Privilege Guard 3.0
Administration Guide
Copyright Notice

The information contained in this document ("the Material") is believed to be accurate at the time of printing, but no representation or warranty is given (express or implied) as to its accuracy, completeness or correctness. Avecto Ltd, its associated companies and the publisher accept no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from any use of or reliance placed on this Material for any purpose.

Copyright in the whole and every part of this document belongs to Avecto Ltd ("the Owner") and may not be used, sold, transferred, copied or reproduced in whole or in part in any manner or form or in or on any media to any person other than in accordance with the terms of the Owner’s Agreement or otherwise without the prior written consent of the Owner.

Trademarks

Microsoft Windows, Windows Vista, Windows Server, Windows PowerShell, ActiveX, Visual C++ and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Copyright ©2008-2010 Avecto Ltd. All rights reserved.
Contents

Introduction ......................................................................................................................... 7
Planning and Preparation ................................................................................................. 8
Defining User Roles ......................................................................................................... 8
Implementing Least Privilege .......................................................................................... 8
  Scenario 1 – Known Admin Applications .................................................................. 9
  Scenario 2 – Unknown Admin Applications ............................................................... 9
  Scenario 3 – Flexible Elevation .................................................................................. 9
Privilege Guard Software Installation ............................................................................. 10
Installing the Privilege Guard Management Console .................................................. 10
Installing the Privilege Guard Client ............................................................................. 14
  Client Packages .......................................................................................................... 14
  Unattended Client Deployment ................................................................................... 15
  Privilege Guard Client Certificate Mode .................................................................... 15
Upgrading Privilege Guard from Previous Versions ..................................................... 16
Planning your deployment .............................................................................................. 16
Recommended Steps ....................................................................................................... 16
  Step 1: Upgrade Privilege Guard Clients ................................................................... 16
  Step 2: Upgrade Privilege Guard Management Console .......................................... 16
  Step 3: Upgrade Privilege Guard Settings ................................................................ 16
Frequently Asked Questions ........................................................................................... 17
  Can I install the 32-Bit Client on a 64-Bit endpoint? ................................................. 17
  Can I install the 32-Bit Management Console on a 64-Bit endpoint? ...................... 17
  Do I need to install the Privilege Guard Client and Management Console together? 17
  What distribution mechanisms do you support? ......................................................... 17
  What pre-requisite components are required for Privilege Guard? ......................... 18
  Where can I find the latest version of Privilege Guard, or previous versions? ........ 18
  Which operating systems are supported by Privilege Guard? .................................. 18
Deploying Privilege Guard Settings with Group Policy .................................................. 19
  Creating Privilege Guard Settings ............................................................................ 19
  Privilege Guard Settings Scope ............................................................................... 21
  GPO Precedence and Inheritance Rules .................................................................. 21
  Order of Processing .................................................................................................... 21
  Exceptions to Default Order of Processing ............................................................... 22
  Privilege Guard Settings Storage and Backup ......................................................... 23
  Disconnected Users .................................................................................................... 23
Managing Privilege Guard Settings without Group Policy ............................................ 24
Editing Privilege Guard Settings .................................................................................... 25
  Policies ....................................................................................................................... 25
  Creating Policies ........................................................................................................ 25
  Disabling Policies ....................................................................................................... 25
  Policy Precedence ....................................................................................................... 26
Policy Description ........................................................................................................... 26
Editing Policies - Filters ................................................................................................. 26
Account Filters .............................................................................................................. 27
Computer Filters .......................................................................................................... 27
Time Filters .................................................................................................................. 28
Expiry Filters ................................................................................................................. 28
Editing Policies - Application Privileges ........................................................................ 28
Editing Policies - Shell Integration ................................................................................ 30
Policy Options .............................................................................................................. 32
Workstation Options .................................................................................................... 32
Monitoring Options ....................................................................................................... 32
Application Groups ....................................................................................................... 33
Creating Application Groups ......................................................................................... 33
Application Group Description ...................................................................................... 33
Inserting Applications .................................................................................................... 33
Application Rules .......................................................................................................... 34
Advanced Options ......................................................................................................... 36
Regular Expressions Syntax ......................................................................................... 37
Inserting ActiveX Controls ............................................................................................ 38
Validation Options ......................................................................................................... 39
Inserting Application Templates .................................................................................... 39
Inserting an Application from a Running Process ......................................................... 40
Application Group Summary ......................................................................................... 41
Messages ....................................................................................................................... 43
Creating Messages ......................................................................................................... 43
Message Description ...................................................................................................... 44
Message Design ............................................................................................................. 45
Miscellaneous Settings ................................................................................................. 45
Message Header Settings ............................................................................................... 45
Reference Hyperlinks ..................................................................................................... 45
Message Body Settings ................................................................................................. 46
Authorization Settings .................................................................................................. 46
Email Settings ............................................................................................................... 47
Message Text ................................................................................................................ 47
Managing Languages .................................................................................................... 47
Setting the Message Text ............................................................................................... 48
Changing the Message Text for Buttons ....................................................................... 48
Image Manager ............................................................................................................. 48
Access Tokens ............................................................................................................... 50
Creating Access Tokens ............................................................................................... 50
Access Token Description ............................................................................................. 51
Editing Access Tokens .................................................................................................. 51
Groups .......................................................................................................................... 51
Privileges ...................................................................................................................... 52
Integrity Level ................................................................................................................ 53
Process Access Rights ................................................................................................. 54
Licensing ....................................................................................................................... 55
Using makecert to generate a suitable test PFX file ..................................................86
Using Microsoft Certificate Services to generate a suitable PFX file .........................87
Creating a Privilege Guard Configuration Certificate Template ..................................87
Issuing the Privilege Guard Configuration Certificate Template ..................................88
Using the Privilege Guard Configuration Certificate Template in a Certificate Request ....89
Distributing Public Keys ..................................................................................................89
Appendix C – Using Privilege Guard with McAfee ePO .............................................91
Pre-requisites ...............................................................................................................91
Manual Installation of Privilege Guard Agent in ePO Mode .........................................91
Disabling ePO Mode .................................................................................................91
Introduction

Privilege Guard provides a policy based approach to privilege management. All users log on with standard user accounts and Privilege Guard assigns the necessary rights and privileges to applications, scripts and software installers.

Privilege Guard is implemented as an extension to Group Policy, enabling policies to be managed through the standard Group Policy Management tools.

If you do not wish to use Group Policy for deployment of the policies then you may import/export polices as an XML file, and use any suitable deployment solution to deploy the XML file to a set location on each client computer.

This guide is split into nine sections:

1. **Planning and Preparation** - provides background information on the various approaches to implementing least privilege.

2. **Software Installation** - walks you through the installation of the Privilege Guard management console and client.

3. **Managing Privilege Guard Settings with Group Policy** - guidance for deploying policies through Active Directory Group Policy.

4. **Managing Privilege Guard Settings without Group Policy** - guidance for deploying policies without Active Directory Group Policy.

5. **Editing Privilege Guard Settings** – a complete guide to all of the policy settings.

6. **Application Templates** – an overview of the standard application templates and guidance on how to create your own application templates.

7. **Troubleshooting** – techniques to troubleshoot common client and policy configuration problems.

8. **Auditing and Reporting** – details the auditing and reporting capabilities.

9. **Deployment Scenarios** – outlines common deployment scenarios.
Planning and Preparation

Defining User Roles

Privilege Guard is an easy solution to deploy, given its integration with Group Policy, but you will want to spend some time preparing suitable policies for your users. Implementing least privilege may require policies to be tailored to users’ roles.

The table below shows three fairly typical user roles, but it is recommended that you come up with roles that are tailored to your environment, as these roles are very generic.

<table>
<thead>
<tr>
<th>Role</th>
<th>Requirement for Admin Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Corporate User</td>
<td>Problem applications and simple admin tasks.</td>
</tr>
<tr>
<td>Laptop User</td>
<td>Problem applications, intermediate admin tasks and authorized software installation.</td>
</tr>
<tr>
<td>Technical User</td>
<td>Complex applications, advanced admin tasks and ad hoc software installation.</td>
</tr>
</tbody>
</table>

Privilege Guard can cater for all types of user roles, including the most demanding technical users.

You should also educate users before moving them to standard user accounts to ensure that they will report any problems they encounter during the process of moving to least privilege.

**NOTE:** Contact your solution provider or Avecto to gain access to templates to cater for more complex use case scenarios.

Implementing Least Privilege

The first step is to identify the applications that require admin privileges for each role you have defined. This can fall into one of three scenarios:

1. **Known Admin Applications** - You already have a definitive list of applications that require admin rights to run.
2. **Unknown Admin Applications** - You are not sure of the applications that require admin rights to run.
3. **Flexible Elevation** - The user will require flexibility and can’t be restricted to a list of applications.
Scenario 1 – Known Admin Applications

For this scenario you should simply add the relevant applications to the Privilege Guard Policies for the users, which will automatically elevate these applications when they are launched. You may then remove admin rights from these users. Refer to Application Elevation in the Deployment Scenarios section of this guide for more information on defining suitable policies.

Scenario 2 – Unknown Admin Applications

For this scenario you have two choices to help you discover the applications that require admin rights:

1. Set up Privilege Guard Policies to monitor privileged application behavior. The Privilege Guard audit logs will highlight all of the applications that require admin rights to run. Please refer to Application Discovery in the Deployment Scenarios section of this guide for more information on monitoring privileged applications.

2. Set up Privilege Guard Policies to give the user the “on demand” elevation facility, and instruct the user to use this facility for any applications that fail to run once you have taken the user’s admin rights away. The Privilege Guard audit logs will highlight all the applications that the user has launched with elevated rights. Refer to On Demand Elevation in the Deployment Scenarios section of this guide for more information on defining suitable policies to allow users to elevate applications on demand.

You may now use the audit logs to determine the relevant set of applications that you want to give admin rights to for these users. Refer to Application Elevation in the Deployment Scenarios section of this guide for more information on defining suitable policies.

Scenario 3 – Flexible Elevation

For this scenario you should set up Privilege Guard Policies that give the user an “on demand” elevation facility, which allows the user to elevate any applications from a standard user account. All elevated applications may be audited, to discourage users from making inappropriate use of this facility. Refer to On Demand Elevation in the Deployment Scenarios section of this guide for more information on defining suitable policies to allow users to elevate applications on demand.
Privilege Guard Software Installation

Installing the Privilege Guard Management Console

The Privilege Guard management console is a Group Policy MMC extension snap-in and may be installed on any number of administrator desktops or servers.

**NOTE:** This guide assumes that you will be using Group Policy Management Console (GPMC), although Privilege Guard fully supports other methods of Group Policy deployment, such as the Group Policy Editor. Ensure that you have the relevant Group Policy management tools installed on the desktop or server where you will be installing the Privilege Guard management console.

The Privilege Guard installation is performed in two stages; first the **Privilege Guard Management Consoles**, and then the **Privilege Guard Client**.

Log on with an administrator account.

To install Privilege Guard run the appropriate installation package:

- For 32-bit systems run `AvectoPrivilegeGuard_x86.exe`
- For 64-bit (x64) systems run `AvectoPrivilegeGuard_x64.exe`

The installation will detect if any prerequisites are needed.

Click **Install** to continue with the setup of Privilege Guard Management Consoles.
The installation will first install the prerequisites, which may take a few minutes.

Once the prerequisites have been installed the **Welcome** dialog will appear.

Click **Next** to continue. The **License Agreement** dialog will appear.
After reading the license agreement, select I accept the terms in the license agreement and click Next to continue. The User Information dialog will appear.

Enter your name and the name of your organization and click Next to continue. The Destination Folder dialog will appear.
If you wish to change the default installation directory then click the **Browse** button and select a different installation directory. Click **Next** to continue. The **Ready to Install the Program** dialog will appear.

Click **Install** to begin the installation. The Management Consoles will now install.
Once the Management Consoles have installed, you will be presented with the following screen asking if you would like to also install the Privilege Guard Client.

Uncheck **Install Privilege Guard Client** and click **Finish** to exit the Management Consoles installation.

**Installing the Privilege Guard Client**

The Privilege Guard Client may be installed independently from the Privilege Guard Console with a client installation package. This is the recommended approach for any computers that do not require the management console to be installed, as the client installation package is much smaller, and has fewer prerequisites.

**Client Packages**

There are two client installation packages available, which are installed with the Privilege Guard management console. The packages can be found in the **Client Installer** subdirectory of the Privilege Guard Management Consoles installation (usually C:\Program Files\Avecto\Privilege Guard Management Consoles\Clients):

- **PGClient_x86.exe** (32-bit) and **PGClient_x64.exe** (64-bit) – this is a complete installation for the Privilege Guard Client, including the Windows Installer 3.1 and MSXML 6 prerequisites.
**PGClient\_x86.msi** (32-bit) and **PGClient\_x64.msi** (64-bit) – this is an installation package that only contains the Privilege Guard Client. The prerequisites must be installed first on the client.

**NOTE:** The prerequisites are only required for versions of Windows XP prior to SP3, as MSXML 6 and Windows Installer 3.1 are standard in Windows XP SP3, Windows Vista and Windows 7.

The client may be installed manually, but for larger installations it is recommended you use a suitable third party software deployment system.

**NOTE:** There is no license to add during the client installation, as this is deployed with the Privilege Guard Policies, so the client may be installed silently.

