# Restrict Access to Programs with AppLocker in Windows 7

If you share a computer and don't want other users accessing certain applications, there is a new feature in Windows 7 that allows you to block them. Today we take a quick look at restricting what programs other users can access using AppLocker.

Note: AppLocker is only available in Ultimate and Enterprise versions of Windows 7.
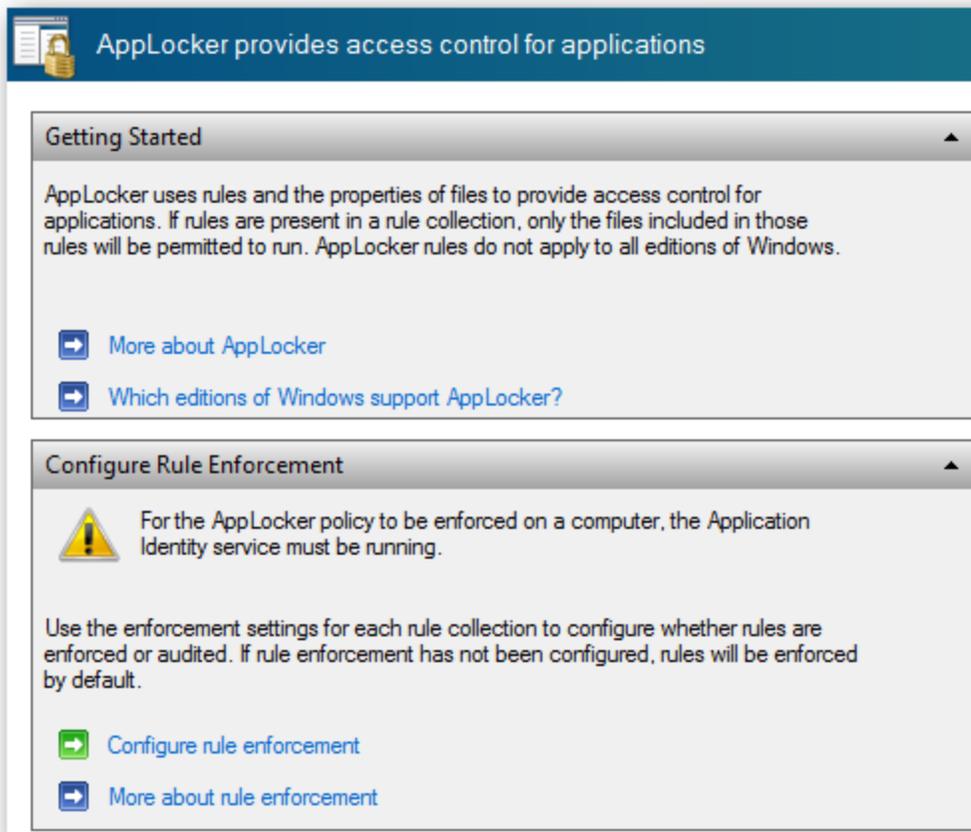
Using AppLocker

