



# Avecto

## Privilege Guard Getting Started 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.

## Contents

Introduction .....	4
Installing Privilege Guard .....	5
Configuring and Testing Privilege Guard .....	10
Running a Test Application.....	10
Launching the Group Policy Editor.....	11
Creating Privilege Guard Policies .....	12
Inserting a License .....	12
Creating an Application Group .....	13
Creating a Policy .....	14
Testing the Privilege Guard Policies .....	16
Further Testing.....	17
Elevating Different Applications.....	17
Shell Integration (on Demand).....	17
Privilege Guard in a Production Environment .....	19

---

## 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 policies 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 2 sections:

1. **Installing Privilege Guard** - walks you through the installation of the Privilege Guard Management Console and Privilege Guard Client on a single computer.
2. **Configuring and Testing Privilege Guard** – walks you through setting up sample policies on a single computer by using Local Computer Policy.
3. **Further Testing** – gives an overview of a few more simple tests that you may wish to perform.
4. **Privilege Guard in a Production Environment** – provides information on next steps, in terms of moving to a pilot or full production environment.

You will need a desktop running Windows XP, Windows Vista or Windows 7 and two user accounts:

- An administrator account, which you will use to install and configure Privilege Guard.
- A standard user account, which you will use to test the policies.

It is recommended that you use fast user switching, as this will enable you to quickly switch between the administrator account and standard user account, in order to test changes to the policies.

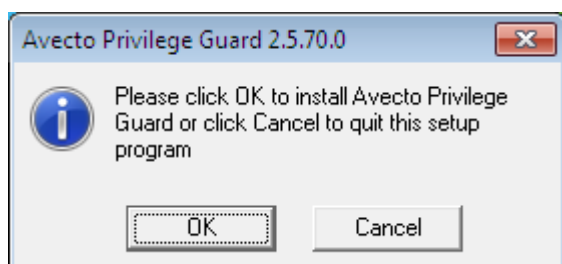
---

## Installing Privilege Guard

Log on with an administrator account.

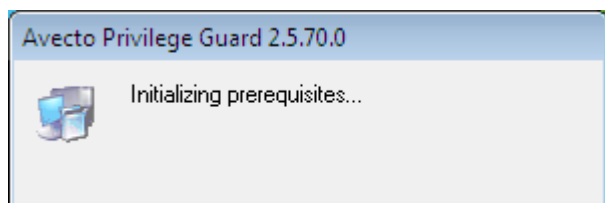
To install Privilege Guard run the appropriate installation package:

- For 32-bit systems run **AvectoPrivilegeGuard.exe**
- For 64-bit (x64) systems run **AvectoPrivilegeGuard\_x64.exe**

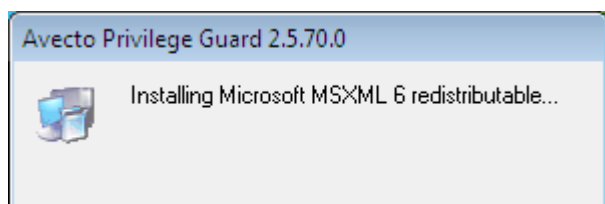


Click **OK** to continue with the setup of Privilege Guard.

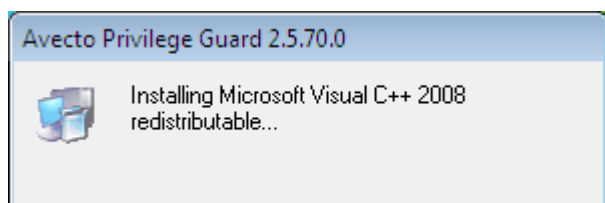
The installation will first install the prerequisites, which may take a few minutes.



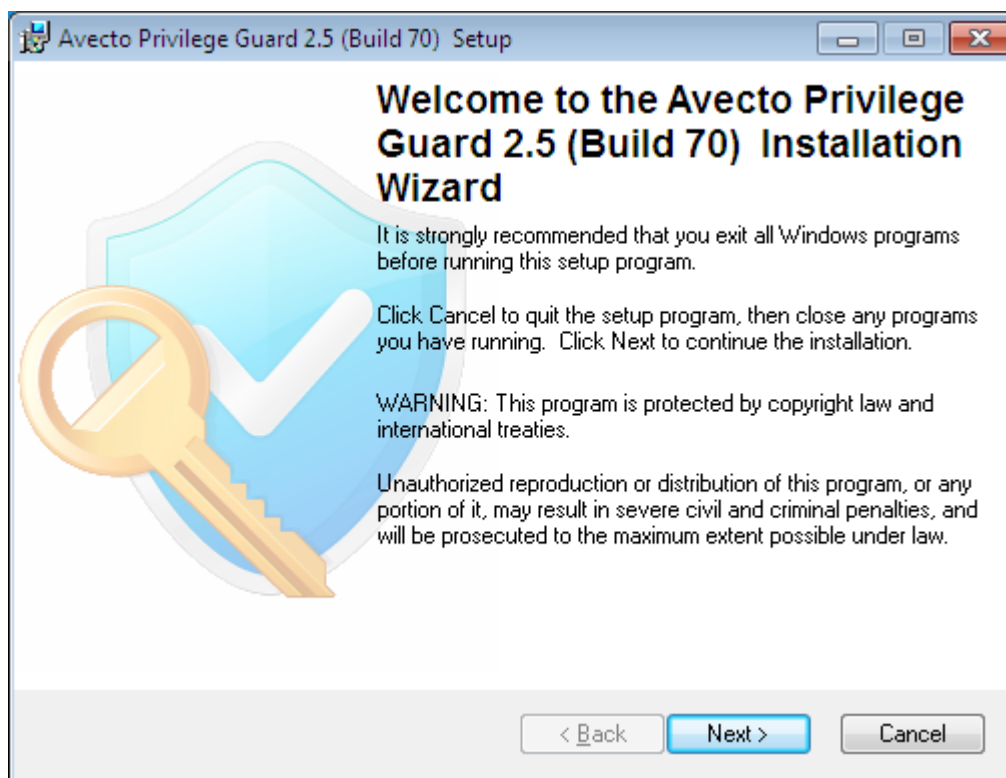
The first prerequisite is the MSXML 6 redistributable.