**Unattended Client Deployment**

When deploying the Privilege Guard client with automated deployment technologies, such as System Center Configuration Manager (SCCM), it usually makes sense to deploy the client silently and hold off the computer from restarting.

To install the client executable silently, without a reboot, use the following command line (the double quotes are required):

```
PGClient.exe /s /v"/qn /norestart"
```

To install the client MSI package silently, without a reboot, use the following command line (double quotes are not required):

```
PGClient.msi /qn /norestart
```

**NOTE:** Privilege Guard will not be fully operationally until a reboot is performed. To perform an unattended deployment with a reboot omit the '/norestart' switch.

**Privilege Guard Client Certificate Mode**

For details on installing the Privilege Guard Client in Certificate Mode, refer to the section **Privilege Guard Client Certificate Mode**

For information on working with Signed Privilege Guard Settings, refer to the section **Signing Privilege Guard Settings**
Upgrading Privilege Guard from Previous Versions

Planning your deployment

Before upgrading any Privilege Guard software or Privilege Guard settings, it is recommended that you test your deployment in a pre-production environment. This will help mitigate any unforeseen compatibility issues, and avoid disruption to the business.

All Privilege Guard MSI and Executable installers will automatically remove old versions when installed. Therefore, it is not necessary to manually remove old versions prior to installation of new versions.

The Privilege Guard Client guarantees backwards compatibility with previous versions of Privilege Guard settings, but does not guarantee forwards compatibility. Therefore it is recommended that all Privilege Guard Clients are upgraded before rolling out new versions of Privilege Guard Settings.

NOTE: When upgrading Privilege Guard software, it may be necessary for a reboot to occur in order to complete the installation. When installing in silent mode, a reboot will occur automatically. Therefore it is recommended that upgrades are performed out of core business hours, or during scheduled maintenance windows, to avoid loss of productivity.

Recommended Steps

Step 1: Upgrade Privilege Guard Clients

To upgrade the Privilege Guard Client manually, simply double click PGClient_x86.exe or PGClient_x64.exe on the target endpoint, and follow the installation wizard.

To upgrade the Privilege Guard Client using a deployment mechanism, refer to the steps detailed in the section Installing the Privilege Guard Client.

NOTE: For larger deployments, Privilege Guard Clients support mixed client environments as they are fully backwards compatible with older versions of the Privilege Guard settings. This allows for phased roll-outs of the Privilege Guard Client if this is preferred.

Step 2: Upgrade Privilege Guard Management Console

Once all Privilege Guard Clients have been upgraded, the next step is to upgrade the Privilege Guard Management Console.

To upgrade the Privilege Guard Management Console, refer to the steps detailed in the section Installing the Privilege Guard Management Console.

Step 3: Upgrade Privilege Guard Settings

Once the Privilege Guard Management Console has been upgraded, the final step is to roll out new versions of the Privilege Guard Settings. Although Privilege Guard Clients are fully
backwards compatible with older versions of Privilege Guard Settings, this step is required if you wish to take advantage of any new features and enhancements in Privilege Guard.

Privilege Guard Settings are automatically saved in the latest format each time a change is made. For details of editing Privilege Guard settings, refer to the steps in section Deploying Privilege Guard Settings with Group Policy.

**NOTE:** Once Privilege Guard Settings have been upgraded, they cannot be downgraded. Therefore it is recommended that upgrading Privilege Guard Settings is performed only once all Privilege Guard Clients have been upgraded.

**Frequently Asked Questions**

Can I install the 32-Bit Client on a 64-Bit endpoint?

No. The 32-Bit Client can only be installed on 32-Bit clients.

Can I install the 32-Bit Management Console on a 64-Bit endpoint?

Yes. The 32-Bit Management Console can be installed on 64-Bit clients if required. However, you will not be given the option of installing the Client.

Do I need to install the Privilege Guard Client and Management Console together?

For standalone installations, you must install both the Client and Console. Avecto also recommends that the Client and Console are installed together during evaluation, to simplify the evaluation process.

For larger deployments, there is no requirement to install the Management Console on endpoints.

What distribution mechanisms do you support?

The Privilege Guard Client can be deployed using any third party software which supports the deployment of MSI and/or Executable files, such as Microsoft Active Directory, Microsoft SMS / SCCM, and McAfee ePolicy Orchestrator (ePO).

For silent installations and advanced installations (such as CERT_MODE and EPOMODE), the 3rd party deployment software must also support the use of command line options.
What pre-requisite components are required for Privilege Guard?

For the Privilege Guard Client:
- Microsoft Core XML Services 6.0 (XP SP2 only)

For the Privilege Guard Management Console:
- Microsoft Core XML Services 6.0 (XP SP2 only)
- Microsoft Visual C++ 2010 Redistributable x86
- Microsoft Visual C++ 2010 Redistributable x64 (for 64-Bit clients)
- Microsoft Group Policy Management Console (for Active Directory integration)

**NOTE:** The executable version of the installation package includes all necessary pre-requisites (excluding the Group Policy Management Console), and will automatically install them as necessary.

Where can I find the latest version of Privilege Guard, or previous versions?

All versions (including the latest version) of Privilege Guard can be downloaded from [www.avecto.com](http://www.avecto.com) by signing in and navigating to the Software section.

Which operating systems are supported by Privilege Guard?

For details of supported operating systems, refer to the Privilege Guard Release Notes.
Deploying Privilege Guard Settings with Group Policy

Creating Privilege Guard Settings

Privilege Guard is implemented as an extension to Group Policy, enabling policy settings to be managed through the standard Group Policy Management tools. Privilege Guard also supports Advanced Group Policy Management (AGPM) from versions 2.5 to 4.0.

Group Policy Objects (GPOs) are usually managed through the Group Policy Management Console (GPMC). GPMC is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. GPMC is the standard tool for managing Group Policy.

Privilege Guard also supports Local Computer Policy, which can be edited in the Group Policy Editor, but this is only recommended for small environments or for test purposes.

You may add Privilege Guard Settings to existing GPOs or create new GPOs for this purpose.

To edit a GPO from the Group Policy Management Console (GPMC):

1. Launch the GPMC (gpmc.msc).
2. In the GPMC tree, double-click Group Policy Objects in the forest and domain containing the GPO that you want to edit.
3. Right-click the GPO, and then click Edit.

The Group Policy Management Editor will launch. Privilege Guard Settings are available in both the Computer Configuration and User Configuration nodes, which allow you to set...
either computer or user settings respectively. Computer settings are updated when a computer starts up, whereas user settings are updated when a user logs on. In addition, a background refresh occurs every 90 minutes by default, which will update settings while the user is logged on.

Once a client has updated its Privilege Guard Settings through Group Policy then the settings are applied dynamically. Any logged on users do not need to log off for the changes to take effect.

**NOTE:** Privilege Guard Settings will either appear directly under the Computer Configuration and User Configuration nodes, or under the Policies sub-node, if it exists.

To create Privilege Guard Settings for a GPO:

1. In the Group Policy Management Editor select the Privilege Guard Settings node for either the Computer Configuration or User Configuration section, as appropriate.
2. On the Group Policy Management Editor Action menu, click Create Privilege Guard Settings.

To edit the Privilege Guard Settings refer to the Editing Privilege Guard Settings section of this guide.
Privilege Guard Settings Scope

When deploying Privilege Guard settings with Active Directory Group Policy there are two factors to consider; the management scope of the GPO you have selected and the user or group accounts listed on the Accounts section of a Privilege Guard policy.

By default, no Account or computer filters are added when you create a new Privilege Guard policy. This ensures that only the management scope of the GPO will be relevant. In other words, the Privilege Guard policy will be applied to all computers or users that are under the scope of management of the GPO.

It is possible to apply the policy to a sub-set of users by adding Account filters to the Filters section of the policy, and adding groups and users (either domain or local). Do not leave the Account filters empty or the policy will still apply to everyone.

Multiple Account filters can be added to a policy, if you need add ‘AND’ logic to your filtering. For example, if wish to target a user who is a member of ‘GroupA’ AND ‘GroupB’, then add two Account filters to your policy, adding GroupA to one filter and GroupB to the other filter.

If you add multiple users and groups to the same Account filter, then this will result in an ‘OR’ match for that Filter.

You can also use Computer filters to apply the policy to specific computers and connecting client devices. These can be used in combination with Account filters to provide more specific targeting of user / computer combinations if required.

Refer to Policies in the Editing Privilege Guard Settings section of this guide for more information.

GPO Precedence and Inheritance Rules

Privilege Guard Settings are associated with an Active Directory GPO and are distributed to all the computers and users under the management scope of the GPO. As a result Privilege Guard Settings are subject to the same Group Policy processing and precedence rules as standard Active Directory GPO’s

Order of Processing

Group Policy settings are processed in the following order:

1. **Local Group Policy Object** - Each computer has exactly one GPO that is stored locally. This applies to both computer and user Group Policy processing.

2. **Site** - Any GPOs that have been linked to the site that the computer belongs to are processed next. Processing is in the order that is specified by the administrator, on
the Linked Group Policy Objects tab for the site in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

3. **Domain** - Processing of multiple domain-linked GPOs is in the order specified by the administrator, on the Linked Group Policy Objects tab for the domain in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

4. **Organizational Units** - GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

At the level of each organizational unit in the Active Directory hierarchy, one, many, or no GPOs can be linked. If several GPOs are linked to an organizational unit, their processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the organizational unit in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

This order means that the local GPO is processed first, and GPOs that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites settings in the earlier GPOs if there are conflicts.

Privilege Guard simply merges settings so that settings with a higher precedence will be processed first. Once an application matches a Privilege Guard policy, no further policies will be processed for that application, so it is important to keep this in mind when multiple GPOs are applied.

**Exceptions to Default Order of Processing**

The default order for processing settings is subject to the following exceptions:

- A GPO link may be enforced, or disabled, or both. By default, a GPO link is neither enforced nor disabled.

- A GPO may have its user settings disabled, its computer settings disabled, or all settings disabled. By default, neither user settings nor computer settings are disabled on a GPO.

- An organizational unit or a domain may have Block Inheritance set. By default, Block Inheritance is not set.

For information about the above modifications to default behavior, see Managing inheritance of Group Policy.

A computer that is a member of a workgroup processes only the local Group Policy object.
Privilege Guard Settings Storage and Backup

Privilege Guard stores its settings within Active Directory’s SYSVOL folder, within the storage area for the relevant GPOs, which are identified by their GUIDs. The settings are stored in an XML file and Activity Directory is then used as the distribution mechanism.

Privilege Guard Settings can be backed up by one of the following methods:

1. Privilege Guard settings files will be backed up as part of a standard ‘System State’ backup, which organizations should be performing as part of their standard backup routines.

2. Perform a manual backup of a GPO from with the GMPC, which will back up the GPO settings and Privilege Guard’s XML files.

3. In addition, Privilege Guard Settings may be manually exported and saved to a location of your choice. For more information on how to perform an export/import of policies refer to the Editing Privilege Guard Settings section of this guide.

Disconnected Users

Disconnected users are fully supported by Privilege Guard. When receiving its settings from a GPO, Privilege Guard automatically caches all the information required to work offline, so the settings will still be applied if the client is not connected to the corporate network. Of course, any changes made to the policy will not propagate to the disconnected computer until it reconnects to the domain and receives a Group Policy refresh. This behavior is identical to most of the standard Microsoft Group Policy settings.

Privilege Guard also supports a completely standalone configuration mode, where the settings are configured via a Local Group Policy for that machine, or deployed in a standalone XML configuration file. Again, these settings contain all of the information required to apply these policies offline.
Managing Privilege Guard Settings without Group Policy

Although Privilege Guard is implemented as a Group Policy extension, it also supports a standalone mode, which is independent of Group Policy.

Standalone mode allows you to deploy the Privilege Guard Settings with an XML file. You will need to employ a suitable deployment mechanism to distribute the XML file to your client computers.

To run the Privilege Guard management console in standalone mode:

1. Launch `mmc.exe`.
2. Select `Add/Remove Snap-in` from the `File` menu.
3. Select `Privilege Guard Settings` from the available snap-ins and click `Add`.
4. Click `OK`.

The Privilege Guard management console is now running in standalone mode and is not connected to a Group Policy Object (GPO).

On Windows XP and Server 2003 the Privilege Guard Settings will be saved to the following local XML file:

- `%ALLUSERSPROFILE%\Application Data\Avecto\Privilege Guard\PrivilegeGuardConfig.xml`

On Windows Vista, Windows 7 and Windows Server 2008 the Privilege Guard Settings will be saved to the following local XML file:

- `%ALLUSERSPROFILE%\Avecto\Privilege Guard\PrivilegeGuardConfig.xml`

If you installed the Privilege Guard Client when you installed the Privilege Guard management console then the client will automatically apply the policies in this XML file. For this reason, it is strongly recommended that you do not install the client if you will be using the console in standalone mode, unless you want the settings to be applied to your management computer. This may be case if you are evaluating Privilege Guard.

The Privilege Guard settings are edited in the same way as when editing GPO based policies. To distribute the XML file to multiple clients you will need to export the policies to an XML file and then deploy it to the location specified above. The Privilege Guard Client monitors this directory and will automatically load the XML file.

