehand.

To set up the Server and Data Collection service offline

1. Install the following components:
    - Microsoft System CLR Types for Microsoft SQL Server 2014
        - 32-bit
        - 64-bit
    - Microsoft SQL Server 2014 Shared Management Objects
        - 32-bit
        - 64-bit
    - Microsoft SQL Server 2022 Express
        - 64-bit
2. Set up the SQL Server manually. For example, you can run the following command to initiate the SQL Server installer with some pre-configuration in place:

    ```
    SQLEXPR_X64_ENU.exe /IACCEPTSQLSERVERLICENSETERMS /ACTION=Install
    /FEATURES=SQL /INSTANCENAME=PAReporting /SECURITYMODE=SQL /SAPWD=<sql-system-
    admin-password> /SQLSVCACCOUNT=<sql-service-account>
    /SQLSYSADMINACCOUNTS="BUILTIN\ADMINISTRATORS" /AGTSVCACCOUNT=<sql-service-
    account> /TCPENABLED=1 /SQLSVCPASSWORD=<sql-service-password>
    /AGTSVCPASSWORD=<sql-service-password>
    ```

3. Once you are done, you can configure the server in the Console using the **Use an existing SQL Server instance** option during server setup.

Installing the Client

Detailed information about this topic

Once the Console is installed, you can deploy Clients to the computers on your domain in one of the following ways:

- **Client Deployment Settings Wizard**: Deploy or uninstall clients on your computers in one pass.

  NOTE: Available only in Privilege Manager Professional Edition and Professional Evaluation Edition.

- **Client Windows Installer file**: Use `PAClient.msi` to install the Client locally on a computer (administrative privileges are required).
- **Microsoft Group Policy Management Console**: Use login scripts or other software deployment techniques for mass-deployment.

Using the Client Deployment Settings Wizard

To use the Client Deployment Settings Wizard to install the Privilege Manager Client

1. Start the Client Deployment Settings Wizard.
   - To add the settings to any available GPO:
2. Open the Console.
3. Under the **Getting Started** section of the left navigation menu, click **Setup Tasks**.
4. Select the **Deploy Client Wizard** icon in the **Advanced Configuration** pane on the right. It always shows the default settings.
   - To change the settings for a specific GPO, double-click **Client Deployment Settings** on the **Advanced Policy Settings** tab of the GPO. The changes made within the wizard are saved here.
5. Choose one of the following options:

- **Not Configured**: Enable child GPOs to inherit Client deployment settings from their parent.
- **Install Client**: Install/upgrade Client software.
- **Remove Client**: Remove Client software (for versions 3.0 and higher).
- **Unregister**: Stop Client software installation GPO settings from applying.

6. Click **Next**.
7. Define the Server.
8. Click **Browse** to locate a Server through Active Directory.
9. To verify the connection of the selected Server to the ScriptLogic PA Reporting Service, click **Test**. If the test fails, check to see if there are network or firewall problems.
10. If you want to configure another Server, click the **Clear the server name** link. The displayed service remains installed.
11. Click **Next** to use Validation Logic to target the settings to specific client computers or user accounts within the GPO, or click **Finish** to save your settings and quit.

    If an error message indicates that the target GPO is not selected:

    a. Click **OK** to close the message window.

    b. Open the **GPO** tab and select the desired GPO.

    c. Click **Save** on the GPO toolbar to save the new settings.
12. To view the Client Deployment Settings, double-click **Client Deployment Settings** on the **Advanced Policy Settings** tab of the GPO.
13. Check that the Client is successfully deployed onto the computer. Ensure that:
    - The `CSEHost.exe` process is running.
    - The Client record is shown in the Add/Remove Programs tool.
    - The Privilege Manager icon and the right-click menu are available in the system tray on the client computer.
    - New GPO rules created by Privilege Manager are applied to Client computers following a group policy update.

Using the Client Windows Installer file

To use the Client Windows Installer file to install the Client locally on a computer

1. To locate the Client MSI setup file, open the Console.
2. Click **Additional Resources** > **Open Client Installation Folder**. The Client file appears in a browser window.
3. Check that the Client is successfully deployed onto the computer. Ensure that:

- The `CSEHost.exe` process is running.
- The Client record is shown in the **Add/Remove Programs** tool.
- The **Privilege Manager** icon and the right-click menu are available in the system tray on the client computer.

  New GPO rules created by Safeguard Privilege Manager for Windows are applied to Client computers following a group policy update.

Using the Group Policy Management Console

To install Clients on your domain via the Microsoft Group Policy Management Console (GPMC)

1. Copy the `PAClient.msi` file to a network share that can be read by all users. Or, just share the file folder (a share with the `PAClient.msi` file is configured automatically upon Server configuration).
   a. To locate the Client MSI setup file, open the Console.
   b. Click **Additional Resources** > **Open Client Installation Folder**. The Client file appears in the browser window.
2. Right-click **Group Policy Objects** and select **New** from the pop-up menu to open the Group Policy Management Console on the Server to create a new Group Policy Object (GPO).
3. Enter a name for the new GPO and click **OK**.
4. Right-click the new GPO and select **Edit** to open it.
5. In the Group Policy Management Editor, select **Computer Configuration** > **Policies** > **Software Settings** > **Software installation**. In the right pane, right-click the new GPO, and select **New** > **Package**.
   a. If the client distribution GPO is computer-based (defined under **Computer Configuration**), enable the **Always wait for the network at computer startup and logon** policy, located in **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Logon**). Otherwise, the Client installs after the second reboot of the client computer.
   b. If the client distribution GPO is user-based (defined under **User Configuration**), then the Client installs after the first logon.
6. In the dialog that appears, browse to the `PAClient.msi` file on the network share where it was copied to.
   a. Use the **File name** field to specify the Client location in the Universal Naming Convention (UNC) format:

      `\\computername\sharename\filename.msi`

   b. Click **Open**.
7. Select **Assigned** in the **Deploy Software** dialog.

8. Assign the new GPO to a domain or OU.
    a. To assign it to a domain, right-click the domain in **GPMC** and select **Link an Existing GPO**.
    b. Select the GPO in the dialog and click **OK**.
9. Check that the Client is successfully deployed onto the computer.

    Ensure that:

    - The `CSEHost.exe` process is running.
    - The Client record is shown in the **Add/Remove Programs** tool.
    - The **Privilege Manager** icon and the right-click menu are available in the system tray on the client computer.

      New GPO rules created by Privilege Manager are applied to Client computers following a group policy update.

      NOTE: During updates, all Client settings and rule group policies are automatically updated. You have two options for initiating updates:

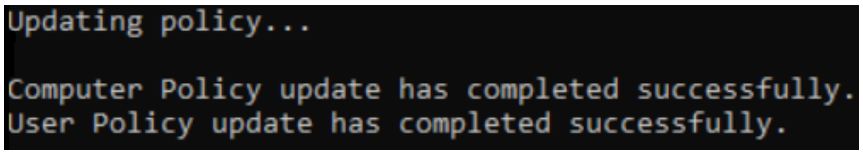
      - Using a console prompt or PowerShell terminal.

        To initiate update using the gpupdate command

        1. Open a console prompt or a PowerShell terminal supported by your operating system.
        2. Run `gpupdate /force`.

           NOTE: The system will find `gpupdate.exe` through `PATH`.

           After a successful update, you will see this message:

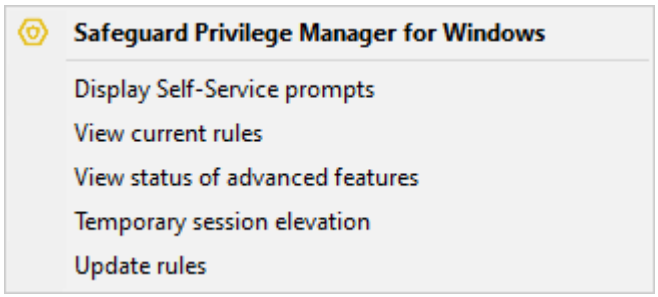
           

      - Using the built-in **Update rules** feature of the **Safeguard Privilege Manager for Windows** menu on the system tray.

        To initiate update using the Update rules built-in feature

        1. Navigate to the Client system tray on your desktop.
        2. Right-click the system tray.

           The **Safeguard Privilege Manager for Windows** menu opens:



3. Click **Update rules**.

   A console window opens to automatically update the client machine Group Policies by synchronizing saved GPOs from Active Directory.

NOTE: The automatic Server upgrade may be unavailable if the ScriptLogic PA Reporting Service is not running.

10. If the Console detects that the Server component is installed on a remote computer, it instruct you to launch it on the remote computer.
11. If a message prompts you to upgrade your Server and database (installed locally with the reporting functionality of some prior Privilege Manager versions):
    a. Click **OK** and follow the Privilege Manager Server Configuration Wizard to complete the following steps:
       i. Install the missing SQL Server components from the Internet.
       ii. Back up your database.
       iii. Configure a shared folder for client mass deployment.
    b. Click **Finish** to save the results and exit the wizard.
    c. If a message displays indicating that the Privilege Manager Host Service that needs to be updated is currently in use, click **OK** to ignore the message.
    d. To upgrade later, open the Privilege Manager Server Configuration Wizard and confirm that you are running the upgrade process before you configure the Server.
    e. Until you have upgraded the Server and database, you will have problems installing the Server locally.

       For more information, see Configuring the Server.
12. Re-configure your Client data collection settings, if necessary.
    a. Select a GPO from the **Group Policy Settings** section.
    b. Switch to the **Advanced Policy Settings** tab.
    c. Double-click **Client Data Collection Settings** to configure settings using the Client Data Collection Settings Wizard. For more information, see Configuring Client data collection.
13. After you upgrade, **By Digital Certificate** rules will be saved as **By Path to the Executable** rules.

14. To upgrade Clients, install the newer version over the older one. For more information, see Installing the Client.

For more information, see Removing the Server.

Upgrading

Privilege Manager components are only compatible with other components of the same version. Upgrading ensures that all of the GPO rules and reporting configurations you created with earlier versions will still be available.

To upgrade prior versions

1. Run the Privilege Manager setup file (`PAConsole_Pro.msi`) and follow the Privilege Manager Console Windows Installer.
    a. If the `Some files that need to be updated are currently in use` message appears, click **OK**.
    b. Once you complete the upgrade, exit the installer.
2. Open the Console and if necessary, apply a license. For more information, see Opening the Console and Applying a license.
3. If an error message notifies you that the ScriptLogic PA Reporting Service has the wrong manual startup type, complete one of the following steps:
    - Go to the Windows Services Console and set the **ScriptLogic PA Reporting Service** to start automatically.
    - To reset the service to start automatically, click **OK** in the message window. If the restart fails, click **NO**, then restart the Safeguard Privilege Manager for Windows Console.

    NOTE: The automatic Server upgrade may be unavailable if the ScriptLogic PA Reporting Service is not running.
4. If the Console detects that the Server component is installed on a remote computer, it instruct you to launch it on the remote computer.
5. If a message prompts you to upgrade your Server and database (installed locally with the reporting functionality of some prior Privilege Manager versions):
    a. Click **OK** and follow the Privilege Manager Server Configuration Wizard to complete the following steps:
        i. Install missing SQL Server components from the Internet.
        ii. Back up your database.
        iii. Configure a shared folder for client mass deployment.

b. Click **Finish** to save the results and exit the wizard.

c. If a message displays indicating that the Privilege Manager Host Service that needs to be updated is currently in use, click **OK** to ignore the message.

d. To upgrade later, open the Privilege Manager Server Configuration Wizard and confirm that you are running the upgrade process before you configure the Server.

e. Until you have upgraded the Server and database, you will have problems installing the Server locally.

f. For more information, see Configuring the Server.

6. Re-configure your Client data collection settings, if necessary.

   a. Select a GPO from the **Group Policy Settings** section.

   b. Switch to the **Advanced Policy Settings** tab.

   c. Double-click **Client Data Collection Settings** to configure settings using the **Client Data Collection Settings Wizard**. For more information, see Configuring Client data collection.

7. After you upgrade, **By Digital Certificate** rules will be saved as **By Path to the Executable** rules.

8. To upgrade Clients, install the newer version over the older one. For more information, see Installing the Client.

To upgrade Safeguard Privilege Manager for Windows to version 4.8

1. Enter your password for the database.
2. Open Safeguard Privilege Manager for Windows once the installation is complete.
3. Follow the on-screen help to finish upgrading the product.
4. If you are not prompted with the on-screen help:

   a. Open Safeguard Privilege Manager for Windows.

   b. Navigate to **Configure a Server** > **Setup**.

   c. Click **Next**.

   d. Choose **Existing SQL Server Instance**.

   e. Enter your password, click **OK**.

   f. Select the **/PAREPORTING Instance Name** option.

   g. Continue the installation according to the previous procedure on upgrading prior versions.

Uninstalling

You must have administrative privileges to uninstall the Console and Client from a local computer.

To uninstall Privilege Manager components

1. Use the **Windows Control Panel** tool. The uninstaller completely removes all of the data.
2. Once Privilege Manager for Windows is removed, its rules no longer apply.

For more information, see Removing the Server.

Repair

Safeguard Privilege Manager for Windows does not support repairing through the `.msi` installer.

To repair Safeguard Privilege Manager for Windows, reinstall the product.

For more information, see Installing Safeguard Privilege Manager for Windows.

NOTE: To ensure you can successfully reinstall the product later, uninstall it by following the steps of Uninstalling.

Configuring Self-Service Elevation

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

To enable users to request permissions to use privileged applications, use the Self-Service Elevation Request Settings Wizard. Whenever a user attempts to run an application which requires administrative permissions for which they do not have rights, they are asked if they would like to send a request to their administrator for permission to run it.

You can select how users access the request form and set up Self-Service notifications to email you, the help desk, and your manager of each request. Then, you can process the request within the **Self-Service Elevation Requests** section of the Console and email your decision to the user, using the **Console Email Configuration** screen.

NOTE: In some cases, Self-Service Elevation and Blacklist rules could be configured for the same target application. In this case, Blacklisting takes precedence over Instant Elevation and prevents the application from starting. For more information about creating Blacklisting rules, see Using the Create Rule Wizard.

