Lesson 18: Configuring Application Restriction Policies

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft® Official Academic Course

WILEY

Overview

- Exam Objective 6.3: Configure Application Restriction Policies
- Installing Software with Group Policy
- Configuring Software Restriction Policies
- Using AppLocker

Installing Software with Group Policy

Lesson 18: Configuring Application Restriction Policies

Installing Software with Group Policy

- Administrators can use Group Policy to **install**, **upgrade**, **patch**, or **remove** software applications:
  - When a computer starts,
  - When a user logs on to the network
  - When a user accesses a file associated with an application that is not currently on the user's computer
- Administrators can use Group Policy to **fix** problems associated with applications by launching a repair process that will fix the application.

Windows Installer

- Windows Server 2012 uses the Windows Installer with Group Policy to install and manage software that is packaged into Microsoft Installer files, with an .msi extension
- The client-side component is called the Windows Installer Service:
  - Responsible for automating the installation and configuration of the designated software
- Server-side component

Windows Installer Service Package File

The package file consists of the following information:

- An **.msi file**, which is a relational database file that is copied to the target computer system, with the program files it deploys. In addition to providing installation information, this database file assists in the **self-healing** process for damaged applications and clean application removal.
- **External source files** that are required for software installation or removal.
- **Summary information** about the software and the package.
- **A reference point** to the path where the installation files are located.

Repackaging Software

Several third-party package-creation applications on the market enable you to repackage software products into a Windows Installer-enabled format.

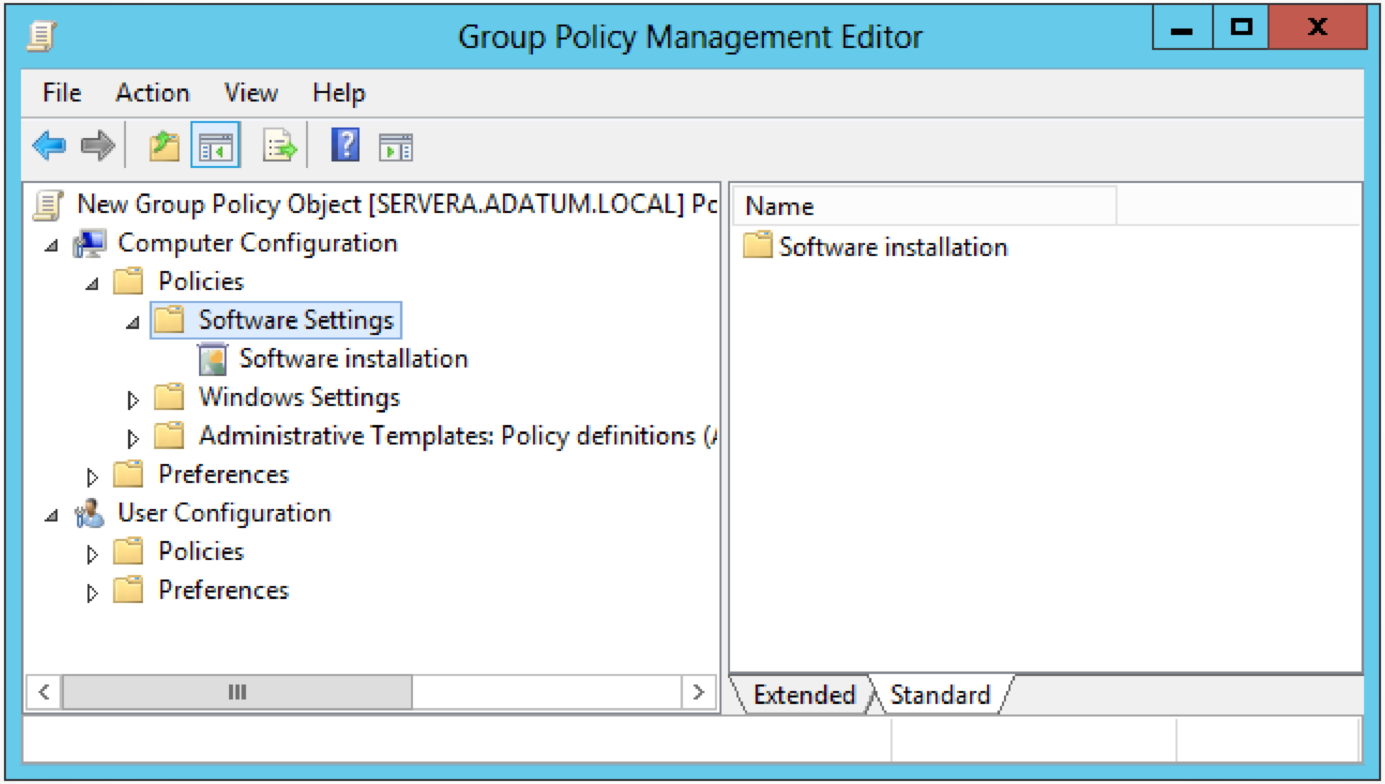
The process of repackaging software for .msi distribution consists of the following steps:

1. Take a snapshot of a clean computer system.
2. Install and configure the application as desired.
3. Take a snapshot of the computer after the application is installed.

Deploying Software Using Group Policy

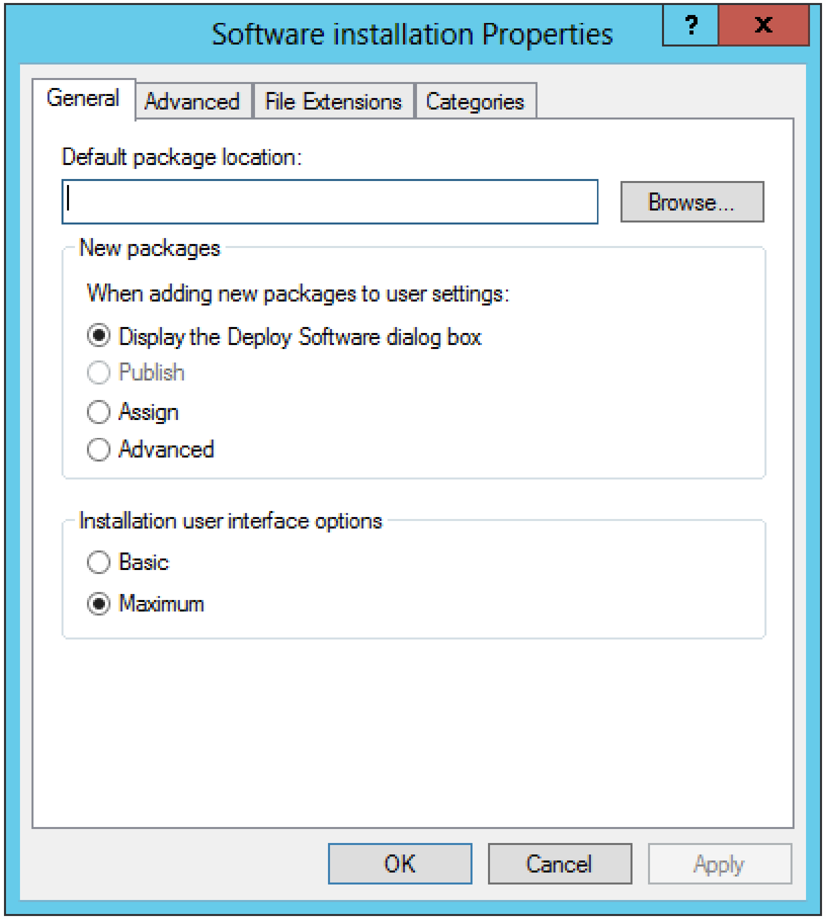
- Before deploying software using Group Policy, you must create a **distribution share**—a network location from which users can download the software that they need.
- Create a GPO or modify an existing GPO to include the software installation settings, plus one of two options:
  - **Assign option:** Helpful when you are deploying required applications to pertinent users and computers.
  - **Publish option:** Enables users to install the applications that they consider useful to them.