You must name the settings file `PrivilegeGuardConfig.xml` once it is deployed, otherwise the Privilege Guard Client will not load the settings. If you make changes to the Privilege Guard settings, simply redeploy the modified XML file and the Privilege Guard Client will automatically reload the settings.
Editing Privilege Guard Settings

The Privilege Guard Settings editor will automatically save any changes back to the appropriate GPO (or local XML file if you are using the standalone console).

Automatic saving may be disabled, by deselecting the Auto Commit Settings menu option on the Privilege Guard Settings node, but this is not recommended unless you are having performance issues. If you deselect the Auto Commit Settings option then you must select the Commit Settings menu option to manually save any changes back to the GPO. The Auto Commit Settings option is persisted to your user profile, so it will be set for all future editing of Privilege Guard Settings.

If you expand the Privilege Guard Settings node you will see 5 sections:

1. **Policies** - assign privileges to applications.
2. **Application Groups** - define logical groupings of applications.
3. **Messages** - define end user messages.
4. **Access Tokens** - define custom access tokens.
5. **Licensing** - manage Privilege Guard licenses.

**Policies**

Policies are defined to assign privileges to applications and audit application activity.

**Creating Policies**

It is recommended that you create your Application Groups before creating Policies. To create an application policy:

1. Expand the Privilege Guard Settings node.
2. Expand and select the Policies node.
3. Right click the Policies node and then click New Policy.

A new policy will be created and it will be highlighted so that you can rename it. Press enter once you have renamed the policy.

You may now fill in the Application Privileges, Shell Integration and Filters sections of the policy.

**Disabling Policies**

You may disable a policy, which will stop it from being processed by the Privilege Guard client. To disable a policy:

1. Select the Policy (in the tree view or results view).
2. Right click the Policy and then click Disable Policy.
To enable a policy (that is currently disabled):

1. Select the **Policy** (in the tree view or results view).
2. Right click the **Policy** and then click **Enable Policy**.

### Policy Precedence

If you create multiple policies then those that are higher in the list will have a higher precedence. Once an application matches a policy, no further policies will be processed for that application, so it is important that you order your policies correctly if an application could match more than one policy.

To give a policy a higher precedence:

1. Select the **Policy** (in the tree view or results view).
2. Right click the **Policy** and then click **Move Up**.
3. Repeat step 2 until you have the **Policy** positioned appropriately.

To give a policy a lower precedence, follow the procedure above, but click **Move Down**.

### Policy Description

You may set a description for a policy by accessing the properties for a policy:

1. Select the **Policy** in the tree view.
2. Right click the **Policy** and then click **Properties**.
3. Set the **Description** in the **Properties** dialog.
4. Click OK.

### Editing Policies - Filters

The **Filters** section of the policy can be used to further refine when a policy will actually be applied.

By default a policy will apply to all users/computers who receive the GPO. However, you can add one or more filters that will restrict the application of the policy:

- **Account Filter** – this filter will restrict the policy to specific users or groups of users.
- **Computer Filter** – this filter will restrict the policy to specific computers (names or IP addresses).
- **Time Filter** – this filter will restrict the policy to being applied at particular days of the week and times of the day.
- **Expiry Filter** – this filter will expire a policy at a set date and time.

If you add multiple filters to a policy then they will be combined with a logical AND. In other words, all of the filters must give a positive outcome for the policy to be applied.

**NOTE:** Time Filters and Expiry Filters can only be used once in a Policy.
Account Filters

The Account Filter specifies the users and groups for who the policy will be applied, assuming they receive the Group Policy Object (GPO).

To restrict the policy to specific groups or users:

- Select **Add a new filter** and then click **Add an Account Filter** from the available filters.
- Click **Add a new account**.
- The **Select Users or Groups** dialog will appear.
- Enter the relevant group or user accounts and click **Check Names** to validate the names or alternatively click **Advanced** to browse for groups and users.
- Click **OK**.

Domain and well known accounts will display a Security Identifier (SID). The SID will be used by the Privilege Guard Client, which will avoid account lookup operations. For local accounts the name will be used by the Privilege Guard Client, and the SID will be looked up when the policy is loaded by the client. Local Account will appear in the SID column of the accounts list for local accounts.

You may add more than one Account Filter if you want the user to be a member of more than one group of accounts for the policy to be applied.

Computer Filters

Computer filters can be used to target specific computers and connecting clients. You can specify a computer either using its host / DNS name, or by an IP Address.

To restrict the policy to specific computers by hostname:

1. Select the **Filters** tab and click **Add a new filter**...
2. Click on **Add a Computer Filter**...
3. In the new **Computer Filter**, click **Add a new hostname rule**...
4. The **Add hostname rule** dialog will appear.
5. Enter the hostname manually or alternatively click the browse button to open the **Select Computers** browser.
6. Click **Add**.
7. If the Computer Filter is intended for matching the hostname of remote computers using remote desktop sessions, check the option **Match the remote desktop (instead of the local computer)**

**NOTE:** To add multiple hostnames at the same time, add them as a comma separated list. You can also use wildcards ? and * to include hostnames with a similar naming convention.

To restrict the policy to specific computers by IP Address:

1. Select the **Filters** tab and click **Add a new filter**...
2. Click on **Add a Computer Filter**...
3. In the new Computer Filter, click Add a new IP rule...
4. The Add IP rule dialog will appear.
5. Enter the IP Address manually, in the format 123.123.123.123.
6. Click Add.
7. If the Computer Filter is intended for matching the IP Address of remote computers using remote desktop sessions, check the option Match the remote desktop (instead of the local computer)

NOTE: You can also use the wildcard * in any octet to include all addresses in that octet range, for example 192.168.*.*. Alternatively, you can specify a particular range for any octet, for example 192.168.0.0-254. Wildcards and ranges can be used in the same IP Address, but not in the same octet.

Time Filters

Time Filters can be used to restrict the policy to a specific 7 day time range.

To set a Time Filter for a policy:

1. Select the Filters tab and click Add a new filter...
2. Click on Add a Time Filter...
3. In the new Time Range Filter click Edit time restrictions.
4. The Time Restrictions dialog will appear.
5. Select Active and Inactive times in the time grid by either selecting individual elements are dragging over areas with the left mouse button held down.
6. Click OK.

The Time Filter is applied based on the user’s timezone by default. Uncheck the Use timezone of user for time restrictions (otherwise use UTC) checkbox to use UTC for the timezone.

Expiry Filters

Expiry Filters can be used to set an expiry time on a policy.

To set an Expiry Filter for a policy:

1. Select the Filters tab and click Add a new filter...
2. Click on Add an Expiry Filter...
3. In the new Expiry Filter set the date and time that you want the policy to expire.

The Expiry Filter is applied based on the user’s timezone by default. Uncheck the Use timezone of user for policy expiry (otherwise use UTC) checkbox to use UTC for the timezone.

Editing Policies - Application Privileges
The **Application Privileges** section of the policy is where access tokens are assigned to application groups.

You must define at least one application group before adding entries. To insert an application group:

1. Right click in the list and click **Insert Application Group**.
2. The **Application Group Actions and Auditing** dialog will appear.
3. Select the relevant **Application Group**.
4. If you wish to prompt the user before the application executes or block execution then select the relevant **End User Message**. You must define one or more messages before you can assign an end user message.
5. Select the **Access Token** dependent on the rights you wish to assign to the application group (see below).
6. If you wish to audit the application launching then select **On** for **Audit – Application Launch**.
7. If you wish to audit any privileged activity performed by the application then select **On** for **Audit- Privilege Monitoring**.

![Application Group Actions and Auditing](image)

**NOTE:** If you have selected a blocking message for the **End User Message** then the **Access Token** and the **Audit- Privilege Monitoring** options will be disabled.

The **Access Token** can be set to one of the following options (or you may define any number of custom access tokens, which will appear at the end of the list of standard options):
- **Passive (No Change)** – this option allows you to audit the applications in the application group without modifying the access token.
- **Enforce User’s Default Rights** – this option will ensure that the applications in the application group are assigned the user’s default rights.
- **Drop Admin Rights** – this option will remove local admin rights from the access token for applications in the application group.
- **Add Admin Rights** – this option will add local admin rights to the access token for applications in the application group.

If you select **On** or **Anonymous** (does not log the username) for **Audit – Application Launch** then an event will be logged to the application event log every time a process launches for the selected application group.

If you select **On** or **Anonymous** (does not log the username) for **Audit – Privilege Monitoring** then an event will be logged to the application event log the first time a process performs a privileged operation (an operation that would fail under a standard user account) for the selected application group. All privileged activity will also be logged to an XML file that can later be viewed with the **Privileged Guard Reporting Console** (an MMC snap-in). You may modify the behavior of Privilege Monitoring on the Privilege Monitoring tab of the policy.

Entries in the list will display an icon to denote whether the application group will be allowed to execute (green tick), blocked from executing (red cross), or passive (grey). An application group is blocked from executing by assigning an **End User Message** with a **Block Execution** message type. In all other circumstances the application will be allowed to execute.

The Summary View and Detail View can be used to show information about your application group entries in either graphical form or in table form.

If you add more than one application group into the list then entries that are higher in the list will have a higher precedence. Once an application matches an application group entry, no further application group entries or policies will be processed for that application. If an application could match more than one policy or application group entry then it is important that you order both your policies and application group entries correctly.

To give an application group entry a higher precedence within a policy:

1. Right click the **Application Group** entry and then click **Move Up**.
2. Repeat step 1 until you have the **Application Group** positioned appropriately.

To give an application group entry a lower precedence, follow the procedure above, but click **Move Down**. You may also click **Move Top** or **Move Bottom** to move an application group entry to the top or bottom of the list.

**Editing Policies - Shell Integration**
The Shell Integration section of the policy provides the ability for users to launch applications with specific privileges (usually admin rights) on demand.

To enable shell integration:

1. Select the Enable integration with shell context menu option.
2. You may change the menu option that is displayed, which defaults to Run with Privilege Guard.
3. If you do not wish to hide the standard Windows “Run As” menu option then deselect Hide “Run As” and “Run As Administrator” commands in shell context menu.
4. Insert one or more application groups into the list (follow the same procedure as outlined in the Application Privileges list).

Unlike Application Privileges, the application groups in the Shell Integration list will only receive the assigned privileges if the user launches a relevant application via the shell menu.
Policy Options

To edit the advanced options for a policy:

1. Expand the Policies node and select the relevant policy.
2. Right click on the selected policy and click Edit Policy Options.
3. The Policy Options dialog will appear.
4. Configure the Workstation and/or Monitoring options.
5. Click OK.

Workstation Options

The Workstation options provide settings to allow (or disallow) a user to unlock a shared workstation on Windows XP. Usually only administrators can unlock a shared workstation, but this policy option enables you to override that standard Windows XP behavior.

Monitoring Options

The Monitoring Options provide settings for Privilege Monitoring.

Privilege Monitoring will log privileged application activity that would fail under a standard user account. For an application to log activity you must enable Privilege Monitoring in the Application Privileges or Shell Integration sections of the policy, when you insert an application group.

In addition the application must be running under a privileged account, such as an administrator or power user. Alternatively an application could be running with elevated privileges because you have added it to Application Privileges or Shell Integration section of the policy and assigned it to run with admin rights.

The following Privilege Monitoring options are available:

- **Privilege Monitoring Events** – this option will log an event to the application event log, the first time an application performs a privileged operation.
- **Privilege Monitoring Log Files** – this option will enable logging of privileged activity to log files. The activity level can be set with the activity slider:
  - **Application Summary** – this option only logs information about the application.
  - **Application Summary and Activity** – this option logs information about the application and unique privileged activity (default option).
  - **Application Summary and Detailed Activity** – this option logs information about the application and all privileged activity.
- **Maximum Activity Records Per Process** – this option determines the maximum number of records that will be recorded per process.
- **Keep Application Logs for** – this option determines how long activity logs are kept before they will be purged.
If Activity Log Files is enabled then privileges activity is logged to XML files that can later be viewed with the Privileged Guard Reporting Console (an MMC snap-in). Refer to the Privilege Guard Reporting Console section of Auditing and Reporting.

**Application Groups**

Application Groups are used to define logical groupings of applications.

Only application groups may be assigned to policies, so you must define application groups for all of the applications you wish to assign to policies.

**Creating Application Groups**

To create an application group:

1. Expand the Privilege Guard Settings node.
2. Expand and select the Application Groups node.
3. Right click the Application Groups node and then click New Application Group.

A new application group will be created and it will be highlighted so that you can rename it. Press <Enter> once you have renamed the application group.

You may now add applications to the application group.

**Application Group Description**

You may set a description for an application group by accessing the properties for an application group:

1. Select the Application Group (in the tree view or results view).
2. Right click the Application Group and then click Properties.
3. Set the Description in the Properties dialog.
4. Click OK.

**Inserting Applications**

To insert an application:

1. Select the Application Group.
2. Right click in the applications list in the result pane to access the context menu.
3. Select Insert Application and then select the application type you wish to add from the sub menu.
4. After selecting an application type to insert, the Insert Application wizard will appear (with the exception of the ActiveX Control, Application Template and Running Process options).
5. Enter a file or folder name for the application or use the Browse File and Browse Folder buttons.
6. Click Next.
7. Enter a description for the application (the description will automatically be extracted from the file you entered, if it has a description).

8. Click Next.

9. Configure the Application Rules (detailed below) for the application (by default the Match File or Folder Name rule will be selected).