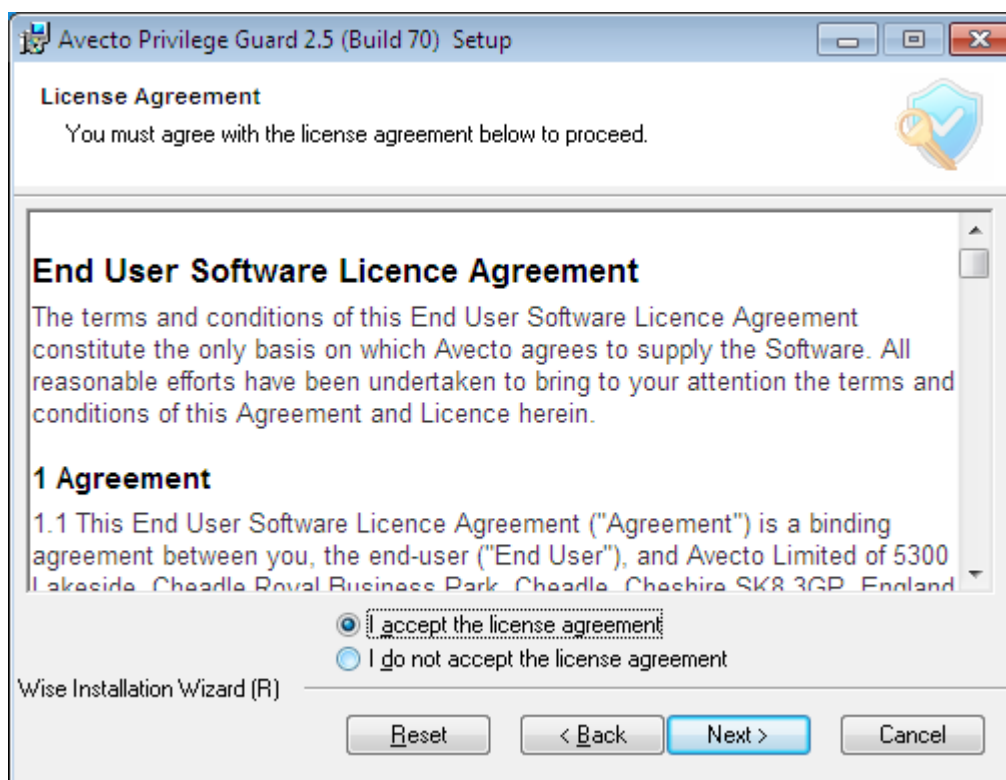
The second prerequisite is the Visual C++ 2008 redistributable.



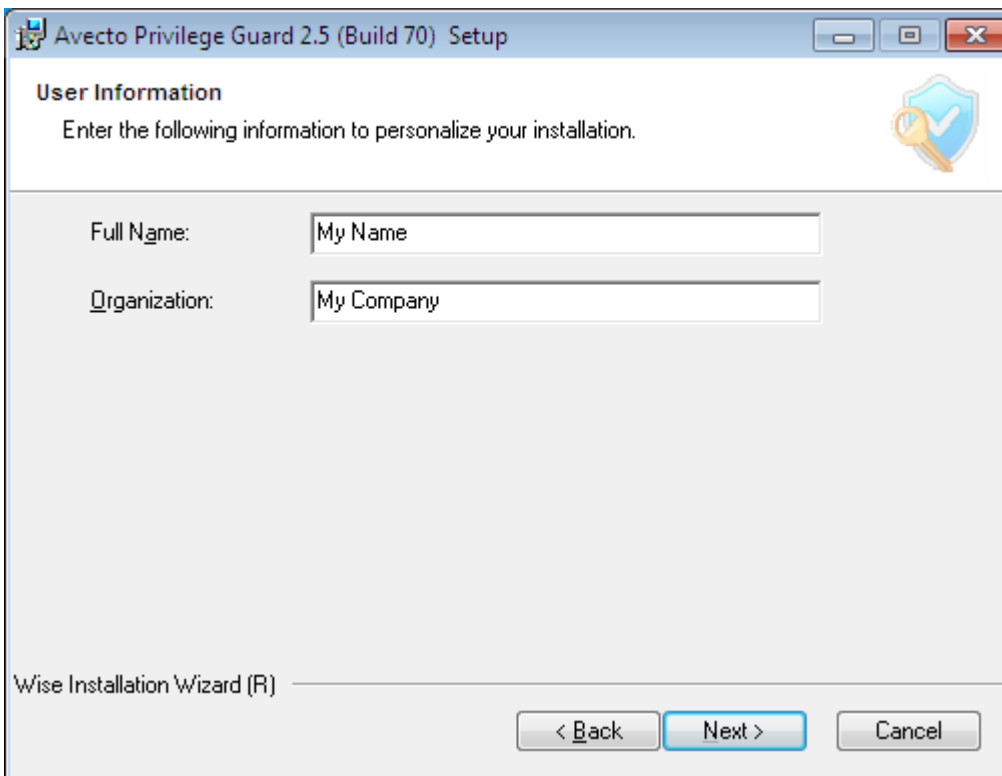
Once the prerequisites have been installed the **Welcome** dialog should appear.



Click **Next** to continue. The **License Agreement** dialog should appear.



After reading the license agreement, select **I accept the license agreement** and click **Next** to continue. The **User Information** dialog should appear.



**Avecto Privilege Guard 2.5 (Build 70) Setup**

**User Information**

Enter the following information to personalize your installation.

