DATASHEET

Privilege Manager for Windows

Enhanced desktop security without increased IT workload. More security, less work.

Benefits

- Enhance security by limiting access to the desktop admin account and privileged applications
- Reduce help desk calls with self-service password-reset for end users
- Increase control with flexible options for granting/denying, limiting or autonomous access to privileged applications
- Reduced attack surface without increasing the risk or workload to the business

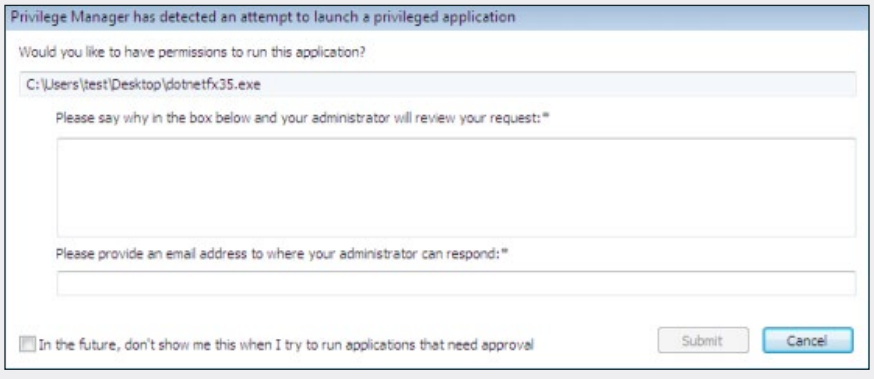
Overview

Issuing the typical user administrator rights to their Windows desktop creates a significant security risk. But, allowing this level of control to users must be weighed against constant help desk calls for assistance basic functions, such as updating applications or simply changing the time zone.

If you don't secure the administrative account on the Windows desktop, threat actors have yet another way to access your infrastructure. On the other hand, if that desktop's admin account is completely locked down, your IT department will see an increase in help desk tickets as end users seek to alter their systems or install new software. It's either lockdown your desktops and deal with the call volume or create a massive security gap at the desktop.

To address this security paradox, you need a way to create, deploy and manage a 'least privileged' model for your desktop infrastructure. The result is you can reduce your threat surface area, keep your end users productive and avoid increasing the workload on your IT staff. How is this possible?

With Privilege Manager for Windows, you can control and secure the admin account on your organization's Windows desktops. It features a number of configuration options for end-user access to the desktop admin account. Privilege Manager for Windows delivers flexibility IT needs while providing the security the organization demands. This enables you to control the elevated permissions for desktop users as part of your organization's privileged account management program.



Privilege Manager for Windows can detect and notify a user when they are trying to launch an application that requires administrator privileges. From the same notification box, the user can request temporary elevated access to launch the application.

Features

Flexible deployment

Your IT team has a bevy of installation options from which to choose, including our client-deployment wizard, a client Windows installer file (.msi) and Microsoft's GPMC.

Client control

With the Client Data Collection Settings Wizard, you can collect client data for reporting, support discovery and to leverage launch on-demand features.

Elevation on-demand

Take advantage 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.

Workflow

Ensure that end users and admins are always on the same page for approval processes with email notifications.

Privileged application discovery

Collect information about the privileged applications used over your network during a specified time. With this critical knowledge, you can create a rule to allow a user without elevated privileges to launch the app they need – or choose to mark it as processed so that it will not display in the applications list for that user (unless the filter is specifically set to display it).

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.

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com

Datasheet_2018_PrivilegeMgrForWindows_US_RS_35458