10. Click Next.

11. Configure the Advanced Options (detailed below) for the application.

12. Click Finish.

It is important to select a file for the application type you have chosen, otherwise it will fail to match when the Privilege Guard Client processes the application group.

For executable and control panel applets the description will automatically be extracted from the file (if it has a description). You may change the Description.

**Application Rules**

The Application dialog provides various Application Rules. The Privilege Guard Client must match every application rule you select before it will trigger a match, and you must select at least one rule. The following rules are available:

- **Match File or Folder Name** - applications are validated by matching the file or folder name entered in the edit box. You may also select a Pattern Matching option for the
filename. By default, pattern matching is set to Off, but this may be changed to either Wildcards (? and *) or Regular Expressions. If you don’t want the client to match the filename then uncheck this option and check one or more of the other validation options. Although you may enter relative filenames, it is strongly recommended that you enter the full path to a file.

- **Match Command Line** – if the filename is not specific enough you may match the command line, by checking this option and entering the command line to match. By default, the client will search for the text you type anywhere on the command line, as opposed to matching the complete command line. You may also select Pattern Matching options. If the Match Case option is set to True then it will force the client to perform a case sensitive match.

- **Match Publisher** – this option can be used to check for the existence of a valid publisher. If you have entered a file that exists on the system where the console is running, then the certificate subject name will automatically be retrieved, if the application has been signed. For Windows system files the Windows security catalog is searched, and if a match is found then the certificate for the security catalog is retrieved. Certificates are supported on Executables, Control Panel Applets, Installer Packages, Windows Scripts and PowerShell Scripts. In addition, any system file that is part of a security catalog, regardless of type, is supported. You may also select Pattern Matching options. If the Match Case option is set to True then it will force the client to perform a case sensitive match.

- **Match File Hash** – if the filename is not considered secure and the file is not signed then a file hash should be considered. Ensure that you have entered a file that exists on the system where the console is running, as this will cause the SHA-1 hash to be calculated automatically. Although you can edit this field, it is strongly recommended that you don’t unless you are typing in a hash that you have retrieved from another system. Although this validation option is the most secure, as it will validate the contents of the file, you must remember to update the file hash if the application file is changed. For this reason, file hashes should be a last resort, and other rules should be used to identify the application where possible.

- **Match Product Name** – if the file you entered has a Product Name property then it will automatically be extracted and you can choose to match on this property. You may also select Pattern Matching options. If the Match Case option is set to True then it will force the client to perform a case sensitive match.

- **Match Product Description** – if the file you entered has a Product Description property then it will automatically be extracted and you can choose to match on this property. You may also select Pattern Matching options. If the Match Case option is set to True then it will force the client to perform a case sensitive match.

- **Match Product Version** – if the file you entered has a Product Version property then it will automatically be extracted and you can choose Check Min Version and/or Check Max Version and edit the respective version number fields.
■ **Match File Version** – if the file you entered has a File Version property then it will automatically be extracted and you can choose **Check Min Version** and/or **Check Max Version** and edit the respective version number fields.

■ **Match Product Code** – if the file you entered is an installer package then the Product Code will automatically be extracted and you can choose to check this code.

■ **Match Upgrade Code** – if the file you entered is an installer package then the Upgrade Code will automatically be extracted and you can choose to check this code.

■ **Match if File Ownership is Trusted** – this option can be used to check if an application’s file is owned by a trusted owner (the trusted owner accounts are SYSTEM, Administrators or TrustedInstaller).

■ **Match if Application Requires Elevation (User Account Control)** – this option can be used to check if an application requires elevated rights to run and would cause User Account Control (UAC) to be triggered. This is a useful way to replace inappropriate UAC prompts with Privilege Guard end user messages to either block or prompt the user for elevation. As Windows XP on Windows Server 2003 do not support UAC, processes running on those systems will never match this rule.

■ **Match Parent Process** - this option can be used to check if an application’s parent process matches a specific application group. You must create an application group for this purpose or specify an existing application group in the **Parent Process Group**. Setting **match all parents in tree** to **True** will traverse the complete parent/child hierarchy for the application, looking for any matching parent process, whereas setting this option to **False** will only check the application’s direct parent process.

**Advanced Options**

The **Application** dialog has a number of **Advanced Options**:

■ **Allow child processes will match this application definition** – if this check box is enabled then any child processes that are launched from this application (or its children) will also match this rule. The rules are still processed in order, so it’s still possible for a child process to match a higher precedence rule (or policy) first. Therefore, this option will prevent a child process from matching a lower precedence rule. It should also be noted that if an application is launched via the shell integration rules and this option is enabled, then its children will be processed against the shell integration rules, and not the application privileges rules. If this option is not enabled then the children will be processed against the application privileges rules in the normal way. You can further refine this option by restricting the child processes to a specific application group. The default is to match **<Any Application>**, which will match any child process.
**Force Standard User Rights on File Open/Save Common Dialogs** – if the application allows a user to open or save files using the common Windows open/save dialog then checking this option will ensure that the user does not have admin privileges within these dialogs. These dialogs have explorer like features, and allow a user to rename, delete or overwrite files. If an application is running with elevated rights then the open/save dialogs would allow a user to replace protected system files. By default, Privilege Guard will force these dialogs to run with the user’s standard rights, which will prevent the user from tampering with protected system files.

**Regular Expressions Syntax**

Privilege Guard’s applications can control applications at a granular level by utilizing regular expression syntax.

<table>
<thead>
<tr>
<th>Meta character</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any character</td>
<td>All characters except the listed special characters match a single</td>
<td>“abc” matches “abc”</td>
</tr>
<tr>
<td>except [^$.]*()</td>
<td>instance of themselves. To match one of these listed characters use a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>backslash escape character (see below)</td>
<td></td>
</tr>
<tr>
<td>\ (backslash)</td>
<td>Escape character: interpret the next character literally.</td>
<td>“a+b” matches “a+b”</td>
</tr>
<tr>
<td>. (dot)</td>
<td>Matches any single character</td>
<td>“a.b” matches “abc” and “acc”, “adc”, etc.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Indicates a character class. Matches any character inside the brackets.</td>
<td>“[abc]” matches “a”, &quot;b&quot;, or &quot;c&quot;</td>
</tr>
<tr>
<td>^ (caret)</td>
<td>Negates the character class. A negated character class matches any</td>
<td>“[^abc]” matches all</td>
</tr>
<tr>
<td></td>
<td>character except those inside the brackets.</td>
<td>characters except “a”, “b”, and “c”</td>
</tr>
<tr>
<td>- (minus character)</td>
<td>In a character class, indicates a range of characters</td>
<td>“[0-9]” matches any of the digits “0” through “9”</td>
</tr>
<tr>
<td>?</td>
<td>Indicates that the preceding expression is optional: it matches once</td>
<td>“ab?c” matches “ac” or “abc”</td>
</tr>
<tr>
<td></td>
<td>or not at all.</td>
<td></td>
</tr>
<tr>
<td>+</td>
<td>Indicates that the preceding expression matches one or more times</td>
<td>“ab+c” matches “abc” and “abbc”, “abbc”, etc.</td>
</tr>
<tr>
<td>* (asterisk)</td>
<td>Indicates that the preceding expression matches zero or more times</td>
<td>“ab*c” matches “ac” and “abc”, “abbc”, etc.</td>
</tr>
<tr>
<td></td>
<td>(vertical pipe)</td>
<td>Alternation operator: separates two expressions, exactly one of which</td>
</tr>
<tr>
<td>()</td>
<td>Grouping operator</td>
<td>“{(One)}</td>
</tr>
</tbody>
</table>
Inserting ActiveX Controls

Unlike other application types, Privilege Guard only manages the privileges for the installation of ActiveX controls. ActiveX controls usually require administrative rights to install, but once installed they will run with the standard privileges of the web browser.

To insert an ActiveX Control:

1. Select the **Application Group**.
2. Right click in the applications list in the result pane to access the context menu.
3. Select **Insert Application** and then select the **ActiveX Control** from the sub menu.
4. The **ActiveX Control** dialog will appear.
5. Type a **Description** for the control and set the appropriate validation options (see below).
6. Click **OK**.

![ActiveX Control Dialog](image)
Validation Options

The ActiveX Control dialog has the following Validation Options:

- **Match Codebase** – this is enabled by default and it is recommended that you should use this option in most circumstances. You must enter the URL to the codebase for the ActiveX control. You may also select a Pattern Matching option for the codebase. By default, Pattern Matching is set to Off, but this may be changed to either Wildcards (?) and * or Regular Expressions. You may also select the Match Case option to force the client to perform a case sensitive match. Although you may enter a relative codebase name, it is strongly recommended that you enter the full URL to the codebase, as it is more secure. If you don’t want the client to match the codebase then uncheck Match Codebase and check one or more of the other validation options.

- **Match CLSID** – this option allows you to match the class ID of the ActiveX control.

- **Match Minimum Version** – this option allows you to set a minimum version number for the ActiveX control.

- **Match Maximum Version** – this option allows you to set a maximum version number for the ActiveX control.

Inserting Application Templates

Application Templates provide a simple way to pick from a list of known applications. A standard set of templates are provided, which cover basic administrative tasks for all supported operating systems, common ActiveX controls, software updaters and Avecto utilities.

To insert an Application Template:

1. Select the Application Group.
2. Right click in the applications list in the result pane to access the context menu.
3. Select Insert Application and then select the Application Template from the sub menu.
4. The Application Template dialog will appear.
5. Use the search box to locate an application template or scroll through the available application templates.
6. Select one or more application templates.
7. Click OK to add the selected application templates to the application group.
Inserting an Application from a Running Process

You may insert an application from a running process.

To insert an application from a Running Process:

1. Select the **Application Group**.
2. Right click in the applications list in the result pane to access the context menu.
3. Select **Insert Application** and then select the **Running Process** from the sub menu.
4. The **Running Process** dialog will appear.
5. Select **Show processes from all users** if you wish to select a process from another user’s session.
6. Select the relevant process from the list.
7. Click **OK**.
Application Group Summary

The Application Groups node displays a summary of all application groups. There are three different views to choose from. The same summary options are available on each Application Group, but only display applications in that group.

The **Summary** view displays a summarized description of the matching rules for each application.
Additionally, each application includes icons identifying where advanced options have been set:

- **Time Date Control Panel Applet**
  - Matched with filename "%SystemRoot%\System32\timeedit.cpl", trusted ownership, elevation required

  - Child processes will match this application definition
  - Match if Application Requires Elevation (UAC)
  - Match if File Ownership is Trusted
The **Light** view is similar to the Summary view, but does not show additional matching information or advanced option settings.

The Detailed view shows a table of all matching information and advanced option settings. The color key is as follows:

- Matching rule has been specified and enabled
- Matching rule has been specified and disabled
- Advanced option has been enabled
- Advanced option has been disabled

Each view includes an instant search option, which allows you to quickly find any application name, path or property which includes the entered text. The applications displayed are automatically filtered as you enter text.

To return to the full list of applications, simply remove any text from the Filter option.

**Messages**

You may define any number of end user messages, which can be displayed before applications launch. Messages may also be used to block the execution of applications. Once defined, a message may be assigned to an application group in the Application Privileges or Shell sections of a policy.

**Creating Messages**
To create a message:

1. Expand the Privilege Guard Settings node.
2. Expand and select the Messages node.
3. Right click the Messages node and then click New Message.
4. The New Message wizard will appear.
5. Select a message type from the drop-down list.
6. Click Next.
7. Customize the message display text and basic message options, or accept the default settings. These can be modified later.
8. Click Finish.

A new message will be created and it will be highlighted so that you can rename it. Press enter once you have renamed the message.

You may now customize the Message Options and Message Text for the message.

Message Description

You may set a description for a message by accessing the properties for a message:

1. Select the Message (in the tree view or results view).
2. Right click the Message and then click Properties.
3. Set the Description in the Properties dialog.
4. Click OK.

**Message Design**

Messages have a wide array of configuration options, which are detailed below.

As you change the various message options the preview message will automatically be updated. To test the message box simply click the preview message (any program information will contain placeholders).

Once you have configured the message options you should configure the Message Text for the message, which includes full multi-lingual support.

**Miscellaneous Settings**

- **Show message on secure desktop** – check this option to show the message on the secure desktop. This is recommended if the message is being used to confirm the elevation of a process, for enhanced security.

**Message Header Settings**

- **Header Style** – select the type of header, which can be No header, Privilege Guard, Warning, Question or Error.
- **Show Title Text** – determines whether to show the title text.
- **Title Text Color** – select the color for the title text (the automatic color is based on the Header Style).
- **Background Type** – set the background of the header, which can be Solid background, Gradient background or Custom image.
- **Color 1** – select the color for a Solid background or the first color for a Gradient background (the automatic color is based on the Header Style).
- **Color 2** – select the second color for a Gradient background (the automatic color is based on the selected Header Style).
- **Custom Image** – select the image for a Custom image background. This option is only enabled if you have selected Custom Image for the Background Type. Click the “…” button to import, export, modify or delete images using the Image Manager.

**Reference Hyperlinks**

If you have enabled the Show Reference hyperlinks option in the Message Design page, you can configure the display text and the URL of the hyperlink. The hyperlink is displayed at the bottom of the message:
NOTE: If the hyperlink is clicked by the user, the message will automatically be cancelled, and the URL will be opened in the default web browser.