Configure Software Installation Defaults



The Software Settings folder in a GPO

Configure Software Installation Defaults



Software installation Properties

Default package location:

New packages

When adding new packages to user settings:

● Display the Deploy Software dialog box

○ Publish

○ Assign

○ Advanced

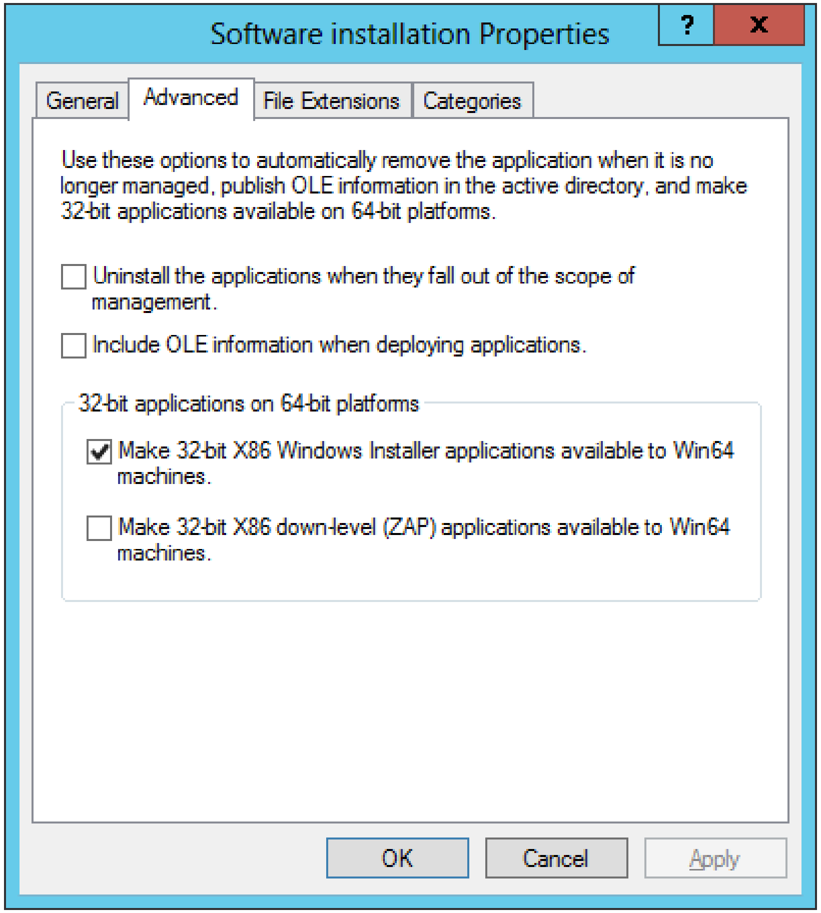
Installation user interface options

○ Basic

● Maximum

The Software Installation Properties sheet

Configure Software Installation Defaults



Use these options to automatically remove the application when it is no longer managed, publish OLE information in the active directory, and make 32-bit applications available on 64-bit platforms.

□ Uninstall the applications when they fall out of the scope of management.

□ Include OLE information when deploying applications.

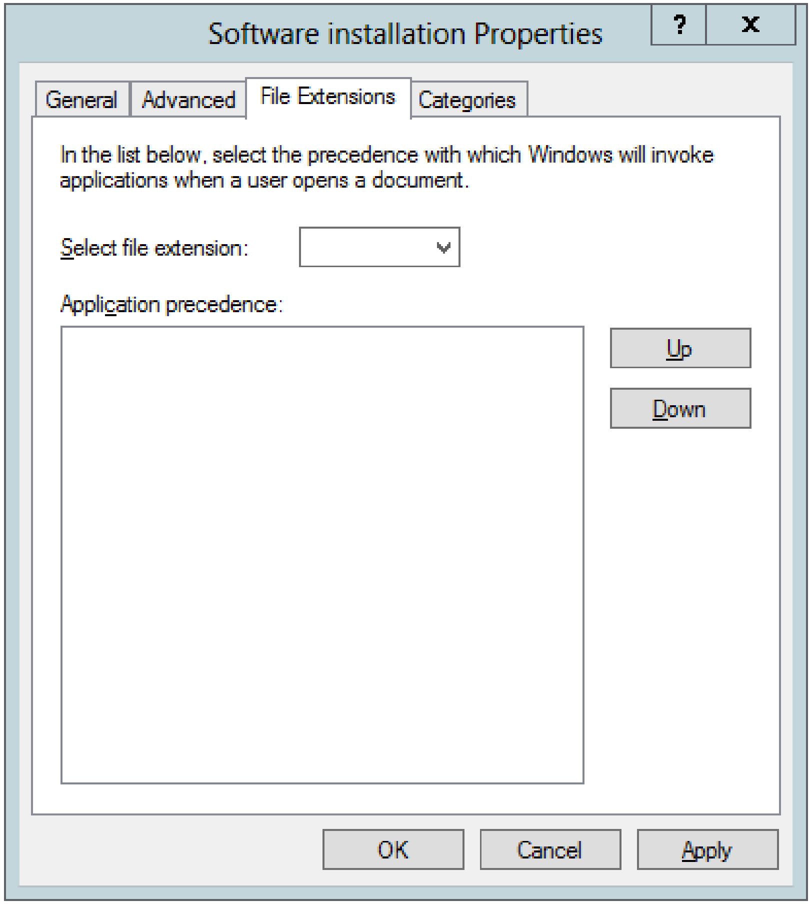
32-bit applications on 64-bit platforms

☑ Make 32-bit X86 Windows Installer applications available to Win64 machines.

□ Make 32-bit X86 down-level (ZAP) applications available to Win64 machines.

The Advanced tab of the Software Installation Properties sheet

Configure Software Installation Defaults



Software installation Properties

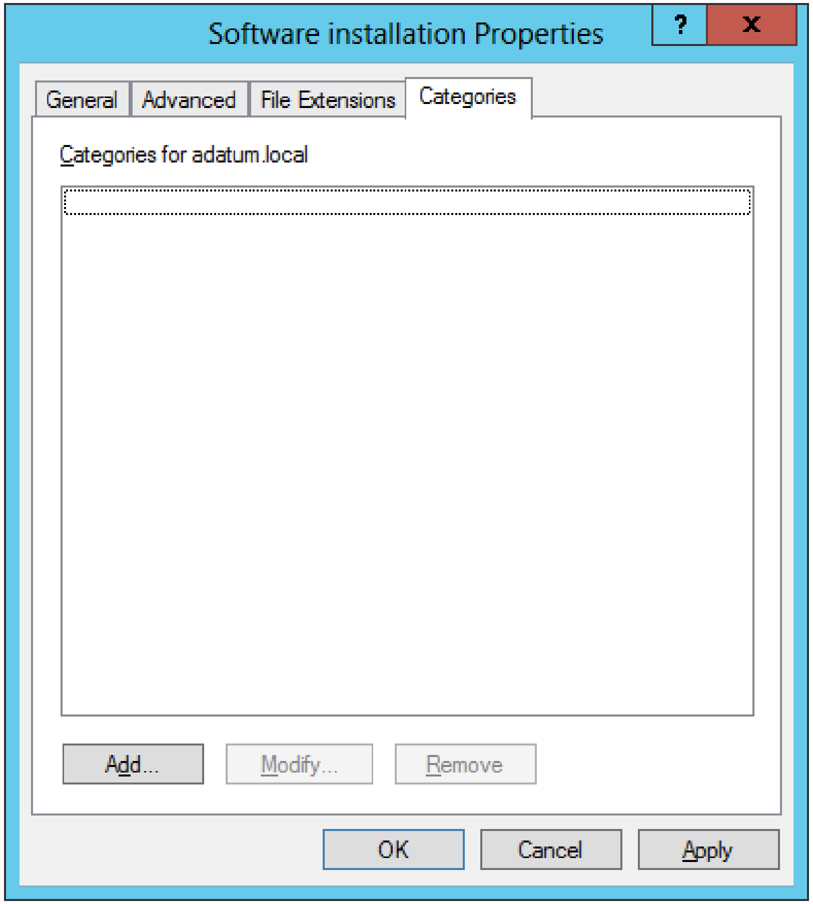
In the list below, select the precedence with which Windows will invoke applications when a user opens a document.