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 2022 Express installation fails

Occasionally, Safeguard Privilege Manager for Windows may fail to install SQL Server 2022 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 2022 manually.
3. If the issue still persists, contact our Support Team. Make sure you provide the SQL Server 2022 installation logs for One Identity Support from the following location:

   ```
   %ProgramFiles%\Microsoft SQL Server\160\Setup Bootstrap\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.

Configuring Client data collection

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Run the Client Data Collection Settings Wizard so that you can compile reports, support discovery, and launch on-demand features.

Using the Client Data Collection Settings Wizard

Client data collection settings only apply on computers running a Client.

Before configuring Client data collection settings, you must configure a Server on your domain.

For more information, see Configuring the Server.

To use the Client Data Collection Settings Wizard to set up, modify, or discard settings,

1. Open the wizard by completing one of the following steps:
    - Open the Client Data Collection Settings Wizard from the Setup Tasks section. It will always show the default settings.
    - On the **Advanced Policy Settings** tab of the target GPO, double-click **Client Data Collection Settings**. The changes made within the wizard are saved here.
2. Enable the **Client Data Collection Settings** on the **State** tab.
    - Choose **Enabled**, to ensure the settings apply to the selected GPO.
    - Choose **Not Configured**, to enable child GPOs to inherit settings from their parent.
3. Define the **Server** on the **Settings** tab. This Server receives data from the Clients of the target GPO.
4. Click **Browse** to locate a Server through Active Directory.
5. Use the **Test** button to verify the selected Server's connection to the ScriptLogic PA Reporting Service. If the test fails, check to see if there are network or firewall problems.
6. Click the **Clear the server name** link if you want to configure another Server. The displayed service remains installed.

    NOTE: To prevent data transfer issues between the Server and linked Clients, check that the port you have selected is open for incoming connections on the Server. Port `8003` is the default port for Server installation.

7. Use the **Advanced Settings** on the **Settings** tab to set these data transfer parameters:
    - **Maximum Sleep Time** (in seconds) sets the stagger time period within which every Client sends its data to the data collection service. This value is set to `60` seconds by default.
    - **Send Retries** defines the number of retries that are made if an attempt to connect to the web service fails. This number is set to `1` by default.
    - **Network Timeout** (in seconds) sets how many seconds a Client should wait to stop sending data if it does not reach the target. This value is set to `600` seconds by default.
    - **Maximum Records Per Transaction** indicates how many portions of cached data the Client sends. This value is set to **`0`** by default, which indicates an unlimited number. To reduce the load on the Server side, you can increase the value to `1` or `2`. This may be useful on large networks where each client computer generates many records and a Client may not be able to connect to the data collection service because it is too busy processing data collection transactions.
8. Click **Next** to use Validation Logic to target the settings to specific client computers or user accounts within the GPO, or click **Finish** to save your settings and quit.

If an error message indicates that the target GPO is not selected:

1. Click **OK** to close the message window.
2. Open the **GPO** tab and select the desired GPO.
3. Click **Save** on the **GPO** toolbar to save the new settings.

   Adjust the parameters that Clients use to send their data to the ScriptLogic PA Reporting data collection web service to your specific needs. The web service supports collecting data from a significant number of Clients running concurrently.

Configuring Instant Elevation

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

To grant on-demand administrative privileges to a group of trusted users and audit their actions, use the Instant Elevation Wizard.

NOTE: In some cases, Instant Elevation and Blacklisting rules could be configured for the same target application. In this case, Blacklisting takes precedence over Instant Elevation and prevents the application from starting. For more information about creating Blacklisting rules, see Using the Create Rule Wizard.

Using the Instant Elevation Wizard

Prerequisites

Before you configure Instant Elevation settings, ensure the following components are set up:

1. The Client is running on the computers you want to apply the settings to;
2. The Server is configured and running with the port that you have selected allowed for incoming data (the default port is **8003**); and
3. Client data collection settings are enabled for the selected GPO.

Using the Instant Elevation Wizard to set up, modify, or discard privileges

To use the Instant Elevation Wizard to set up, modify, or discard privileges

1. Open the wizard by completing one of the following steps:
    - Open the Instant Elevation Wizard from the Setup Tasks section. It will always show the default settings.
    - Double-click the **Advanced Policy Settings** > **Instant Elevation Settings** tab of the target GPO. The changes made with the wizard will be saved here.
2. Enable the **Instant Elevation Settings** on the **State** tab.
    - Choose **Enabled**, to ensure the settings apply to the selected GPO.
    - Choose **Not Configured**, to enable child GPOs to inherit settings from their parent.
3. Use the **Groups** tab to alter the settings. By default, users of the target GPO automatically inherit the administrator's settings (`BUILTIN\Administrators`).
4. Complete the advanced options in the **Privileges** and **Integrity** tabs.
5. Click **Next** to use Validation Logic to target the settings to specific client computers or user accounts within the GPO, or click **Finish** to save your settings and quit.

If an error message indicates that the target GPO is not selected:

1. Click **OK** to close the message window.
2. Open the **GPO** tab and select the desired GPO.

3. Click Save on the **GPO** toolbar to save the new settings.
4. Users can click **Elevate!** to launch privileged applications without interruptions. The button is available on the context menu of Windows Explorer objects that require elevated privileges to start up, including: `.bat`, `.cmd`, `.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs` (`.lnk` is for shortcuts).
5. Run an Instant Elevation Report to view the processes that are launched. For more information, see Instant Elevation Report.

Configuring Self-Service Elevation

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

To enable users to request permissions to use privileged applications, use the Self-Service Elevation Request Settings Wizard. Whenever a user attempts to run an application which requires administrative permissions for which they do not have rights, they are asked if they would like to send a request to their administrator for permission to run it.

You can select how users access the request form and set up Self-Service notifications to email you, the help desk, and your manager of each request. Then, you can process the request within the **Self-Service Elevation Requests** section of the Console and email your decision to the user, using the **Console Email Configuration** screen.

NOTE: In some cases, Self-Service Elevation and Blacklist rules could be configured for the same target application. In this case, Blacklisting takes precedence over Instant Elevation and prevents the application from starting. For more information about creating Blacklisting rules, see Using the Create Rule Wizard.

Using the Self-Service Elevation Request Settings Wizard

NOTE: Before you configure Self-Service Elevation request settings, ensure the following components are set up:

1. The Client is running on the computers you want to apply the settings to;
2. The Server is configured and running with the port that you have selected allowed for incoming data (the default port is **8003**); and
3. Client data collection settings are enabled for the selected GPO.

To use the Self-Service Elevation Request Settings Wizard to set up, modify, or discard privileges

1. Open the wizard by completing one of the following steps:
   - Open the **Self-Service Elevation Request Settings Wizard** from the **Setup Tasks** section. This section always shows the default settings.
   - On the **Advanced Policy Settings** tab of the target GPO, double-click **Self-Service Elevation Request Settings**. The changes made within the wizard are saved here.
2. Enable the **Self-Service Elevation Request Settings** on the **State** tab.
   - To ensure the settings apply to the selected GPO, choose **Enabled**.
   - To enable child GPOs to inherit settings from their parent, choose **Not Configured**.
3. For Selecting how users access the request form, use the **Settings** tab.
4. To use **Validation Logic** to target the settings to specific client computers or user accounts within the GPO, click **Next**, or to save your settings and quit, click **Finish**.

   If an error message indicates that the target GPO is not selected:

   a. To close the message window, click **OK**.

   b. Open the **GPO** tab and select the desired GPO.
5. To use the **Filters** tab to filter out Self-Service Request data according to different application specific criteria, click **Next** .

   Enter filter criteria in one or more of the available boxes:

- **Path to .exe contains**
- **Product name contains**
- **Publisher name contains**
- **File description contains**

NOTE: The **Publisher name contains** field looks at the Publisher or Company Name attribute.

An application only needs to meet a single filter criteria in order for its Self-Service Request data to be filtered out. A comma delimiter can be used to enter multiple criteria in each filter box.

NOTE: The Privilege Manager Client does not transmit any Self-Service Request data for any application that meets at least one of the existing filter criteria.

6. To save the new settings, click **Save** on the **GPO**.

Selecting how users access the request form

Use the **Settings** tab of the **Self-Service Elevation Request Settings Wizard** to select how end users access the request form and set up email confirmation and notification settings. You can combine the following options:

OPTION	ACTION
Automatically ask users if they would like to request that a privilege elevation rule be created whenever they attempt to launch applications which require privilege elevation to run *This option is enabled by default.*	Once a user closes the **User Account Control (UAC)** window, a **Self-Service Elevation Request Prompt** will display. NOTE: Not all applications that display UAC windows will automatically pop up a Self-Service Elevation Request Form. You can allow the user to manually submit Self-Service requests by enabling the Add a Windows explorer shell extension allowing the user to right-click on a program or shortcut in order to request that a privilege elevation rule be created for that program option. Windows Installer files (`.msi`) do not automatically trigger Self-Service Prompts, so the Self- Service Elevation Request Form must be manually triggered by users.
Allow users to hide or disable these prompts *This option is enabled by default.*	• Users can select whether the request form displays in the future by checking the **In the future, don't show me this when I try to run applications that need approval** check box. • A user on a client computer can re-enable/disable the prompt using the **Display Self-Service Prompts** icon on the context menu of the system tray. NOTE: This setting does not affect the **Self-Service Elevation Request Form** launched with the **Elevate!** button. It only affects the request forms displayed automatically.

OPTION	ACTION
Add a Windows explorer shell extension allowing the user to right-click on a program or shortcut in order to request that a privilege elevation rule be created for that program *This option is enabled by default.*	• Users can click **Elevate!** to launch privileged applications without interruptions. The button is available on the context menu of Windows Explorer objects that require elevated privileges to start up, including: `.bat`, `.cmd`,`.exe`, `.js`, `.lnk`, `.msc`, `.msi`, `.msp`, `.pl`, `.ps1` or `.vbs` (`.lnk` is for shortcuts). • Users can click **Elevate!** to launch the Self-Service Elevation Request Form or Instant Elevation, if it is enabled.
Allows the user to specify the email address where the confirmation email will be sent once the administrator processed the request for the privilege elevation rule. If this option is not checked, the email will be sent to the Exchange account of the user specified in Active Directory. *This option is disabled by default.*	The user can enter an email address into the corresponding text field. By default, the field is pre-populated with the email address of the user who is logged in (provided that it is specified in Active Directory).
Send an email notification to the administrator whenever a user submits a Self-Service Elevation Request *This option is disabled by default.*	Enter the **Email Address** for the administrator and/or the help desk or other recipients. Click **+** to add entries and **x** to remove them. By default, the **Email Subject** is pre-populated with `Privilege Manager Self-Service Elevation Request` as the subject line. You can enter your own subject and click **Reset** to reset it to the default.

Customizing Self-Service request email messages

The approval and denial email messages that are sent as a response to the user's Self-Service Elevation request can be customized.

Approval messages

Denial messages

Customizing Approval and Denial messages

Approval messages

Example: Default Approval message

The default Approval message says the following:

```
MESSAGE_NAME:ApprovedRequest
MESSAGE:
Your request to run the following application with elevated privileges has
been "approved".Request Date: <ExecutionDate>
Requested Application:
<ProductName>
<Path>
<Arguments>
Reason for request: <Reason>
This new privilege should be available on your computer once Windows has
refreshed its domain security policies.
```

Denial messages

Example: default Denial message

The default Denial message says the following:

```
MESSAGE_NAME:NotApprovedRequest
MESSAGE:
Your request to run the following application with elevated privileges has
"not" been approved.
<ProductName>
<Path>
Please contact your administrator for more details.
```

Customizing Approval and Denial messages

These messages can be customized by opening the `MessageTemplates.cfg` file in the `Privilege\Console` folder. Each message in the CFG file starts with `======StartOfMessage=========` and ends with `======EndOfMessage===========`. The text between these delimiters can be customized to your liking. Text delimited with angle brackets (`< >`) are variables that are replaced with data at runtime.

The following variables may be used in the Approval message:

- `ExecutionDate`
- `ProductName`
- `Path`
- `Arguments`
- `Reason`

The following variables may be used in the Denial message:

- `ProductName`
- `Path`

Using Self-Service Notifications

If you would like to receive an email when a user on a client computer submits a **Self-Service Elevation Request Form**, you can set up a Self-Service Notification. You can configure it to go to multiple recipients, including you, your manager, and/or the help desk. In addition, you can set the subject line to meet the requirements of your help desk.

To set up Self-Service Notifications

1. Configure the Server.
    a. Use the **Privilege Manager Server Setup Wizard** to configure the **Server Email Notification Configuration** settings on the first screen of the wizard.
    b. If you previously completed the wizard, the remaining screens are automatically populated.
    c. Refer to the *Safeguard Privilege Manager for Windows Quick Start Guide* for step-by-step instructions.
2. Configure the recipient.
    a. Use the **Settings** tab on the **Self-Service Elevation Request Settings Wizard** to configure the **Email Notification Settings**.
3. For more information on the wizard, see Using the Self-Service Elevation Request Settings Wizard.
4. For more information on setting up **Email Notification Settings**, see .
5. Check your email for the Self-Service Notification, containing information on the user, the request, and the client's computer.
6. Accept or reject the user's request Using the Self-Service Elevation Request Processing Wizard.
7. Inform the end user of your decision Using the Console Email Configuration screen.

Using the Self-Service Elevation Request Processing Wizard

Shortly after a user on a client computer has submitted a Self-Service Elevation Request Form, you can view and/or process it within the **Self-Service Elevation Requests** section of the Console (provided that your environment is properly configured according to the **Maximum Sleep Time** setting).

You can only view data stored in the database of the server that is selected in the Server configuration (under **Setup Tasks** > **Configure a Server**).

When processing a Self-Service Elevation request, you can either create a rule to elevate privileges for the process or deny the request. You can then email your decision to the user using the **Console Email Configuration** screen.

To view or process Self-Service Elevation requests

1. Open the **Self-Service Elevation Requests** section from the navigation pane of the Console. The requests appear in the window on the right.
2. Click **Display requests** to list the Self-Service Elevation requests submitted by users, based on the default filter settings shown in the **Applied Filters** section at the top of the screen.
3. Select a request in the **Self-Service Elevation Requests** grid below. Use the grid's column headers to sort the requests.

   By default, the following information appears:

   a. Requests to elevate any type of applications;

   b. Requests sent during the last 30 days; and

   c. Requests that have never been processed with using **Process request** from the current section.
4. Use the **Applied Filters Wizard** to modify the list. You can create multiple shared filter sets and save settings that other administrators can use. For more information, see Using the Applied Filters Wizard.
5. Select a record and then click **Process request** to open the **Self-Service Elevation Request Processing Wizard**.
6. On the first tab of the wizard, view the details for a process that failed to start, and the reason for requesting Elevation privileges. Click **Next**.

7. Indicate whether you want to create a rule to elevate the privileges for this process, or deny the request.
    a. If you approve the request, the **Create Rule** wizard appears, allowing you to create a rule for the requested process. By default, the rule is created for a specific user at a specific computer, and the Administrators group (stored within the `BUILTIN\Administrators` Active Directory OU) is added to the rule. Use the **Validation Logic** tab to modify this setting.
    b. When a request is processed and a rule is created for it (or it has been denied), the **Processed Action** column displays a rule created or ignored value.
    c. To view ignored requests or requests for which the rules were created, change the **Process Date of Item** filter on the **Applied Filters Wizard** from **None: Item has not been processed to the corresponding Date Range**.
8. Select whether or not to email your decision to the user. This feature requires that you set up the **Console Email Configuration** settings.
9. Click **Finish** to save.

    The rule created from the request is added to the selected GPO with a default name.
10. Select **Export** to export the list of requests presented on the grid. The list will be saved as an `.xls` file.

    After the rule has been created:
    - The rule is added to the target GPO of the **Group Policy Settings** section.
    - The rule applies after the GPO settings are updated on the client computer.

Using the Console Email Configuration screen

If you want Safeguard Privilege Manager for Windows to send an email message to the user after approving or denying their Self-Service Elevation request, configure the settings using the **Setup Tasks** > **Console Email Configuration** screen.

To configure the Server to send your Self-Service Elevation request approval or refusal:

1. Select **Console Email Configuration** from the **Setup Tasks** section.
2. Configure the following fields:
    a. **Host Name**: Enter the SMTP Server name of the email account from which you are going to send your emails.
    b. **SMTP Port**: Enter the port number.
    c. **SMTP User Name and Password**: If necessary, enter the authentication information and check the SSL check box.
    d. **From Email**: Enter the corresponding email.
3. Click **Send Test Email** to send an email to the account specified in the **From Email** field.
    a. If Safeguard Privilege Manager for Windows succeeds in sending the email, the corresponding message appears.
    b. Log into an email program with the corresponding account and locate the sent email folder, with **Privilege Manager Test Email** in the subject.
4. Click **OK** to save the settings and quit.

Configuring Temporary Session Elevation

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Temporary Session Elevation (TSE) allows an administrator to generate Elevation passcodes that can provide end users the ability to temporarily elevate the privileges of any process or application on their machine. The passcodes work for both on-network and off-network machines, even if there are active internet connections.

Temporary Session Elevation passcodes are intended to be used during a specific user session. A user session comprises the period between the user logon and logoff times, regardless of the reason that caused the logoff.

Temporary Session Elevation passcode usage can be limited by time or number of uses. More granular limitations can selected by using Validation Logic in the passcode. Examples of this are limiting use by computer name, user name or time and date range. When the passcode is used on a client computer, Validation Logic allows or denies usage based on selected options.

> NOTE: In some cases, Temporary Session Elevation and Blacklisting rules are configured for the same target application. In this case, Blacklisting takes precedence over Temporary Session Elevation and prevents the application from starting. For more information about creating Blacklisting rules, see Using the Create Rule Wizard.

For more information, see the following Knowledge Base Articles:

- Temporary Session Elevation: Duration (4231432)
- Temporary Session Elevation: What is a session? (4225404)

Using the Temporary Session Elevation Passcode Manager

Before you configure Temporary Session Elevation settings, ensure the following components are set up:

1. The Client is running on the computers you want to apply the settings to.
2. The Server is configured and running with the port that you have selected allowed for incoming data (the default port is `8003`).
3. Client data collection settings are enabled for the selected GPO.
4. The Client is enabled to use offline passcodes to create Temporary Elevated Sessions (enabled in the Client Deployment Settings wizard).

To use the Temporary Session Elevation Wizard to set up privileges

1. Open the wizard:
    a. Open **Passcode Manager** from the **Temporary Session Elevation** section on the navigation pane of the Console.
2. Create a new passcode:
    a. Click **New** to start the **Instant Elevation TSE passcode generator**.
3. Enable the **Instant On Demand Privilege Elevation settings** on the **State** tab.
    - Choose **Enabled**, to ensure the settings apply to the selected GPO.
    - Choose **Not Configured**, to enable child GPOs to inherit settings from their parent.
4. Use the **Groups** tab to alter the settings. By default, users of the target GPO will automatically inherit the administrator's settings (`BUILTIN\Administrators`).
5. Complete the advanced options in the **Privileges**, **Integrity** and **Validation Logic** tabs.
6. The Passcode is created on the next tab, **Passcode**.
    a. Enter a **Title** to describe the passcode.
    b. Enter a **Maximum allowed usage**. This is the number of times the passcode can be used before expiring.

c. Enter a **Duration**. The duration is the amount of time the passcode remains active, after being activated.

d. Optionally, select the check box to **End all elevated processes (and child processes)** when **Passcode duration** expires. If selected, all windows that are opened with a Temporary Session Elevation passcode are closed.

e. Click **Export** to file to save the passcode for end-user use.

7. Click **Finish** to complete the wizard.

   a. The passcode is delivered to the user for usage.

8. Run a **Temporary Session Elevation Usage Report** to view the processes that have been launched. For more information, see Temporary Session Elevation Request Report.

Configuring privileged application discovery

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Use the Privileged Application Discovery Settings Wizard to collect information about the privileged applications used over your network during a specified time period. By default, once this feature is enabled, it is set to collect information for two weeks, but you can adjust the setting.

Using the Privileged Application Discovery Settings Wizard

NOTE: Before you configure privileged application discovery settings, ensure the following components are set up:

1. The Client is running on the computers you want to apply the settings to;
2. The Server is configured and running with the port that you have selected allowed for incoming data (the default port is **8003**); and
3. Client data collection settings are enabled for the selected GPO.

To use the Privileged Application Discovery Settings Wizard to set up, modify, or discard settings

1. Open the wizard by completing one of the following steps:
    - Open the Privileged Application Discovery Settings Wizard from the **Setup Tasks** section. It always shows the default settings.
    - On the **Advanced Policy Settings** tab of the target GPO, double-click **Privileged Application Discovery Settings**. The changes made within the wizard are saved here.
2. Enable the Privileged Application Discovery Settings on the **State** tab.
    - Choose **Enabled**, to ensure the settings apply to the selected GPO.
    - Choose **Not Configured**, to enable child GPOs to inherit settings from their parent.
3. Use the **Settings** tab to set the period during which the settings apply and the data is collected (a month by default).
4. Click **Next** to use **Validation Logic** to target the settings to specific client computers or user accounts within the GPO, or click **Finish** to save your settings and quit.

If an error message indicates that the target GPO is not selected:

1. Click **OK** to close the message window.
2. Open the **GPO** tab and select the desired GPO.
3. Click **Next** to use the **Filters** tab to filter out **Application Discovery** data according to different application specific criteria.

On the **Filters** tab, select the check box to enable application filters.

Enter filter criteria in one or more of the available boxes:

- **Executable path contains**
- **Product name contains**
- **Publisher name contains**
- **File description contains**

An application only needs to meet a single filter criteria in order for its **Application Discovery** data to be filtered out. A comma delimiter can be used to enter multiple criteria in each filter box.

NOTE: The Privilege Manager Client does not transmit any Application Discovery data for one or more applications that meet any of the existing filter criteria.

4. Click **Save** on the GPO toolbar to save the new settings.

Processing discovered privileged applications

Once a privileged process starts (or failed to start) on a client computer, the corresponding information is sent to the Server and displayed in the **Privileged Application Discovery** section of the Console (provided that your environment is properly configured according to the **Maximum Sleep Time** setting).

You can only view data stored in the database of the server that is selected in the Server configuration (under **Setup Tasks** > **Configure a Server**).

When processing a discovered privileged application, you can either create a rule for it so that a user without elevated privileges can launch it, or choose to mark it as processed so that it will not display in the list (unless the filter is specifically set to display it).

Use the **Generate Rules** wizard to automatically create a number of rules for different types of applications in one pass. Rules are created based on the preferences with which the application was started. You can select an application and view its preferences in the **Privileged Applications Discovered** grid.

Processing discovered privileged applications

Detailed information about this topic

Once a privileged process starts (or failed to start) on a client computer, the corresponding information is sent to the Server and displayed in the **Privileged Application Discovery** section of the Console (provided that your environment is properly configured according to the **Maximum Sleep Time** setting).

You can only view data stored in the database of the server that is selected in the Server configuration (under **Setup Tasks** > **Configure a Server**).

When processing a discovered privileged application, you can either create a rule for it so that a user without elevated privileges can launch it, or choose to mark it as processed so that it will not display in the list (unless the filter is specifically set to display it).

Use the Generate Rules wizard to automatically create a number of rules for different types of applications in one pass. Rules are created based on the preferences with which the application was started. You can select an application and view its preferences in the **Privileged Applications Discovered** grid.

Using the Generate Rules Wizard

To view discovered privileged applications and generate rules for them

1. Open the **Privileged Application Discovery** section from the navigation pane of the Console. The applications are displayed in the window on the right.
2. Click **Display applications** to list the privileged applications and other processes that are started (or failed to start), based on the default filter settings shown in the **Applied Filters** section on the top of the screen.
3. Select an application in the **Privileged Applications Discovery** grid below. Use the grid's column headers to sort the applications.

   By default, the following information appears:

   - Any type of privileged applications
   - Privileged applications that were discovered during the last 30 days
   - Privileged applications that have no generated rule in the current section, or are marked as ignored
4. Use the **Applied Filters** wizard to modify the list. You can create multiple shared filter sets and save settings that other administrators can use. For more information, see Using the Applied Filters Wizard.
5. Select a record and then click **Generate rules** to open the **Generate Rules Wizard**.
6. On the first tab of the wizard, specify your rule type preferences. Click **Next**.
7. Add Validation Logic preferences into the rule, if necessary. The selected preferences will be used to create the corresponding Validation Logic type. Click **Next**.