To access Group Policy Editor and create rules in AppLocker you'll need to be logged in as Administrator. Click on Start and type gpedit.msc into the search box and hit Enter.
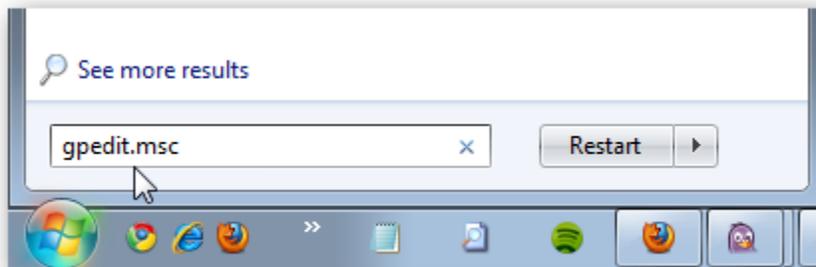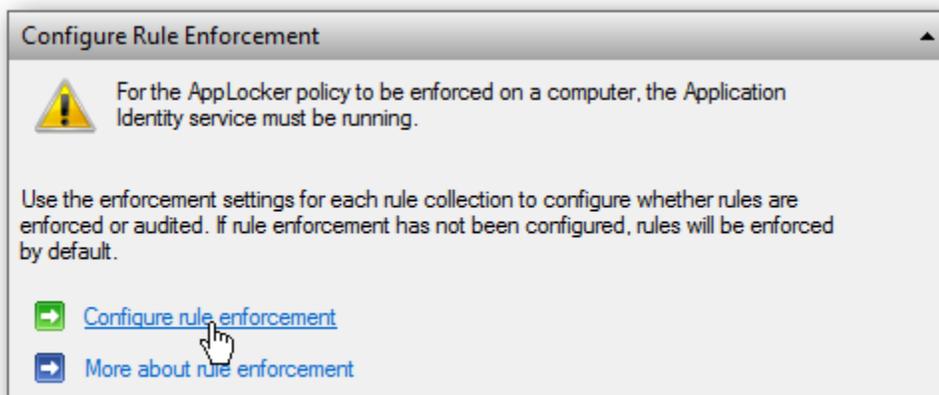

Under Local Computer Policy go to Computer Configuration \ Windows Settings \ Security Settings \ Application Control Policies \ AppLocker.
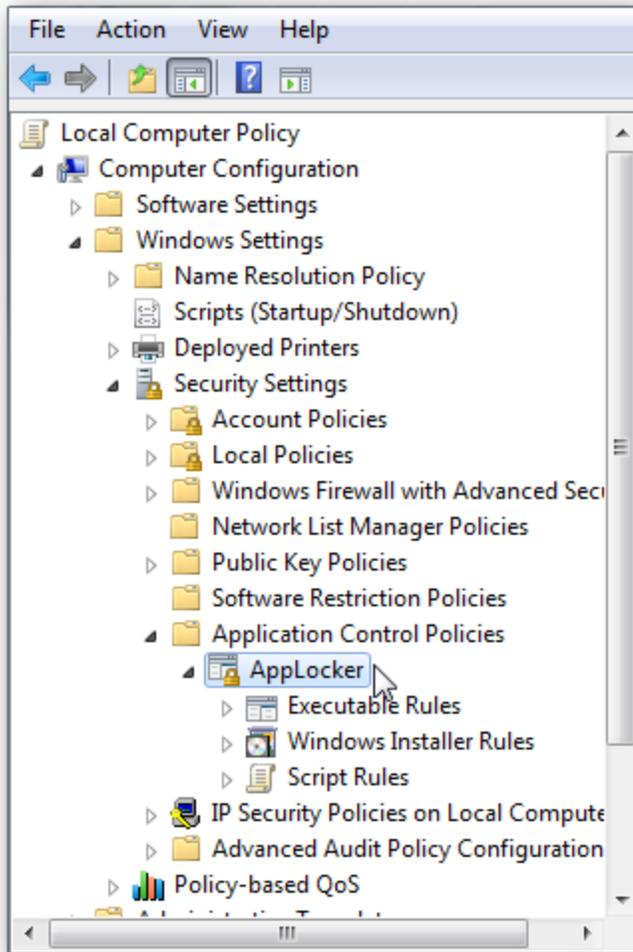
Now you will see the overall controls for the applications.

Under Configure Rule Enforcement click on the Configure rule enforcement link.