Select file extension:

Application precedence:

The File Extensions tab of the Software Installation Properties sheet

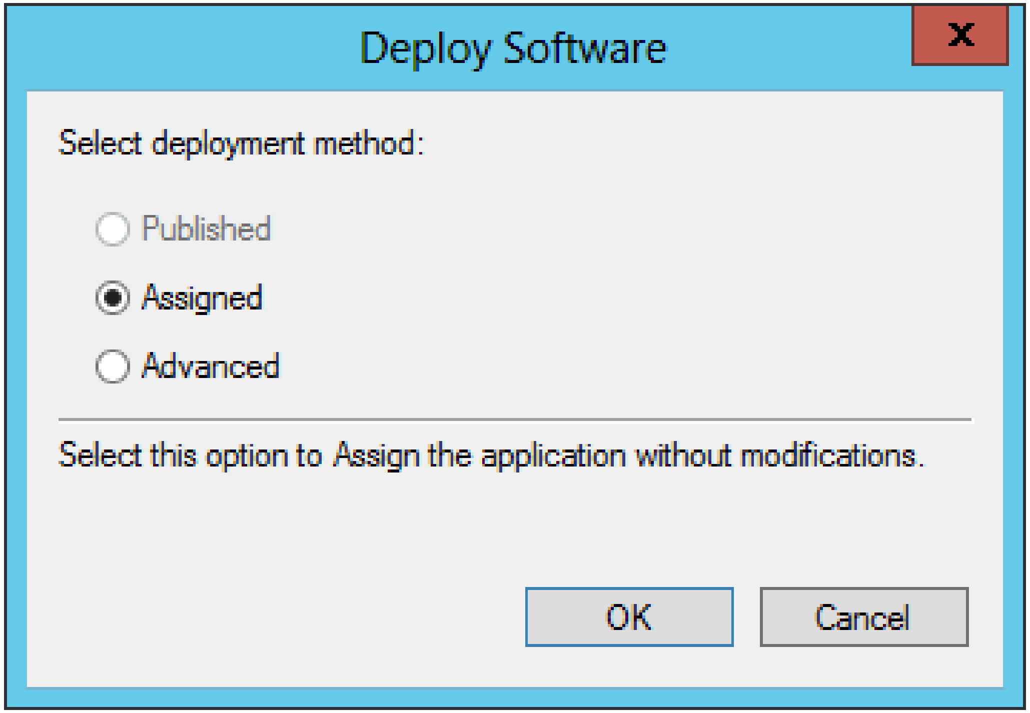
Configure Software Installation Defaults


Software installation Properties

Categories for adatum.local

The Enter new category tab of the Software Installation Properties sheet

Create a New Software Installation Package



Deploy Software

Select deployment method:

○ Published

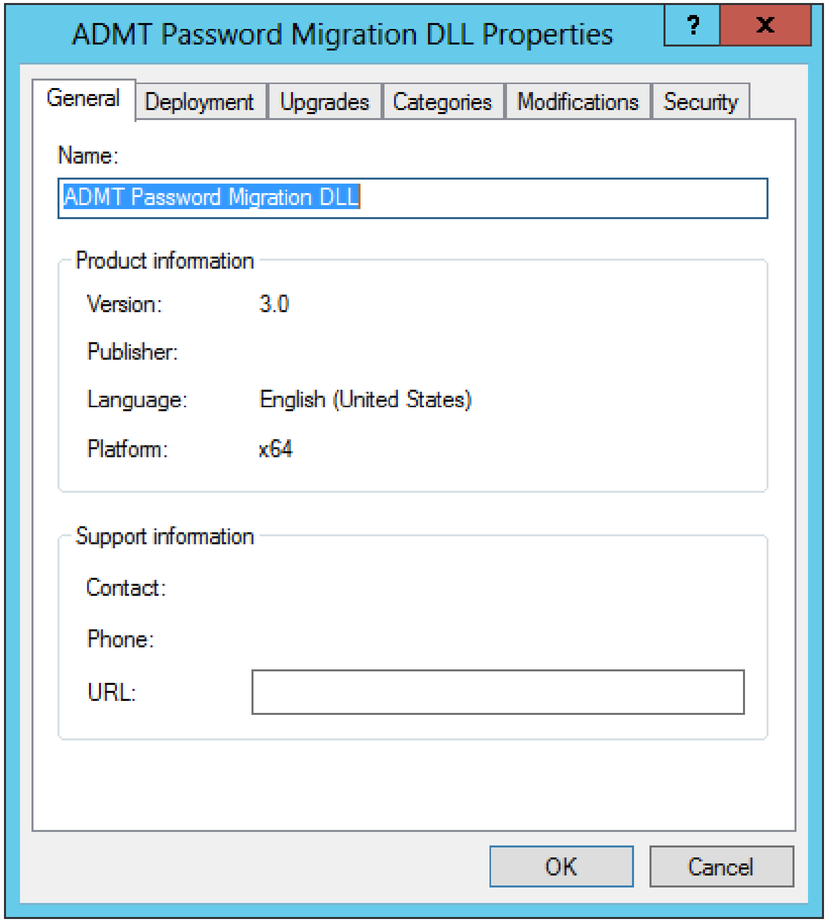
● Assigned

○ Advanced

Select this option to Assign the application without modifications.

The Deploy Software dialog box

Customizing Software Installation Packages



Name: ADMT Password Migration DLL

Product information

Version: 3.0

Publisher:

Language: English (United States)

Platform: x64

Support information

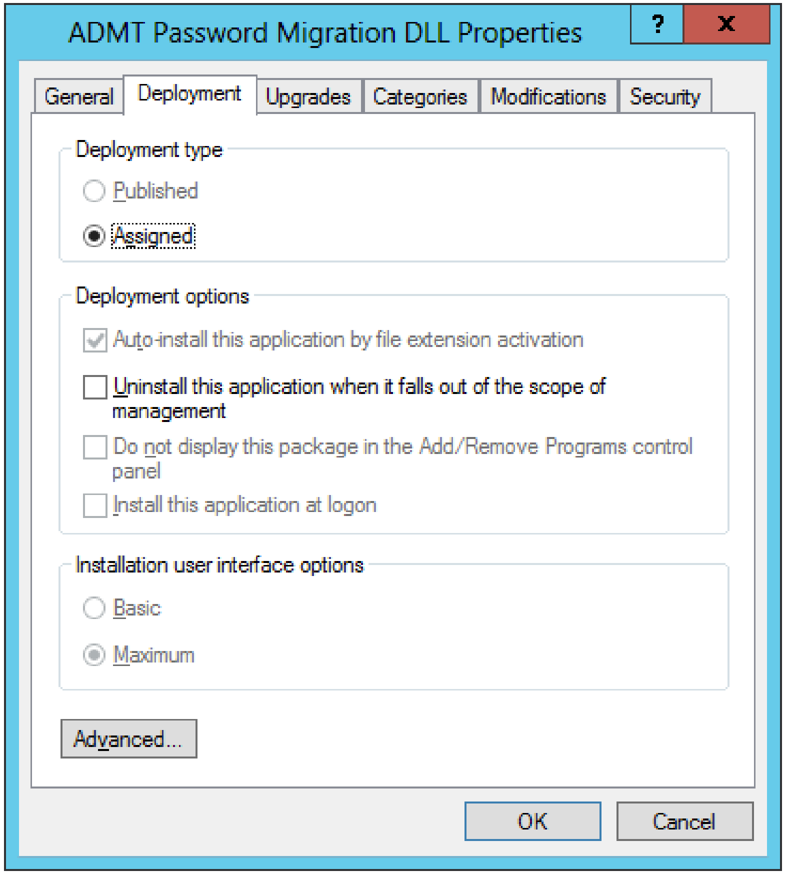
Contact:

Phone:

URL:

The Properties sheet of a Windows Installer package

Customizing Software Installation Packages



ADMT Password Migration DLL Properties

Deployment type

○ Published

● Assigned

Deployment options

☑ Auto-install this application by file extension activation

□ Uninstall this application when it falls out of the scope of management

□ Do not display this package in the Add/Remove Programs control panel

□ Install this application at logon

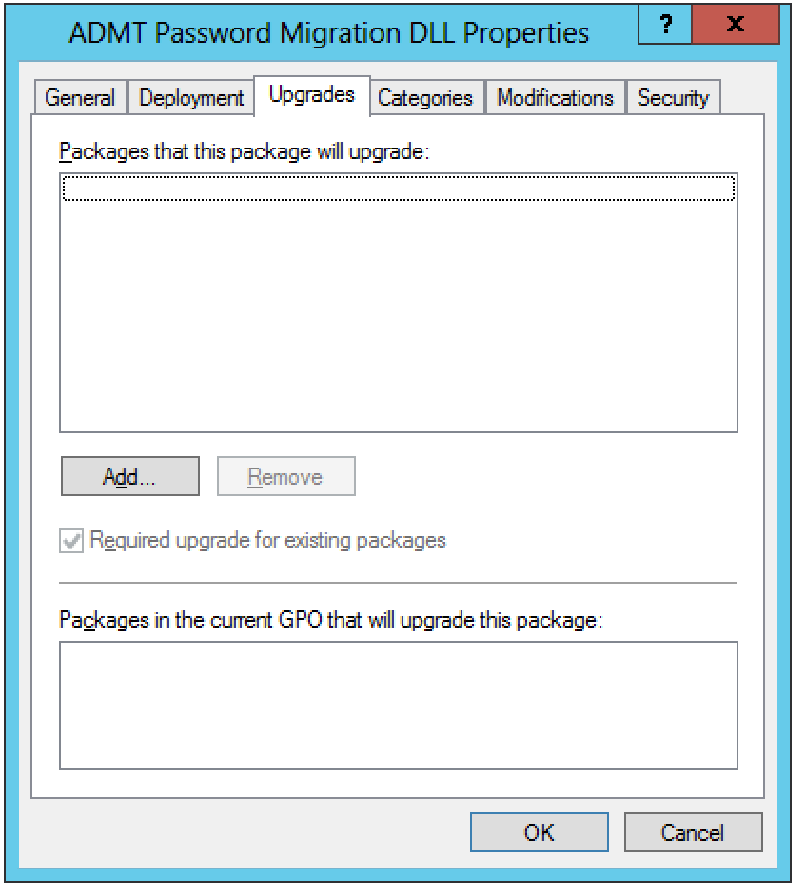
Installation user interface options

○ Basic

● Maximum

The Deployment tab on a software installation package's Properties sheet

Customizing Software Installation Packages



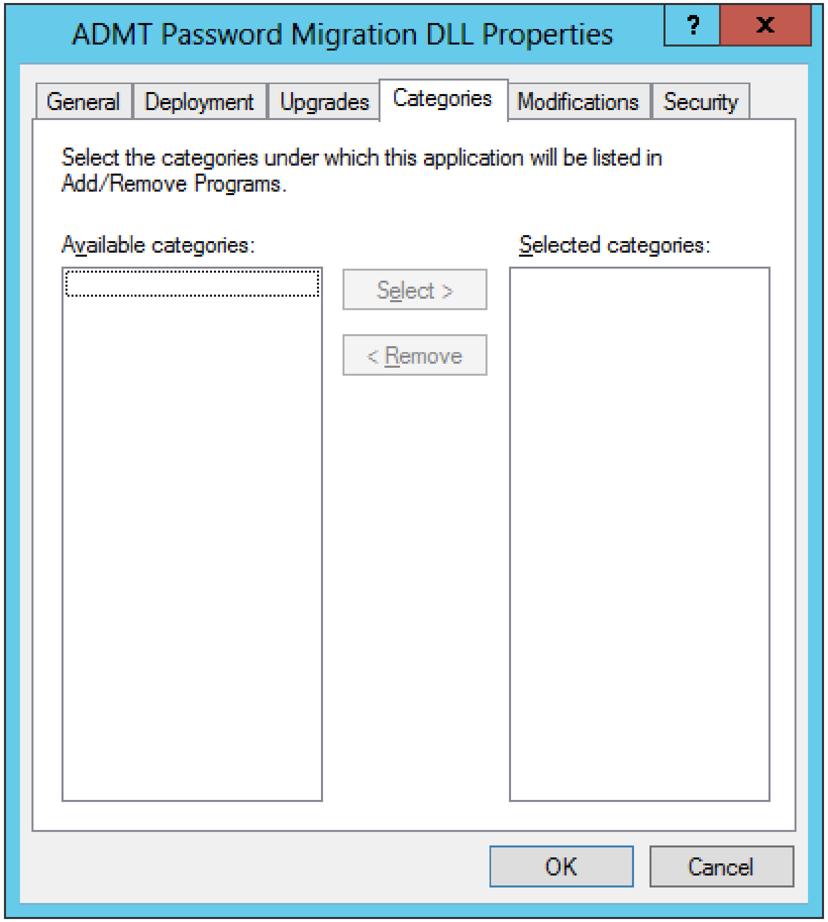
Packages that this package will upgrade:

☑ Required upgrade for existing packages

Packages in the current GPO that will upgrade this package:

The Upgrades tab on a software installation package's Properties sheet

Customizing Software Installation Packages



ADMT Password Migration DLL Properties

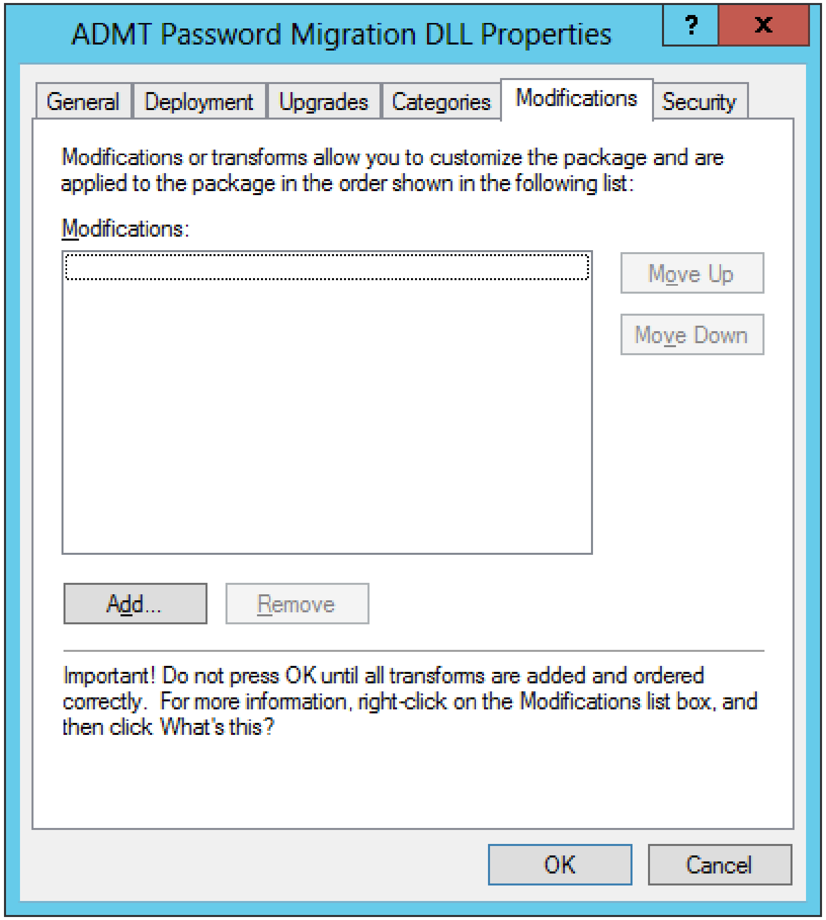
Select the categories under which this application will be listed in Add/Remove Programs.

Available categories:

Selected categories:

The Categories tab on a software installation package's Properties sheet

Customizing Software Installation Packages



ADMT Password Migration DLL Properties

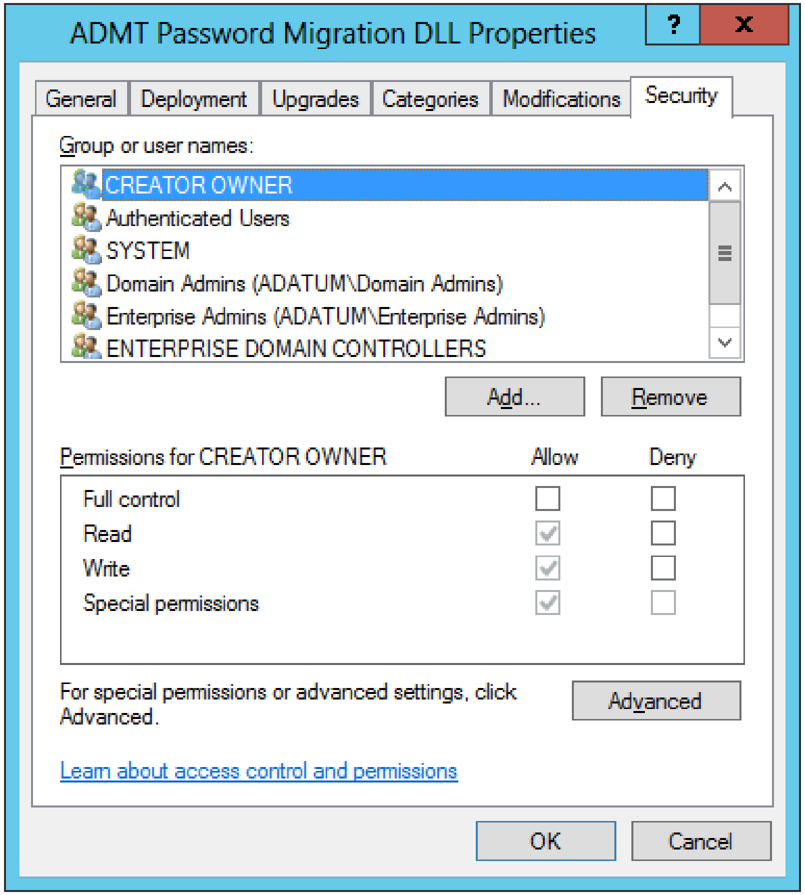
Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