8. Review your rules and click **Next**, or
   a. Click the **Review rules that will be created** button to open a window with more information.
   b. Click **Details** for more information, or click **Close**.
9. Select a target GPO for the rule and specify the GPO policy type. By default, the Administrators group (stored in the `BUILTIN\Administrators` Active Directory OU) is added to the rule. Click **Create** to save the rule.
10. Once a discovered privileged application is processed and a rule is created for it, or it has been marked as ignored, the application is considered processed.

11. To view ignored applications or applications for which the rules are created, change the **Process Date of Item** filter on the **Applied Filters Wizard** from **None: Item has not been processed** to the corresponding **Date Range**.
12. The rule created from the application is added to the selected GPO with a default name.
13. Select **Export** to export the list of applications presented on the grid. The list is saved as an `.xls` file.

After the rule has been created

- The rule is added to the target GPO of the **Group Policy Settings** section.
- The rule applies after the GPO settings are updated on the client computer.

1

Deploying rules

Detailed information about this topic

Safeguard Privilege Manager for Windows can create Privilege Elevation Rules and Blacklisting Rules. Privilege Elevation rules are rules that raise the permissions level of the user for an application. Blacklisting rules deny a user access to an application, regardless of what their default domain user permissions allows.

Creating rules

You can create five types of rules with Safeguard Privilege Manager for Windows:

- **Available in all editions of Safeguard Privilege Manager for Windows:**

  By Path to the Executable: A file rule that applies to the path to an executable. For more information, see Creating file rules.

  By Folder Path: A folder path rule that applies to all processes run from a path. For more information, see Creating folder path rules.

  By ActiveX Rule: An ActiveX rule that applies to a specific URL. For more information, see Creating ActiveX rules.

- **Available only in Safeguard Privilege Manager for Windows Professional and Safeguard Privilege Manager for Windows Professional Evaluation editions:**

  By Path to Windows Installer: A rule that applies to the path to Windows Installer files and patches. For more information, see Creating rules for Windows Installer files.

  By Path to Script File: A rule that applies to the path to a script file. For more information, see Creating rules for script files.

You can create a rule in one of the following ways:

- Create a default rule using the **Create GPO with Default Rules Wizard**.
- Create a new rule using the **Group Policy Management Editor** or the **Create Rule Wizard**.

Once you create a rule, you can:

- Test the rule. For more information, see Testing rules.
- Edit or delete the rule. For more information, see Managing rules.
- Build a report to view the rule's settings, save them into a file, and get statistics on the rule’s usage. For more information, see Reporting.

Using the Create GPO with Default Rules Wizard (Privilege Elevation Rules only)

Safeguard Privilege Manager for Windows contains a range of useful default rules that you can add to a new or existing GPO. To create the default rules provided by the product, use the **Create GPO with Default Rules Wizard**. To access the wizard from the **Getting Started** screen, navigate to the **Setup Tasks** tab and then double- click **Create GPO with default rules**.

NOTE: Rules created with this process are Privilege Elevation rules only. You cannot create deny list rules here.

To use the Create GPO with Default Rules Wizard

1. Double-click **Create GPO** with default rules to open the wizard.
2. Review the text in the **Introduction** dialog and click **Next**.
3. In the Select privilege elevation rules dialog, select your operating system from the drop-down menu and select the corresponding rules from a list of common ones. Click **Next**.
4. In the **Select target GPO** dialog, select or create a GPO to assign the rule to complete one of the following steps:
    - Select a GPO from the list under the domain that your local computer is a part of.
    - Select a domain, click **Create GPO**, name it, and click **OK**. The newly created GPO is added to the **All GPOs** list in the **Group Policy Objects** container.
    - Link any GPO not marked with the icon to your domain or Active Directory OU.
5. Highlight the GPO in the left pane and click the **Link GPO** button on the right to link the GPO to the domain or an OU.
6. Browse for an OU or add the GPO to the domain in the dialog that appears.
7. Click **OK**.

8. Once the rule is created, its icon changes to  to indicate that it contains a rule and it is listed in the GPOs with Policy Settings node.

   NOTE: You can only link a GPO to an item for which you have sufficient rights. For more information, see Select user policy or computer policy:.

   - To save and apply the rule, click **Finish**. If you did not specify the required data, the wizard notifies you.

9. An error message will notify you if you have insufficient permissions to perform any of the operations listed above.
   - You must have permission to perform the same actions in the **GPMC**.
   - Contact your system administrator to get the proper permissions.
10. The displays in the list of rules for the corresponding GPO under the **Group Policy Settings** section.
11. The rule is applied once the Group Policy is updated on the client computer.
12. A message notifies you that the rule's parameters change when the trial period expires, if you create a rule with any of the Privilege Manager Professional features while using the evaluation edition. For more information, see Editions.
13. Modify the rule, as necessary. For more information, see Managing rules.

Using the Group Policy Management Editor

The **Group Policy Management Console (GPMC)** is a built-in **Microsoft Management Console (MMC)** snap-in. You can use the features in Privilege Manager based on your Windows rights within the **GPMC**.

You can use the **Group Policy Management Editor** in the **GPMC** to manage and create rules or you can use the **Create Rule Wizard** in the **Privilege Manager for Windows Console**.

To use the Group Policy Management Editor to create and manage rules

1. Open the **MMC**. On the **Start** menu, click **Run**, type `MMC`, and then click **OK**.
2. From the **File** menu, select **Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog appears.
3. Select **Group Policy Management** under the list of snap-ins.
4. Click **Add**.
5. Click **OK**.

   The **Console Root** window now has a snap-in, **Group Policy Management**, rooted at the **Console Root** folder.
6. Right-click a GPO under your forest in the **Group Policy Management** pane on the right and select **Edit**.

   The **Group Policy Management Editor** will open. The editor now has **Privilege Manager for Windows** nodes, under **Computer Configuration** and **User Configuration**.

   The right pane has an **Extended** and a **Standard** tab.
7. Click the **Extended** tab for more information about an item.

Available only in Privilege Manager Professional and Professional Evaluation editions:

To create new rule, use either of the following methods:

- Select a **Privilege Manager for Windows** node and use ✚ **New Rule**.
- Use the other toolbar buttons to delete or modify the selected **Privilege Manager for Windows** node.

  NOTE: Before clicking ✚ **New Rule**, ensure that the **Privilege Elevation Rules** or **Blacklist Rules** tab is selected.

Using the Create Rule Wizard

To use the Create Rule Wizard

1. Select or create a GPO in the **All GPOs** node in the left pane of the **Privilege Manager for Windows Console**:
    a. Select a GPO from the list under the domain that your local computer is a part of.
    b. Select a domain, click **New GPO**, name it, and click **OK**. The newly created GPO is added to the **All GPOs** list in the **Group Policy Objects** container.
2. Link any GPO not marked with the icon to your domain or Active Directory OU.
    a. Highlight the GPO in the left pane and click **Link** above it.
    b. Browse for an OU or add the GPO to the domain in the dialog that appears.
    c. Click **OK**.
    d. Once the rule is created, its icon changes to to indicate that it contains a rule and it is listed in the **GPOs with Policy Settings** node.

    NOTE: You can only link a GPO to an item for which you have sufficient rights. For more information, see Select user policy or computer policy:.
3. Use the **Create Rule Wizard** to configure the rule.
    a. Select the **Privilege Elevation Rules** or **Blacklist Rules** tab based on the type of rule to be created.
    b. Click **New Rule** to open the **Create Rule Wizard**.
    c. Specify the data requested in each tab and click **Next**.
        i. Privilege Elevation rules only. Follow the prompts through the default tabs:
            - **Start**
            - **Description**
            - **Type**
            - **Groups**

- **Validation Logic** (available only for Safeguard Privilege Manager for Windows Professional)

The **Privileges and Integrity tabs** display as advanced options.

ii. Blacklist rules only. Follow the prompts through the default tabs:

- **Start**
- **Description**
- **Type**
- **Validation Logic** (available only for Privilege Manager Professional)

d. Enter the required fields, marked with an asterisk '*' on the **Description** and **Type** tabs.

> NOTE: Blacklist rules only. In some cases, Blacklist rules could be configured with Instant, Temporary Session, or Self-Service Elevation, for the same target application. In this case, Blacklisting takes precedence over any type of Elevation and prevents the application from starting. For more information, see the following sections:
>
> - Configuring Instant Elevation
> - Configuring Temporary Session Elevation
> - Configuring Self-Service Elevation

e. To save and apply the rule, click **Finish**. If you did not specify the required data, the wizard notifies you.

4. Click **Save** on the menu bar of the **Rule** section. Or, if prompted, confirm that you want to save the rule.
5. An error message will notify you if you have insufficient permissions to perform any of the operations listed above.
   - You must have permission to perform the same actions in the **GPMC**.
   - Contact your system administrator to get the proper permissions.
6. The rule is applied once the Group Policy is updated on the client computer.
7. A message notifies you that the rule's parameters change when the trial period expires, if you create a rule with any of the Privilege Manager Professional features while using the evaluation edition. For more information, see Editions.

Getting started

To use the Start tab in the Create Rule Wizard

1. To create your own settings, select **Create your own rule**, or
2. Create a rule with predefined settings:
    a. Select the **Select common rule** from the list below option.
    b. To sort the rules according to the operating system they apply to, use the Operating System menu.
    c. To modify the default settings, click **Next**. To save your settings for the target GPO and quit, click **Finish**.

To use the Description tab in the Create Rule Wizard

1. Enter a title to identify the rule and an optional description.
    a. To display the title of the rule when using the **View current rules** option on the Client system tray, select the **Advertise this rule in the system tray on client computers** option.

    The system tray also shows a notification message any time there is a change to the set of rules flagged as advertised.
    b. To enable or disable data collection for a specific rule, select **Disable data collection activity for this rule**.
    c. To stop the rule from applying, select **Disable the rule regardless of validation**. To apply the rule again, clear the option.
2. Click **Next**.

To use the Type Tab in the Create Rule Wizard to specify the essential parameters of the processes for the rule

- **Available in all editions of Safeguard Privilege Manager for Windows:**

  By Path to the Executable: A file rule that applies to the path to an executable. For more information, see Creating file rules.

  By Folder Path: A folder path rule that applies to all processes run from a path. For more information, see Creating folder path rules.

By ActiveX Rule: An ActiveX rule that applies to a specific URL. For more information, see Creating ActiveX rules.

- **Available only in Privilege Manager Professional Edition and Professional Evaluation Edition:**

  By Path to Windows Installer: A rule that applies to the path to Windows Installer files and patches. For more information, see Creating rules for Windows Installer files.

  By Path to Script File: A rule that applies to the path to a script file. For more information, see Creating rules for script files.

1. Specify the options that correspond to the type of rule you have selected.
2. Select user policy or computer policy:
   - **User Policy**: Select this option to apply the rule to the user logged into the computer. This option corresponds to the **User Configuration** node of the Group Policy Management Editor and is the default policy for all editions of Safeguard Privilege Manager for Windows.
   - **Computer Policy**: Select this option to apply the rule to a computer irrespective of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor. Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Creating file rules

Use the **By Path to the Executable** rule to elevate or decrease privileges for processes that start from an executable file.

To create a By Path to the Executable file rule using the Create Rule Wizard

1. Open the **Create Rule Wizard**. For more information, see Using the Create Rule Wizard.
2. Specify the **Path** to an executable file on the client computer or a network share in one of the following ways:
   - Type the path to the file, including its extension, in the following format:

     `\\ComputerName\SharedFolder\Filename.exe`

     `DriveLetter:\Filename.exe`
   - Use the common `%` variable and the `*` and `?` wildcards to identify the path, for example, `*\filename.exe`.
   - Use **Browse** to locate the path. Once you locate the process, a dialog will prompt you to:
     1. Retrieve a digital signature for the rule's **Publisher** field. Click **Yes** to add the available digital signature. Click **No** to skip the prompt.
     2. Create a file version for the file. Click **Yes** to add the setting. Click **No** to skip the prompt.
     3. Create a unique cryptographic hash for the file to secure its identification. Click **Yes** to add the setting. Click **No** if you are creating the rule for the file for which data is likely to be updated in the future, or for any file with its name within the specified folder.

        NOTE: When saving the rule, Safeguard Privilege Manager for Windows converts the path into environment variables.
3. To simplify adding parameters into the rule, click **Processes**.

   NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

   a. Select whether you will create the rule from a process on a local or remote computer.

b. A list of processes running on the computer will open. Locate the process and view its details in the fields to the right:
    - **Path**: the path to the process's executable.
    - **Arguments**: the arguments with which the process was started.
    - **Publisher**: the digital certificate of a publisher.
    - **Version**: the File Version property.
    - **Hash**: a unique cryptographic hash.
    - **Integrity level**: the security level with which the process runs in Windows.
    - **Privileges**: the privileges granted to the process.

c. Click **OK**. The data for the processes will be saved to the rule and displayed on the corresponding tabs of the wizard.

d. To troubleshoot a **Failed to retrieve** processes, refer to documentation for more info error, check the following on the remote computer:
    i. The computer is turned on and accessible from the network;
    ii. The domain administrator credentials have been provided; and
    iii. Windows Management Instrumentation (WMI), Distributed Component Object Model (DCOM), File and Printer Sharing, and Remote Administration are allowed through the firewall.

4. Fill in these optional fields, as necessary:
    - **Arguments**: Specify the common or user-defined arguments with which the executable will run. For example, to build a rule that will allow a non-administrator to access the **Date/Time** tool in the **Control Panel** from the task bar, enter this data:
        - **Path**: `%SystemFolder%\rundll32.exe`
        - **Arguments**: `/d c:\windows\system32\shell32.dll,Control_RunDLL timedate.cpl`
    - Available only in Privilege Manager Professional Edition and Professional Evaluation Edition.
        - **Publisher**: Limit Elevation to files signed with the digital certificate of a publisher. Enter the exact name or use **Browse** to locate it.
        - **File Version**: Limit Elevation to those whose File Version property match the ones specified.