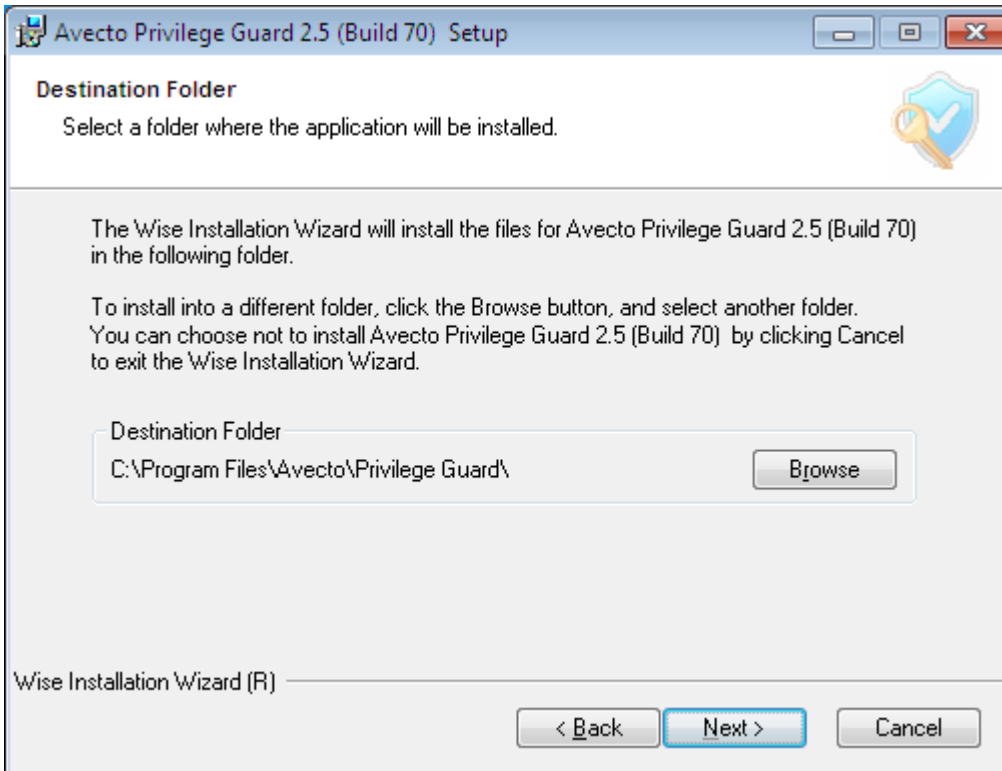
Full Name:

Organization:

Wise Installation Wizard (R)

< Back   Next >   Cancel

Enter your name and the name of your organization and click **Next** to continue. The **Destination Folder** dialog should appear.



**Avecto Privilege Guard 2.5 (Build 70) Setup**

**Destination Folder**

Select a folder where the application will be installed.

The Wise Installation Wizard will install the files for Avecto Privilege Guard 2.5 (Build 70) in the following folder.

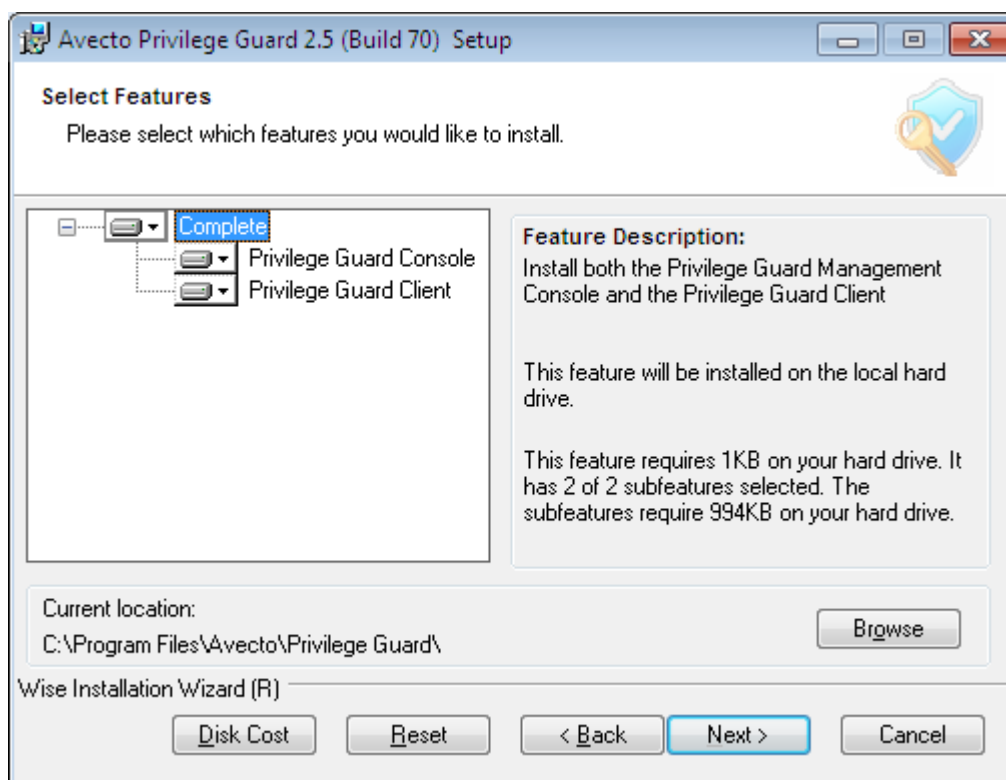
To install into a different folder, click the Browse button, and select another folder. You can choose not to install Avecto Privilege Guard 2.5 (Build 70) by clicking Cancel to exit the Wise Installation Wizard.