Now under AppLocker Properties check the boxes next to Configured under Executable rules then click Ok.
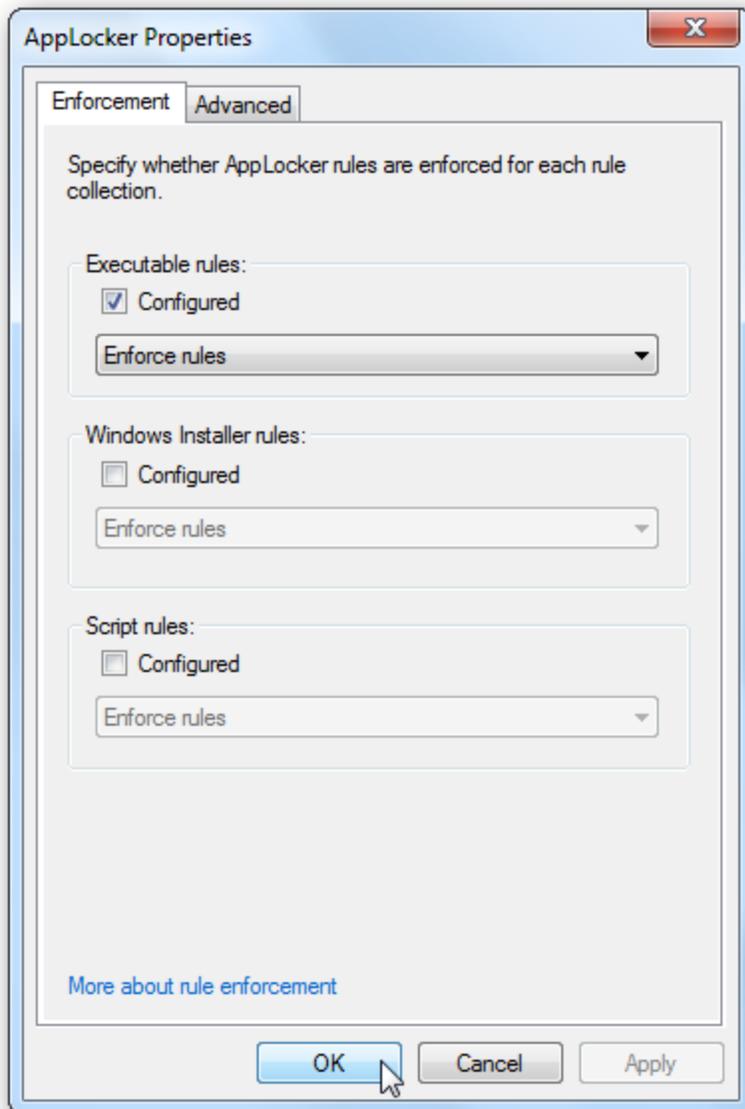
Blocking Apps from Running