        - **File Hash**: Click **Browse** to locate the file and create a unique cryptographic hash that limits Elevation to files that match it. This ensures that the rule will not apply to dangerous content that is similarly named and will help prevent security issues.

          NOTE: The file hash will not apply to a file that you have modified during program updates, so do not add it to the rule for a file which is

likely to be updated, or for any file with the same name in that location.

- **Apply settings to child processes**: Ensure that child processes triggered by the rule will not fail due to lack of privileges. This check box is enabled by default.
- **User's context will be used to resolve system and resource access**: Ensure that the Client uses the target's user environment to resolve file and registry access. This might be required to resolve drive mappings, and also if the rule specifies the publisher, version, or file hash for the target process running from a network location.

5. Define whether the rule will be user-based or computer-based.
    - **User Policy**: Select this option to apply the rule to the user logged into the computer. This option corresponds to the User Configuration node of the Group Policy Management Editor and is the default policy for all editions of Safeguard Privilege Manager for Windows.
    - **Computer Policy**: Select this option to apply the rule to a computer regardless of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor.

      NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.
6. Complete the **Privileges** (see Granting or denying privileges (Privilege Elevation Rules only)) and **Integrity** (see Differentiating security levels (Privilege Elevation Rules only)) tabs to modify the rule.
7. Click **Finish** to quit the wizard.
8. The rule will be named after the executable.

Creating folder path rules

Use the By Folder Path rule to elevate or decrease privileges for processes that start from a folder path.

To create a By Folder Path rule using the Create Rule Wizard

1. Open the Create Rule Wizard. For more information, see Using the Create Rule Wizard
2. Specify the location of a Folder on the client computer or a network share in one of the following ways:
    - Type the folder path in the following format:

      `\\ComputerName\SharedFolder DriveLetter:\Folder`
    - Use the common `%` variable and the `*` and `?` wildcards to identify the folder, for example, `*\Folder`
    - Use **Browse** to locate the folder.

    NOTE: When saving the rule, Privilege Manager for Windows converts the path into environment variables.
3. Fill in these optional fields, as necessary:
    - **Publisher**: Limit Elevation to files signed with the digital certificate of a publisher. Enter the exact name or use **Browse** to locate it.

      NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.
    - **Apply settings to sub folders**: Apply the rule to processes started from any file under any sub folders of the path.
    - **Apply settings to child processes**: Ensure that child processes triggered by the rule will not fail due to lack of privileges. This check box is enabled by default.
    - **User's context will be used to resolve system and resource access**: Ensure that the Client uses the target's user environment to resolve file and registry access. This might be required to resolve drive mappings, and also if the rule specifies the publisher, version, or file hash for the target process running from a network location.
4. Define whether the rule will be user-based or computer-based.

- **User Policy**: Select this option to apply the rule to the user logged into the computer. This option corresponds to the **User Configuration** node of the Group Policy Management Editor and is the default policy for all editions of Privilege Manager for Windows.
- **Computer Policy**: Select this option to apply the rule to a computer regardless of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor.

  NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

5. Complete the **Privileges** (see Granting or denying privileges (Privilege Elevation Rules only)) and **Integrity** (see Differentiating security levels (Privilege Elevation Rules only)) tabs to modify the rule.
6. Click **Finish** to quit the wizard.
7. The rule will be named after the folder path.

Creating ActiveX rules

Use the By ActiveX Rule to allow installation of ActiveX controls from the Internet.

To create an ActiveX Rule using the Create Rule Wizard

1. Open the **Create Rule Wizard**. For more information, see Using the Create Rule Wizard.
2. Specify the URL for the ActiveX control in the **Source URL** field, for example:

   `http://*.macromedia.com`
3. Available only in Privilege Manager Professional Edition and Professional Evaluation Edition.
   a. To view details of the ActiveX controls installed on the local computer and create rules based on them, click **Installed ActiveX Controls**.
   b. Fill in these optional fields, as necessary.
      - **Control**: Enter the name of the ActiveX control from the CodeBase attribute of the web page.
      - **CLSID/MIME**: Restrict loading a control unless the CLSID or MIME value on the web page matches the one specified.
      - **ActiveX Version**: Restrict Elevation to ActiveX controls with a matching version number on the web page from which it will be downloaded.
4. Define whether the rule will be user-based or computer-based.
   - **User Policy**: Select this option to apply the rule to the user logged into the computer. This option corresponds to the User Configuration node of the Group Policy Management Editor and is the default policy for all editions of Safeguard Privilege Manager for Windows.
   - **Computer Policy**: Select this option to apply the rule to a computer regardless of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor.

     NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.
5. Click **Finish** to quit the wizard.
6. The rule will be named after the ActiveX control.

Applying ActiveX rules

In order for an ActiveX rule to take effect on clients, set up the following components

1. Enable the GPE ActiveX Installer add-on in the Internet Explorer browser.
2. Open the **Internet Options** menu.
    a. Clear the **Enable Protected Mode** check box on the **Security** tab.
    b. Select the **Enable third-party browser extensions*** check box on the **Advanced** tab.
3. Restart Internet Explorer.

To centrally enable third-party browser extensions by modifying a GPO:

1. Create a dedicated GPO or open the Group Policy Management Editor.
2. Navigate to **Computer Configuration** > **Administrative Templates: Policy definitions (ADMX files)** > **Windows Components** > **Internet Explorer** > **Internet Control Panel** > **Advanced Page**, double-click **Allow third-party browser extensions** in the list to the right, and enable it.
3. Open the **User Configuration** node and perform the configurations described in step 2.

Creating rules for Windows Installer files

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Use the **By Path to Windows Installer** rule to elevate or decrease privileges for processes that start from Windows Installer files (`.msi`) and patches (`.msp`).

To create a By Path to Windows Installer rule using the Create Rule Wizard

1. Open the **Create Rule Wizard**. For more information, see Using the Create Rule Wizard.
2. Fill in the following fields:
    - **Name**: Set a path to an `.msi` or `.msp` file. Wildcards are supported and you can use **Browse** to locate the path.

      Optional:

        - **Publisher**: Limit Elevation to files signed with the digital certificate of a publisher. Enter the exact name or use **Browse** to locate it.
        - **Product Code**: Limit Elevation to those whose ProductCode MSI property match the one specified. Enter the exact name or use **Browse** to locate it.
        - **Product Version**: Limit Elevation to those whose ProductVersion MSI property match the one specified.
        - **File Hash**: Click **Browse** to locate the file and create a unique cryptographic hash that limits Elevation to files that match it. This ensures that the rule will not apply to dangerous content that is similarly named and will help prevent security issues.
        - **Apply settings to child processes**: Ensure that child processes triggered by the rule will not fail due to lack of privileges. This check box is enabled by default.
        - **User's context will be used to resolve system and resource access**: Ensure that the Client uses the target's user environment to resolve file and registry access. This might be required to resolve drive mappings, and also if the rule specifies the publisher, version, or file hash for the target process running from a network location.
3. Define whether the rule will be user-based or computer-based.

- **User Policy**: Select this option to apply the rule to the user logged into the computer. This option corresponds to the User Configuration node of the Group Policy Management Editor and is the default policy for all editions of Safeguard Privilege Manager for Windows.
- **Computer Policy**: Select this option to apply the rule to a computer regardless of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor.

  NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

4. Complete the **Privileges** (see Granting or denying privileges (Privilege Elevation Rules only)) and **Integrity** (see Differentiating security levels (Privilege Elevation Rules only)) tabs to modify the rule.
5. Click **Finish** to quit the wizard.
6. The rule will be named after the installer file or patch.

Creating rules for script files

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Use the **By Path to Script File** rule to elevate or decrease privileges for processes that start from a script file.

To create a By Path to Script File rule using the Create Rule Wizard

1. Open the **Create Rule Wizard**. For more information, see Using the Create Rule Wizard.
2. Set the absolute or relative path to one of the following types of script files:
   - **Command Prompt**: `.cmd`
   - **Batch File**: `.bat`
   - **JavaScript**: `.js`
   - **VBScript**: `.vbs`
   - **PowerShell**: `.ps1`
   - **Perl**: `.pl`

     TIP: You can use **Browse** to locate the path and wildcards are supported.
3. Fill in these optional fields, as necessary:
   - **Publisher**: Limit Elevation to files signed with the digital certificate of a publisher. Enter the exact name or use **Browse** to locate it.

     This field is not supported for `.pl`, `.cmd`, and `.bat` files.
   - **File Hash**: Click **Browse** to locate the file and create a unique cryptographic hash that limits Elevation to files that match it. This ensures that the rule will not apply to dangerous content that is similarly named and will help prevent security issues.
   - **Apply settings to child processes**: Ensure that child processes triggered by the rule will not fail due to lack of privileges. This check box is enabled by default.
   - **User's context will be used to resolve system and resource access**: Ensure that the Client uses the target's user environment to resolve file and registry access. This might be required to resolve drive mappings, and also if

the rule specifies the publisher, version, or file hash for the target process running from a network location.

4. Define whether the rule will be user-based or computer-based.
   - **User Policy**: Select this option to apply the rule to the user logged in to the computer. This option corresponds to the **User Configuration** node of the Group Policy Management Editor and is the default policy for all editions of Safeguard Privilege Manager for Windows.
   - **Computer Policy**: Select this option to apply the rule to a computer regardless of the user logged in. This option corresponds to the **Computer Configuration** node of the Group Policy Management Editor.

     NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.
5. Complete the **Privileges** (see Granting or denying privileges (Privilege Elevation Rules only)) and **Integrity** (see Differentiating security levels (Privilege Elevation Rules only)) tabs to modify the rule.
6. Click **Finish** to quit the wizard.
7. The rule will be named after the script file.

Using Active Directory user groups (Privilege Elevation Rules only)

Use the **Groups** tab to add or remove an Active Directory user group from the security token of the target process. Removing a group decreases the privileges with which the process will run.

To add or remove an Active Directory user group using the Groups tab in the Create Rule Wizard

1. If the Administrators group (stored within the `BUILTIN\Administrators` Active Directory OU) does not appear on the list by default, click to add it.
    - Select this group of users, who have complete and unrestricted access to a local computer, instead of domain administrators.
    - The button will not be active if the group is already on the list.
2. Use the button to add or remove other groups. When the window opens:
3. Click **Browse** to specify the group name.
4. Select **add or remove**.
5. To delete or modify a record within the **Security Group** list, select it and use the or button.
    - You can only add security groups in Active Directory which have a group scope property of Built-in local to the security token of a process on a client computer if the Client also has the same security identifier definition (SID) in its built-in security groups.
    - When removing a group from the security token, ensure that the user account under which the process is launched is a member of more than one primary group. Otherwise, the rule will not apply as intended.

Using Validation Logic

Detailed information about this topic

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

By default, a rule will apply to all client computers to which the previously selected GPO is linked. For more granular targeting, you can use the **Standard Rules** and **Validation Logic Rules** sub-tabs of the **Validation Logic** tab in the **Create Rule Wizard** to target the rule based on the client's operating system, their IP address, and/or a logged-in user.

Using standard rules

Within the **Standard Rules** sub-tab in the **Create Rule Wizard**, you can set a rule to apply only to clients with specified operating systems, servers, or workstations. By default, all operating systems are selected. If no options are selected, then the rule will apply to all supported operating systems.

To use the Standard Rules sub-tab in the Create Rule Wizard

- Select the **Server** check box in the **Class** section to apply the rule to your Windows Server installation.
- Select the **Workstation** check box in the **Class** section to apply the rule to Windows 10.
- In the **Operating System** section, select the check boxes for your operating systems.

Using Validation Logic rules

The **Validation Logic Rules** sub-tab in the **Create Rule Wizard** allows you to set additional parameters to target the rule. You can define whether the rule will run on computers with a prefix in the name, a group or IP address range, or a user currently logged in. For example, you can target the rule to computers belonging to OUs that end with `DEPARTMENT` and are in subnet `192.168.0.X`, except for the IP address `192.168.0.1`.

NOTE: Client Deployment Settings can only be targeted to specific computers and not to user accounts or groups.

Setting rule parameters

To set rule parameters using the Validation Logic Rules sub-tab in the Create Rule Wizard

1. Click **Add** to open the **Add Validation Logic Rule** window.
2. Select the type of rule:

Type of Rule	Action
 **Computer Group**	Set a rule for one or several names, or partial names, of your Active Directory computer groups. Enter the NetBIOS name, for example: `DERPA\DOMAIN CONTROLLERS`
 **User Group**	Set a rule for one or several names, or partial names, of your Active Directory user groups. The group membership value you enter will be compared against the groups that the user belongs to during the logon process and must match for the configuration to be processed. Enter the NetBIOS name, for example: `DERPA\ADMINISTRATORS`
 **User Name**	Set a rule if specific users are logged into client computers. Enter the NetBIOS name, for example: `DERPA\HELPDESK`
	Set a rule for names, or partial names, of computer-based OUs or the Computers container in your Active Directory.

Type of Rule	Action
OU (Computer)	The OU value you enter will be compared against the OU the client computer belongs to during the logon process and must match for the configuration to be processed. Enter the fully qualified domain name (FQDN), for example: `DERPA.DERPADEV.LOCAL\DOMAIN CONTROLLERS` • To select OUs, select the **OU** checkboxes. • To select all containers (instead of OUs), select the domain so that it is highlighted. • To include child objects, highlight the parent object and check **Include child objects**.