The Modifications tab on a software installation package's Properties sheet

Customizing Software Installation Packages



ADMT Password Migration DLL Properties

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (ADATUM\Domain Admins)
- Enterprise Admins (ADATUM\Enterprise Admins)
- ENTERPRISE DOMAIN CONTROLLERS

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	☑	□
Write	☑	□
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

The Security tab on a software installation package's Properties sheet

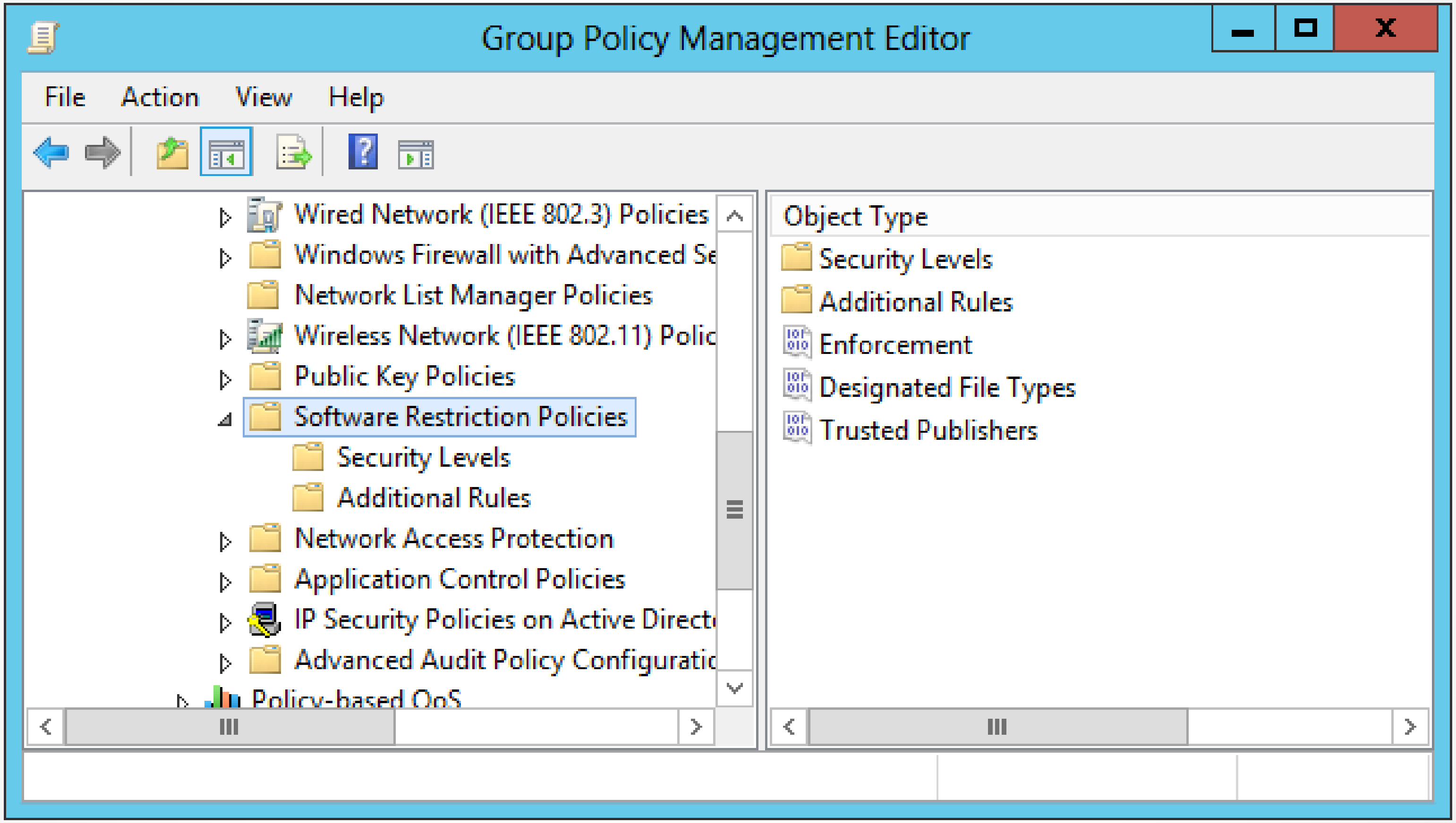
Configuring Software Restriction Policies

Lesson 18: Configuring Application Restriction Policies

Configuring Software Restriction Policies

- Software restriction policies are designed to identify software and control its execution.
- Provides organizations greater control in preventing potentially dangerous applications from running.
- You can control who is affected by the policies.

Configuring Software Restriction Policies



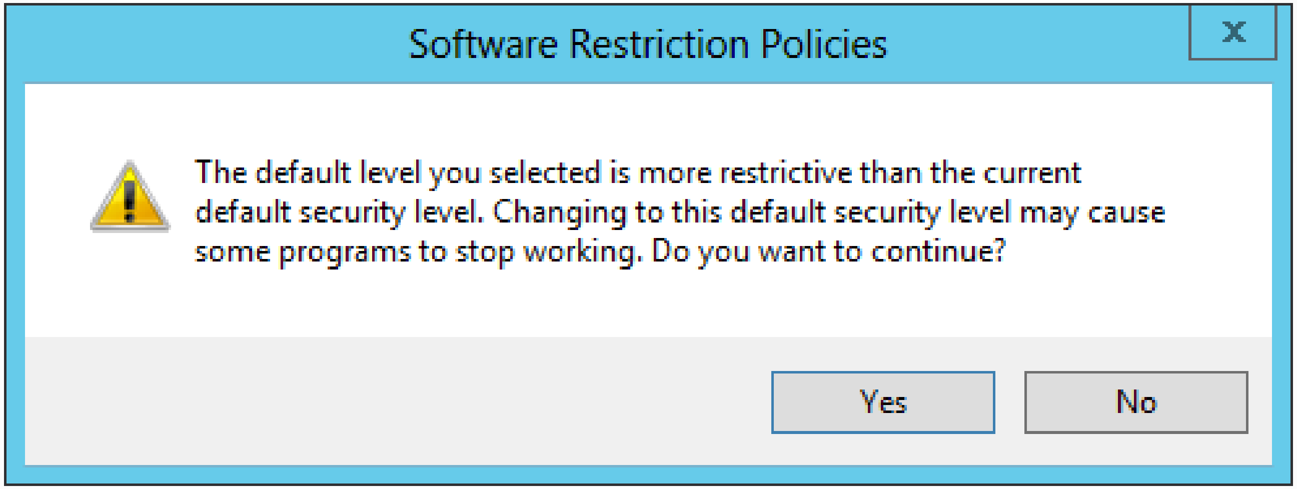
Group Policy Management Editor
File
Action
View
Help
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
Application Control Policies
IP Security Policies on Active Direct
Advanced Audit Policy Configuratic
Policy-based QoS
Object Type
Security Levels
Additional Rules
Enforcement
Designated File Types
Trusted Publishers

The Software Restriction Policies folder

Enforcing Restrictions

- If a policy does not enforce restrictions, executable files run based on the permissions that users or groups have in the NTFS file system.
- You can use three basic strategies for enforcing restrictions:
  - **Unrestricted:** Enables all applications to run, except those that are specifically excluded.
  - **Disallowed:** Prevents all applications from running except those that are specifically allowed.
  - **Basic User:** Prevents any application from running that requires administrative rights, but enables programs to run that only require resources that are accessible by normal users.