In this scenario, Jack wastes time playing games like Minesweeper and Solitaire when he should be doing his homework, so we are going to block all of the games. After completing the steps above, under the Overview section click on Executable Rules.
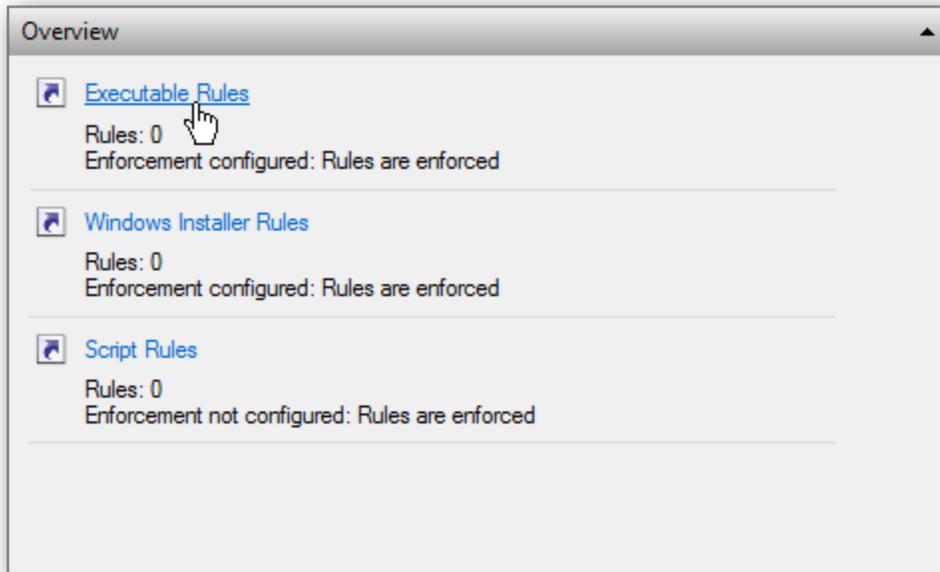
Since this is your first time accessing AppLocker, there will be no rules listed. Right-click and select Create New Rule…
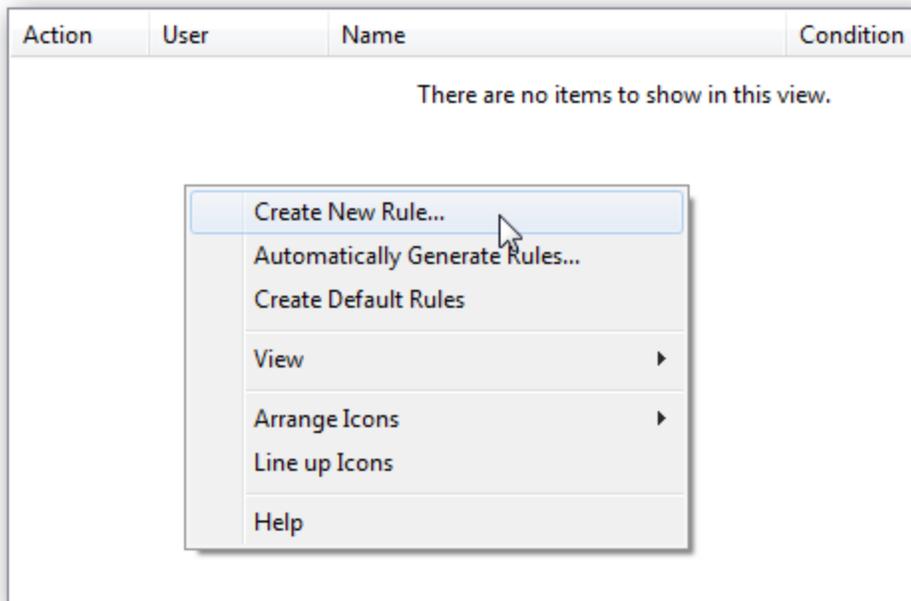
This opens up the Create Executable Rules wizard and you can select not to show the introduction screen at start up for the next time you access it.

Before You Begin

Before You Begin
Permissions
Conditions
   Publisher
   Exceptions
Name

This wizard helps you create an AppLocker rule. A rule is based on file attribu
file path or the software publisher contained in the file's digital signature.

Before continuing, confirm that the following steps are complete:

- Install the applications you want to create the rules for on this computer.
- Back up your existing rules.
- Review the AppLocker documentation.

To continue, click Next.

☑ Skip this page by default

Select Permissions under Action select Deny.

Permissions

Before You Begin
Permissions
Conditions
   Publisher
   Exceptions
Name

Select the action to use and t
allow action permits affected
files from running.