Destination Folder

Wise Installation Wizard (R)

< Back   Next >   Cancel

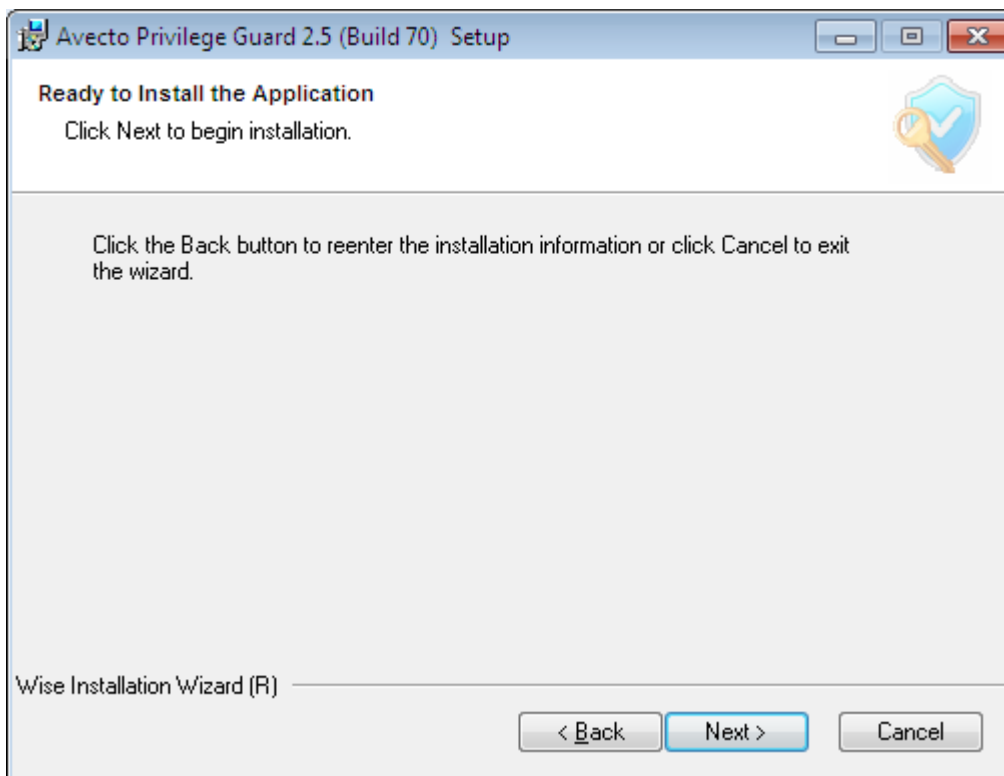
If you wish to change the default installation directory then click the **Browse** button and select a different installation directory. Click **Next** to continue. The **Select Features** dialog should appear.



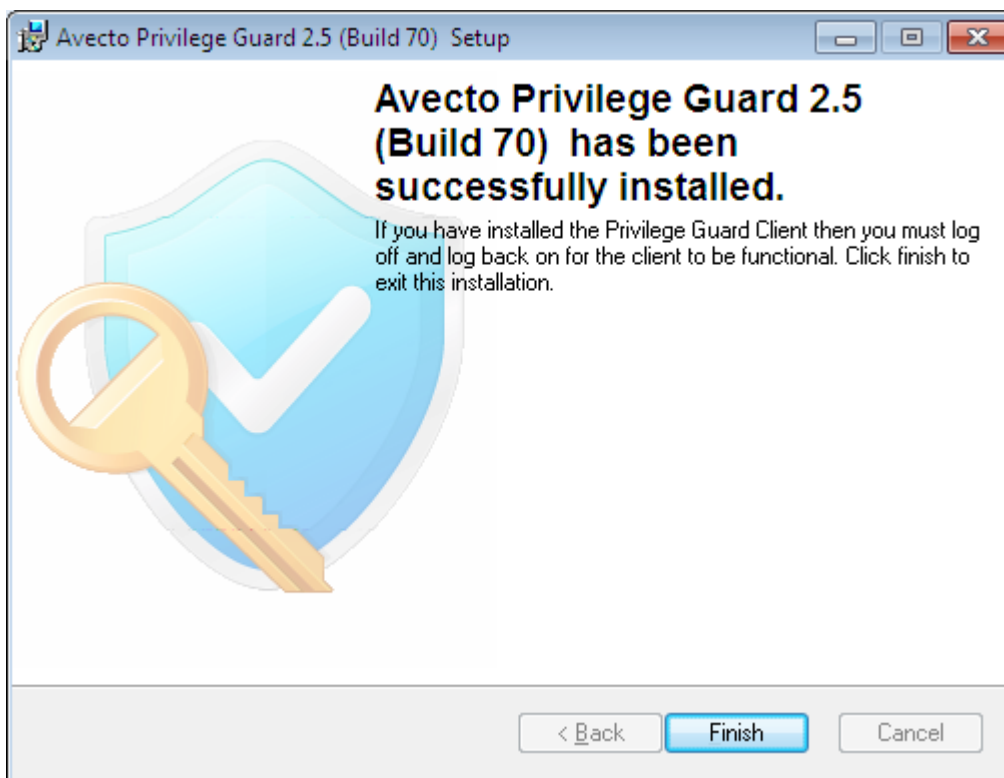
Click **Next** to install both the Privilege Guard Console and Privilege Guard Client.

**NOTE:** When installing Privilege Guard in a production environment you will probably want to install just the Privilege Guard Console on computers where you will manage Privilege Guard, and deselect the Privilege Guard Client feature.

The **Ready to Install the Application** dialog should appear.



Click **Next** to begin the installation. The software should now install.



Once the software has installed, click **Finish** to exit the installation.