 **OU (User)**	Set a rule for names or partial names of the user-based OUs or the Users container in your Active Directory. The OU value you enter will be compared against the OU the user belongs to during the logon process and must match for the configuration to be processed. Enter the FQDN, for example: `DERPA.DERPADEV.LOCAL\USER ACCOUNTS` • To select OUs, select the **OU** checkboxes. • To select all containers (instead of OUs), select the domain so that it is highlighted. • To include child objects, highlight the parent object and check **Include child objects**.
 **Computer Name**	Set a rule for computers with names or partial names. Enter the FQDN, for example: `DERPA.DERPADEV.LOCAL\PASERVER`
 **IP Address Range (v4/v6)**	Set a rule for IP addresses or ranges of computers.
 **Registry Key Exists**	Set a rule based on the registry keys on client computers.
 **File Exists**	Set a rule for files on the client computer or on the network. Specify a file that must exist on the client computer or on the network in order for the rule to run, for example:

Type of Rule	Action

	`\\ComputerName\SharedFolder\Filename.exe`
	`DriveLetter:\Filename.exe`
	NOTE: On the **Type** tab of the **Create Rule Wizard**, check the **User's context will be used to resolve system and resource access** check box to ensure that the rule will apply.

 **Date and Time Range**	Define when a rule should start and/or stop being enforced. Select the check boxes before the **date** and/or **time** fields in the **Date Range** / **Time Range** sections. In the **Date Range** and **Time Range** sections: 1. Set the values. 2. The rule will apply according to the time/date parameters of the Console used to create the rule.

User's context will be used to resolve system and resource access to ensure that the rule will apply.

1. Specify the rule's parameters in the dialog window that will display on the right:
   - Use the common asterisk (`*`) and question mark (`?`) wildcards in the **validation value**, as necessary.
     - `*` : Stands for no or any number of any characters
     - `?` : Stands for a single character
   - Check the **NOT** check box to exclude the items specified from the rule.
   - For **Computer Group**, **User Group**, **User Name**, **OU (Computer)**, **OU (User)**, and **Computer Name** use one of the following options:
     - Use the **Name** field to specify the rule's value manually (see example values in the table above), and then click the button.
     - Use the **Browse** button to select the items available on your network. You can filter the items by the first letters. Wildcards are not supported in the **Filter** field.

     The desired value will be added to the list. You may add as many rule values as necessary.
2. Click **OK** when you are finished specifying the settings within the rule type. The record will display in the main **Validation Logic Rules** list.
3. To add another Validation Logic rule, repeat the steps above.
4. Add or combine Validation Logic rules with `AND` or `OR` Boolean logic. By default, rules will combine with `OR` Boolean logic. To make the rule use the `AND` operator, select

AND at the bottom of the **Validation Logic Rules** window.

5. To edit a rule setting:
    a. Within the **Validation Logic Rules** list, double-click a rule value or click **Edit**.
    b. Make changes in the dialog.
6. When finished specifying Validation Logic rules, click **Next**. If the **Display Advanced Options** check box has not been selected, complete the rule creation process.

Granting or denying privileges (Privilege Elevation Rules only)

On the **Privileges** tab in the **Create Rule Wizard** you can grant or deny privileges for a process, based on the standard Windows policies in the **User Rights Assignment** list (`Local Security Settings\Local Policies`).

To grant or deny privileges for processes (including child processes) using the Privileges tab in the Create Rule Wizard:

1. Select the privilege and click **Grant** or **Deny**. To select multiple privileges, hold down the `CTRL` (or `SHIFT`) key while selecting the items.
2. To discard your choices, select the privilege and click **Not Set**.

Differentiating security levels (Privilege Elevation Rules only)

You can differentiate the security levels with which a process will run using the **Integrity** tab in the **Create Rule Wizard**. The integrity level is a feature of Windows operating systems.

This parameter can be applied to clients running any of the following operating systems:

- Windows Server 2012 or newer.
- Windows 10 or newer.

By default, this setting will not apply and is set to the **`High`** integrity level.

Managing rules

Detailed information about this topic

Once a rule is created, you can:

- change its settings,
- delete it,
- import it, and
- export it.

To delete, modify, or share a rule

- Use the applicable toolbar buttons.

To use the Edit Rule Wizard to configure a rule

1. Select the **Privilege Elevation Rules** or **Blacklist Rules** tab based on the type of rule to be created.
2. To open the **Edit Rule Wizard**, double-click a rule's title or click **Details** on the toolbar.
3. Specify the data requested in each tab and click **Next**.
    a. Follow the prompts through the default tabs:
        - **Description**
        - **Type**
        - **Groups**
        - **Validation Logic**

        NOTE: This option is available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

    The **Privileges** and **Integrity** tabs display as advanced options.

    b. Enter the required fields, marked with an asterisk '*' on the **Description** and **Type** tabs.
4. To save nd apply the rule, click **Finish**. If you did not specify the required data, the wizard notifies you.

5. Click the **Save** button on the menu bar of the **Rule** section. Or, if prompted, confirm that you want to save the rule.

More information for managing rules:

- To delete or modify a GPO created with Safeguard Privilege Manager for Windows, use the Microsoft Group Policy Management Console (**GPMC**). You can also edit rules using the **GPMC**. For more information, see Using the Group Policy Management Editor.
- If you are using Safeguard Privilege Manager for Windows Community Edition and open a rule with a Professional Edition feature to view or modify its settings, you will receive a notification. To open the **Edit Rule** window to display all the rule settings except for the Professional ones, click **Yes**.

  NOTE: Modifying the rule will discard its Professional features.

Import/Export Rules

Once rules are created for a GPO they can be exported in order to share the rules, copy the rules to another GPO or even for backup purposes.

To export rules

1. Select a GPO in the domain tree.
2. Right-click on the GPO name and select **Export Rules**.
3. Enter the path and file name of the export file to be created. Click **...** to select a path using File Explorer.
4. In the pop-up window that displays a count of the Privilege Elevation Rules and Blacklist Rules for the GPO, complete the following steps, as applicable:
    - To include the privilege elevation rules in the export, select **Export all Privilege Elevation Rules**.
    - To include the blacklisted rules in the export, select **Export all Blacklist Rules**.
5. To begin the export process, click **Export**.

To import rules

1. Select a GPO in the domain tree.
2. Right-click on the GPO name and select **Import Rules**.
3. Enter the path and file name of the file to be imported. Click **...** to select a path using File Explorer.
4. In the pop-up window that displays a count of the Privilege Elevation Rules and Blacklist Rules for the GPO, complete the following steps, as applicable:
    - Select **Import all Privilege Elevation Rules** to include those rules in the import.
    - Select **Import all Blacklist Rules** to include those rules in the import.
5. To begin the import process, click **Import**.

Testing rules

You can test a rule to ensure that the settings you specified map to a process on a local or remote computer. You can test all types of rules, except ActiveX.

Before you test a rule, ensure the following components are set up

1. The Client is running on the computer on which you intend to test the rule.
2. The remote computer is switched on and is accessible from the network.
3. The correct credentials to connect to the remote computer are provided.
4. The following exceptions are added for remote computers with a firewall turned on:
    - Windows Management Instrumentation (WMI): `dllhost.exe`
    - Host process for Windows services: `svchost.exe` for 32-bit OS and `%SystemRoot%\SysWOW64\svchost.exe` for 64-bit OS.

To test a rule

1. Within the **Group Policy Settings** section, select a rule, and click the **Test** button.
2. Select whether to test the rule on a local or remote computer.

   A test window appears and the test starts. The window displays the initial conditions necessary for the rule to run and present its status in the **Test Progress** section, testing if:
    - The connection with the target computer has been established;
    - The Client is installed on your computer;
    - The Group Policy update has run successfully on the client computer;
    - The GPO with the selected rule is present on the domain; and
    - The rule exists on the client side and on the domain.
3. If the test fails any of the steps, resolve the issue. If you encounter a `"Failed to retrieve processes. Please refer to documentation for more info"` error, complete the steps above before you test the rule.
4. Click **Next**.

5. When the **Detecting Process** window opens, manually run the process the rule applies to. Use the parameters specified in the **Rule Details** section of the Test File Rule window. The window shows two tabs:
    - The **Started Processes** tab with the processes started after you switched from the **Detecting Process** window.
        - The process that you start to test the will display with either a tick or a cross sign.
        - If the process is marked with the cross sign, look at **Process Details** and check that you started the process with the right parameters, or modify the rule settings.
    - The **All Processes** tab with all currently running processes.
6. When the rule is created and distributed to clients through Group Policy, the rule is applied to the corresponding process.

Removing local admin rights

Detailed information about this topic

The last step in preparing your environment for least privileged use is to remove administrative access from users who no longer require it.

Using the Active Directory Users and Computers utility

To scrub the Domain Administrators group of users that should no longer have administrative rights to every computer in the domain, use the native Active Directory Users and Computers utility of the supported Windows Server operating systems.

To remove users from the Domain Administrators group,

1. Select **Domain Admins Properties** > **Members tab** > **Remove**.
2. To discover users and domain groups with local administrator rights, click **Discover Accounts in local Administrator groups**.

   NOTE: By default, the search results will only include domain users and domain groups. However, you can optionally opt to include local and built-in (for informational purposes only) users.

Using the Users with Local Admin Rights screen

Available only in Safeguard Privilege Manager for Windows Professional Edition and Professional Evaluation Edition.

Under the **Discovery & Remediation** tab on the Console, select the **Users with Local Admin Rights** screen to discover which domain users have been assigned to the local Administrators group on client computers and remove them.

Before you begin, check the following on each target computer

1. The computer is turned on and accessible from the network; and
2. Windows Management Instrumentation (WMI), Distributed Component Object Model (DCOM), File and Printer Sharing, and Remote Administration are allowed through the firewall.

To remove domain users from the local Administrators group on computers on your domain

1. Within the **Select Computers** section, click **Add** and **Remove** to add and remove computers.
    - You cannot select a domain controller computer.
    - If the **File and Printer Sharing** exception is not enabled for a computer, it will not display in the list.
    - If the **Windows Management Instrumentation** exception is not enabled, the **Class** and **OS** columns will display the **Unavailable** value.
2. Click **Clear all entries** to remove all computers from the list.
3. Click **Discover Accounts in local Administrator groups** to discover users and domain groups with local administrator rights. By default, the search results will only include domain users and domain groups. However, you can optionally opt to include local and built-in (for informational purposes only) users.
4. In the window that opens, specify whether to search for local Administrator groups, users, or both.

5. Check the **Only display domain accounts discovered in the results list** option to restrict the search to Domain accounts only. Clear the option to include local accounts from the Administrators group on client machines.

   A window displays your progress as the list builds.

6. Complete the following steps.

   a. If an error occurs, it will display in the **Errors** section with a description. The **Unable to open log file...** notification signifies that no users in the local Administrators group have been detected.

   b. Click **Open report file** to view data on detected users. The button will not be activated if no users have been found in the local Administrators group.

   c. When the discovery operation is completed, click **Close**.

The list of discovered users will display in the **User Accounts Discovered in Local Administrators Groups** section.

1. Revise the list to only include users you are potentially going to revoke rights from then make your final selection from the remaining list.
2. Click the **Exclude selected entries from list** link to remove users from this list.
3. Select users from the remaining list, for which you want to revoke their local administrator rights.
4. Click **Remove all selected users from local Administrators groups**.
5. In the window that opens, click **Yes** to confirm that you want to remove the users or groups. A window displays your progress as the users are removed.
6. Complete the following steps:

   a. If an error occurs, it will display in the Errors section with a description.

   b. Click **Open report file** to view the operation log.

   a. When the operation is complete, the users no longer have local administrator rights.

1

Reporting

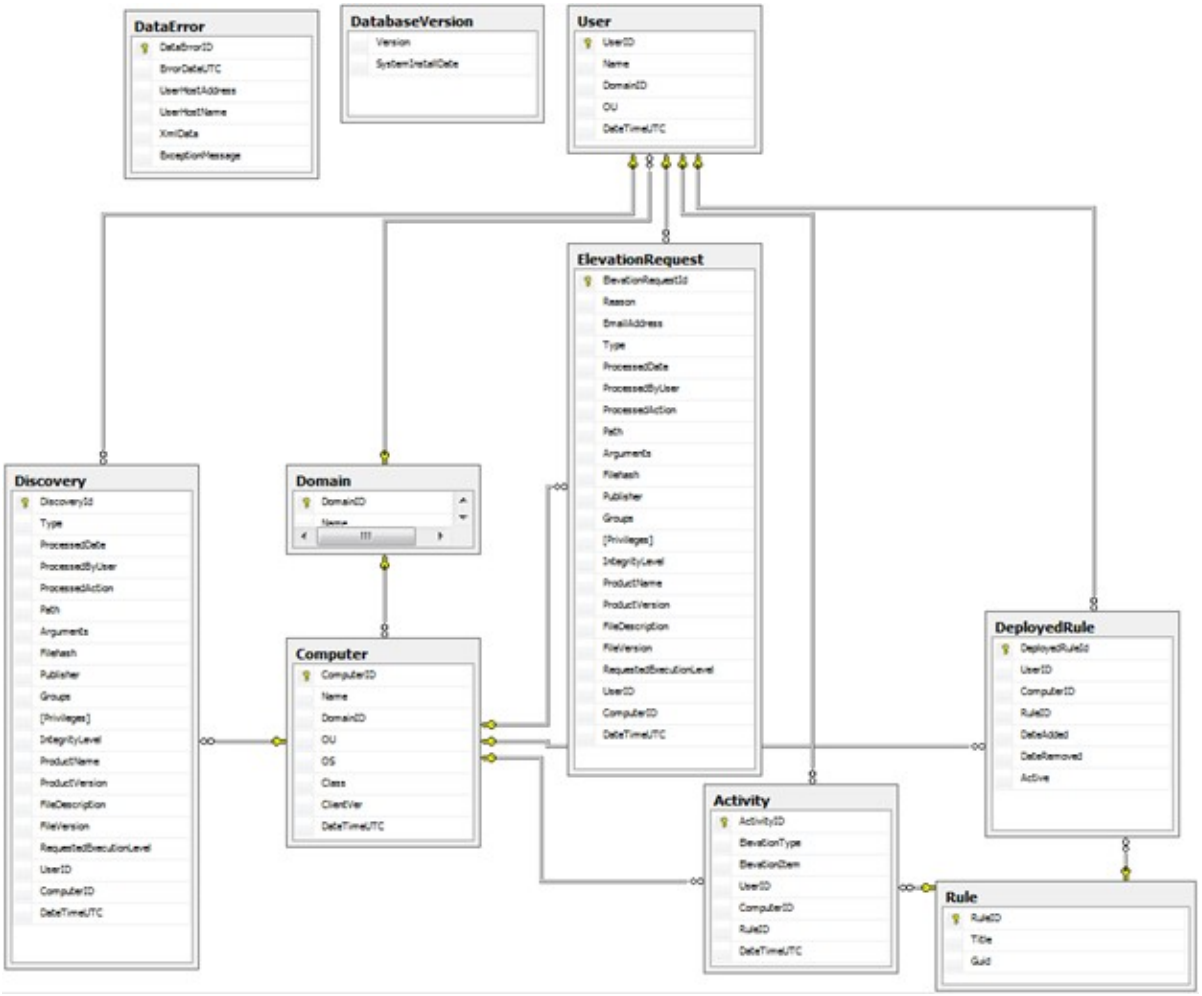
Reporting is available only in Safeguard Privilege Manager for Windows Professional Edition or an active Professional Evaluation Edition. Once your trial evaluation license expires, reporting no longer collects data, and no longer generates reports.

Detailed information about this topic

You can build five types of reports on activities from client computers:

- Blacklist Activity Report: Lists how frequently a rule is used.
- Rule Deployment Report: Lists rules deployed on the client computer.
- Instant Elevation Report: Lists processes that are elevated using Instant Elevation.
- Rule Details Report: Lists rules that are configured.
- Advanced Policy Settings Report: Lists Advanced Policy Settings, except those set to the **Not Configured** option.

  In addition to these out of the box reports, you can create custom reports using third-party tools to query the SQL-based Safeguard Privilege Manager for Windows reporting database. Use this database schema to create your own custom reports or data analysis:



A **PAReporting database** is created when you set up the server and is configured to work with the ScriptLogic PA Reporting Service, the data collection web service running on a Console host.

Before you generate reports, ensure the following components are set up

1. The Server is configured and you can successfully join the data collection web service running on it.
2. Client data collection settings are configured for the GPOs you will report on. You can generate reports on GPOs for which you have read/write access in Windows.

To learn how to create this type of report and manage the data, see Generating and using reports.

Elevation Activity Report

This report allows you to track which rules were used to elevate processes during a period of time on managed client computers. With this report, you can see when users have run privileged processes and on which computers.

Each privilege Elevation event reported contains these details:

- **Type**: The privilege Elevation rule type.
- **Elevated Item**: The path to the elevated application or command with the argument (if any).
- **Rule Name**: The privilege Elevation rule name.
- **Rule GUID**: The privilege Elevation rule globally unique identifier (GUID).
- **User (Domain\Name\OU)**: The user, domain name, and OU.
- **Computer (Domain\Name\OU\Class\OS)**: The computer, domain name, OU, class, and OS.
- **Elevation Time**: The time of the privilege Elevation on the client computer.

To learn how to create this type of report and manage the data, see Generating and using reports.

Blacklist Activity Report

This report allows you to track which rules were used to Blacklist processes during a period of time on managed client computers. With this report, you can see when users have attempted to run blacklisted processes and on which computers.

Each Blacklist event reported contains these details:

- **Type**: The privilege Elevation rule type.