Action:
  ○ Allow
  ◉ Deny

User or group:
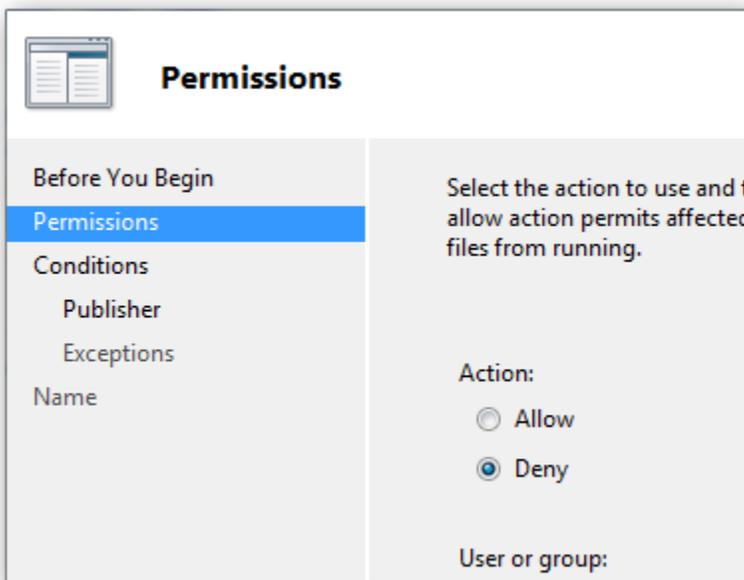
Add the user you want to block, in this case it's Jack.
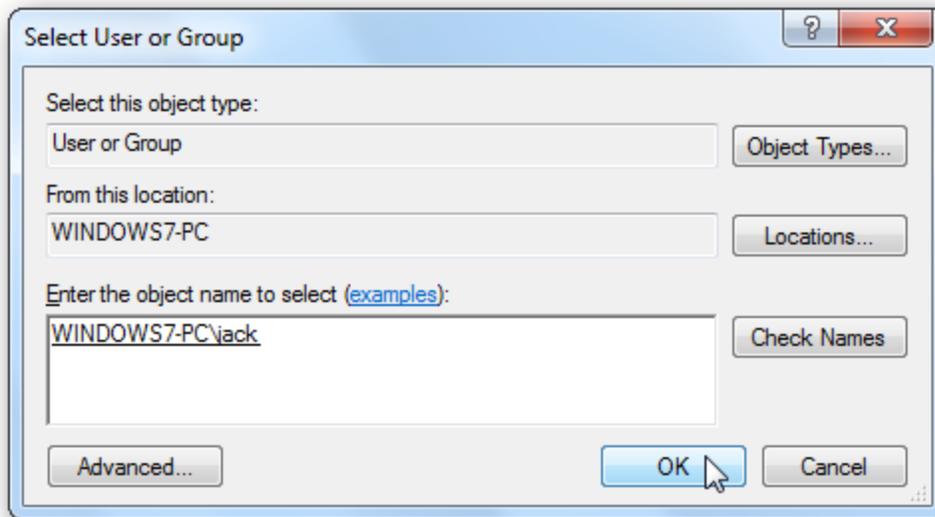
After you've selected the deny action and selected the user continue to the next step.

Select the action to use and the user or group that this rule should apply to. An allow action permits affected files to run, while a deny action prevents affected files from running.

Action:

○ Allow

● Deny

User or group:

Windows7-PC\jack   [Select...]

[ore about rule permissions]

[< Previous] [Next >] [Create] [Cancel]
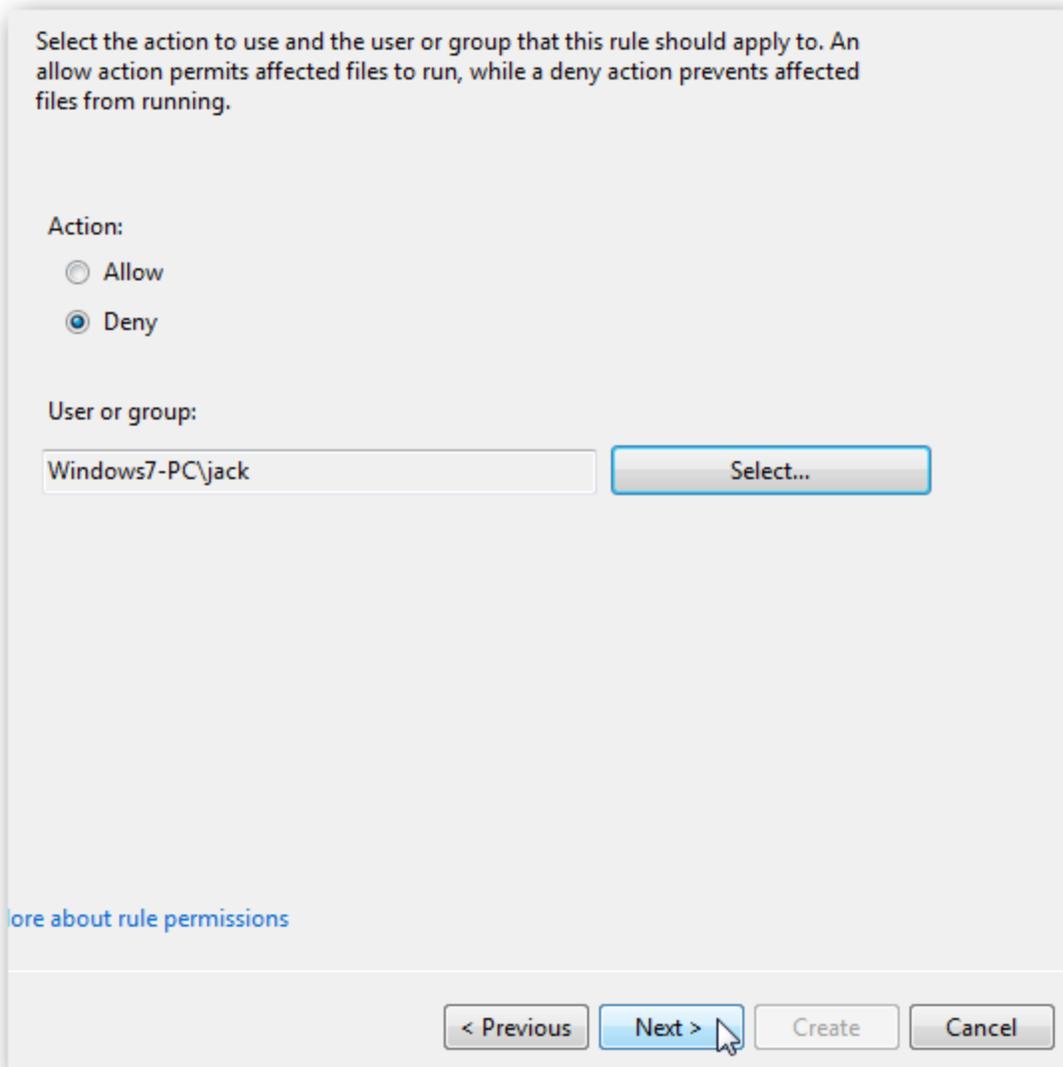
In Conditions you can select from Publisher, Path or File hash. We don't want Jack to have access to any of the games. so we will select Path.