Message Body Settings

- **Show Program Name** – this option determines whether to show the program name, which is either the description of the application or the relative file path if the application has no description.
- **Show Program Publisher** – this option determines whether to show the program publisher.
- **Show Program Path** – this option determines whether to show the full path to the application.
- **Show reference Hyperlink** – this option determines whether to show a hyperlink in the message (the hyperlink is configured in the Message Text section).
- **Show User Reason Prompt** – this option determines whether to prompt the end user to enter a reason before an application launches (Allow Execution message type) or to request a blocked application (Block Execution message type).

Authorization Settings

- **Authorization Type** – set this option to **User must authorize** to force the user to re-authenticate before proceeding. If you wish to use this option for over the shoulder departmental administration then set this option to **Designated user must authorize**.
- **Designated Users** – if the **Authorization Type** has been set to **Designated user must authorize** then click the “…” button to add one more user accounts or groups of users that will be allowed to authorize.
- **Run application as Authorizing User** – if the **Authorization Type** has been set to **Designated user must authorize** then this option determines whether the application runs in the context of the logged on user or in the context of the authorizing user. The default is to run in the context of the logged on user.
NOTE: If Run application as Authorizing User is set to Yes, then Privilege Guard will attempt to match a policy of the same type (Application Rule or Shell Elevation) for the authorizing user. If no policy is matched, then Privilege Guard will fall back to the original user policy.

Email Settings

The email settings are only enabled for blocking messages.

- **Allow user to email an application request** – check this option to allow the user to email a request to run an application (only available for the Block Execution message type).
- **Mail To** – email address to send the request to (separate multiple email addresses with semicolons).
- **Subject** – subject line for the email request.

Message Text

All of the text in the message may be configured in the Message Text section, which includes support for any number of end user languages.

As you change the message text the preview message will automatically be updated, based on the selected language. To test the message box simply click the preview message (any program information will contain placeholders).

Managing Languages

By default, a single language is defined (English) with a set of default text strings. You may add additional languages as follows:

1. Right click in the languages list and click **Insert Language**.
2. The Insert Language dialog will appear.
3. Select the relevant language (and region) from the drop down box.
4. Click **OK**.

If you have more than one language then you can set the default language. This is the language that will be used if an end user is using a language that has not been defined. The default language is set to English, but you may change the default language:

1. Select the language you want to set as the default language.
2. Right click and click **Set as Default Language**.

If you delete a language that has been set to the default language then the language at the top of the language list is set to the default language. You must always have at least one language defined.

**Setting the Message Text**

It is highly recommended that you change the default text strings, as many are simply placeholders, and all are defined in English.

To set the message text strings, select the relevant language in the languages list and simply edit the text values in the text property grid.

**NOTE:** The **Body Message** text supports multi-line text. The pipe symbol (|) is used to denote a newline, e.g. “line1|line2|line3”

**Changing the Message Text for Buttons**

Depending on the message options the message box will have either one or two buttons:

- For a prompt the message box will have OK and Cancel buttons.
- For a blocking message with **Allow user to email an application request** enabled the message box will have OK and Cancel buttons. It is highly recommended you change the **OK Button** text to be “Email”, unless you make it clear in the message text that the OK button will send an email request.
- For a blocking message with **Allow user to email an application request** disabled the message box will only have an OK button.

You may change the **OK Button** and **Cancel Button** text. For instance, you may change it to “Yes” and “No” if you are asking the end user a question.

**Image Manager**

The Image Manager allows you to add, modify, export and delete images that are referenced in message headers.

All images are stored inside the policies as compressed and encoded images.

It is strongly recommended that you delete any unused images to minimize the size of the policies, as Privilege Guard does not automatically delete unreferenced images.
To add an image:
1. Click **Add**.
2. The **Image Properties** dialog will appear.
3. Click **Import**.
4. Browse for an image and click **Open**.
5. Set a description for the image.
6. Click **OK**.

To modify an image:
1. Select the image in the list and click **Modify**.
2. The **Image Properties** dialog will appear.
3. Click **Import**.
4. Browse for the modified image and click **Open**.
5. Click **OK**.

To export an image:
1. Select the image in the list and click **Export**.
2. Browse to a folder and click **Save**.

To delete an image:
1. Select the image in the list and click **Delete**.
2. When prompted, click **Yes** to delete the image.
NOTE: If an image is referenced by any messages then you will not be allowed to delete it.

Access Tokens

Access Tokens allow you to optionally define any number of custom access tokens, which may be assigned to applications. Once defined, an access token may be assigned to an application group in the Application Privileges or Shell sections of a policy.

Creating Access Tokens

To create a new access token:

1. Expand the Privilege Guard Settings node.
2. Expand and select the Access Tokens node.
3. Right click the Access Tokens node and then click New Access Token.
4. The New Token wizard will open.
5. Select and access token type.
6. If you have not selected a blank token then click Next and you will be presented with the default privileges for the token type, which you may modify. For a token that adds Administrator rights, privileges are added to the token. For a token that removes Administrator rights, privileges are removed from the token.
7. Click Finish to exit the wizard.
The new access token will be displayed in the Access Tokens node. Right click the new token and choose Rename to enter a new name.

You may now define the Groups, Privileges, Integrity Level and Process Access Rights for the access token.

Access Token Description

You may set a description for an access token by accessing the properties:

1. Select the Access Token (in the tree view or results view).
2. Right click the Access Token and then click Properties.
3. Set the Description in the Properties dialog.
4. Click OK.

Editing Access Tokens

Groups

The Groups section of the access token specifies the groups that will be added or removed from the access token.

To insert a group:
1. Right click in the groups list and click **Insert Accounts**.
2. The **Select Groups** dialog will appear.
3. Enter the relevant groups and click **Check Names** to validate the names or alternatively click **Advanced** to browse for groups.
4. Click **OK**.

By default, when you insert a group the **Add** checkbox is checked, and the group will be added to the access token. If you wish to remove the group from the access token then click the **Remove** checkbox for the relevant group.

Domain and well known groups will display a **Security Identifier (SID)**. The SID will be used by the Privilege Guard Client, which will avoid account lookup operations. For local groups the name will be used by the Privilege Guard Client, and the SID will be looked up when the access token is created by the client. **Local Account** will appear in the SID column of the groups list for local groups.

**Setting the Token Owner**

By default, the owner of an access token that includes the Administrators group will have the owner set to the Administrators group. If the Administrators group is not present in the access token then the User is set as the owner.

If you wish the User to be the owner, regardless of the presence of the Administrators group, then click the **Ensure the User is always the Token Owner** checkbox.

**Anti-Tamper Protection**

By default, Privilege Guard prevents elevated processes from tampering with the files, registry and service that make up the Agent installation. It also prevents any elevated process from reading or writing to the local Privilege Guard policy cache.

If you wish to disable anti-tamper protection, then uncheck the **Enable anti-tamper protection** checkbox.

**Note:** Under normal circumstances, this option should remain enabled, except in certain scenarios where elevated tasks require access to protected areas. For instance, if you are using an elevated logon script to update the local Privilege Guard policy.

**Privileges**

The **Privileges** section of the access token specifies the privileges that will be added or removed for the access token.

If you wish to add a privilege to the access token then click the **Add** checkbox for the relevant privilege.

If you wish to remove a privilege from the access token then click the **Remove** checkbox for the relevant privilege.
To clear, add or remove multiple privileges, select the relevant privileges and then right click to access the context menu. Select Reset Privilege, Add Privilege or Remove Privilege respectively.

To add or remove the privileges associated with an administrator, select Add Admin Privileges or Remove Admin Privileges respectively.

To clear all of the privileges in the access token before applying privileges, check the Remove all existing privileges in access token before applying privileges checkbox. If this checkbox is left unchecked then the privileges are added or removed from the user’s default access token.

Refer to Appendix A (Windows Privileges) for further information.

**Integrity Level**

The Integrity Level section of the access token specifies the integrity level for the access token. The integrity level is ignored if the Privilege Guard Client is running on Windows XP or Windows Server 2003.

To set the integrity level:

1. Select the Set the integrity level in access token radio button.
2. Set the appropriate integrity level with the slider.

The integrity level should be set as follows:

<table>
<thead>
<tr>
<th>Integrity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Included for completion and should not be required</td>
</tr>
<tr>
<td>High</td>
<td>Set the integrity level associated with an administrator</td>
</tr>
<tr>
<td>Medium</td>
<td>Set the integrity level associated with a standard user</td>
</tr>
<tr>
<td>Low</td>
<td>Set the integrity level associated with protected mode (an application may fail to run or function in protected mode)</td>
</tr>
<tr>
<td>Untrusted</td>
<td>Included for completion and should not be required</td>
</tr>
</tbody>
</table>
Process Access Rights

The Process Access Rights section of the access token specifies the access rights that other processes, running in the same session, will have to processes that are assigned this access token.

Tokens that include the administrators group have a secure set of access rights applied by default, which will prevent code injection attacks on elevated processes initiated by processes running with standard user rights in the same session.

Adding or Removing an Access Right
If you wish to add an access right to the access token, click the checkbox for the relevant access right.

If you wish to remove an access right from the access token, click the checkbox for the relevant access right to clear it.

To add or remove multiple access rights, select the relevant access rights and then right click to access the context menu. Select Add Right or Remove Right respectively.

To reset all access rights to the most secure setting, select Reset all to default.

The access rights should be set as follows:

<table>
<thead>
<tr>
<th>Access Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROCESS_ALL_ACCESS</td>
<td>All possible access rights for a process object.</td>
</tr>
<tr>
<td>PROCESS_CREATE_PROCESS</td>
<td>Required to create a process.</td>
</tr>
<tr>
<td>PROCESS_CREATE_THREAD</td>
<td>Required to create a thread.</td>
</tr>
<tr>
<td>PROCESS_DUP_HANDLE</td>
<td>Required to duplicate a handle using DuplicateHandle.</td>
</tr>
<tr>
<td>PROCESS_QUERY_INFORMATION</td>
<td>Required to retrieve certain information about a process, such as its token, exit code, and priority class</td>
</tr>
<tr>
<td>PROCESS_QUERY_LIMITED_INFORMATION</td>
<td>Required to retrieve certain information about a process</td>
</tr>
<tr>
<td>PROCESS_SET_INFORMATION</td>
<td>Required to set certain information about a process, such as its priority class</td>
</tr>
<tr>
<td>PROCESS_SET_QUOTA</td>
<td>Required to set memory limits using SetProcessWorkingSetSize</td>
</tr>
<tr>
<td>PROCESS_SUSPEND_RESUME</td>
<td>Required to suspend or resume a process</td>
</tr>
<tr>
<td>PROCESS_TERMINATE</td>
<td>Required to terminate a process using TerminateProcess</td>
</tr>
<tr>
<td>PROCESS_VM_OPERATION</td>
<td>Required to perform an operation on the address space of a process</td>
</tr>
<tr>
<td>PROCESS_VM_READ</td>
<td>Required to read memory in a process using ReadProcessMemory</td>
</tr>
<tr>
<td>PROCESS_VM_WRITE</td>
<td>Required to write to memory in a process using WriteProcessMemory</td>
</tr>
</tbody>
</table>
**Licensing**

The Privilege Guard Client will not function unless it receives a valid license code. If multiple Group Policy Objects (GPOs) are applicable for a computer or user then as long as a valid license code appears in one of the GPOs then the Privilege Guard client will function. For instance, you may decide to add the Privilege Guard licenses to computer configuration section of a GPO that is applied to the domain, which will ensure that all computers in the domain will receive a valid license (for those computers that have the Privilege Guard client installed). If you are unsure then it is recommended that you always add a valid license when you are creating Privilege Guard Policies for a GPO.

**Inserting Licenses**

To insert a license:

1. Expand the **Privilege Guard Policies** node.
2. Select the **Licensing** node.
3. Right click in the licenses list and click **Insert License**.
4. Enter the **License Code** and click **Validate**.
5. If the license is valid then click **OK**.

**Signing Privilege Guard Settings**

The Privilege Guard Settings may be digitally signed and the Privilege Guard client can either enforce or audit the loading of signed settings.

**Creating and editing signed settings**

In order to digitally sign Privilege Guard settings, a PFX file containing an appropriate certificate and private key must be supplied, alongside the corresponding password for the PFX file.

**Note:** For settings to be correctly signed the certificate must have an OID that is specific to Avecto Privilege Guard. The chain of trust and revocation status is also checked by the client. If the settings have been tampered with since signing then the settings will also fail the signing check. For more information about creating certificate suitable for use with Privilege Guard, refer to **Appendix B – Signing Policies with Certificates**.

To digitally sign the Privilege Guard Settings:

1. Select the **Privilege Guard Settings** node.
2. Right click and select **Digitally Sign Settings**.
3. The Digitally sign your Privilege Guard Settings wizard will appear.
4. Select the Sign the settings with the following private key option.
5. Click the Select key button and browse for the PFX file that contains your digital certificate.
6. Enter the password for the pfx file.
7. Click Finish

To remove the digital signature from the Privilege Guard Settings:

1. Select the Privilege Guard Settings node.
2. Right click and click Digitally Sign Settings.
3. The Digitally sign your Privilege Guard Policy wizard will appear.
4. Select the Do not sign the settings option.
5. Click Finish

Once the Privilege Guard Settings have been digitally signed, the Privilege Guard Console will prompt the administrator for the corresponding PFX password when the settings are opened.
To modify the signed settings, you must enter a valid password for the PFX. Alternatively, you can select to remove the certificate from the settings, or open the settings in **Read Only** mode. Cancelling this prompt automatically opens the settings in **Read Only** mode.