- **Blacklisted Item**: The path to the blacklisted application or command with the argument (if any).
- **Rule Name**: The privilege Elevation rule name.
- **Rule GUID**: The privilege Elevation rule globally unique identifier (GUID).
- **User (Domain\Name\OU)**: The user, domain name, and OU.
- **Computer (Domain\Name\OU\Class\OS)**: The computer, domain name, OU, class, and OS.
- **Blacklisted Time**: The time of the blacklisted event on the client computer.

To learn how to create this type of report and manage the data, see Generating and using reports.

Rule Deployment Report

This report tracks the overall usage of privilege Elevation rules across a domain. The report lists each rule, showing how many clients it has been deployed to and how many times it is used.

Each record about a deployed rule contains these details:

- **Rule Name**: The privilege Elevation rule name.
- **Rule GUID**: The privilege Elevation rule globally unique identifier (GUID).
- For a Summary report:
  - **# Comp**: The number of client computers on which the rule is deployed.
  - **# Used**: The number of times the rule has been enforced.
- For a Details report:
  - **User (Domain\Name\OU)**: The user, domain name, and OU.
  - **Computer (Domain\Name\OU\Class\OS)**: The computer, domain name, OU, class, and OS.
  - **Deployed Date**: The date the rule was deployed on the client computer.

Instant Elevation Report

This report allows you to track Instant Elevation activity during a period of time on managed client computers. With this report, you can see when users have been granted Instant Elevation privileges and on which computers.

Each privilege Elevation event reported contains these details:

- **Type**: The privilege Elevation rule type.
- **Elevated Item**: The path to the elevated application or command with the argument (if any).
- **Rule Name**: The privilege Elevation rule name.
- **Rule GUID**: The privilege Elevation rule globally unique identifier (GUID).
- **User (Domain\Name\OU)**: The user, domain name, and OU.
- **Computer (Domain\Name\OU\Class\OS)**: The computer, domain name, OU, class, and OS.
- **Elevation Time**: The time of the privilege Elevation on the client computer.

To learn how to create this type of report and manage the data, see Generating and using reports.

Temporary Session Elevation Request Report

This report allows you to track Temporary Session Elevation passcode requests from managed client computers. With this report, you can see when a passcode has been generated based on a request, if the request was denied, or if the request is still pending review.

The Temporary Session Elevation Request report contains these details:

- **User (Domain\Name)**: The user that used the passcode on their machine.
- **Action**: The state of the Elevation request. This can be:
  - **Pending** (when a request is received),
  - **Granted** (when a passcode is generated for the request) or
  - **Denied** (when a passcode request is not granted).
- **Processed Date**: The date the administrator responded to the request.
- **Reason**: The reason given for the Elevation request.
- **Maximum Allowed Usage**: The number of times the passcode can be used before expiring.
- **Duration**: The amount of time the passcode remains active for when used.
- **Computer (Domain\Name)**: The computer that the passcode is requested from.
- **Request Sent**: The date and time the user submits the request for a passcode.

To learn how to create this type of report and manage the data, see Generating and using reports.

Temporary Session Elevation Usage Report

This report allows you to track Temporary Session Elevation activity during a period of time on managed client computers. With this report, you can see when users are granted temporary Instant Elevation privileges using passcodes, on which computers, and also which specific applications were elevated.

The Temporary Session Elevation Usage report contains these details:

- **User (Domain\Name)**: The user that used the passcode on their machine.
- **Maximum Allowed Usage**: The number of times the passcode can be used before expiring.
- **Remaining Usage**: The number of times that are left to use this passcode.
- **Usage Count**: The number of times this passcode is used so far.
- **Elevated Item**: The application that was run in an elevated state.
- **Computer (Domain\Name)**: The computer that the passcode was used on.
- **Time Elevated**: The date and time the Elevation occurred.
- **Passcode ID**: The exact passcode provided by the administrator.

Rule Details Report

This report lists all the configuration details for a rule in a single view. The details for each privilege Elevation event are specified in the Create Rules Wizard. For more information, see Using the Generate Rules Wizard.

To learn how to create this type of report and manage the data, see Generating and using reports.

Advanced Policy Settings Report

This report lists all configuration details, except those set to the **Not Configured** option, of the **Advanced Policy Settings** for your GPOs in a single view:

- **Client Data Collection Settings**
- **Client Deployment Settings**
- **Self-Service Elevation Request Settings**
- **Privileged Application Discovery Settings**
- **Instant Elevation Settings**

The details for each privilege Elevation event are specified in the corresponding section for each of the settings. To learn how to create this type of report and manage the data, see Generating and using reports.

Generating and using reports

To generate a report

1. Under the **Reporting** section of the Console, select the type of report. The window for the report will open to the right.
2. Click **Generate Report** to generate a report based on the default filter settings displayed in the **Applied Filters** section on the top of the screen. You can create multiple shared filter sets and save settings that other administrators can use. For more information, see Using the Applied Filters Wizard.
3.  Use the toolbar next to the **Applied Filters** drop-down menu to add, edit, copy, or delete a filter.

   The results appear below.
4. For the Rule Deployment report, use the **Type** and **Sort** menus to view additional information and sort data.
5. To navigate the pages or organize them and search for data, use the toolbar at the top of the results window:

6. To navigate across a multi-page report, use the  and  buttons.
7. The **Number of Records** field in the upper part of the results page refers to the number of rules listed in the report.

To save the data, use either of the following methods on the results window:

- Using the **Copy** button
  1. Click anywhere on the results window.
  2. Click **Copy**.
  3. Paste the copied data into a file.
- Using the **Export To** button
  1. To save the data into a `PDF`, `Excel`, `HTML`, or `RTF` file, in the toolbar of the of the results window, click **Export To PDF**, **Export To Excel**, **Export To Html**, or **Export To RTF** .

2. In the **Save As** window that appears, name the report.
3. Click **Save**.

Using the Applied Filters Wizard

To use the Applied Filters Wizard to modify displayed requests and save shared filters for other administrators

1. Open the Console and select the area for your shared filter set by completing one of the following steps:
   - Under the **Reporting** section, open the screen for **Elevation Activity**, **Rule Deployment**, **Instant Elevations**, **Rule Details**, or **Advanced Policy Settings**, or
   - Under the **Discovery and Remediation** section, open the screen for **Privileged Application Discovery** or **Self-Service Elevation Requests**.

   The **Applied Filters** section appears on the top of the screen.
2.  Use the toolbar next to the **Applied Filters** drop-down menu to add, edit, copy, or delete a filter.

   The **Applied Filters Wizard** appears when you add a filter.
3. Complete the following steps:
   a. Enter a name for your filter set.
   b. Select a filter type in the left section.
   c. Set the desired parameters in the right section.
   d. Press **Reset** to reset to the default screen, **OK** to save your settings, or **Cancel** to close the screen.
      i. You can create multiple shared filter sets and save settings that other administrators can use.

      When you select a filter type, it is saved automatically and you can proceed to another modification. Select as many filter types as necessary by switching between them and configuring settings.

   NOTE: Each filter type can have only one value specified. Every time you set a new value for the same filter type, the newer one overwrites the older one.
4. When finished, click **OK** to save your changes.

   The specified filter values appear in the **Applied Filters** list.

Using the Scheduled Reports Details Wizard

After you create a shared filter set to modify your report criteria, you can select a report and set its schedule and delivery. You can configure it to go to multiple recipients, including you, your manager, and/or the help desk. In addition, you can set the subject line to meet the requirements of your help desk. You can also specify network and file share locations to send it to.

To use the Scheduled Reports Details Wizard to generate a scheduled report

1. Configure the Server.
    a. Use the **Privilege Manager Server Setup Wizard** to configure the **Server Email Notification Configuration** settings on the first screen of the wizard.
    b. If you previously completed the wizard, the remaining screens are automatically populated.
    c. Refer to the *Safeguard Privilege Manager for Windows Quick Start Guide* for step-by-step instructions.
2. Create shared filter sets to modify your report criteria. You must create at least one shared filter set to generate a scheduled report. Scheduled reports work only for shared filter sets configured in the **Reporting** tab (except for the built-in Local Filters), not in **Discovery & Remediation**. For more information, see Using the Applied Filters Wizard.
3. In the **Reporting** section of the navigation pane, select **Scheduled Reports**. The **Scheduled Reports** section appears on the top of the screen.
4. Complete the following steps:
    a. Click **Refresh** to refresh the screen and update the last run time.
5.  Use the toolbar to add, edit, copy, or delete a report.
6. The **Scheduled Reports Details Wizard** will open when you add a report.
7. Complete the **Type** tab and click **Next**.
8. Complete the **Schedule** tab.

a. Select the **Start time**.

b. Select the **Cycle** for how often the report will run. Changes to scheduled reports may take up to 10 minutes to take effect.

c. Click **Next**.

9. Complete one of the sub-tabs under the **Delivery** tab.

a. Complete the **Email** sub-tab.

Or,

1. Use the ✚ button to add email addresses and the ✘ button to remove them.
2. Enter a subject.
3. Select the report format.
4. Complete the **File share** sub-tab.

a. Type the folder path in the following format: `\\ComputerName\SharedFolder`

b. Use the **Browse** button to locate the folder.

5. Use the ✚ button to add folder paths and the ✘ button to remove them.
6. Select the report format.
7. Click **Finish**.
8. After the report is created, check your email or file share to confirm receipt.

Using the Resultant Set of Policy Wizard

The Resultant Set of Policy (RSoP) Wizard is a built-in MMC snap-in. It helps you view policy settings applied to selected computers and users (in logging mode), or simulate a policy implementation to plan changes to your network (in planning mode). You have to enable .NET Framework 3.5 with the **Turn Windows features on or off** dialog or the PM Console installed in order to view the values of the RSoP Wizard.

NOTE: You might have to restart your computer after enabling .NET Framework 3.5.

To use the Resultant Set of Policy Wizard to report on policies you have applied

1. Install the Client on the computer for which you are viewing or simulating a policy.
2. Open the MMC. On the **Start** menu, click **Run**, type `MMC`, and then click **OK**.
3. From the **File** menu, select **Add/Remove Snap-in**. The **Add or Remove Snap-ins** dialog appears.
    a. Select **Resultant Set of Policy** under the list of snap-ins.
    b. Click **Add**.
    c. Click **OK**.
4. The **Console Root** window now has a snap-in, **Resultant Set of Policy**, rooted at the Console Root folder.
5. Under the **Name** column, click **Resultant Set of Policy**.
6. Complete one of the following steps:
    a. Right-click **Resultant Set of Policy** and select **Generate RSoP Data**.
    b. Under the **Resultant Set of Policy** pane in the **Actions** column, click **More Actions** and select **Generate RSoP Data**.

    The Resultant Set of Policy Wizard appears.
7. Complete the following steps:
    a. Choose the **Logging mode** to review policy settings or the **Planning mode** to simulate a policy implementation.
    b. Specify the data requested in each tab and click **Next**.
    c. Click **Finish** to quit the wizard.

The **Console Root** window now has **Privilege Manager for Windows** nodes, rooted at the **Console Root** folder under **Computer Configuration** and **User Configuration**. **Privilege Manager for Windows Details** appears on the right, showing the rules and advanced policy settings that are applied.

Client-side UI customization

Detailed information about this topic

Safeguard Privilege Manager for Windows supports the text customization of all user-facing dialogs on client computers. In addition to the ability to change the default English dialog text, admins can also create client-side UI customization files for any non-English client language locale.

Language translation files

To customize the language used in the client-side UI, one or more translation files must be located in the same folder where the client files are installed, by default: `C:\Program Files (x86)\Common Files\One Identity\Safeguard Privilege Manager for Windows\Client`.

A language-specific translation file must be named as follows: `<two_letter_language_code>-pmlang.ini`

Example:

- Spanish translation language file name: `es-pmlang.ini`
- English translation language file name: `en-pmlang.ini` (used to customize client computers with English locale)
- French translation language file name: `fr-pmlang.ini`

NOTE: The `en-pmlang.ini` file is used. For information on language translation files currently available for download, as well as configuration and troubleshooting tips, see Knowledge Base Article Safeguard Privilege Manager for Windows User Interface Language Translation (4228235).

Safeguard Privilege Manager for Windows automatically searches for the language translation file corresponding to the language local setting on a client computer. If no translation file is found, default English client-side text strings are used.

A specific language translation file can be used regardless of the Window's local settings with the use of a registry setting.

- **Hive**: `HKCU\Software\Scriptlogic Corporation\Privilege Authority`
- **Key**: Preferred Language
- **Type**: REG_SZ
- **Value**: name of language file, for example, `es-pmlang.ini`

  The corresponding translation file must exist as described above.

In addition to checking locally on the client computer for language translation files, the Safeguard Privilege Manager for Windows Client automatically copies (and overwrites older, already existing) language files found on the NETLOGON share.

NOTE: NETLOGON is checked for updated language files every time a user logs on to a computer.

Additionally, Administrators can configure the Safeguard Privilege Manager for Windows Client to check an alternate location for updated language translation files. This can be done by updating the **`TranslationFilesFolder`** value `in HKLM\Software\Scriptlogic Corporation\Privilege Authority`.

3

Using Microsoft tools

You can use Microsoft tools with Safeguard Privilege Manager for Windows to:

- Install the Client using the Group Policy Management Console.

  For more information, see Using the Group Policy Management Console.
- Create and manage rules using the Group Policy Management Editor in the Group Policy Management Console.

  For more information, see Using the Group Policy Management Editor.
- Remove local administrator rights using the Active Directory Users and Computers Utility.

  For more information, see Using the Active Directory Users and Computers utility.
- Report on policies you have applied using the Resultant Set of Policy Wizard.

  For more information, see Using the Resultant Set of Policy Wizard.

Maintaining a least privileged use environment

Detailed information about this topic

Maintain a least privileged use environment by processing Self-Service Elevation requests, using the **Console Email Configuration** screen, and using group policy settings.

Processing Self-Service Elevation Requests

Detailed information about this topic

Monitor and process Self-Service requests from users using **Self-Service Notifications** and the **Self-Service Elevation Requests** screen under the **Discovery & Remediation** tab. You can approve or deny requests for access to run privileged applications. If approved, an Elevation rule is automatically generated for each request. For more information, see Using Self-Service Notifications and Using the Self-Service Elevation Request Processing Wizard.