Conditions

Before You Begin
Permissions
Conditions
   Path
   Exceptions
Name

Select the type of primary condition that you would like to create.

○ Publisher
   Select this option if the application you want to create the rule for
   software publisher.

◉ Path
   Create a rule for a specific file or folder path. If you select a folder,
   folder will be affected by the rule.

○ File hash
   Select this option if you want to create a rule for an application th

Click on Browse Folders and select the Microsoft Games folder.

Select the file or folder path that this rule should affect. If you specify a folder path, all files underneath that path will be affected by the rule.

Path:

%PROGRAMFILES%\Microsoft Games*

Browse Files...   Browse Folders...

Browse For Folder   [x]

Select a folder containing the necessary files.

> ▷ 📁 Internet Explorer
> ▷ 📁 iPod
> ▷ 📁 iTunes
> ▷ 📁 Java
> ▷ 📁 Laplink
> ▷ 📁 Microsoft
> ▷ 📁 microsoft frontpage
> ▷ 📁 Microsoft Games
> ▷ 📁 Microsoft Security Essentials

Date created: 7/13/2009 11:52 PM

Make New Folder   OK   Cancel

< Previous   Next >   Create   Cancel

In the next screen you could add Exceptions like allowing certain files, but because we are blocking the entire games directory we'll skip to the next screen.

Exceptions

Before You Begin
Permissions
Conditions
   Path
   Exceptions
Name

Primary condition:
%PROGRAMFILES%\Microsoft Games*

Add exception:

Publisher ▼

Exceptions:

Exception	Type
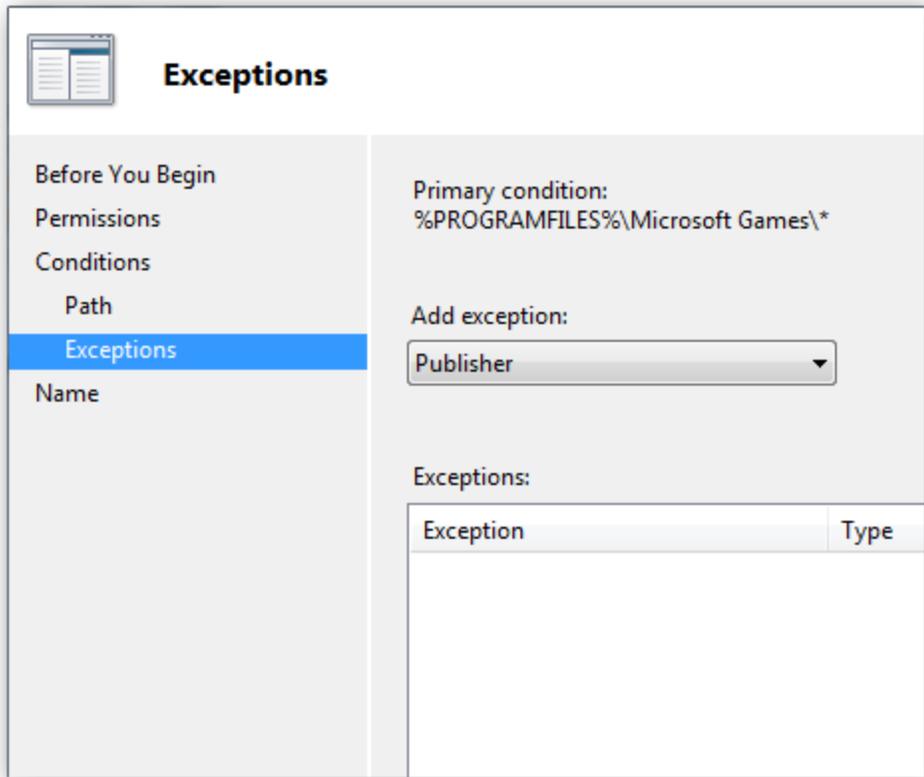
Here you can add a description to the rule so you can keep track of them is there are several rules configured. When everything looks right click on Create.
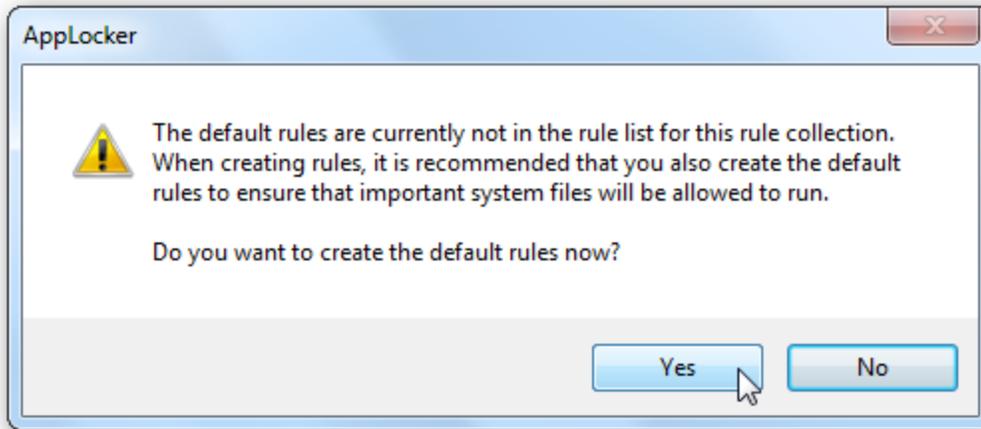
Enter a name to identify this rule.

Name:

%PROGRAMFILES%\Microsoft Games*

Description: (Optional)