Privilege Guard Client Certificate Mode

The Privilege Guard client will verify the certificate on any signed settings that it loads, regardless of where those settings originate. The verification process includes:

- Checking that the contents of the settings have not been altered.
- Establishing a chain of trust.
- Checking that the certificate used to sign the settings contained the **Privilege Guard Configuration Signing OID** in its **Enhanced Key Usage** extension.
- Checking for revocation where network connectivity allows.

Should the signature verification process fail for any reason, the course of action that is taken will depend upon the mode of operation. There are three modes of operation within the Privilege Guard Client. The mode is set via a command line option during installation:

**0 - Standard Mode**
The loading of unsigned settings will be audited as information events (event 200). Signed settings will be audited as information events (event 200) if they are correctly signed and as warning events (event 201) if they are incorrectly signed.

The Privilege Guard client is installed in **Standard Mode** by default.

1 - **Certificate Warning Mode**
The loading of unsigned settings will be audited as warning events (event 201). Signed settings will be audited as information events (event 200) if they are correctly signed and as warning events (event 201) if they are incorrectly signed.

2 - **Certificate Enforcement Mode**
Unsigned or incorrectly signed settings will not be loaded and audited as error events (event 202). Signed settings will be audited as information events (event 200) if they are correctly signed.

**Client Installation Mode Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CERT_MODE=0</td>
<td>Standard Mode</td>
</tr>
<tr>
<td>CERT_MODE=1</td>
<td>Certificate Warning Mode</td>
</tr>
<tr>
<td>CERT_MODE=2</td>
<td>Certificate Enforcement Mode</td>
</tr>
</tbody>
</table>

For example, to install the client MSI package silently in **Certificate Warning Mode**, use the following command line:

```
PGClient.msi -qn CERT_MODE=1
```

To install the client executable silently in **Certificate Warning Mode**, use the following command line:

```
PGClient.exe /s /v"/qn CERT_MODE=1"
```

**HTML View and Report**

The Privilege Guard Settings may be viewed as a HTML report, which follows the same style as the GPMC reports.

To show the HTML view:

1. Select the **Privilege Guard Settings** node.
2. Right click and click **View** and **HTML Report**.
Privilege Guard uses the same style as the GPMC for its HTML reports. You can expand and collapse the various sections of the HTML report to show or hide more detailed information.

To return to the Policy Editor view:

1. Select the **Privilege Guard Settings** node.
2. Right click and click **View** and **Policy Editor**.

You may also save the HTML report to a file (the HTML view does not have to be displayed to save the HTML report).

To save a HTML report:

1. Select the **Privilege Guard Settings** node.
2. Right click and click **Save Report**.
3. Enter a filename for the report and click **Save**.

**NOTE:** When displaying Resultant Set of Policy (RSoP) results the Privilege Guard Settings console will default to HTML view, but a read-only Policy Editor view may also be displayed.
Exporting and Importing XML

The Privilege Guard Settings may be exported to an XML file and imported back into the console.

This may be used to back up Privilege Guard Settings or to distribute them using an XML file, as opposed to using Group Policy.

To export the Privilege Guard Settings to an XML file:

1. Select the Privilege Guard Settings node.
2. Right click and click Export Privilege Guard Settings.

To import the Privilege Guard Settings from an XML file:

1. Select the Privilege Guard Settings node.
2. Right click and click Import Privilege Guard Settings.
3. When prompted, either click Yes to merge the imported policies into the current policies or No to overwrite the current settings.

Deleting Items and Conflict Resolution

Some items within the Privilege Guard Settings are referenced in other areas, such as Application Groups, Custom Messages and Custom Access Tokens. These items can be deleted at any time, and if they are not being referenced elsewhere, they delete without any further action required.

When an item is deleted, the Privilege Guard Console will check for any conflicts which may need to be resolved.
It the item being deleted is already in use elsewhere in your settings, then a conflict will be reported which will need to be resolved.
You can review each detected conflict and observe the automatic resolution which will take place if you proceed. If more than 1 conflict is reported, use the Next conflict and Previous conflict links to move between conflicts.

If you wish to proceed, click Resolve All to remove the item from the areas of your Privilege Guard Settings where it is currently in use.

Deleting Privilege Guard Settings

To delete Privilege Guard Settings from a Group Policy Object (GPO):

1. Select the Privilege Guard Settings node for either the Computer Configuration or User Configuration section, as appropriate.
2. On the Group Policy Management Editor Action menu, click Delete Privilege Guard Settings.
3. When prompted for confirmation, click Yes to delete the Privilege Guard Settings.
Application Templates

Standard Application Templates

Privilege Guard ships with some standard application templates to simply the definition of applications that are part of the operating system, common ActiveX controls and software updaters.

The standard application templates are split into convenient categories:

- Avecto Utilities
- Common ActiveX Controls
- Common Printer Driver Manufacturers
- Software Updaters
- Tools and utilities for administrators and developers
- Windows 7 and Windows Server 2008 R2
- Windows Vista and Windows Server 2008
- Windows XP and Windows Server 2003

Each category then has a list of applications for that category. Picking an application will cause the Application or ActiveX control dialogs to be pre-populated with the appropriate information.

Creating Custom Application Templates
Application templates are stored as XML files.

On Windows XP and Server 2003 the application templates are stored in:

- %ALLUSERSPROFILE%\Application Data\Avecto\Privilege Guard Templates\n
On Windows Vista, Windows 7 and Windows Server 2003 the application templates are stored in:

- %ALLUSERSPROFILE%\Avecto\Privilege Guard Templates\n
The Standard Application Templates are stored in a single file named WindowsTasks.xml, and it is highly recommended that you do not change these templates.

Instead, you should create your own XML template files. Application templates are simply a set of Application Groups that have been exported from the Privilege Guard Management console as an XML file.

It is recommended that you create templates on a computer that is not running the Privilege Guard client, as you will rely on Privilege Guard’s standalone console to create the application templates.

To run the Privilege Guard management console in standalone mode:

1. Launch mmc.exe.
2. Select Add/Remove Snap-in from the File menu.
3. Select Privilege Guard Settings from the available snap-ins and click Add.
4. Click OK.

The Privilege Guard management console is now running in standalone mode and is not connected to a Group Policy Object (GPO). However, it will be saving any settings locally, and these would be picked up by the client, if it was installed.

To create a set of application templates, simply create some application groups and populate the application groups with applications. The application groups will become the Categories, and the applications in each application group will be the list of Applications for that Category. Once you have defined your application templates, simply export the settings to an XML file:

1. Select the Privilege Guard Settings node.
2. Right click and click Export Privilege Guard Settings.

To import an application template file back into the management console for editing:

1. Select the Privilege Guard Settings node.
2. Right click and click Import Privilege Guard Settings.
3. When prompted click No to overwrite the current policies.
Remember to re-export your application templates once you’ve modified them.

The final step is to copy your application templates to the application templates directory on any machines where the management console is being used to create Privilege Guard settings. The management console automatically loads all of the application templates in the application templates directory and merges them to create a single list of categories.
Avecto End User Utilities

Privilege Guard includes three end user utilities to enable users to manage advanced network adapter settings, printer settings, and software installations, as many of these capabilities would usually be hosted in the explorer shell, making it difficult to give these tasks elevated rights.

Avecto Network Adapter Manager

The network adapter manager presents the network adapters to the end user in a familiar format.

![Avecto Network Adapter Manager](image)

From this utility a user may modify the properties of a network adapter, rename an adapter or disable an adapter.

In order to make the network adapter manager available to a user you must perform the following steps:

1. Add the **Avecto Network Adapter Utility** to the **Privilege Guard Settings** and assign **Admin Rights** to this application for the relevant users (the utility is included in the **Application Templates**).

2. Create a shortcut on the user’s desktop to the network adapter manager, **PGNetworkAdapterUtil.exe**, which can be found in the Privilege Guard client installation directory (usually **C:\Program Files\Avecto\Privilege Guard Client**).
Avecto Printer Manager

The printer manager utility presents the printers to the end user in a familiar format.

From this utility a user may add and delete printers, access printer properties and preferences, view the printer queue, access Print server properties and print a test page.

In order to make the printer manager available to a user you must perform the following steps:

1. Add the **Avecto Printer Management Utility** to the **Privilege Guard Settings** and assign **Admin Rights** to this application for the relevant users (the utility is included in the **Application Templates**).

2. Create a shortcut on the user’s desktop to the printer manager, **PGPrinterUtil.exe**, which can be found in the Privilege Guard client installation directory (usually **C:\Program Files\Avecto\Privilege Guard Client**).
Avecto Programs and Features Manager

The programs and features manager presents the installed software to the end user in a familiar format.

![Avecto Programs and Features Manager](image)

From this utility a user may uninstall, change and repair software that is installed on their computer.

In order to make the programs and features manager available to a user you must perform the following steps:

1. Add the **Avecto Programs and Features Manager** to the **Privilege Guard Settings** and assign **Admin Rights** to this application for the relevant users (the utility is included in the **Application Templates**).

2. Create a shortcut on the user’s desktop to the programs and features manager, **PGProgramsUtil.exe**, which can be found in the Privilege Guard client installation directory (usually C:\Program Files\Avecto\Privilege Guard Client).
Troubleshooting

Resultant Set of Policy

Privilege Guard provides full support for Resultant Set of Policy (RSoP). Resultant Set of Policy is usually accessed through the Group Policy Management Console (GPMC).

The GPMC supports two modes of operation for RSoP:

- Group Policy Modeling (RSoP planning mode)
- Group Policy Results (RSoP logging mode)

RSOP can be used to establish the policy being applied to a particular user or computer, to aid troubleshooting. Detailed HTML reports are generated, which may also be exported to aid policy documentation.

Group Policy Modeling

To run a Group Policy Modeling query (RSoP planning), perform the following steps from the Group Policy Management Console (GPMC):

1. Double click the forest in which you want to create a Group Policy Modeling query.
2. Right click Group Policy Modeling and then click Group Policy Modeling Wizard.
3. In the Group Policy Modeling Wizard click Next and enter the appropriate information.
4. After completing the wizard, click Finish.
5. Right click the node for the completed query in the console tree, and then click Advanced View to launch the Resultant Set of Policy window.
6. Select the Privilege Guard Settings node under the Computer Configuration or User Configuration node to view the RSoP HTML report for Privilege Guard.

Privilege Guard will also appear in the Summary tab of the Group Policy Modeling node. Expand the Component Status section of the HTML report to find out whether RSoP data has been collected for Privilege Guard.

Privilege Guard does not appear in the Settings tab of the Group Policy Modeling node, as third party Group Policy extensions are not detailed in this HTML report. You must use the Advanced View, as outlined above, to view Privilege Guard Policies for an RSoP query.

Group Policy Results

To run a Group Policy Results query (RSoP logging), perform the following steps from the Group Policy Management Console (GPMC):

1. Double click the forest in which you want to create a Group Policy Results query.
2. Right click Group Policy Results and then click Group Policy Results Wizard.
3. In the Group Policy Results Wizard click Next and enter the appropriate information.
4. After completing the wizard, click **Finish**.
5. Right click the node for the completed query in the console tree, and then click **Advanced View** to launch the **Resultant Set of Policy** window.
6. Select the **Privilege Guard Settings** node under the **Computer Configuration** or **User Configuration** node to view the RSoP HTML report for Privilege Guard.

Privilege Guard will also appear in the **Summary** tab of the **Group Policy Results** node. Expand the **Component Status** section of the HTML report to find out whether RSoP data has been collected for Privilege Guard.

Privilege Guard does not appear in the **Settings** tab of the **Group Policy Results** node, as third party Group Policy extensions are not detailed in this HTML report. You must use the **Advanced View**, as outlined above, to view Privilege Guard Policies for an RSoP query.

**General Troubleshooting Tips**

**Check Privilege Guard Client is Installed and Functioning**

If you are having problems the first step is to check that you have installed the client and that the client is functioning.

The easiest way to determine if the client is installed and functioning is to check for the existence of the **Avecto Privilege Guard Service** in the services management console. Ensure that this service is both present and started. The Privilege Guard service is installed by the Privilege Guard Client and should start automatically.

**NOTE:** On Windows XP SP2 and Windows Server 2003 ensure that you have installed the client with the executable installer, which includes MSXML6. Alternatively you may use the MSI package, but you must also install Microsoft MSXML6 or ensure that it is already installed.

The Privilege Guard service requires MSXML6 in order to load the Privilege Guard settings, but the service will still run even if MSXML6 is not present.


**Check Settings are Deployed**

Assuming the Privilege Guard Client is installed and functioning, the next step is to check that you have deployed settings to the computer or user.

You can use RSoP logging mode to determine whether the computer has received settings. Assuming the RSoP query shows that Privilege Guard Settings have been applied, you should check the contents of the settings (including licensing and policy precedence).
Check Settings are Licensed

One of the most common reasons for Privilege Guard not functioning is the omission of a valid license from the Privilege Guard Settings. If you are creating multiple GPOs, then you must ensure that the computer or user receives at least one GPO that contains a valid license. To avoid problems it is simpler to add a valid license to every set of Privilege Guard Settings that you create.