Modify the Default Security Level


Software Restriction Policies

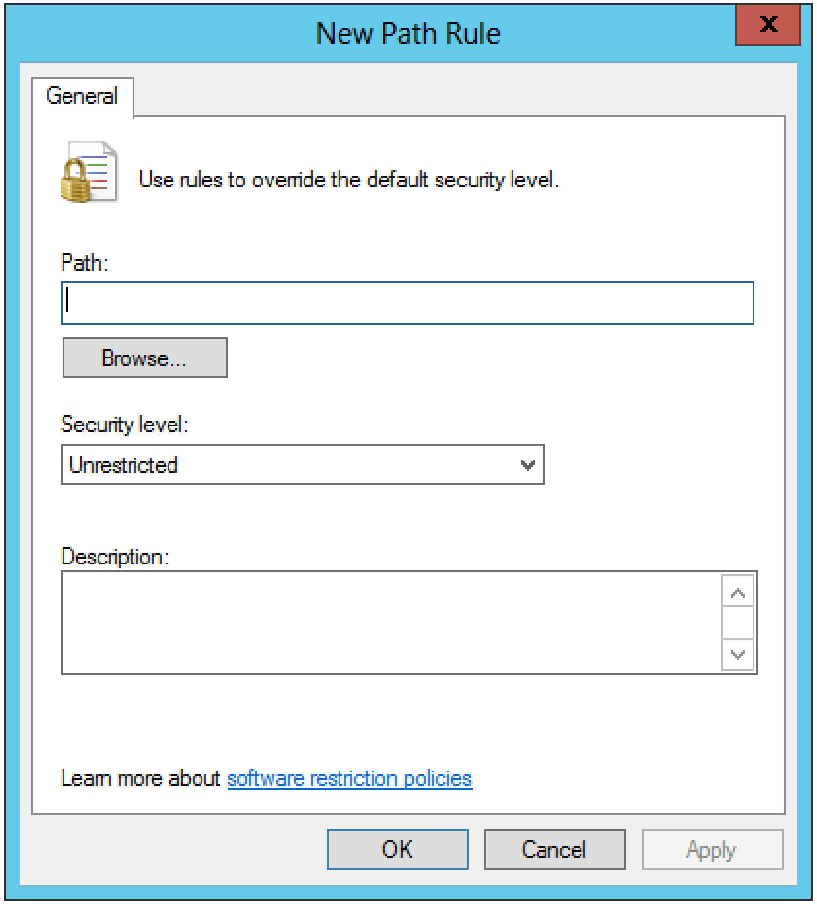
The default level you selected is more restrictive than the current default security level. Changing to this default security level may cause some programs to stop working. Do you want to continue?

Setting the Default Security Level of a software restriction policy

Configuring Software Restriction Rules

- There are four types of software restriction rules to specify which programs can or cannot run on your network:
  - Hash rules
  - Certificate rules
  - Path rules
  - Network zone rules
- You can use multiple rules and they are applied in the order listed above.

Configuring Software Restriction Rules



New Path Rule

Use rules to override the default security level.

Path:

Security level: Unrestricted

Description:

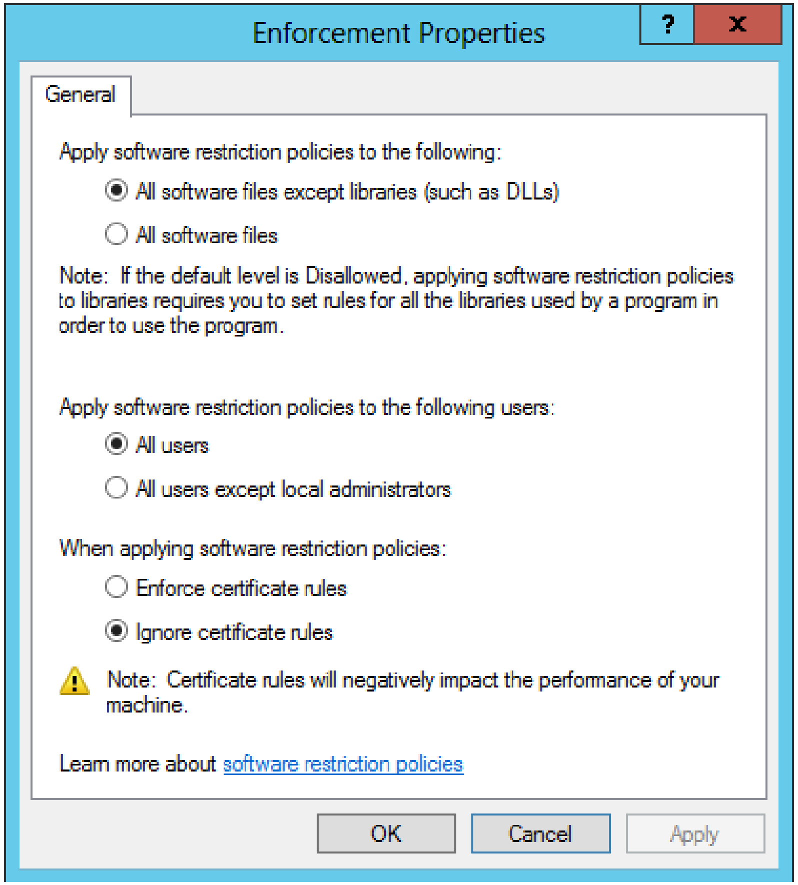
Learn more about software restriction policies

The New Path Rule dialog box

Configuring Software Restriction Properties

- Within the Software Restriction Policies folder, you can configure three specific properties to provide additional settings that apply to all policies when implemented.
- These three properties are:
  - Enforcement
  - Designated file types
  - Trusted publishers

Configuring Software Restriction Properties



Apply software restriction policies to the following:

● All software files except libraries (such as DLLs)

○ All software files

Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.

Apply software restriction policies to the following users:

● All users

○ All users except local administrators

When applying software restriction policies:

○ Enforce certificate rules

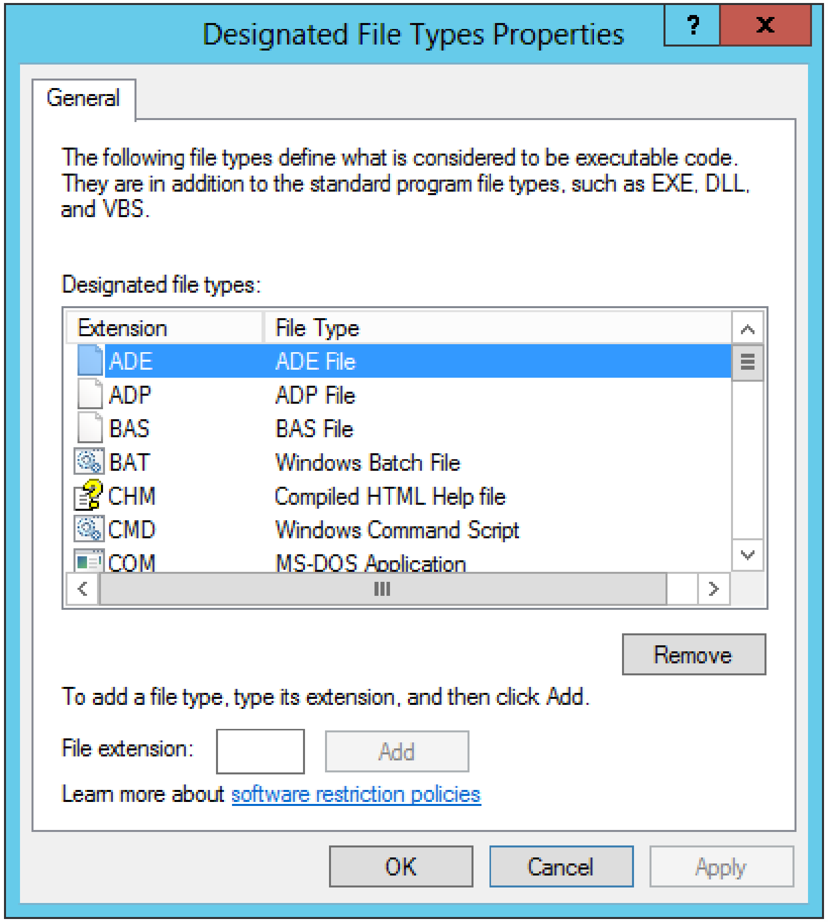
● Ignore certificate rules

⚠ Note: Certificate rules will negatively impact the performance of your machine.