No Games for Jack!
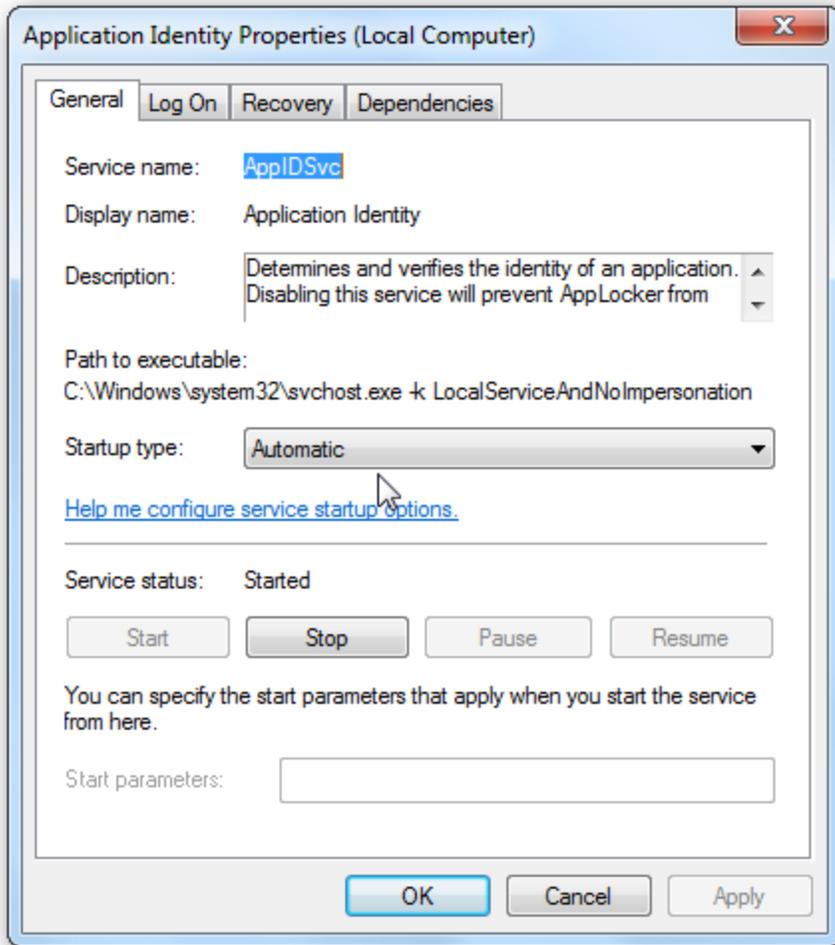
< Previous   Next >   Create   Cancel

A message pops up saying default rules haven't been created yet. It is important to make sure they are created so click Yes to this message.
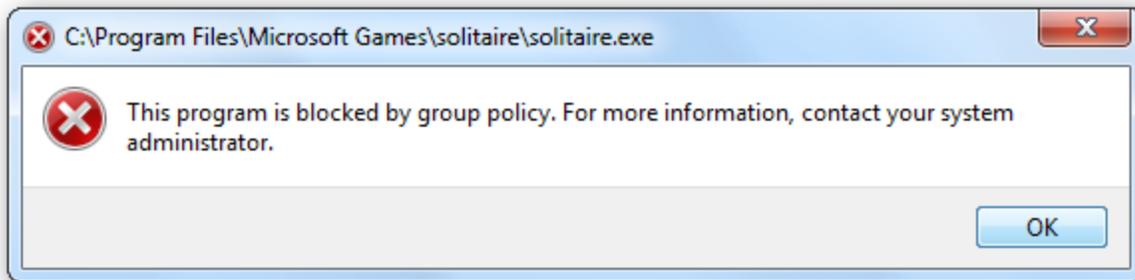
Now you will see the default rules and the new one you created showing Jack is denied access to the Microsoft Games directory.

After creating the rule make sure and go into services and make Application Identification is started and that it's set to automatically start as well otherwise the rules won't work. By default this service is not started so you will need to enable it.

Application Identity Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from

Path to executable:
C:\Windows\system32\svchost.exe -k LocalServiceAndNoImpersonation

Startup type: Automatic

Help me configure service startup options.

Service status: Started

Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

Now, when Jack logs into his user account and tries to access the games he will only see the following message. Only an Administrator can go in and change the rule.

C:\Program Files\Microsoft Games\solitaire\solitaire.exe

This program is blocked by group policy. For more information, contact your system administrator.

OK

Conclusion

Use caution when configuring the rules and only start the Application Identity service after everything looks right. Otherwise you have the potential of locking yourself out of all applications including AppLocker.AppLocker is a powerful feature included in Windows 7 and we showed you a basic rule so

14

you can get an idea of how it works. In the future we'll take a look at more complex tasks to accomplish and gain tight control over what programs each user is able to access.