Check Policy Precedence

Assuming that Privilege Guard is functioning and licensed, most other problems are caused by configuration problems or policy precedence problems.

Once an application matches an application group entry in the Application Privileges or Shell sections of a policy then processing will not continue for that applications. Therefore, it is vital that you order your entries correctly:

- If you create multiple policies then policies higher in the list have a higher precedence.
- If you have multiple application group entries in the Application Privileges and Shell sections of a policy then entries higher in the list have a higher precedence.

The Application Privileges section is applied to applications that are launched either directly by the user or by a running process. The Shell section is only applied to applications that are launched from the Privilege Guard shell menu (if enabled).

If you have multiple GPOs applying to a user and/or computer then you should ensure that GPO precedence rules are not causing the problem. If multiple GPOs are applied to a computer or user then the Privilege Guard client will merge the computer GPOs and user GPOs by following Group Policy precedence rules. Once merged the user policies will take precedence over the computer policies. In other words the computer policies will only be processed if an application does not match an entry in the user policies.

For this reason, it is highly recommended that you do not create over-complex rules that rely on the merging of many GPOs, as this can become difficult to troubleshoot. If however, it makes sense to split rules over multiple GPOs, you should make use of RSoP to ensure that policies are being combined correctly. You must also remember that computer and user policies are processed separately, with user policies always being processed ahead of computer policies, if both exist.
Auditing and Reporting

Events

The Privilege Guard client sends events to the local application event log, dependent on the audit and privilege monitoring settings within the Privilege Guard Settings.

The following events are logged by the Privilege Guard client:

Process Events

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>process has started with admin rights added to token.</td>
</tr>
<tr>
<td>101</td>
<td>process has been started from the shell context menu with admin rights added to token.</td>
</tr>
<tr>
<td>102</td>
<td>process has started with admin rights added to token, which was inherited from its parent.</td>
</tr>
<tr>
<td>103</td>
<td>process has started with admin rights dropped from token.</td>
</tr>
<tr>
<td>104</td>
<td>process has been started from the shell context menu with admin rights dropped from token.</td>
</tr>
<tr>
<td>105</td>
<td>process has started with admin rights dropped from token, which was inherited from its parent.</td>
</tr>
<tr>
<td>106</td>
<td>process has started with no change to the access token (passive mode).</td>
</tr>
<tr>
<td>107</td>
<td>process has been started from the shell context menu with no change to the access token (passive mode).</td>
</tr>
<tr>
<td>108</td>
<td>process has started with no change to the access token, which was inherited from its parent (passive mode).</td>
</tr>
<tr>
<td>109</td>
<td>process has started with user’s default rights enforced.</td>
</tr>
<tr>
<td>110</td>
<td>process has started from the shell context menu with user’s default rights enforced.</td>
</tr>
<tr>
<td>111</td>
<td>process has started with user’s default rights enforced, which was inherited from its parent.</td>
</tr>
<tr>
<td>112</td>
<td>process requires elevated rights to run.</td>
</tr>
<tr>
<td>113</td>
<td>process has started with custom token applied.</td>
</tr>
<tr>
<td>114</td>
<td>process has started from the shell context menu with user’s custom token applied.</td>
</tr>
<tr>
<td>115</td>
<td>process has started with custom token applied, which was inherited from its parent.</td>
</tr>
<tr>
<td>116</td>
<td>process execution was blocked.</td>
</tr>
</tbody>
</table>
Each process event contains the following information:

- Command line for the process
- Process ID for the process (if applicable)
- Parent process ID of the process
- Policy that applied
- Application Group that contained the process
- End user reason (if applicable)
- Custom access token (if applicable)
- File hash
- Certificate (if applicable)

Note: Each process event also contains Product properties, where applicable, but these can only be viewed in the Privilege Guard Reporting Console.

**Configuration Events**

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Successfully loaded Privilege Guard configuration (information)</td>
</tr>
<tr>
<td>201</td>
<td>Loaded Privilege Guard configuration but encountered non-critical problem (warning)</td>
</tr>
<tr>
<td>202</td>
<td>Failed to load Privilege Guard configuration (error)</td>
</tr>
</tbody>
</table>

Each configuration event contains the following information:

- File Name (Cached XML file)
- Configuration Source (Group Policy or Local Computer)
- Configuration Security (Plain Text XML or Signed XML)
- Security Information (Subject DN of Signed Certificate)
- GPO Name
- GPO display Name
- GPO Version
- GPO Active Directory Path
- GPO File System Path
- GPO Link Information

**Privilege Guard Reporting Console**

The Reporting Console is an MMC snap-in and may connect to the local computer or a remote computer. The Reporting Console enables you to view Privilege Guard events and Privilege Monitoring logs for the relevant computer.

To run the Privilege Guard Reporting console:

1. Launch `mmc.exe`.
2. Select *Add/Remove Snap-in* from the *File* menu.
3. Select **Privilege Guard Reporting** from the available snap-ins and click **Add**.

Before the snap-in is added you will be prompted to select a computer to manage. The local computer will be selected by default. To connect to a remote computer select the **Another computer** radio button and enter the name of the remote computer or click the **Browse** button to browse for a computer. Privilege Guard supports connection to a central event collector if you are using event forwarding to centralize events to a server.

You may also select an alternative location for the Privilege Monitoring logs, if you have a scripted solution in place to centralize the Privilege Monitoring logs to a server. Simply enter the network location or click the **Browse** button to browse to the location.

4. Click **Finish**.
5. Click **OK**.

![Property Page](image)

**NOTE:** You may add multiple instances of the Privilege Guard Reporting snap-in and connect them to different computers, if you wish.

**Auditing Report**

The Auditing Report lists all the Privilege Guard events that have been logged at that computer.
For each event the following information is available:

- Date
- Event ID
- Filename (Codebase for ActiveX controls)
- Command Line
- Event Description
- Username
- Computer Name
- Policy
- Application Group
- Reason
- Custom Token
- Hash (CLSID for ActiveX controls)
- Certificate
- PID
- Parent PID

By default, the report will show all Privilege Guard events from the event log, but you may filter the report on date, event number, username and computer name. Click **Update Report** to reload the report.

The application definitions that are contained within each event may be copied and then pasted into application groups in the Privilege Guard Management Console. Simply select one or more events and then select **Copy** from the context menu. You will now be able to paste the applications into an application group.

**Privilege Monitoring Report**

**Application View**

The application view shows a list of all applications that have been monitored. Applications are identified by their file hash.

For each application the following information is available:

- Filename/Codebase
- Type
- Instances
- Description
- Certificate
- Hash (CLSID for ActiveX controls)
- Version (ActiveX controls only)
The instances column shows the number of times the application has been run. To view the individual instances for an application, double click the entry in the list or select Show Details from the context menu. The Process View will be displayed.

By default, the report will show all the monitored applications, but you may filter the report on date, username and computer name. Click Update Report to reload the report.

Process View

The process view shows a list of the individual processes that have been monitored for an application.

For each process the following information is available:

- Date
- PID
- Command Line
- Filename

To view the activity for a process, double click the entry in the list or select Show Details from the context menu. The Activity View will be displayed.

Activity View

The activity view shows a list of all the privileged activity that has been carried out by a process. Privileged activity is any activity that would have failed under a standard user account.

For each activity entry the following information is available:

- Date
- Operation
- Object
- Parameters

To go back to the process view double click the “back up” entry in the list or select Back Up from the context menu. The Process View will be displayed.

Diagnosing Connection Problems

The Privilege Guard Reporting console needs to connect to the registry and administrator file shares when connecting to a remote computer.

If the console fails to connect or fails to retrieve data then the most common causes are:

1. The Remote Registry service needs to be started on the remote machine. On Windows Vista and Windows 7 this service is not set to start automatically, so you should ensure that it has been started.
2. The Windows Firewall may be blocking the incoming requests. Enabling the **File and Printer Sharing** exception in the Windows Firewall Settings should resolve this problem.
Deployment Scenarios

Privilege Guard has an extremely flexible rules system that can be used to elevate applications and white list applications. It is also possible for Privilege Guard to discover the applications that require elevated rights to run or function correctly.

This section provides some common scenarios, and understanding these basic scenarios should help you to build more complex settings.

Each scenario will create new settings, but you may wish to combine several of these scenarios into single settings.

It is assumed that you are already familiar with creating Privilege Guard Settings and adding policies and application groups, which was covered earlier in this guide.

Application Elevation

The most fundamental concept within Privilege Guard is the elevation of applications under a standard user account. Here are the steps to elevating a single application. We will elevate taskmgr.exe in this example, but you may add any applications you wish:

1. Create Privilege Guard Settings in a GPO or Local Computer Policy.
2. Create a new application group and rename it Elevated Applications.
3. Insert an Executable application and browse for taskmgr.exe (in windows\system32).
4. Create a new policy and rename it Elevation Policy.
5. Add the Elevated Applications group to the Application Privileges section of the Elevation Policy (the Access Token will default to Add Admin Rights, but you should change Audit – Application Launch to On).

You may wish to extend this policy to:

- Add more applications to the Elevated Applications group.
- Add an end user message before the application is elevated. This is only recommended if you need to convey a message to the user or want them to re-authenticate or provide a reason. Refer to the Messages section of Editing Privilege Guard Policies.
- Use a custom token, as opposed to adding Admin Rights. In most situations this is not necessary and can lead to problems if you do not give an application the privileges it requires to function correctly. However, if you have identified the precise set of privileges that an application requires then you may create a custom token to assign a more restrictive set of privileges. Refer to the Access Tokens section of Editing Privilege Guard Settings.
On Demand Elevation

For more demanding users or during the initial phase of implementing least privilege you may wish to give the user the flexibility to launch any application with admin rights. Crucially this is achieved under a standard user account and applications that are elevated can be audited. For advanced users, you may wish to leave this feature in place permanently, but if you are using it to find out which applications the user needs to run with admin rights, you may remove it once you have used the audit logs to create a more locked down policy as outlined in the Application Elevation scenario.

Here are the steps to creating an “On Demand” policy:

1. Create Privilege Guard Settings in a GPO or Local Computer Policy.
2. Create a new application group and rename it All Applications.
3. Insert an Executable application and enter *.exe for the filename (matches any application).
4. Create a new policy and rename it On Demand Policy.
5. Enable the shell context menu in the Shell Integration section of the On Demand Policy.
6. Add the All Applications group to the Shell Integration section of the On Demand Policy (the Access Token will default to Add Admin Rights, but you should change Audit – Application Launch to On).

You may wish to extend this policy to:

- Add an end user message before an application is elevated. This is highly recommended as the user is making the decision on which applications to elevate. You should convey a suitable message to the user and inform them that their actions will be audited. You may also wish to ask the user for a reason for elevating an application and to re-authenticate for added security. Refer to the Messages section of Editing Privilege Guard Settings.
- Turn on Privilege Monitoring for the on demand applications, which will audit privileged operations. This will provide application forensics in the situation where a user has launched an application with elevated rights and you wish to understand the privileged behavior of that application. This can be valuable when auditing server administrators or to troubleshoot any problems that may have been caused by privileged applications. Refer to the Shell Integration and Privilege Monitoring Options sections of Editing Privilege Guard Settings for more information on turning on Privilege Monitoring for an application group entry and configuring Privilege Monitoring options.
- Combine the On Demand Policy with the Elevation Policy as outlined in the Application Elevation scenario. This is a common scenario for advanced users, where you automatically elevate any basic admin tasks and other privileged applications that you know the user requires as part of their role. The user then has the shell integration to elevate any additional applications on demand.
Application Discovery

It is a common scenario to have many users logging on with admin rights without fully understanding why those users need to log on with a privileged account. Privilege Guard policies may be defined to monitor privileged application behavior, in order to understand why a user requires a privileged account. Once the applications have been identified they can be added to an elevation policy, as outlined in the Application Elevation scenario.

Here are the steps to creating an application discovery policy:

1. Create Privilege Guard Settings in a GPO or Local Computer Policy.
2. Create a new application group and rename it All Applications.
3. Insert an Executable application and enter *.exe for the filename (matches any application).
4. Create a new policy and rename it Discovery Policy.
5. Add the All Applications group to the Application Privileges section of the Discovery Policy (change the Access Token to Passive (No Change) and Audit – Privilege Monitoring to On).

This policy will now monitor the behavior of all applications and log an event the first time a process performs a privileged operation. It will also log all of the privileged operations for that process into an XML file that can be viewed with the Privilege Guard Reporting Console. Only privileged operations will be logged, and in order for an application to perform a privileged operation it must be running with elevated rights, so the user must be logging on with an administrator or power user account. For this reason, you should leave your users with privileged accounts, while you are performing application discovery.

Ideally you will perform application discovery on a cross section of your user base, based on their role, as it will be easier to analyze the audit data from a sample of your user population.

After an appropriate period, maybe one or two weeks, you can review the audit logs, with the Privileged Guard Reporting Console, and use this information to create suitable Privilege Guard Settings to automatically elevate the relevant applications.

It is good practice to supplement the policy with an On Demand Elevation policy for all users before giving them a standard user account. This provides a simple mechanism to allow a user to elevate an application that has been omitted from the policy. Once you are confident with the policies you have defined you may remove the On Demand Elevation policy from users.
Application White Listing

In addition to controlling application privileges, Privilege Guard may also be used to block applications from running. Although this can be used to simply block a handful of unauthorized applications, a common scenario is the concept of application white listing, where a user is prevented from installing or running any unauthorized applications.