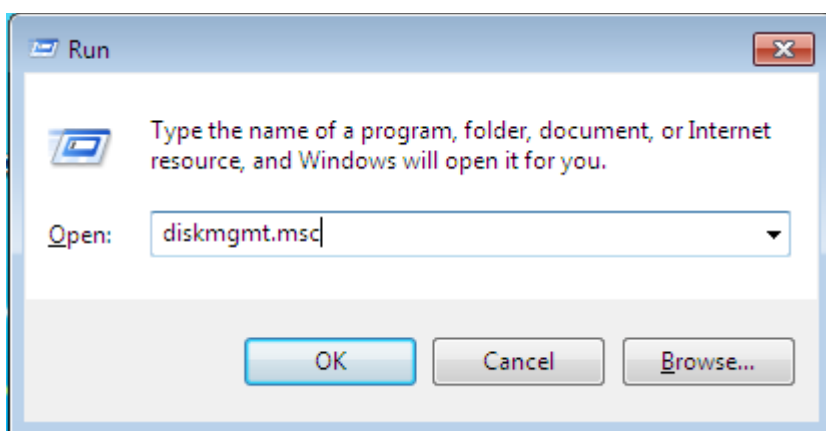
---

## Configuring and Testing Privilege Guard

### Running a Test Application

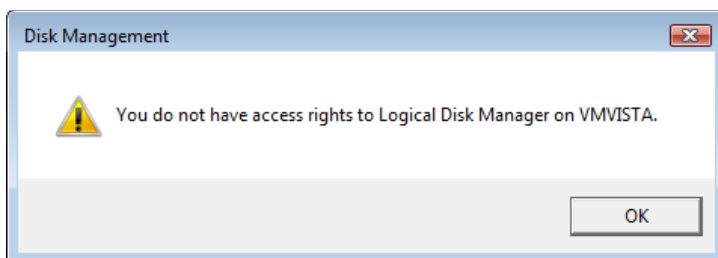
The easiest way to test Privilege Guard is to use the fast user switching feature in Windows. If you do not have this feature enabled then you will need to log off and log on as a standard user to test Privilege Guard. Assuming that you have fast user switching enabled, switch to a standard user.

Once logged on as a standard user, run the Disk Management system tool (diskmgmt.msc). On Windows XP use the **Run** option in the **Start Menu** and type **diskmgmt.msc**. Click **OK** to launch the Disk Management system tool.



On Windows Vista or Windows 7 simply type **diskmgmt.msc** in the **Search Box** from **Start Menu** and press the **Enter** key.

The application should display an error message, as a standard user does not have access rights to run the Disk Management system tool.

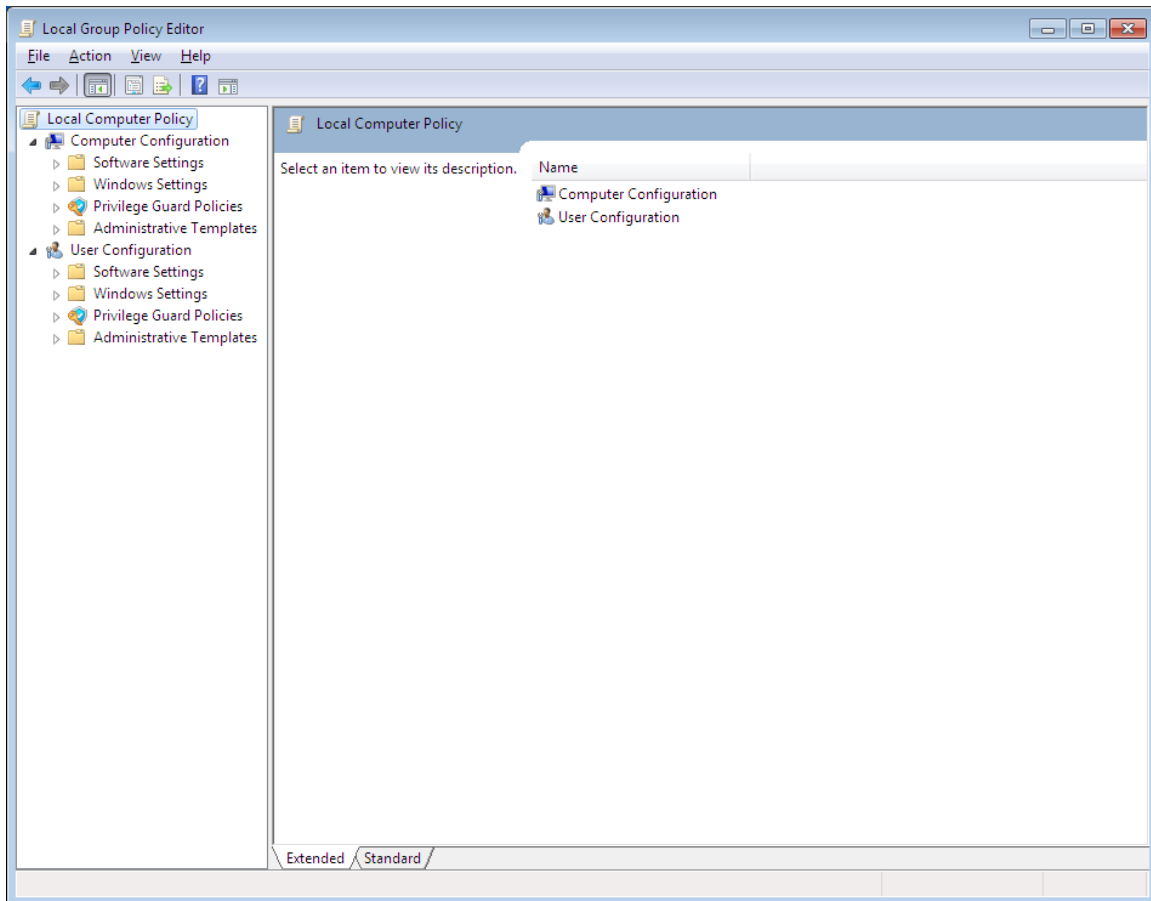


We will now set up a Privilege Guard policy so that a standard user can be granted admin rights for the Disk Management system tool.