Using the Console Email Configuration screen

If you want Safeguard Privilege Manager for Windows to send an email message to the user after approving or denying their Self-Service Elevation request, configure the settings using the **Setup Tasks** > **Console Email Configuration** screen.

To configure the Server to send your Self-Service Elevation request approval or refusal:

1. Select **Console Email Configuration** from the **Setup Tasks** section.
2. Configure the following fields:
    a. **Host Name**: Enter the SMTP Server name of the email account from which you are going to send your emails.
    b. **SMTP Port**: Enter the port number.
    c. **SMTP User Name and Password**: If necessary, enter the authentication information and check the SSL check box.
    d. **From Email**: Enter the corresponding email.
3. Click **Send Test Email** to send an email to the account specified in the **From Email** field.
    a. If Safeguard Privilege Manager for Windows succeeds in sending the email, the corresponding message appears.
    b. Log into an email program with the corresponding account and locate the sent email folder, with **Privilege Manager Test Email** in the subject.
4. Click **OK** to save the settings and quit.

Using Group Policy Settings

Use the **Group Policy Settings** screens to create custom Elevation rules or modify existing ones for your environment. The **Advanced Policy Settings** tab can also be used to modify the settings for advanced features at the GPO level. These features include **Client deployment settings**, **Client data collection settings**, **Instant Elevation settings**, **Self-Service Elevation request settings**, and **Privileged application discovery settings**.

Database Planning

Detailed information about this topic

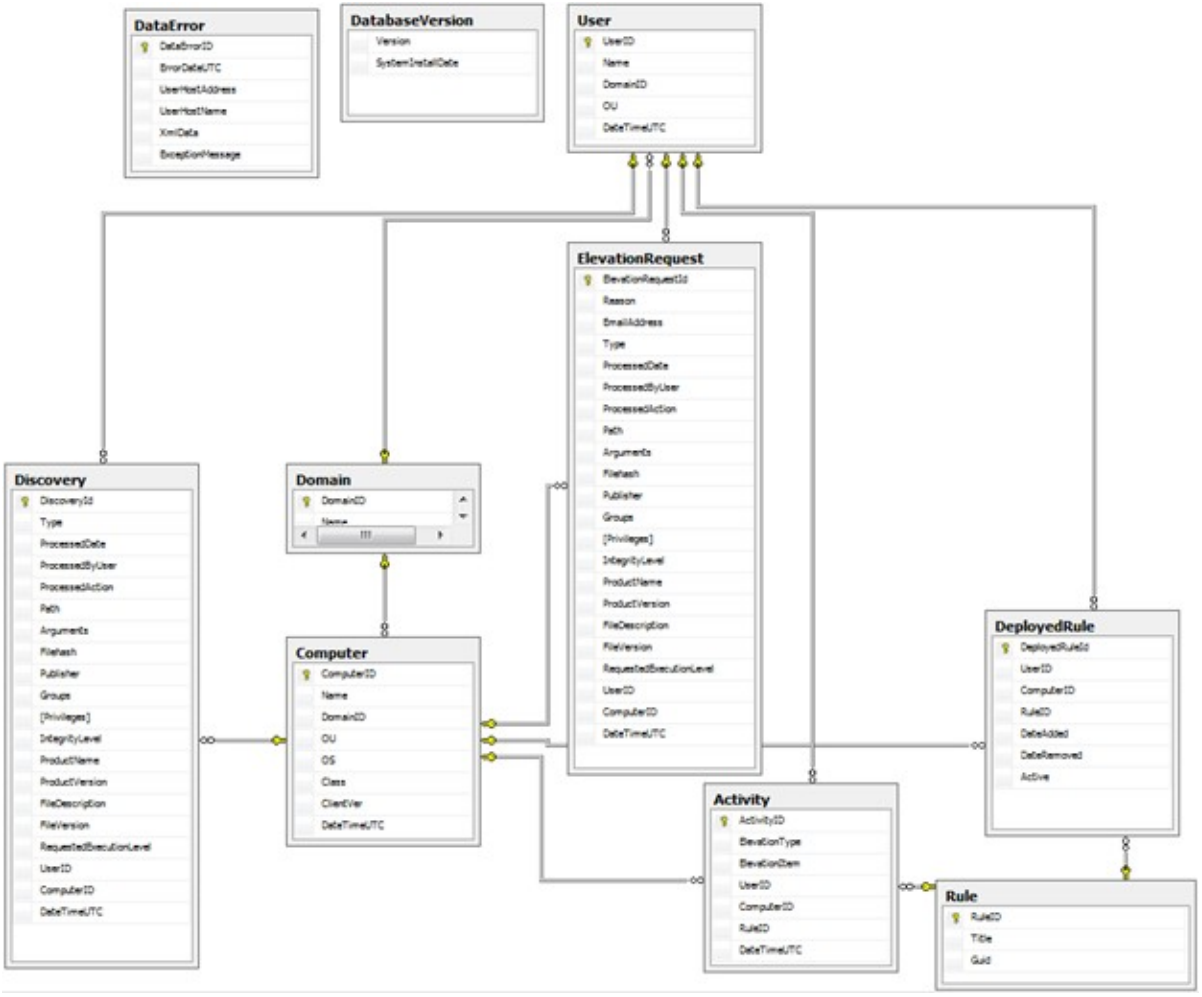
The goal of this topic is to proactively manage disk capacity as it relates to Safeguard Privilege Manager for Windows. The capacity planning information provided here contains steps to help understand, install, and configure the Safeguard Privilege Manager for Windows database environment.

Eighty percent of database issues deal with disk capacity problems and in many cases, they are caused by failure to adhere to best practices. Failure to adhere to best practices should never happen as these issues are very predictable and could be prevented with a comprehensive database plan.

This section gives you a breakdown of the Safeguard Privilege Manager for Windows database structure to better understand the database environment and walks through capacity planning best practices to minimize the risk of disk over- utilization.

Safeguard Privilege Manager for Windows Database Diagram

Figure 2: Safeguard Privilege Manager for Windows Database Diagram



Users	Database size	Initial size
1	4.7 MB	9.4 MB
10	10.5 MB	21.0 MB
100	73.0 MB	146.0 MB
1,000	692.6 MB	1385.2 MB
2,000	1,378.6 MB	2,757.2 MB
5,000	3,439.9 MB	6,879.8 MB
10,000	6,876.4 MB	13,752.8 MB
15,000	10,313.0 MB	21,626.0 MB
20,000	13,749.5 MB	27,498.0 MB
50,000	34,368.8 MB	68,736.0 MB
100,000	68,734.2 MB	137,468.4 MB

Safeguard Privilege Manager for Windows Tables

Table Name	Description
Activity	Contains rule and Instant Elevation activity. Includes Elevation type and item.
Computer	Contains client computer information such as its name, domain, class, Organizational Unit, operating system and the version of Safeguard Privilege Manager for Windows installed.
Database	Contains the database version of the Safeguard Privilege Manager for Windows database.
DataError	Contains database exceptions and includes exception messages, host address, host name and the XML data document that caused the exception.
DeployedRules	Every time a new rule is deployed, a record is created for every user associated with this rule. This keeps track of all deployed rules, assigning the rules a status (active | inactive), and tracks date (added | removed).
Discovery	Contains information on any process that starts or fails to start on a client computer. Data stored here includes the product name and requested execution level. It is used by the Privileged Application Discovery component.
Domain	Contains records of the network domains.
ElevationRequest	Contains Elevation requests made on the client, including information about the name of products the request is being made for and the reason for the request.
Reports_ Scheduled	Contains records of the scheduled reports to be generated.
SharedFilters	All shared filters created.
Rules	Rules created and saved in the Safeguard Privilege Manager for Windows Console.

Table Name	Description
Users	Users who have logged into a Safeguard Privilege Manager for Windows Client machine.

Data Storage Estimates

Table 1: Table size estimate for one Safeguard Privilege Manager for Windows user

Table Name	Number of Rows	Byte Size per Row	Total Size (bytes)
Activity	1,000	4,222.68	422,268.00
Computer	1	84.38	84.38
DatabaseVersion	1	72.09	72.09
DataError	20	8,834.25	176,685.00
DeployedRules	20	49.15	983
Discovery	30	3,8049.23	1,141,476.9
Domain	1	84.38	84.38
ElevationRequest	20	54,540.61	1,090,812.2
Reports_ Scheduled	10	4,575.25	45,752.50
Reports_ SharedFiles	10	9,436.70	94,367.0
Rule	20	304.99	6,099.8
User	1	4,443.48	4,443.48
Total Size 4,683,128.73 bytes			

As the number of users grow, some tables increase in size more rapidly than others. For this reason, the database size does not grow proportionately.

Database size calculation uses the following rules:

1. The **Activity** table generates one thousand records per user.
2. The number of Computer records are equal to the number of user records.
3. 20 reports represent one user.

4. The **DatabaseVersion** table should be one record irrespective of the number of user in the environment.
5. The **DataError** table is estimated to be twenty records to one user.
6. The **DeployedRules** table should generate twenty records per one user.
7. The **Discovery table** should generate roughly thirty records per user.
8. The number of **Domain** table records are set to one per user.
9. Twenty **ElevationRequest** records are generated per user.
10. There are ten **Reports_Scheduled** records per user.
11. There are ten **Reports_SharedFilters** per user.
12. Twenty **Rule** records are generated per user.
13. One user record exists in the **User** table per user.

Table 2: Database size for multiple users

Users	Database size
1	4.7 MB
10	10.5 MB
100	73.0 MB
1,000	692.6 MB
2,000	1,378.6 MB
5,000	3,439.9 MB
10,000	6,876.4 MB
15,000	10,313.0 MB
20,000	13,749.5 MB
50,000	34,368.8 MB
100,000	68,734.2 MB

Database hardware and software requirements

One Identity recommends installing the full SQL Server version for databases above 6876.4 MB or 10,000 users. For databases below 6,000 MB, you can install SQL Server Express, and can later upgrade to the full version of SQL Server in case of a database growth. For more information on how database sizes relate to the number of users in the database environment, see the following table.

NOTE: SQL Server Express databases have a size capacity limit of 10,000 MB.

Also, when selecting the SQL Server version, consider that certain SQL Server installations may not be able to take advantage of the available processing power and memory storage.

Table 3: Maximum database size, compute capacity, and maximum memory of different SQL Server installations

	Enterprise	Standard	Web	Express
Maximum database size	524 PB	524 PB	524 PB	10 GB
Compute Capacity	OS Max	4 sockets or 24 cores	4 sockets or 16 cores	1 socket or 4 cores
Maximum Memory	OS Max	128 GB	64 GB	1 GB

Table 4: Recommended SQL Server versions for various Safeguard Privilege Manager for Windows environment sizes

Users	Database size	Recommended SQL Server version
1	4.7 MB	SQL Server Express
10	10.5 MB	SQL Server Express
100	73.0 MB	SQL Server Express
1,000	692.6 MB	SQL Server Express
2,000	1,378.6 MB	SQL Server Express
5,000	3,439.9 MB	SQL Server Express

Users	Database size	Recommended SQL Server version
10,000	6,876.4 MB	SQL Server Express
15,000	10,313.0 MB	SQL Server
20,000	13,749.5 MB	SQL Server
50,000	34,368.8 MB	SQL Server
100,000	68,734.2 MB	SQL Server

Auto-Growth

Safeguard Privilege Manager for Windows uses the default auto-growth configuration settings that comes installed on SQL Server. This setting sets the initial database size of SQL Server to 3 MB, then grows it by 1 MB every time the data limit is exceeded. The log file starts at 2 MB and is set to grow by 10% increments until the disk is full.

Even though the default auto-growth configuration settings work for Safeguard Privilege Manager for Windows, it may not be the most appropriate configuration for all environments (especially for customers exceeding 10,000 users).

Every time the database grows it takes a performance hit. In SQL Server storage terms, 1024 KB is 128 pages. These pages are stored in 8 KB blocks. For Safeguard Privilege Manager for Windows, which is going to potentially load millions of records, growing the data file of a database every 128 pages may result in a large performance hit, especially since SQL Server I/O requests are a major bottleneck.

Additionally, since auto-growth allocates chunks of data at a time it is easier for the database to become fragmented. With that in mind it is recommended to update the auto-growth settings.

The table below displays the recommended settings based on the size of the network environment. These values are not set in stone but are based on database growth rates of your specific environment. The rule of thumb is to set this value to one eight of the estimated database size. Ideally you should use auto-grow as a fail/safe parameter, and use alerts or monitoring programs to monitor file sizes and grow files proactively. This helps you avoid fragmentation and permits you to shift these maintenance activities to non-peak hours.

Table 5: Auto-growth recommendation for various Safeguard Privilege Manager for Windows environment sizes

Users	Database size	Auto-growth
1	4.7 MB	1 MB
10	10.5 MB	1.3 MB
100	73.0 MB	9.1 MB
1,000	692.6 MB	86.5 MB

Users	Database size	Auto-growth
2,000	1,378.6 MB	172.3 MB
5,000	3,439.9 MB	429.9 MB
10,000	6,876.4 MB	859.5 MB
15,000	10,313.0 MB	1289.1 MB
20,000	13,749.5 MB	1718.7 MB
50,000	34,368.8 MB	4296.1 MB
100,000	68,734.2 MB	8591.8 MB

How to change auto-growth on SQL Server 2022

NOTE: Steps may be slightly different for other supported versions of SQL Server.

To change the auto-growth settings:

1. Start **SQL Server Management Studio**.
2. Highlight, then right click the **PAReporting database** and navigate to Properties.
3. In the left Panel, select the **Files from the Database Properties** dialog. The **Properties** window will be used to change Auto-growth.
4. Identify the PAReporting name under **Logical Name** and change the Auto-growth based on table 5 above. In this example, we have set the auto-growth to `430MB` and a max size of unlimited and left the log file to grow my 10% to a limit of 20971252MB. 430 is roughly one eighth of the 3,439.9MB database size for the 5000-user environment.

Initial database size

When Safeguard Privilege Manager for Windows is installed, it uses the default file and log sizes specified by SQL Server. The default file size is 3 MB for the database and 2 MB for the database logs.

NOTE: Consider that once these files exceed the initial file size settings, further file size increases may result in data fragmentation in the disk, and corresponding performance issues.

To prevent such performance issues, scale the log file sizes accordingly. For example, if the database is expected to grow to a specific size in a month, One Identity recommends that you take the expected value, double it, then use the doubled value for the initial size.

For example, if the database is expected to grow to 2,000 MB in a month, set the initial database size to 4,000 MB. This will reduce the number of auto-growths and reduce fragmentation, as a larger allocation means that more database-related information can be accessed from the same disk location. The following table breaks down the recommended initial size for the database based on a range of 1 to 100,000 users for the different database size estimations.

Table 6: Initial size recommendation for different Safeguard Privilege Manager for Windows environment sizes

Users	Database size	Initial size
1	4.7 MB	9.4 MB
10	10.5 MB	21.0 MB
100	73.0 MB	146.0 MB
1,000	692.6 MB	1385.2 MB
2,000	1,378.6 MB	2,757.2 MB
5,000	3,439.9 MB	6,879.8 MB
10,000	6,876.4 MB	13,752.8 MB
15,000	10,313.0 MB	21,626.0 MB
20,000	13,749.5 MB	27,498.0 MB

Users	Database size	Initial size
50,000	34,368.8 MB	68,736.0 MB
100,000	68,734.2 MB	137,468.4 MB

How to change the size on SQL Server 2022

NOTE: Steps may be slightly different for other supported versions of SQL Server.

To change the size settings

1. Start **SQL Server Management Studio**.
2. Highlight, then right click the **PAReporting database** and navigate to **Properties**.
3. In the left panel, select **Files** from the **Database Properties** dialog box. Use the **Properties** window to change the size.
4. Identify the **PAReporting** name under **Logical Name** and change the size. For example, you can set the **Size (MB)** to `13,752.8 MB`. This value is two times the size of the database. For more information, see Initial database size.

Product Improvement Program

To assist in the development of new features, as well as drive future improvements, we implemented a Product Improvement Program. Feedback from this program provides Product Management with valuable insight into how our products are being used. This information is essential to help the R&D team prioritize existing enhancement requests within the roadmap of each product. Participation is voluntary, and no personal contact information is ever collected.

Frequently asked questions

Detailed information about this topic

How do I participate in the Product Improvement Program? What if I change my mind?

There is an option in Safeguard Privilege Manager for Windows that can be used to verify or change your participation at any time. Select the **Help** menu and then click on **Product Improvement Program** to change your participation option.

How will the collected information be used?

Information collected will be used to develop new features and improve Safeguard Privilege Manager for Windows.

Where is the data being stored?

The data is stored on a secure server within the USA and will be accessed only by the members of the Safeguard Privilege Manager for Windows R&D team.

What information is collected?

- Safeguard Privilege Manager for Windows features usage data such as Console configuration settings
- System information such as operating system, processor, and memory installed
- Domain information such as number of users, servers, and workstations being managed
- Browser type and version
- Product information such as version
- License information such as type and number of seats

NOTE: The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) define a set of data protection and security measures that restrict access to personally identifiable information (PII). The Safeguard Privilege Manager for Windows Client collects user-specific data from managed devices, and sends it to the Server. This information is not shared with One Identity. The only exception are domain names associated with users who ran the elevated or Blacklisted process.

How does the Product Improvement Program work?

You choose to participate and allow Safeguard Privilege Manager for Windows to send usage data, associated with an anonymous user ID from your computer. If you are offline at any time, the data will be sent the next time an internet connection is available.

How long will collected data be stored?

We will store the collected data on our secure server for as long as the Product Improvement Program is in place.

Will I receive spam if I participate in the Product Improvement Program?

You will not receive any e-mail regarding the Product Improvement Program, regardless of whether you participate. We do not collect personally identifiable information.

Do I need an Internet connection?

An Internet connection is required for participation. However, it can be an intermittent connection. When an internet connection becomes available, the information is automatically transmitted with minimal impact to your system.

Can I see the data that is collected before it is transmitted?

No, the information cannot be displayed on the customer side. The collection of the desired data occurs seamlessly in the background without affecting the product. Additionally, all formatting and processing of the collected data are done post transmission.

How long will my participation in the program last?

Information is actively collected as long as you use the product version for which you have agreed to participate or until you decide to end your participation.

How is my privacy protected?

We take many precautions in protecting the information that is collected and transmitted. You can learn more about how we handle user information by reviewing our Privacy Policy.

Since no personally identifiable information is collected, the anonymous data will not be meaningful to anyone outside of our company.

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