Learn more about software restriction policies

Configuring Enforcement properties

Configuring Software Restriction Properties



The following file types define what is considered to be executable code. They are in addition to the standard program file types, such as EXE, DLL, and VBS.

Designated file types:

Extension	File Type
ADE	ADE File
ADP	ADP File
BAS	BAS File
BAT	Windows Batch File
CHM	Compiled HTML Help file
CMD	Windows Command Script
COM	MS-DOS Application

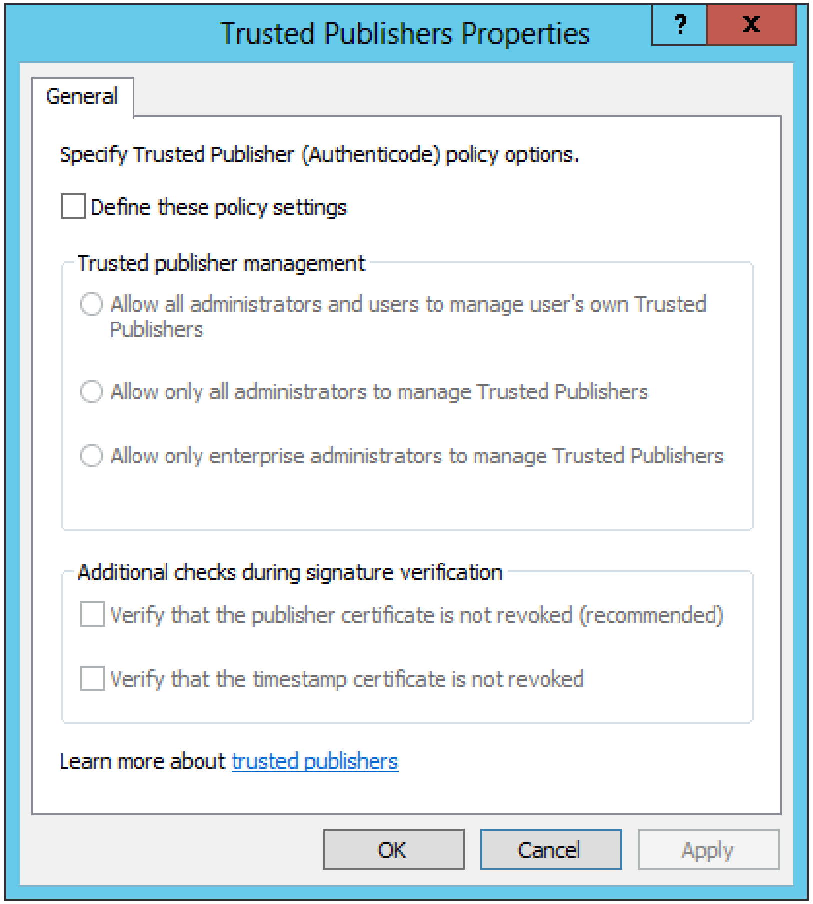
To add a file type, type its extension, and then click Add.

File extension:

Learn more about software restriction policies

Configuring Designated File Types properties

Configuring Software Restriction Properties



Specify Trusted Publisher (Authenticode) policy options.

□ Define these policy settings

Trusted publisher management

○ Allow all administrators and users to manage user's own Trusted Publishers

○ Allow only all administrators to manage Trusted Publishers

○ Allow only enterprise administrators to manage Trusted Publishers

Additional checks during signature verification

□ Verify that the publisher certificate is not revoked (recommended)

□ Verify that the timestamp certificate is not revoked

Learn more about trusted publishers

Configuring Trusted Publishers properties

Software Restriction Best Practices

- Software restriction policies should be used with standard access control permissions.
- The Disallowed Default Security Level should be used cautiously, because all applications are restricted unless explicitly allowed.
- If you accidentally create policies that cause undesirable restrictions on a workstation, reboot the computer in Safe Mode to troubleshoot and make changes, because software restriction policies cannot be applied in Safe Mode.
- When editing software restriction policies, you should disable them first so that a partially complete policy does not cause undesirable results on a computer.
- Creating a separate GPO for software restriction policies enables you to disable or remove them without affecting other policy settings.
- Test all policies before deploying them to the users.

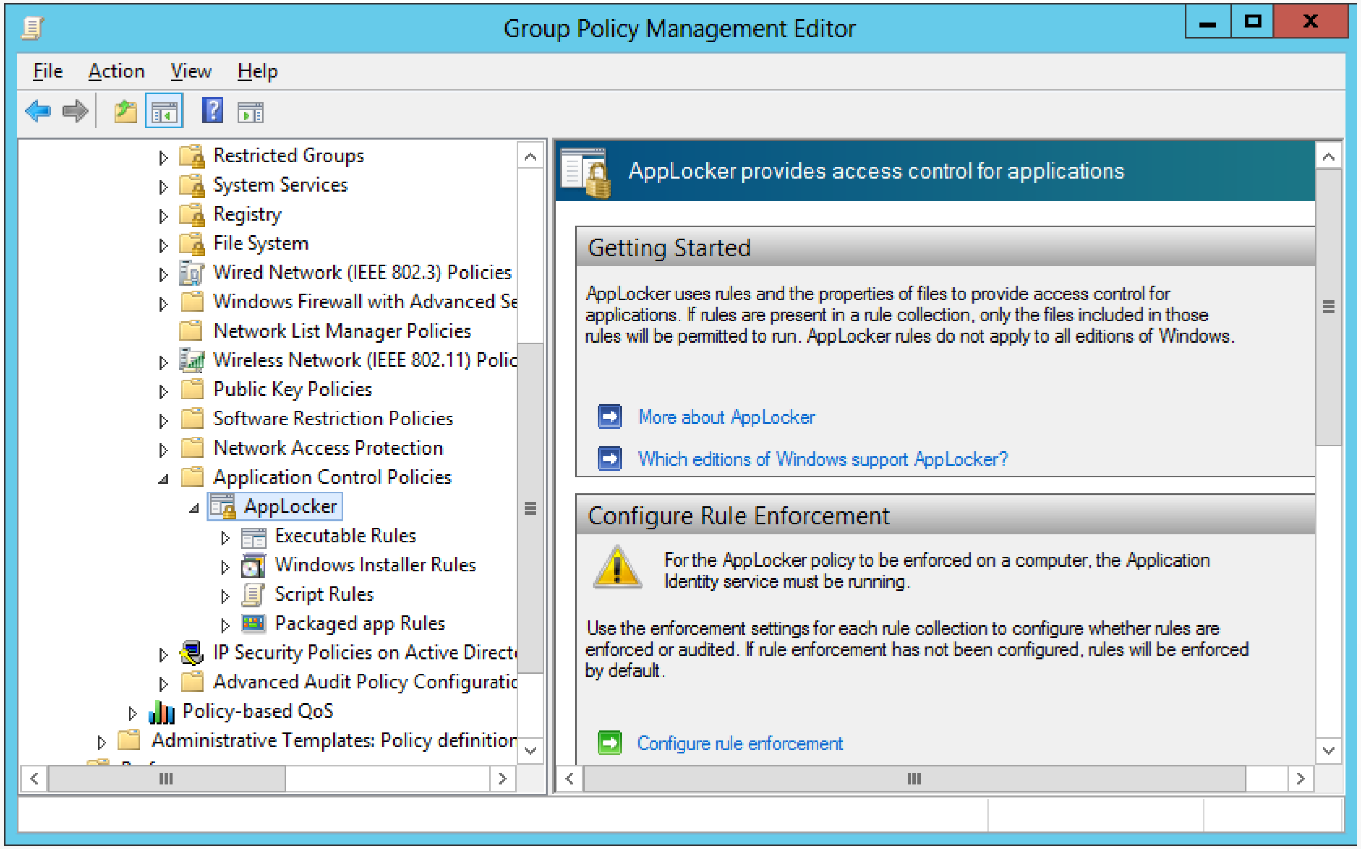
Using AppLocker

Lesson 18: Configuring Application Restriction Policies

AppLocker

- **AppLocker**, also known as **application control policies**, is a Windows feature that is an updated version of the concept implemented in software restriction policies.
- Uses rules, which you must manage, using a wizard-based interface.
- More flexible than software restriction policies

Rule Types


Group Policy Management Editor
File
Action
View
Help
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Policy-based QoS
Administrative Templates: Policy definition
More about AppLocker
Which editions of Windows support AppLocker?
Configure rule enforcement

AppLocker provides access control for applications

Getting Started

AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.

