Quest

Quest Privilege Manager for Windows 4.2

Quick Start Guide

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

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

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

Privilege Manager for Windows Quick Start Guide
Updated - May 2018
Version - 4.2

Contents

1

About this guide

Welcome to the Quest Privilege Manager for Windows Quick Start Guide. Privilege Manager lets system administrators grant selected privileges to users so they can update their own PCs, reducing help desk calls while maintaining a secure network. This guide instructs system administrators on how to set up the Privilege Manager console, server, and client. This guide also provides an overview of the product's key features and the wizards that will help you use them.

For more information, refer to these additional resources:

For system administrators:

- **Privilege Manager Administrator Guide**: Learn how to use Privilege Manager. Find in-depth instructions on how to prepare your environment for least privileged use, maintain a least privileged environment, run reports, and interface with Microsoft tools.
- **Privilege Manager for Windows Console**: Find more information on the **Getting Started** screen under the **Additional Resources** tab.

For end users with the Privilege Manager client service installed on their computers:

- **Privilege Manager for Windows User Guide**: Learn the basics of using Privilege Manager for Windows, including how to use self-service elevation, instant elevation, and view rules.

2

System requirements

Console software and hardware system requirements

- .NET Framework 4.0
- Microsoft Group Policy Management Console
- PDF reader to open the Privilege Manager guides
- Screen resolution of 1024x768 or higher

Console and client operating system requirements

- Windows Server 2008
- Windows 7 Enterprise, Professional, or Ultimate Editions
- Windows Server 2008 R2
- Windows Server 2012
- Windows 8.1
- Windows Server 2012 R2

- Windows 10
- WIndows Server 2016

Network requirements

The Privilege Manager console and client must be installed on a computer within the Active Directory domain.

Required permissions

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

Reporting database requirements

When setting up the Privilege Manager for Windows server, Microsoft SQL Server (hosted either locally on the Privilege Manager for Windows machine or remotely) is required. Privilege Manager supports Microsoft SQL Server 2008 to Microsoft SQL Server 2016. Privilege Manager for Windows can optionally install SQL Server 2014 R2 Express.

3

Components

There are three software components included with Privilege Manager: the console, server and client.

Console

The Privilege Manager console, installed via `PAConsole_Pro.msi`, is a management application. It is installed on a domain computer (server/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 Privilege Manager server, installed via 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 Privilege Manager client, installed via `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 Privilege Manager 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.

Preparing your environment for least privileged use

Prepare your environment for least privileged use by installing Privilege Manager for Windows, configuring reporting, discovery, and remediation settings, configuring approved privileged applications, and removing local admin rights.

Product Licensing

Refer to the Privilege Manager for Windows Administrator Guide for information on editions and applying a license.

Each Privilege Manager license file is compatible with only a single major version of the product (ex.3.x or 4.x). This means existing 3.x licenses will not be valid after upgrading to a 4.x build.Therefore, existing customers are required to obtain a new license file via the License Assistance portal (https://support.quest.com/contact-us/licensing) in order to be properly registered after upgrade.

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

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

Installing the console

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 dialog boxes:

1. Run the Privilege Manager setup file, `PAConsole_Pro.msi`.
2. The installer will check to see if your system is missing any of the required components. Please review the system requirements for Privilege Manager. A window will display and let you install any of the missing components.
    - 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 then resume the installation.

    a. Click the link and download the component.

    b. Close the console setup notification window with the download link to .Net 4.0 Framework.

    c. Install the component.
3. The initial dialog box is the installation **Welcome**. Click **Next**.
4. The **License Agreement** dialog box displays. Select **I accept the terms in the License Agreement** and click **Next**. Refer to the Privilege Manager Administrator Guide for more information on applying a license.
5. On the **Destination Directory** dialog box, select a destination folder. The installation path depends on the system architecture and defaults to: `%PROGRAMFILES%\Quest` or `%ProgramFiles(x86)%\Quest`. Click the **Browse** button to select a different installation path; however, accepting the default values is recommended. Click **Next**.
6. Click **Install** on the final installation dialog. Once the installation is complete, click **Finish**.

Configuring the server

Available only in Privilege Manager Professional and Professional Evaluation editions.

After installing the console, a server must be configured. Configuring the server will set up the back-end services needed to automatically deploy the client, as well as enable 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 will open.
    a. Click the **Browse** button to locate a server via Active Directory.
    b. Use the **Test** button to test 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.
    c. Click the **Clear the server name** link if you want to configure another server. The displayed service will not be uninstalled.
3. Click **Setup/configure the Privilege Manager Server on this computer** to install a new server or configure one on the local computer.
4. The **Privilege Manager for Windows Server Setup Wizard** will open.
   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. Check 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.

   Fill in 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** checkbox.
    d. **From Email**: Enter the corresponding email.

    > Note: You must enter the SMTP Password each time you configure the server or you will receive an error.

6. Click **Send Test Email** to send an email to the account specified within the **From Email** field.
    a. If Privilege Manager succeeds in sending the email, the corresponding message will display.
    b. Log into an email program with the corresponding account and locate the sent email 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 Microsoft SQL Server 2008 R2 Express** to have the Server Wizard install it. Then click **Next**.

> Note: By default, the SQL Server installed via the console uses Windows authentication.

b. Select **Use an existing SQL Server instance** to instruct Privilege Manager to connect to an existing local or remote SQL instance (Microsoft SQL Server 2008 or Microsoft SQL Server 2014 is required) and then click **Next**.

If you are using a remote SQL database, follow these steps:

i. Enable TCP/IP protocol for the selected SQL Server instance;

ii. Enable the console host to address the remote SQL Server; and

iii. 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 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 the SQL Server 2008 R2 Express software via the Privilege Manager for Windows Server Configuration wizard.

