

**Avecto Privilege Guard** enables organizations to adopt the principle of least privilege. It is no longer necessary to assign admin rights to users, as these rights can now be assigned dynamically to applications, tasks and scripts. Privilege Guard enables users to log on with minimal rights and empowers them to perform their day to day role, without compromising the integrity and security of the corporate systems.

**Privilege Guard Overview**

Removing admin rights for corporate users is a difficult problem to resolve for almost all organizations, making desktop lockdown a real challenge. 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.

Privilege Guard gives control back to the IT department by providing 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.

**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.

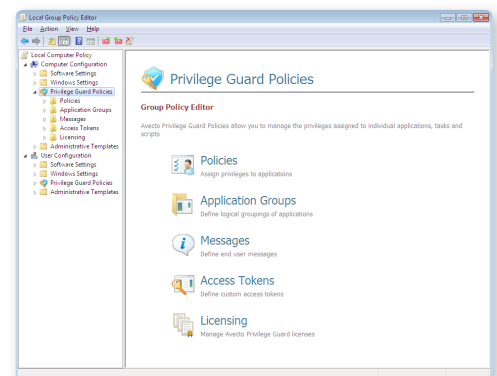
Both computer and user policy settings may be applied, and support for background refresh makes sure that policies are updated even if a user remains logged on. For Novell environments, Privilege Guard is compatible with Group Policy configuration through ZENworks. Privilege Guard policy settings may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



**Privilege Guard Platforms**

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

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



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

Avecto Europe  
Weena 290  
3012 NJ Rotterdam  
The Netherlands

Avecto Americas  
800 Turnpike Street, Suite 300,  
North Andover MA 01845  
USA

Learn more  
Visit: [www.avecto.com](http://www.avecto.com)  
Email: [info@avecto.com](mailto:info@avecto.com)



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

Phone: +31 621 527 426  
Facsimile: +31 848 306 833

Phone: 978-557-0714  
Facsimile: 978-557-0792

## Simple Policy Configuration

Enabling an application to run with elevated rights couldn't be simpler. Define the application in the Privilege Guard Policies and set its identification options, such as filename, file hash, trusted publisher or command line. Next, assign the application to the users who require elevated rights over the application and set up any additional options, such as end user messaging, auditing and privilege monitoring. The policies are automatically committed to Active Directory Group Policy and will be deployed during the next Group Policy refresh cycle.

## Privilege Monitoring

To assist in policy definition, Privilege Guard can be deployed in "passive mode" to users who have local admin or power user rights. Privilege monitoring will analyze application behaviour 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 or power users groups.

## 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 full customization and multi-lingual support. Users can optionally be forced to re-authenticate or provide a reason before continuing, which is then audited.

## Application Control

In addition to controlling the privileges assigned to applications, 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, by identifying applications based on a combination of trusted folders, files, publishers or hashes. 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 email a request for a blocked application. More advanced users may be allowed to run unauthorized applications, and in this scenario the user can simply be warned and their actions audited.

## 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.

## 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 and privileges may be added or removed from the access token, and the integrity level may also be set, where applicable.

## 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. FDCC and Government Connect

## Privilege Guard Features

- ✓ Centralized management through Active Directory Group Policy
- ✓ 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
- ✓ Flexible and secure application identification options:
  - File path matching
  - Command line matching
  - File hashing (SHA-1)
  - Trusted publisher (including support for the Windows security catalog)
- ✓ 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 of privileged and blocked applications