One Identity Safeguard Privilege Manager for Windows

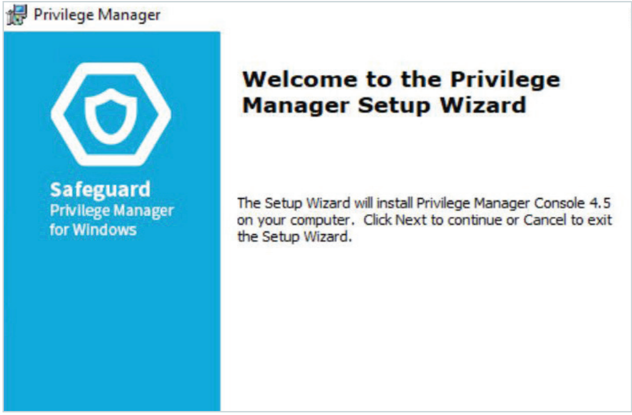
Straightforward and effective Windows privilege management

As your environment grows in number applications and complexity, the balancing act of privilege access management (PAM) becomes that much more complicated. Different types of users need different levels of admin rights, while more applications add call volume to your overworked help desk and stretch your security policies in ways you couldn't have predicted a few years ago. And managing traditional privilege access management platforms can be as much of a problem as the situation that they are supposed to alleviate. But this doesn't have to be complicated. Learn how One Identity's Safeguard Privilege Manager for Windows can simplify privileged access for Windows endpoints.

One Identity Safeguard Privilege Manager for Windows helps end users quickly elevate and manage their own user and administrative rights, yet maintain a least-privileged, GDPR-compliant environment. It includes both prepackaged and community elevation rules for you to address the most common needs. Applying the elevation rules is more effective with the integration of Quest's patented and powerful Validation Logic targeting technology. Privilege Manager works seamlessly with Active Directory and Group Policy Objects (GPOs). You won't find an easier or more affordable way to maintain security while allowing users more self-service capabilities in a locked-down PC environment.

Benefits

- **Self-service** – Allow users to quickly and easily elevate and manage their own user and administrative rights while maintaining a least- privileged environment.
- **Automation** – Avoid the pain of managing each user and desktop individually by automatically elevating permissions with privilege elevation rules.
- **Visibility** – Discover applications that require administrative privileges and apply predefined privilege elevation rules.
- **Flexibility** – Delegate privilege management responsibilities to OU-level admins in organizations of all sizes.
- **Security** – Control user-level access to unwanted or suspect applications.
- **Integration** – Seamlessly integrate with Active Directory and Group Policy Objects.



Welcome to the Privilege Manager Setup Wizard

The Setup Wizard will install Privilege Manager Console 4.5 on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Features

Elevation on demand — Leverage myriad options for end-user admin access to optimize productivity and security. Options types include Instant Elevation, Self-service Elevation, Requested Elevation, Temporary Session Elevation and No Elevation.

Validation Logic — Use our Validation Logic technology to target access rights to any combination of users, user groups, platforms or applications.

Digital certificate verification and support — Automatically elevate all applications from a specific publisher so that anything signed with that publisher's certificate will be elevated.

Targeting for a user, computer, group, platform and organization — Use our Validation Logic technology to target access rights to any combination of users, user group, organizational unit (OU), OS, computer group, office or applications.

Reporting — Stay apprised of what's happening on your Windows desktops with reports that provide a quick and simple status of Elevation Activity, Blacklist Activity, Rules Deployment, Instant Elevation, Temporary-Session Elevation Requests and Rule Details reports.

Community Rules Exchange and technical support — Maximize your investment by using or adding to the more than 100 pre-existing rules in the Community Rules Exchange.

Blacklisting — Deny user access to unnecessary or unwanted applications for increased security and efficiency.

Use cases

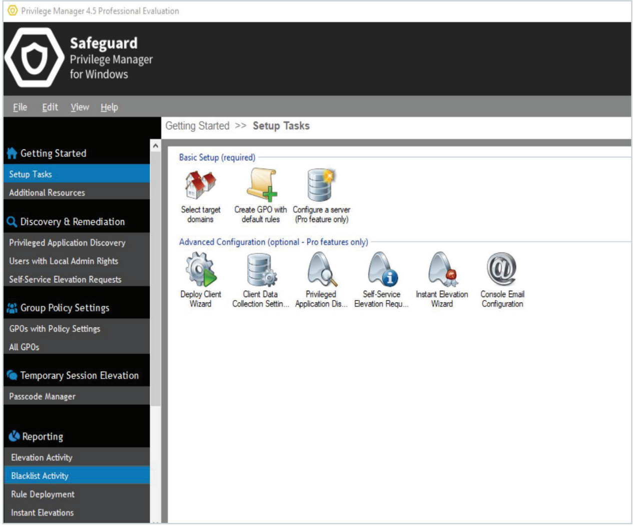
Perform core functions

- Manage privileges centrally through an intuitive console
- View, select and deploy common, predefined or custom rules attached to GPOs
- View and assign rules to specific clients, domains or OUs using Active Directory

Import rules from a Rules Exchange

Apply rules developed by other users for actions such as:

- Add a network printer
- Run iTunes installer as administrator
- Change time zone or date/time from taskbar
- Change system date and time
- Allow Java Runtime updater to run as administrator
- Allow Adobe Reader updater to run as administrator


Privilege Manager 4.5 Professional Evaluation
Safeguard
Privilege Manager
for Windows
File
Edit
View
Help
Getting Started
Setup Tasks
Additional Resources
Discovery & Remediation
Privileged Application Discovery
Users with Local Admin Rights
Self-Service Elevation Requests
Group Policy Settings
GPOs with Policy Settings
All GPOs
Temporary Session Elevation
Passcode Manager
Reporting
Elevation Activity
Blacklist Activity
Rule Deployment
Instant Elevations
Getting Started >> Setup Tasks
Basic Setup (required)
Select target domains
Create GPO with default rules
Configure a server (Pro feature only)
Advanced Configuration (optional - Pro features only)
Deploy Client Wizard
Client Data Collection Settin...
Privileged Application Dis...
Self-Service Elevation Requ...
Instant Elevation Wizard
Console Email Configuration

Remove local admin rights and give users with elevated execution privileges.

Create custom rules

- Assign to an application publisher's certificate for one application or a brand (for example, Adobe, Microsoft)
- Assign to a digital or software publisher's certificate for one application or a brand (for example, Adobe, Microsoft)
- Assign to the path of an executable program
- Assign to a folder path and apply to all processes run from the path
- Assign to an ActiveX object with a URL

SYSTEM REQUIREMENTS

For a detailed and current list of system requirements, please visit https://www.oneidentity.com/products/privilege-manager-for-windows/

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Identity and Access Management (IAM), Privileged Access Management (PAM) and Active Directory Management and Security (ADMS) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 250 million identities for more than 5,000 organizations worldwide. For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest