Application security with AppLocker

AppLocker is a new integrated tool on Windows 7 and Windows Server 2008 R2 helps block unwanted applications on the network.

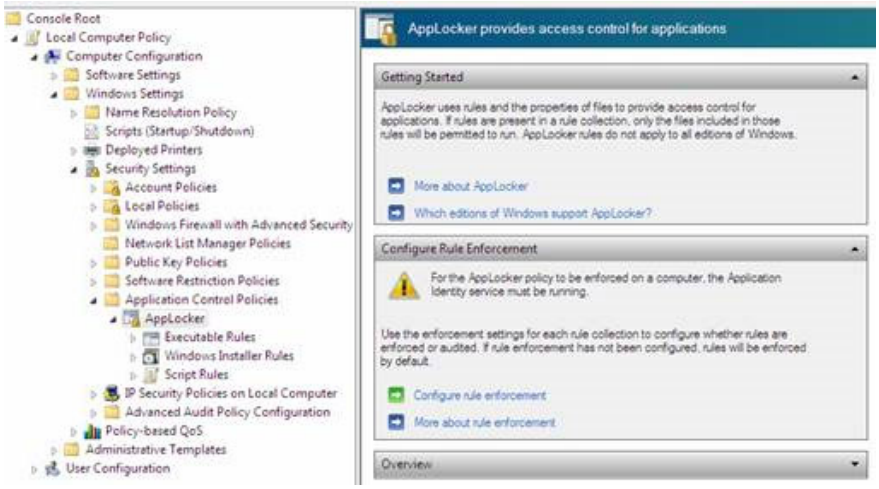
***Network Administration* - AppLocker is a new integrated tool on Windows 7 and Windows Server 2008 R2 helps block unwanted applications on the network. Therefore it is used to establish security for many different network systems.**

Block a single application

This section will guide you to configure security policies for a local system and apply those configurations to a computer on the network. You can also configure the security policy in **Group Policy Management** of **Windows Server 2008 R2** , but if you understand AppLocker then you should use this tool when dealing with security policies. AppLocker is very powerful and flexible, so you should also be careful when working with it because only a small mistake can damage your computer.

Suppose we use **AppLocker** to block the operation of **MSTSC** application with the executable file **mstsc.exe** .

You can launch **AppLocker** by typing **gpedit.msc** into the **Windows 7 Start** menu, or create a new **Group Policy** object in **Windows Server 2008 R2** . After launching this tool, browse for **AppLocker** in the following path: **Computer Configuration | Windows Settings | Security Settings | Application Control Policies | AppLocker** .



You will then see three options in the left panel when you expand AppLocker. These three options are rule collection rules and groups used to separate file extensions. You can also manage these extensions using AppLocker.

Rule Collection ***File*** **type** *.exe, .com* ***executable*** *file .ps1, .bat, .cmd, .vbs, .js* ***File of Windows Installer*** *.msi, .msp*
The goal is to block an executable file so we'll have to create a new **rule** in the executable **rules collection** . To create a new rule, right-click **Executable Rules** and select **Create New Rule** .

The **Create Executable Rules Wizard** will then appear, click **Next** to bypass the wizard screen. Since you want to deny access to the executable file **mstsc.exe** , select the **Deny** option. Also in this window you can select the user or user group that this policy will apply. If you want to ensure that system administrators and highly authorized users can still run this application when logging in to the system, select the user group to apply this policy.

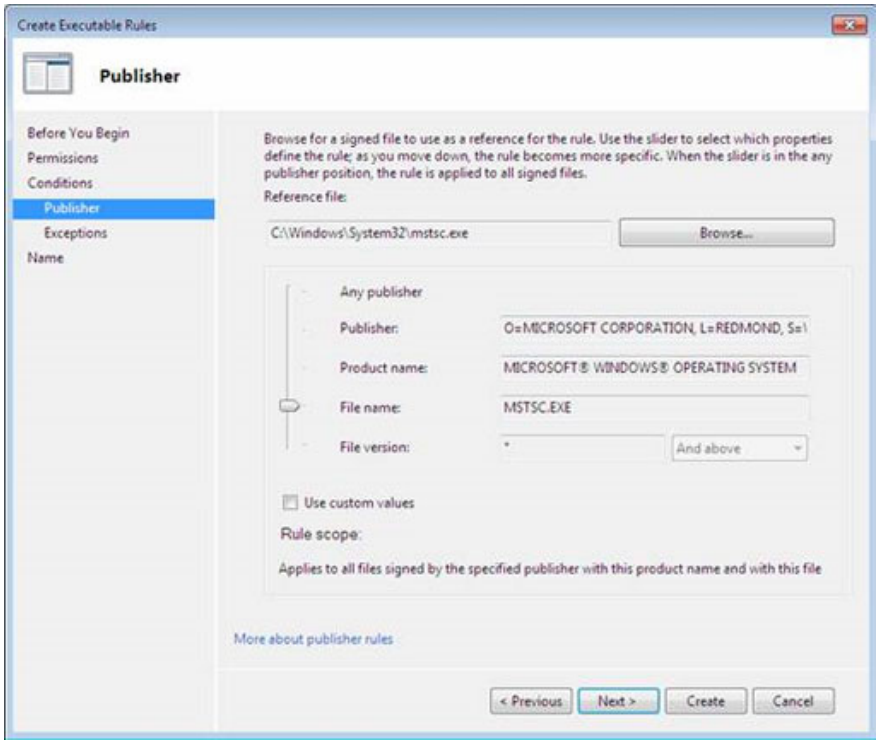
In the next window you will get a message to select the main condition for the rule. You will have to select one of the three options used in the **Rule Collection** , including:

1. **Publisher** : This option is very flexible in selecting conditions but it can only be used with the application software signed by the provider.

1. **Path** : This condition creates a rule for a specific file or folder path.

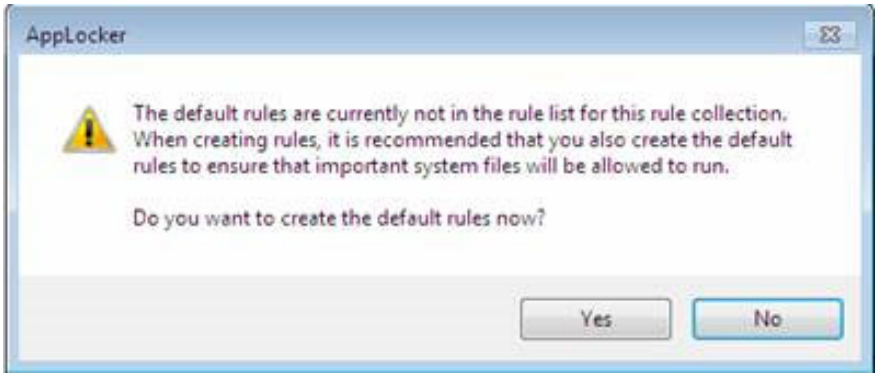
1. **File Hash** : This option is best suited if an application is not signed. And this type of Rule is created when this application is broken.

The **MSTSC** application is a signed application, so we will select the main condition that is **Publisher** and then click **Next** . Then click the **Browse** browser button to find the file you want to block. Find the file **mstsc.exe** in the path **C: WindowsSystem32mstsc.exe** . After selecting this file, you will see a vertical slider appear. With the signed application we will have several levels of selection for **Rule** . You can use **Publisher** to block all applications.



These options are very powerful and flexible, you can also use them to prevent users from running an application, blocking file names related to viruses and even forcing users to new applications. most by blocking old applications. In this section, the purpose is to block the mstsc.exe file so we will not pay attention to its version, so the slider needs to move to the **File name** option.

The next window will allow you to make exceptions if necessary, and the final window allows you to name the new rule. Then click **Create** to end the rule creation process. If this is the first rule created, you will be prompted to create a default rule that allows users and administrators to access the file system. This is necessary (especially if you are using a version before Windows 7) because if you do not set these rules correctly, your system may not boot. After clicking **Yes** on the notice that these rules are automatically created.



This is the last stage to ensure your rules promote their effects. You must first run and install the automatic launch mode for the **Application Identity** service so that AppLocker can determine the application correctly.

To run and install the automatic launch for this service by entering **services.msc** in the **Start** menu search **box** , then find the **Application Identity** service, double-click it, select **Start | Automatic** in the **Startup Type** field. After restarting the system **AppLocker** will apply these rules, and every time the user tries to launch **MSTSC** application they will receive the following message:

Block untrusted applications

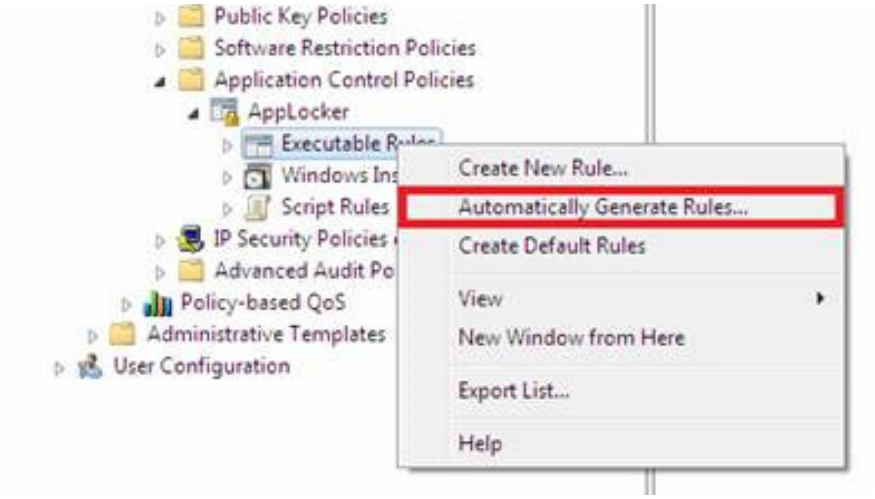
In the previous section, when executing an application block, we know exactly which application. The above situation is very suitable for environments where users are only allowed a little free access on the system, but for larger organizations the IT policy will specify which objects are not started All applications that are not authorized by the system administrator. The most effective method in this case is to block all applications that do not guarantee the required reliability. And AppLocker can perform this function quite easily.

AppLocker is designed for security direction so it can help you create a Allow Rule that blocks any other

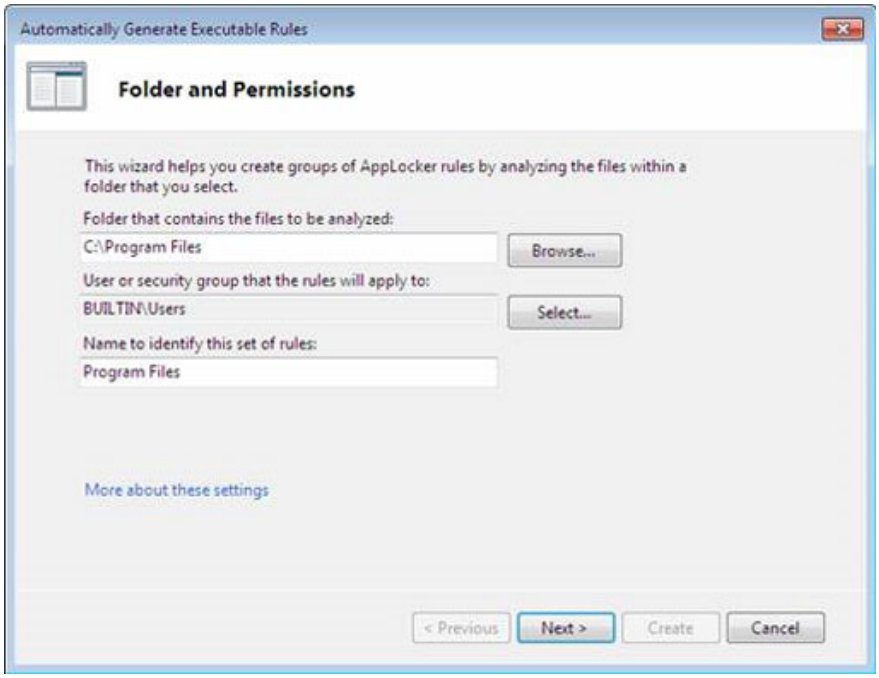
application except for the allowed application. For example, if you create a Allow Rule that only allows applications to run the application in **C: folderfile.exe** , then this rule will be used to block all applications in **C: folder** except **file.exe** . This means that in this section we will initialize a Allow Rule for all allowed applications.

