

Flexibility is power. It's now simple to give all your users the privileges they need to remain productive, empowering them wherever they are without impacting the security posture of your systems and networks. Privilege Guard combines application elevation, application control, end user messaging and a complete auditing and reporting framework for all your Windows based systems.

Privilege Guard Overview



Effectively managing user privileges remains a challenge for almost all organizations. The need for users to configure certain settings on their computer, run legacy applications and install authorized software are just some of the reasons why users are often given excessive privileges. For server administration, Privilege Guard may be used to grant local admin rights over specific applications, making it unnecessary to give local admin rights directly to a system administrator. In addition to creating a more secure server environment, any privileged

activity may also be audited, with the option of logging detailed information, regarding changes to a server's underlying configuration, such as registry settings, system files and services.

Whether you need to restrict the rights of system administrators, or grant additional rights to standard users, Privilege Guard provides a solution that enables all users to run with standard rights. Policy settings determine which applications should be elevated and Privilege Guard assigns the relevant privileges to the process tokens of individual applications as they launch. The experience is seamless to the end user and does not require them to have access to a local admin account, as all elevated applications still run in the full context of the logged on user.

Privilege Guard Benefits

- ✓ Enables users to logon with standard user rights without compromising their ability to perform their job function
- ✓ Enables users to run legacy applications or any other applications that require admin rights
- ✓ Enables users to perform approved computer configuration tasks, such as adding local printers and changing the time
- ✓ Restricts users to installing and running only trusted applications
- ✓ Enables server administrators to work under least privilege, with an audit trail of privileged operations
- ✓ Works seamlessly with User Account Control (UAC) and eliminates or replaces inappropriate UAC prompts
- ✓ Achieve desktop compliance e.g. USGCB, PCI-DSS and Government Connect

Centralized Management through Windows Group Policy

Privilege Guard is tightly integrated with Windows Group Policy and no additional backend infrastructure is required to implement the solution. It can be configured in minutes and deployed through Active Directory Group Policy to an entire desktop and server estate. Once deployed, Privilege Guard policies take effect immediately and are cached on the client computer, ensuring that policies continue to be enforced when a user is not connected to the network.

Both computer and user policy settings may be applied, and support for background refresh makes sure that policies are updated even if a user remains logged on. Privilege Guard policy settings may also be exported to an XML file and deployed using any suitable cloud deployment mechanism, where Group Policy is not a viable option.

Avecto Americas

3 Dundee Park, Andover
Ma. 01810
USA

Phone: 978-703-4169
Facsimile: 978 910 0448

Avecto UK

5300 Lakeside, Cheadle Royal
Business Park, Cheshire,
SK8 3GP, United Kingdom

Phone: +44 (0)845 519 0114
Facsimile: +44 (0)845 519 0115



Supported Platforms

- ✓ Windows XP
- ✓ Windows Vista
- ✓ Windows 7

- ✓ Windows Server 2003
- ✓ Windows Server 2008
- ✓ Windows Server 2008 R2



32-bit and 64-bit versions are available for all supported platforms



Simple Policy Configuration

Enabling an application to run with elevated rights couldn't be simpler.

Define the application and set its identification options, such as filename, hash, publisher, command line, parent process or product information. Next, assign the application to the users and computers who require elevated rights over the application and set up any additional options, such as end user messaging, auditing and privilege monitoring. Settings are automatically committed to Active Directory Group Policy and deployed during the next Group Policy refresh. Policies may optionally be digitally signed to ensure authenticity.



Privilege Monitoring

To assist in policy definition, Privilege Guard can be deployed in

"passive mode" to users who have local admin rights. Privilege monitoring will analyze application behavior and log events for any application that would fail to run under a standard user account. More detailed activity logs can also be captured, which enable closer inspection of any privileged operations performed by applications. Once this information is collated, suitable policies may be defined to elevate the individual applications, enabling users to be removed from the local administrators group.



End User Messaging

It may be beneficial to display a message to the user before an application is launched (or blocked), to provide the user with additional information, such as warning the user of their actions. Any number of end user messages may be defined, with multi-lingual support, embedded hyperlink and

full customization, including the ability to include a corporate logo in the message header. Users can optionally be forced to re-authenticate or provide a reason before continuing, which is then audited.



Designated User Authorization

Designated User Authorization allows you to restrict which users are able to authorize the use of an application, without the need to roll out new policies. This 'over-the-shoulder' authorization adds a flexible layer of policy management by delegating the decision process for one off, or temporary usage requests, to office based support admins. You can also define which applications should 'Run As' the authorizing user, providing a policy controlled, fully audited alternative to traditional Windows Run As operations.



On Demand Elevation

For the more demanding user, Privilege Guard integrates with the Windows shell to provide the user with an "On-Demand" elevation facility. The user logs on with a standard user account and can elevate applications from a shell context menu. All elevated applications are audited, ensuring the user does not abuse this privilege. To avoid end user confusion, the standard Windows "Run as" and "Run as administrator" menu options can also be hidden.



Application Control

Privilege Guard may also be used to control the applications that a user is allowed to install or run. Policies may be configured that whitelist the trusted applications on a system. Any unauthorized applications, including software installers and scripts may be

blocked and audited. The end user is informed with a fully customizable message, including the option for the user to submit (or email) a request for a blocked application.



Custom Access Tokens

Privilege Guard includes pre-configured access tokens to assign or revoke admin rights to applications. If it is necessary to assign more granular rights then any number of custom access tokens may be defined for this purpose. Groups, privileges and permissions may be added or removed from the access token. Token ownership and integrity level may also be set, where applicable. Elevated applications are secured to prevent inappropriate interaction from standard user processes and a built-in "Anti-Tamper" mechanism protects the Privilege Guard solution.



Policy Filters

Each Privilege Guard policy allows you to apply granular filters based on any combination of user, group, computer, remote desktop client, time restrictions and expiry time. With Policy Filters you can rapidly deploy privilege settings to where they are needed, from companywide policies to individual role based needs.



Auditing and Reporting

Built on proven scalable technologies, Privilege Guard records all privileged activity and offers a number of options to review and report on the data, from the built-in reporting console to optional Enterprise Reporting Packs for Microsoft SQL Server and McAfee ePO.

Privilege Guard Features

- ✓ Centralized management through Active Directory Group Policy
- ✓ Digital signing of deployed policies
- ✓ Elevation or revocation of privileges for individual applications
- ✓ Application control enables whitelisting of trusted applications
- ✓ Comprehensive application support:
 - Executables
 - Control panel applets
 - Management console snap-ins
 - Windows installer packages
 - Windows Scripting Host scripts
 - Batch files
 - Registry settings
 - PowerShell scripts
 - ActiveX controls

- ✓ Application templates, for easy configuration of common Windows tasks, ActiveX controls and software updaters
- ✓ Client Anti-Tamper mechanism
- ✓ Flexible and secure application rules:
 - File path matching
 - Command line matching
 - File hashing (SHA-1)
 - Trusted publisher
 - Trusted ownership
 - Product and file information
 - Parent Process
- ✓ Granular control of application definitions
- ✓ Policy filtering to target any combination of user, group, computer, RDS client, time period and expiry time.

- ✓ Optional shell extension enables users to elevate applications "on demand"
- ✓ Fully customizable and multi-lingual end user messaging
- ✓ Granular privilege control through custom access tokens
- ✓ Privilege Monitoring identifies applications that require admin rights to run
- ✓ Auditing and reporting of privileged and blocked applications, including support for event forwarding.
- ✓ Optional Enterprise Reporting Pack
- ✓ Optional McAfee ePO Integration Pack

Visit: avecto.com | Email: info@avecto.com