

Quest® KACE® Privilege Manager

Straightforward and effective Windows privilege management

As your software environment grows and becomes more complex, the careful balancing act of privilege management becomes that much more complicated. Different types of users need different level of administration rights, while more and more software applications puts added stress on your security policies and your help desk. Traditional privilege management platforms can be just as complex as the problem they are built to solve. Quest KACE Privilege Manager is different.

KACE Privilege Manager helps end users quickly elevate and manage their own user and administrative rights, yet maintain a least privileged, GDPR-compliant environment. It includes both pre-packaged 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. 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.

FEATURES

Elevation on-demand — Leverage of 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 of the applications from a specific publisher so that anything signed with that publisher's certificate will be elevated.

According to a recent Gartner Report, privilege management is the number one cybersecurity priority for 2018, followed closely by endpoint security.

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 pre-defined 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.



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

SYSTEM REQUIREMENTS

CONSOLE SOFTWARE AND HARDWARE

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

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

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, 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

Create custom rules

- Assign to an application publisher's certificate for one application or a brand (e.g. Adobe, Microsoft)
- Assign to a digital or software publisher's certificate for one application or a brand (e.g. 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

ABOUT QUEST

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats and regulatory requirements. Our portfolio includes solutions for database management, data protection, unified endpoint management, identity and access management and Microsoft platform management.