Before creating Allow Rule, you will have to create a Rule for every individual executable file, including third-party applications that are installed on the system or default installed Windows applications. AppLocker can perform automatic rule creation based on applications installed for a specific workstation.

If you have not created a default rule that allows all necessary system applications to launch, you must first create these rules. Right-click the **Executable Rules Collection and** select **Create Default Rules** . Once these rules have been created, delete the rules that allow all users to run all files in the **C: Program Files** folder.



Next create the Allow Rule for the system. Just right-click on the **Executable Rules Collection and** select **Automatically Generate Executable Rules** . Applications on the system are stored in two main areas. The first area is the Windows folder, in this area the default rules will allow users to run all files in this directory so you don't need to create any Allow Rule for it. The remaining container is the Program Files folder. Please select this folder in the first field of the window that appears. In the field below select the user group that this rule will apply. Finally, you need to give a name to this Rule group (the name of the Rule will appear in parentheses before each Rule description). Then click the **Next** button.

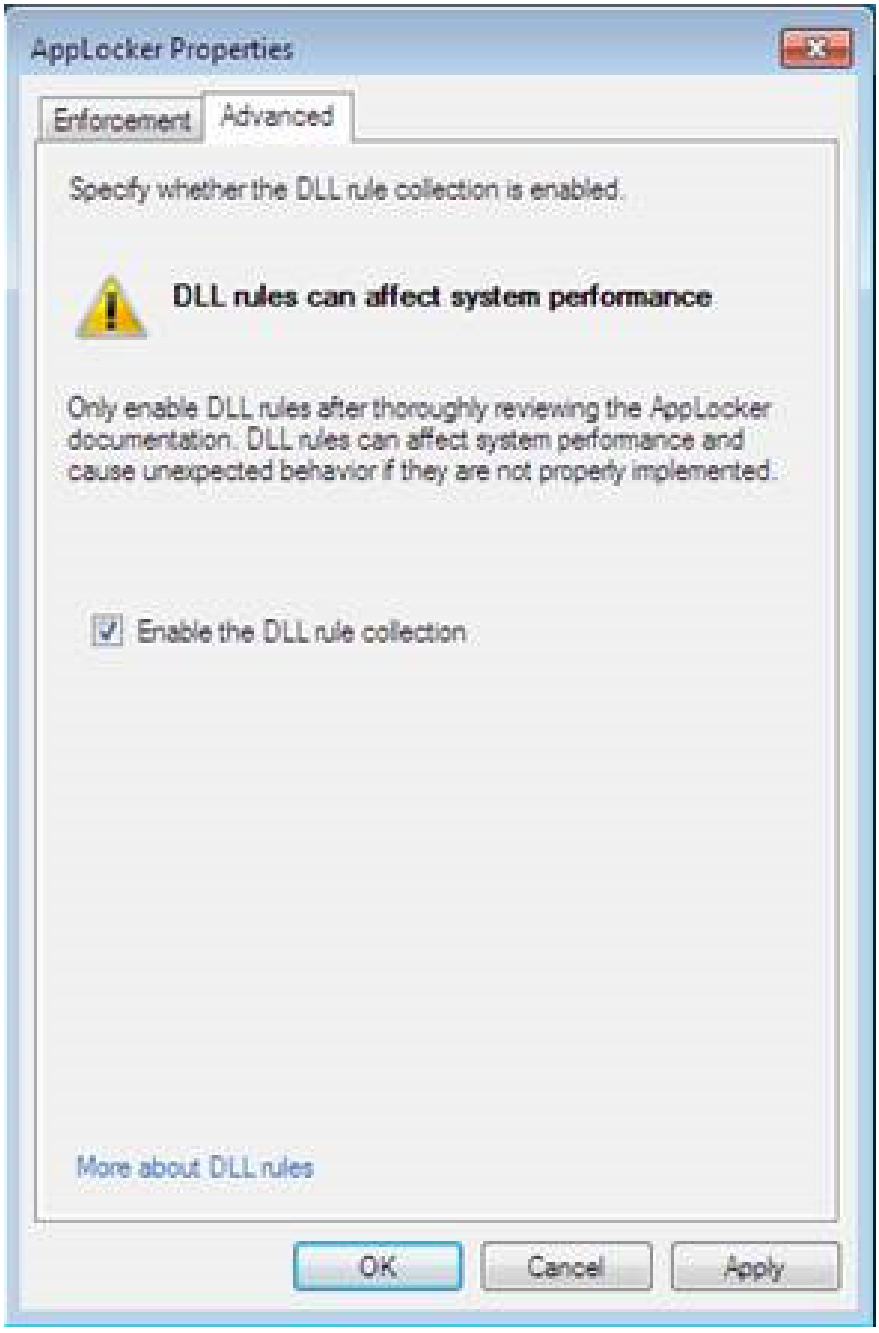


At **Rule Preferences** , you can select the type of rule you want to initialize. It's best to choose **Pulisher** for all **digitally** signed files and create **File Hash Rules** for the remaining file types. You can also choose to reduce the number of rules created by grouping the same files. This option will significantly reduce the amount of rules but if you want more access control, deselect this option. Click **Next to** start the **Rule Application Discovery** process. After this process has finished you will see a dialog box showing the rules that are being created. Click the **Create** button to complete creating these Rules.

DLL Rule Collection

In addition to the above three DLL Rules Collection, there is another DLL Rule Collection that needs to be mentioned. The DLL Rule file is used to block applications that call specific DLL files. This is a high level rule set and you should not use it unless you understand it well. This type of rule can affect the performance of the system because it requires AppLocker to check every DLL that an application uses when launching.