Here are the steps to creating a simple application white listing policy, which assumes that all authorized applications reside in the Windows and Program Files directories:

1. Create new Privilege Guard Settings in a GPO or Local Computer Policy.
2. Create a new application group and rename it **Trusted Applications**.
3. Insert an Executable application into the **Trusted Applications** group and enter %SystemRoot% for the folder name and accept the default rules in the wizard.
4. Insert another Executable application into the **Trusted Applications** group and enter %ProgramFiles% for the folder name and accept the default rules in the wizard.
5. If you are configuring policies for a 64-bit system then insert another Executable application into the **Trusted Applications** group and enter %ProgramFile(x86)% for the folder name and accept the default rules in the wizard.
6. Create another application group and rename it to **All Applications**.
7. Insert an Executable application into the **All Applications** group and enter *.exe for the filename (matches any application) and accept the default rules in the wizard.
8. Create a new message and pick the **Block Execution** message type. You may wish to tailor the default text for the message.
9. Create a new policy and rename it **Whitelist Policy**.
10. Add the **Trusted Applications** group to the Application Privileges section of the **Whitelist Policy** and change the Access Token to Passive (No Change).
11. Add the **All Applications** group to the Application Privileges section of the **Whitelist Policy** and change the Message to Block Execution and Audit – Application Launch to On.

If you have authorized applications that reside in locations other than %SystemRoot% (usually C:\Windows) and %ProgramFiles% (usually C:\Program Files) then ensure you add them to the **Trusted Applications** group.

Although you can add individual applications to the **Trusted Applications** group, it is highly recommended that you add folders where possible. This assumes that standard users are not permitted to modify or add files to the folders you define in the **Trusted Applications** group.

If it is not possible to rely purely on folders to define **Trusted Applications** then ideally you should use either the **Match Publisher** application rule to match applications from trusted publishers or the **Match if File Ownership is Trusted** to match applications that are owned by trusted accounts. You can also set rules based on product information, such as **Product Name**, **Product Description** and **Product Version**. As a last resort you may need to use the **Match File Hash** application rule. Although Privilege Guard fully supports file hashing, you should avoid excessive use of file hashing, as policies based on file hashes can become
difficult to maintain, as updates to authorized software will require new hashes to be added to the policies.

The application rules provide the flexibility to deal with many scenarios without resorting to file hashing, such as:

- Allowing all applications to run that have been installed by trusted accounts (Administrators, SYSTEM and TrustedInstaller). Use the **Match if File Ownership is Trusted** rule. This can be an extremely effective mechanism to trust all operating system files and applications that have been installed by these trusted accounts. Anything introduced by a user, will not run (assuming the user does not log on with an administrator account).

- Trusting all operating system files (including Windows updates) with a single **Publisher** rule that matches **Microsoft Windows** (Windows 7 and Vista), as Privilege Guard is integrated with Windows Security catalogs. This is also supported on Windows XP, but the Publisher name will be either **Microsoft Windows Publisher** or **Microsoft Windows Component Publisher**.

- Allowing all applications from a particular vendor to run by using the **Publisher** rule. You can also use a wildcard rule to match all signed applications, and then allow certain groups of users to run signed applications with a warning message, while blocking unsigned applications.

- Allowing software to be installed based on **Product Name** and **Publisher**. You may also need to elevate software packages by choosing **Add Admin Rights** for the **Access Token**, as many software packages will require admin rights to install.

**IMPORTANT NOTE:**

Although application white listing can be an extremely effective mechanism to eliminating all unauthorized software, you should spend sufficient time planning a suitable policy based on the roles of your users.

Application white listing may be unsuitable for some users, or you may need to implement a less severe implementation, where users are warned before unauthorized applications run, and their actions are audited. Simply replace the **Block Execution** message with a **Warning Message**, where the **Message Type** is set to **Allow Execution**. For instance, this may be a more suitable policy for technical users or laptop users, who may need to run unauthorized applications, but you wish to audit this activity. You may even remove the message altogether and simply audit the use of unauthorized applications.

Remember that both **Policies** and their **Application Privileges** entries are processed in order. When an application matches a policy or entry then it will not be processed against any remaining policies or entries. For this reason, it is important to get the order of your policies and their entries correct. For instance, ensure that any elevated applications appear above the white listed applications. If you have a catch all entry to block all remaining applications (*.exe) then ensure that it is the very last entry in your policies.
# Appendix A – Windows Privileges

## Standard User Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeChangeNotifyPrivilege</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeIncreaseWorkingSetPrivilege</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeShutdownPrivilege</td>
<td>Desktop Only</td>
<td></td>
<td>Desktop Only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeTimeZonePrivilege</td>
<td>N/A</td>
<td></td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeUndockPrivilege</td>
<td>Desktop Only</td>
<td></td>
<td>Desktop Only</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Administrator Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeBackupPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreateGlobalPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreatePagefilePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeCreateSymbolicLinkPrivilege</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SeDebugPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeEnableDelegationPrivilege</td>
<td>Server Only</td>
<td>Server Only</td>
</tr>
<tr>
<td>SeImpersonatePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeIncreaseBasePriorityPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeIncreaseQuotaPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeLoadDriverPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeMachineAccountPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeManageVolumePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeProfileSingleProcessPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeRemoteShutdownPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeRestorePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSecurityPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeShutdownPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemEnvironmentPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemProfilePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeSystemTimePrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SeTakeOwnershipPrivilege</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
## System Privileges

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SeAssignPrivilegeTokenPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeAuditPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeCreatePermanentPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeCreateTokenPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeLockMemoryPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeRelabelPrivilege</td>
<td>Yes</td>
<td>Server 2008 R2 Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeSyncAgentPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeTcbPrivilege</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeTrustedCredManAccessPrivilege</td>
<td>Yes</td>
<td>Server 2008 R2 Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SeUnsolicitedInputPrivilege</td>
<td>Yes</td>
<td>Server 2008 R2 Only</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix B – Signing Settings with Certificates

Creating a PFX file suitable for use with Privilege Guard

The Privilege Guard Settings Console requires access to a certificate and private key in order to digitally sign XML configuration. They must both be contained within a PFX or PKCS#12 format file, and the certificate must specifically be designated as suitable for signing Privilege Guard XML configuration. This is done via the Enhanced Key Usage extension when generating certificates.

This approach provides another means of ensuring that configuration cannot be created and signed by rogue users with access to a digital signature certificate intended for a different purpose.

Avecto has defined the following OID that should be added to the Enhanced Key Usage extension:

```
1.2.826.0.1.6538381.1.1.1 (Avecto Privilege Guard - Configuration - XML Configuration Signing)
```

Note that the Privilege Guard Settings Console does not check for the existence of this key usage. The checks are performed when verifying digital signatures in the Privilege Guard service. A configuration that is signed with a key that does not contain the specified Enhanced Key Usage extension, will ALWAYS fail signature verification checks.

The following sections provide details of two methods that can be used to generate a suitable PFX file, but it should be possible to use any Certification Authority to produce certificates with the appropriate Enhanced Key Usage extension.

Using makecert to generate a suitable test PFX file

Makecert is a certificate generation tool available from Microsoft that can be used to generate certificates for testing purposes.

The following makecert command line can be used to generate a certificate suitable for signing Privilege Guard configuration:

```
makecert -r -pe -n "CN=PG Signed XML Configuration" -sky signature -eku 1.2.826.0.1.6538381.1.1.1 -ss my
```

The parameters can be changed as required. The example will generate a self-signed certificate with an exportable private key, and adds it to the calling user’s local certificate store. The certificate must then be exported to a PFX file along with the private key in the usual way.

Note that the important parameter in the example is the addition of the Privilege Guard Configuration Signing OID to the Enhanced Key Usage extension (-eku 1.2.826.0.1.6538381.1.1.1)
If a self-signed certificate is used to sign the Privilege Guard settings, the certificate must be distributed to all clients in order for a chain of trust to be established and for signature verification to be successful. See Distributing Public Keys for more information.

**Using Microsoft Certificate Services to generate a suitable PFX file**

Microsoft Certificate Services is a useful way for organizations to run their own Certification Authority. In its enterprise editions, Certificate Services integrates with Active Directory to publish certificates and Certificate Revocation Lists to a location that is accessible to all computers in the Active Directory domain.

**NOTE:** Custom certificate templates can only be managed using enterprise CAs, therefore the following procedure is only possible on Enterprise Editions of Windows 2003/2008.

**Creating a Privilege Guard Configuration Certificate Template**

The easiest way to create a certificate with the Avecto Privilege Guard Configuration Signing Enhanced Key Usage extension is to create a new certificate template. Certificate templates allow the content and format of certificates to be defined so that users can request a certificate using a simple template rather than having to generate a complex certificate request.

There is a Microsoft guide for creating certificate templates available for download here: [Implementing and Administering Certificate Templates in Windows Server 2008](#).

In order to create a new certificate template an existing template must be duplicated and then modified:

**To create a new version 2 or 3 certificate template:**

1. Open the Certificate Templates snap-in.
2. In the Details pane, right-click an existing certificate that will serve as the starting point for the new certificate, and then click Duplicate Template.
4. On the General tab, enter the Template display name and the Template name, and then click OK.
5. Define any additional attributes for the newly created certificate template.

The template must then be edited in order to make it suitable for signing Privilege Guard configuration. This is done by adding the Avecto Privilege Guard Configuration Signing OID as an application policy for the template.

Firstly, the Configuration Signing OID must be defined.

**To define an object identifier:**

1. Open the Certificate Templates snap-in.
2. In the Details pane, right-click the certificate template you want to modify, and then click Properties.
3. On the **Extensions** tab, click **Application Policies**, and then click **Edit**.
4. In the **Edit Application Policies Extension** dialog box, click **Add**.
5. In **Add Application Policy**, ensure that the Privilege Guard Configuration Signing policy that you are creating does not exist, and then click **New**.
6. In the **New Application Policy** dialog box, provide the name and OID for the new application policy, as shown below, and then click **OK**.

![New Application Policy dialog box](image)

Now that the application policy has been defined, you can then associate it with the certificate template.

**To associate the application policy with the certificate template:**

1. Open the Certificate Templates snap-in.
2. In the details pane, right-click the certificate template you want to change, and then click **Properties**.
3. On the **Extensions** tab, click **Application Policies**, and then click **Edit**.
4. In **Edit Application Policies Extension**, click **Add**.
5. In **Add Application Policy**, click the desired application policy, and then click **OK**.

**Issuing the Privilege Guard Configuration Certificate Template**

Once the certificate template has been created in the Certificate Templates snap-in and has replicated to all domain controllers in the forest, it can now be published for deployment. The final task for publishing the certificate template is to select it for the CA to issue.

**To define which certificate templates are issued by a CA:**

1. In Administrative Tools, click **Certification Authority**.
2. In the console tree, expand **CAName** (where **CAName** is the name of your enterprise CA).
3. In the console tree, select the **Certificate Templates** container.
4. Right-click **Certificate Templates**, and then click **New, Certificate Template to Issue**.
5. In the **Enable Certificate Templates** dialog box, select the Privilege Guard Configuration certificate template that you want the CA to issue, and then click **OK**.

**NOTE:** In a Windows 2000 Server–based CA, the container is named Policy Settings.
Using the Privilege Guard Configuration Certificate Template in a Certificate Request

Once the certificate template has been issued, the template can be used during advanced certificate requests via the certsrv web interface, as shown below.

Once the certificate has been issued, it must be installed by the user before it can be exported to a PFX file in the usual way.

**NOTE:** The private key must exported to the PFX file as well.

Distributing Public Keys
In order for signature verification to be successful at every client that reads signed Privilege Guard Settings, a chain of trust must be established. For this to be done, a suitable trust point must be distributed to each client that will receive the Privilege Guard Settings. This should be done automatically when using a Microsoft enterprise CA.

Alternatively, public keys can be distributed via Group Policy, as discussed in the following TechNet article: Use Policy to Distribute Certificates.
Appendix C – Using Privilege Guard with McAfee ePO

The Privilege Guard Agent can optionally be configured to raise events into McAfee ePO.

NOTE: For more information on the Privilege Guard / McAfee ePO integration, refer to the Avecto Privilege Guard / McAfee ePO Integration Guide

Pre-requisites

The McAfee ePO Agent must be installed on the same machine as the Privilege Guard Agent.

Manual Installation of Privilege Guard Agent in ePO Mode

The Privilege Guard Agent must be installed in ePO Mode, by using a command-line option. This will install additional components required to communicate with the McAfee ePO Agent.

To install the client MSI package silently in ePO Mode, use the following command line:

   PGClient.msi -qn EPOMODE=1

To install the client executable silently in ePO Mode, use the following command line:

   PGClient.exe /s /v"/qn EPOMODE=1"

NOTE: If you are deploying Privilege Guard using ePO, then ePO Mode is automatically enabled. For more information, refer to the Avecto Privilege Guard / McAfee ePO Integration Guide

Disabling ePO Mode

Once installed in ePO Mode, the Privilege Guard Agent will automatically raise events to the ePO Agent, as well as raising events to the Application Event Log. If you wish to disable ePO mode at any time, set the following registry key:

   HKEY_LOCAL_MACHINE\Software\Avecto\Privilege Guard Agent\ DWORD “EPOMode”=0

To re-enable ePO logging, set the above DWORD value to 1.