9. 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 will be configured as the Super User group. If a different group is required, click the browse button to locate it via Active Directory.

b. In the **Data Collection Web Service Account** section, enter the password of the account that will be 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 Microsoft SQL Server 2008 R2 Express.

> Note: If you plan to use the configured server domain-wide, i.e., from other consoles run either by domain or organizational unit level admins, then ensure the provided Database Super User Group includes all the user accounts that may address the PAReporting database. Otherwise, a user that has no rights to the database will encounter an error.

10. Click **Next** to install a list of SQL Server Management Objects (SMOs) if the local computer is missing them. These prerequisites are required in order to connect to SQL Server instances on the network.

11. 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. Use the  button to view the server instances available on your network.
    c. When using Windows authentication, ensure that the Windows account you are currently logged into the console:
        i. Is assigned to the system administrator server role on the specified SQL Server instance;
        ii. Is a member of the db_owner role for the master database; and
        iii. Is a member of the db_owner role for the PAReporting database, when you are upgrading a database previously created with the Privilege Manager for Windows Server Configuration Wizard.

    If you are targeting a remote SQL database, it must use Windows authentication for runtime access to data (although SQL authentication can be used for the database setup).
12. Click **Next** to install the prerequisites and launch the services.
    a. During installation, a command prompt window may be shown for a short period of time.
    b. Click **OK** and then **Finish** to exit the **Privilege Manager Server Setup** wizard.
13. 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.

Installing the client

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:
        a. Open the console.
        b. Under the **Getting Started** section of the left navigation menu, click **Setup Tasks**.
        c. Select the **Deploy Client Wizard** icon in the Advanced Configuration right pane. It will always show the default settings, or
    - 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 will be saved here.
2. 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.

3. Click **Next**.
4. Define the server.
    a. Click the **Browse** button to locate a server via Active Directory.
    b. Use the **Test** button to test 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.
    c. Click the **Clear the server name** link if you want to configure another server. The displayed service will not be uninstalled.
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 has not been selected:
    a. Click **OK** to close the message window.
    b. Open the **GPO** tab and select the desired GPO.
6. Click **Save** on the GPO toolbar to save the new settings.
7. Double-click **Client Deployment Settings** on the Advanced Policy Settings tab of the GPO to view the **Client Deployment Settings**.
8. Check that the client has been successfully deployed onto the computer. Ensure that:
    a. The `CSEHost.exe` process is running;
    b. The client record is shown in the Add/Remove Programs tool; and
    c. The Privilege Manager icon and the right-click menu are available in the system tray on the client computer.

    New GPO rules created via Privilege Manager will be applied to client computers following a group policy update.

Configuring reporting, discovery, and remediation settings

Access the wizards described below under the **Setup Tasks** tab on the **Getting Started** screen.

Configuring client data collection

Run the **Client Data Collection Settings Wizard** so that you can compile reports, support discovery, and launch on-demand features. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Client Data Collection Settings Wizard**. Follow the prompts or see the Administrator Guide for step-by-step instructions.

Configuring instant elevation

To grant on-demand administrative privileges to a group of trusted users and audit their actions, use the **Instant Elevation Wizard**. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Instant Elevation Wizard**. Follow the prompts or see the Administrator Guide for step-by-step instructions.

Configuring self-service elevation

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 will be asked if they would like to send a request to their administrator for permission to run it. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Self-Service Elevation Request Settings Wizard**. Follow the prompts or see the Administrator Guide for step-by-step instructions.

1. 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 checkbox to enable application filters.

   Enter filter criteria in at least one of the available boxes (Executable path contains, Product name contains, Publisher name contains, and 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 will not transmit any Application Discovery data for application(s) that meet any of the existing filter criteria.

Configuring privileged application discovery

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. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click the **Privileged Application Discovery Settings Wizard**. Follow the prompts or see the Administrator Guide for step-by-step instructions.

Configuring approved privileged applications

Processing discovered privileged applications

Use the **Privileged Application Discovery** screen under the **Discovery & Remediation** tab to process the privileged applications that were reported by the client computers. If these applications are approved and need to continue even after the least-privileged environment is in place, use this screen to automatically create and assign elevation rules to appropriate groups. If a discovered application will not be approved for use in the least

privileged environment, you can ignore these applications and they will no longer display. Follow the prompts or see the Administrator Guide for step-by-step instructions.

Deploying rules

To create the default rules provided by Privilege Manager, use the **Create GPO with Default Rules Wizard**. To access the wizard from the **Getting Started** screen, select the **Setup Tasks** tab and then double-click **Create GPO with default rules**. Follow the prompts or see the Administrator Guide for step-by-step instructions.

Removing local admin rights

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

Use the Windows utility **Active Directory Users and Computers**, installed on Windows Server operating systems such as Windows 2008, to scrub the Domain Administrators group of users that should no longer be given administrative rights to every computer in the domain. Select **Domain Admins Properties > Members** tab **> Remove**.

1. Click the **Discover Accounts in local Administrator groups** button 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 as well.

Using the Users with Local Admin Rights screen

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. See the Administrator Guide for step-by-step instructions.

Congratulations - You are now running in a least privileged use environment!

Maintaining a least privileged use environment

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

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 will automatically be generated for each request. See the Administrator Guide for step-by-step instructions.

Using the Console Email Configuration screen

If you would like an email message to be sent to the user when you have approved or denied their self-service elevation request, you can configure the settings using the **Console Email Configuration screen** found under **Setup Tasks**. See the Administrator Guide for step-by-step instructions.

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. See the Administrator Guide for step-by-step instructions.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product