## Launching the Group Policy Editor

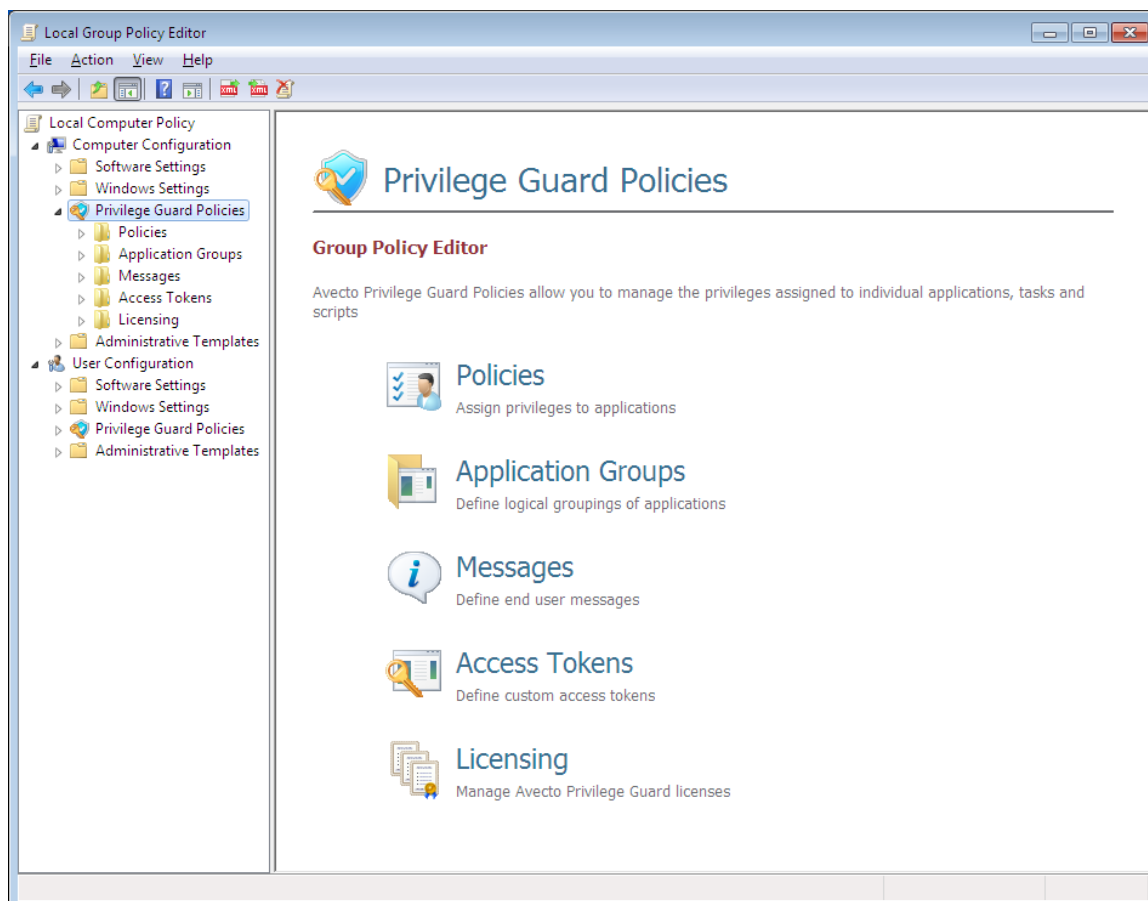
For the purposes of this test, we will be using Local Computer Policy.

Switch to your administrator account and launch the **Group Policy Editor** from the **Start Menu (gpedit.msc)**, which is used to edit Local Computer Policy.



## Creating Privilege Guard Policies

Select **Privilege Guard Policies** in the Computer Configuration section of the Group Policy Editor. Right click the **Privilege Guard Policies** node and click **Create Privilege Guard Policies**.



## Inserting a License

First, insert your license code(s):

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**.

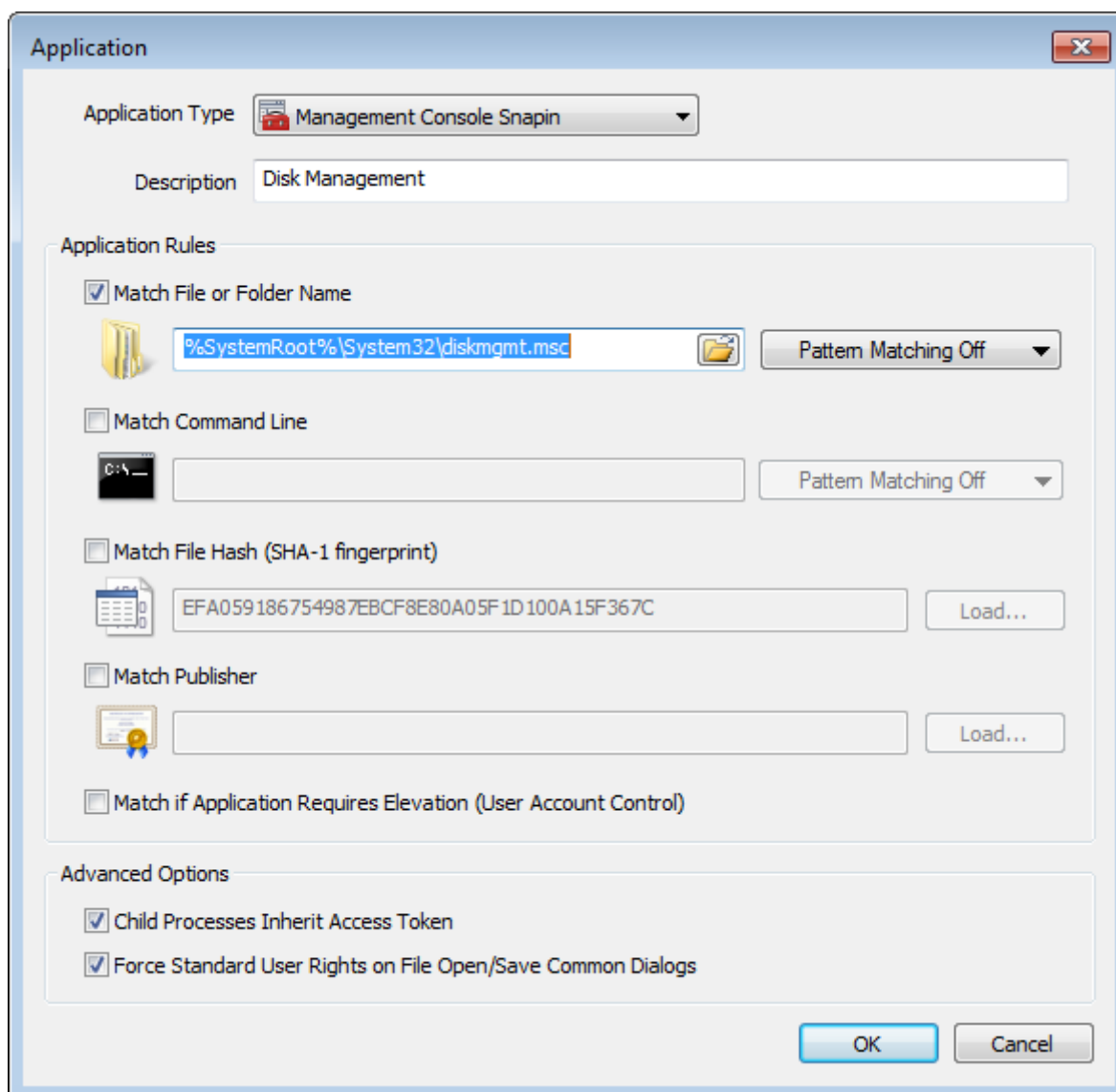
## Creating an Application Group

The next step is to create an application group:

1. Expand the **Privilege Guard Policies** node.
2. Expand and select the **Application Groups** node.
3. Right click the **Application Groups** node and then click **New Application Group**.
4. A new application group will be created and it will be highlighted so that you can rename it. Rename the application group to **Test Apps** and press enter.

The next step is to add the disk management application:

1. Select the **Test Apps** 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. Select the operating system you are testing on from the **Category** drop down list.
6. Select **Disk Management** from the **Application** drop down list.
7. Click **OK**.
8. The **Application** dialog should appear and will be populated with the **Disk Management** application settings.
9. Click **OK**.



## Creating a Policy

The next step is to create a policy:

1. Expand the **Privilege Guard Policies** node.
2. Expand and select the **Policies** node.
3. Right click the **Policies** node and then click **New Policy**.
4. A new policy will be created and it will be highlighted so that you can rename it. Rename the policy to **Test Policy** and press enter.
5. Select the **Test Policy** node.

The **Accounts** tab should be selected for this policy, but if it isn't then select the **Accounts** tab.

By default the accounts list will have a single entry for the well known **Everyone** group, and therefore the policy will be applied to all users.

**NOTE:** When deploying Privilege Guard policies 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. For example, if Privilege Guard policies have been added to the Default Domain GPO and the Everyone group is selected, everyone under the management scope of this GPO will receive the Privilege Guard policies.

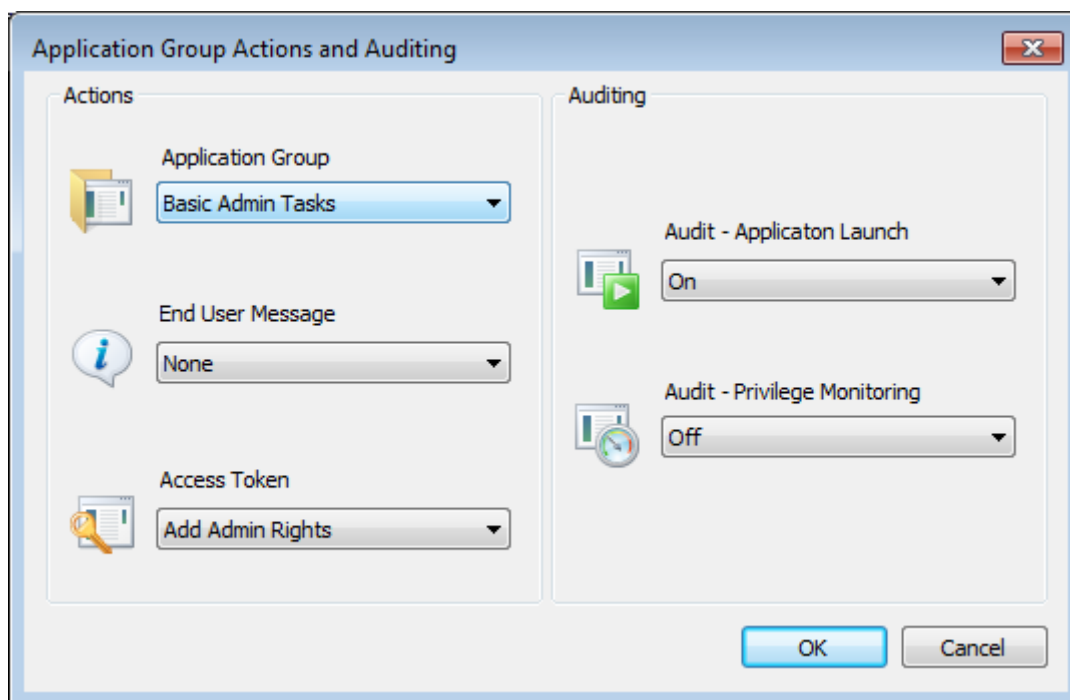
If you want to be more granular the Everyone group can be replaced with specific user or group accounts. Alternatively Privilege Guard policies may be added at the OU level.

**Do not leave the Account list empty or the policy will never be applied.**

Now select the **Application Privileges** tab.

To insert an application token:

1. Right click in the application tokens list and click **Insert Application Group**.
2. The **Insert Application Group** dialog will appear.
3. The **Test Apps** group will automatically be selected for the **Application Group**.
4. The default **Access Token** is **Add Admin Rights**, which is also correct for this test.
5. If you wish to audit the application launching then select **On** for **Audit – Application Launch**.
6. Leave **Audit- Privilege Monitoring** in the **Off** position.
7. Click **OK**.