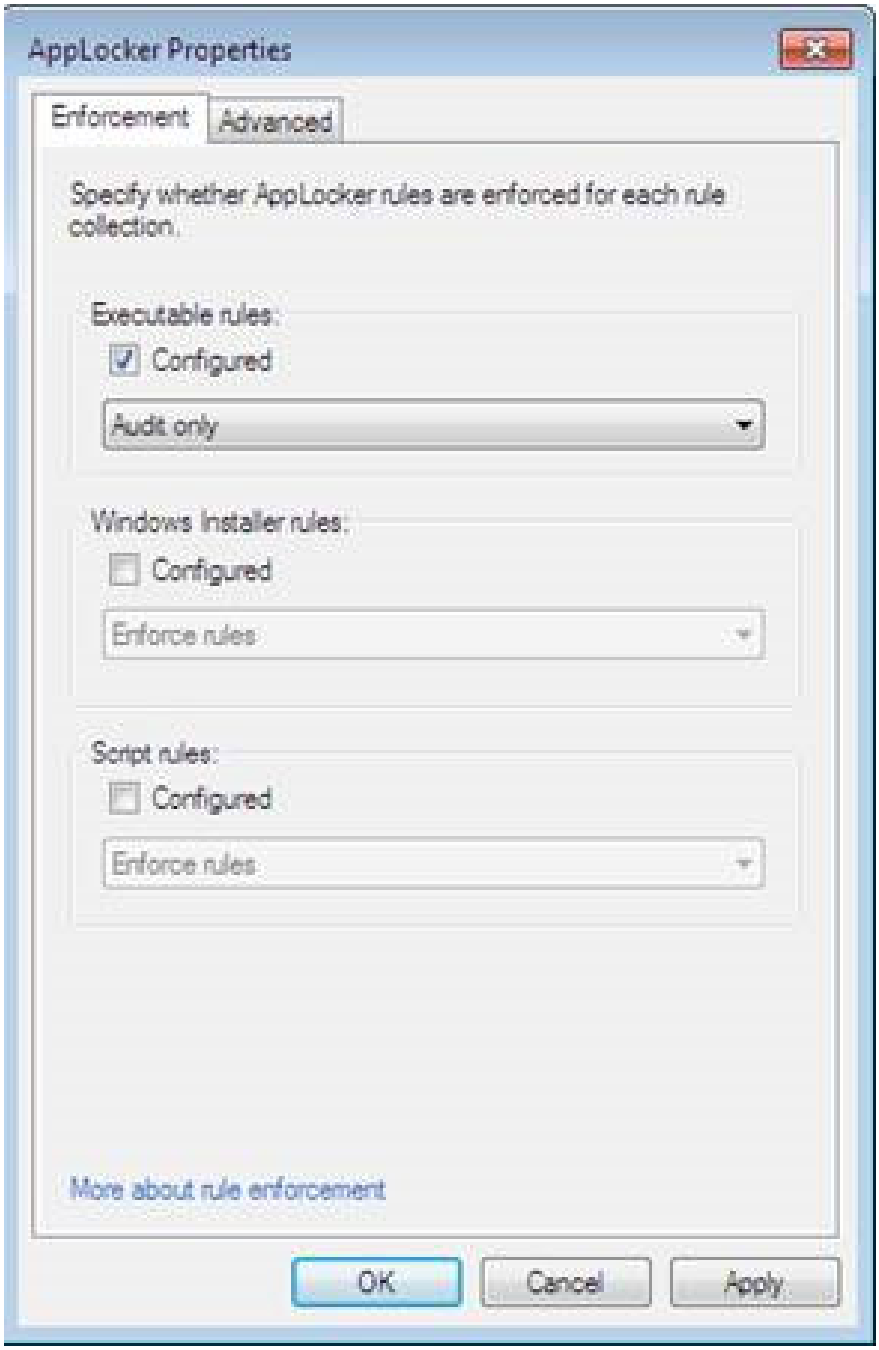
The DLL Rule file will not be enabled by default for a number of reasons mentioned above. If you want to create a Rule DLL, open the AppLocker main configuration window, select C **onfigure Rule Enforcement** , select the **Advanced** tab and click the **Enable the DLL Rule collection** check box. You will then see the DLL Rule file in the left panel along with three other Rule sets.



Verify and apply Rule

Every rule you created is designed to implement policies that allow or deny use of the application. Some tools can support the verification process before applying a policy. AppLocker provides a very useful verification setting in this case. When a user runs an AppLocker one Rule violation application, the information about this application will be saved to the **AppLocker Event Log** .

To use this setting, click **Configure Rule Enforcement** on the AppLocker main configuration window. In the AppLocker dialog you can select the **Configured** check box for the set of Rules you want to verify and select the **Audit Only** option in the drop-down list. This feature is very useful in determining the type of book an application uses.



Conclude

It is not difficult to see the features of AppLocker when using it in the network. Thanks to the dynamic rule system, you can now block desired applications to help secure the system. Along with that, AppLocker in Windows 7 and Windows Server 2008 R2 will be an important tool in the administrative toolkit.