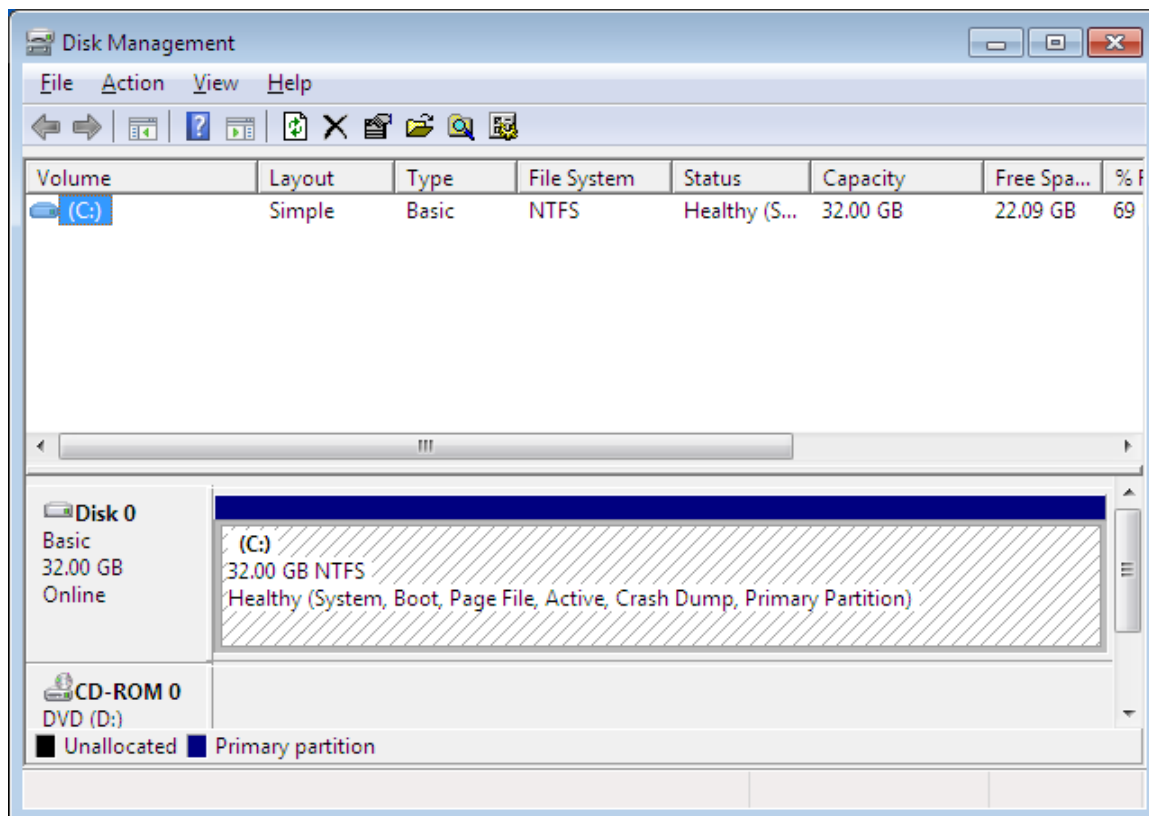


You are now ready to test this sample policy.

## Testing the Privilege Guard Policies

Switch back to the standard user account.

Once logged on as the standard user, run the Disk Management system tool again. This time the Disk Management system tool should launch with no errors.



You have now validated that Privilege Guard is installed, licensed and functioning correctly and may perform further testing.

---

## Further Testing

### Elevating Different Applications

To perform further testing simply switch back to the administrator account and add more applications to the **Test Apps** application group. The table below suggests a few standard applications that you can add to the policy that require admin rights to function (assumes Windows is installed in c:\windows). These applications are also included as **Application Templates**. You may also add some applications that are specific to your environment that require elevated rights to run.

Description	Application Type	Filename
Setting the Time & Time Zone	Control Panel Applet	c:\windows\system32\timedate.cpl
Managing Services	Management Console	c:\windows\system32\services.msc
Disk Defragmenter (XP)	Management Console	c:\windows\system32\dfrg.msc
Disk Defragmenter (Vista)	Executable	c:\windows\system32\dfrgui.exe
Adding Hardware (XP)	Control Panel Applet	c:\windows\system32\hdwwiz.cpl
Adding Hardware (Vista)	Executable	c:\windows\system32\hdwwiz.exe
DPI Scaling (Vista)	Executable	c:\windows\system32\dpiscaling.exe

**NOTE:** Management consoles will only be elevated by Privilege Guard if the user launches them via the msc file in the policy. Launching mmc.exe and adding the console as a snap-in will not cause the console to run elevated, as the user has the freedom to add other snap-ins. Similarly if the user runs an msc file in author mode then Privilege Guard will detect this and not launch it with elevated rights.

### Shell Integration (on Demand)

If you wish to allow a user to choose when to run an application with elevated rights then you may create one or more application groups for this purpose.

For instance, to allow a user to elevate cmd.exe on demand:

1. Create a new application group and name it **Shell Apps**.
2. Select the **Shell Apps** application group and then select **Executable** from the **Insert Application** menu.

3. In the **Application** dialog, enter `c:\windows\system32\cmd.exe` for the **Source Filename** and click **OK**.
4. Next select the **Test Policy** and then select the **Shell Integration** tab.
5. Click the **Shell Integration** button to enable shell integration.
6. Next select **Insert Application Token** and add the **Shell Apps** application group with **Add Admin Rights** for the **Application Token**. You may also choose to audit this entry.

By default, the Windows “Run as” and “Run as administrator” options will be hidden in the shell context menu when the Privilege Guard shell menu option is present. Deselect the checkbox if you would like these shell menu options to be shown.

Now switch to the standard user to test this policy change.

Add a shortcut to `cmd.exe` on the user’s desktop and then right click on the shortcut to access the shortcut menu. The **Run with Privilege Guard** option should be available, which will also include the Privilege Guard icon on Windows Vista.

If you select **Run with Privilege Guard** then `cmd.exe` will launch with admin rights. Try setting the time or running an application that requires admin rights to prove the `cmd.exe` is running with admin rights.

**NOTE:** The Shell extension may also be applied to every application by entering `*.exe` for the filename. This is a common scenario for more advanced users, who need flexibility, and with Privilege Guard this activity may be audited.

---

## Privilege Guard in a Production Environment

When you are ready to deploy Privilege Guard in a production environment (or an extended test environment), you will want to configure Privilege Guard centrally and then deploy it to multiple client computers.

You should refer to the **Privilege Guard Administration Guide** before deploying Privilege Guard in a production environment, which will guide you through planning and deployment with Active Directory Group Policy.

This **Getting Started Guide** has touched briefly on a few of the core features of Privilege Guard, and you should refer to the **Administration Guide** for a complete description of the many features and capabilities within Privilege Guard.