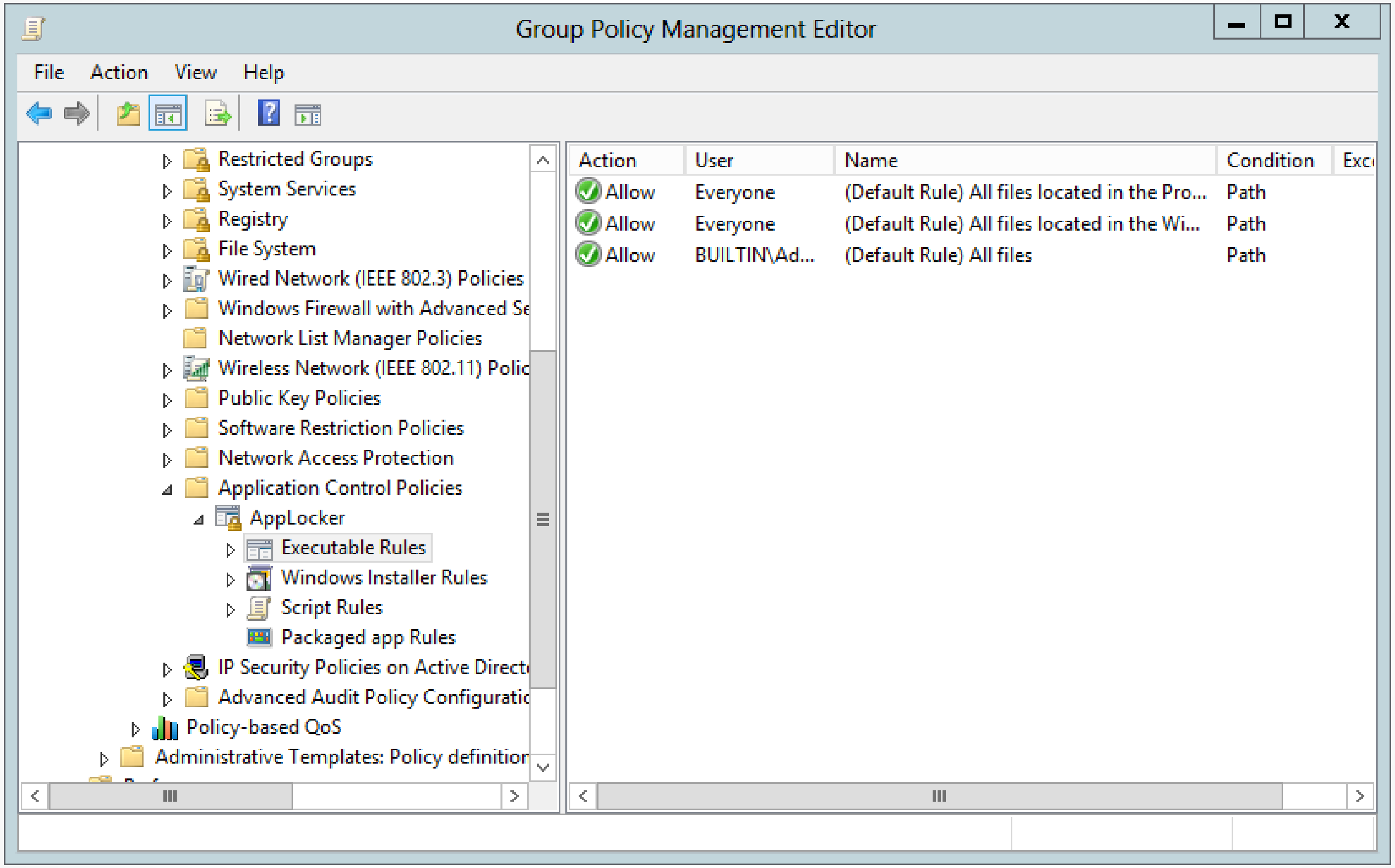
Configure Rule Enforcement

For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.

Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.

The AppLocker container in a GPO

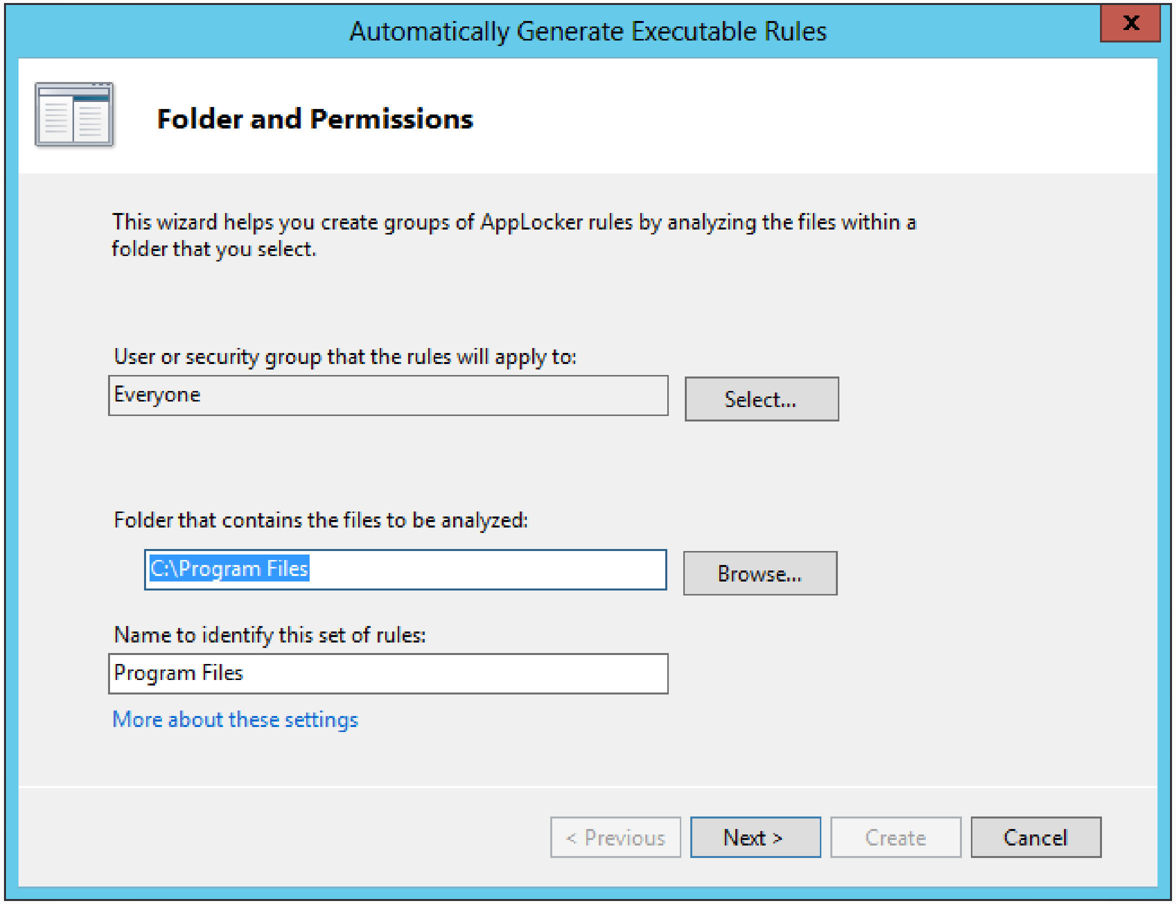
Creating Default Rules


Group Policy Management Editor
File
Action
View
Help
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Polic
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
Packaged app Rules
IP Security Policies on Active Directo
Advanced Audit Policy Configuratio
Policy-based QoS
Administrative Templates: Policy definition

Action	User	Name	Condition	Exc
✓ Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
✓ Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
✓ Allow	BUILTIN\Ad...	(Default Rule) All files	Path	

The default AppLocker executable rules

Creating Rules Automatically



This wizard helps you create groups of AppLocker rules by analyzing the files within a folder that you select.

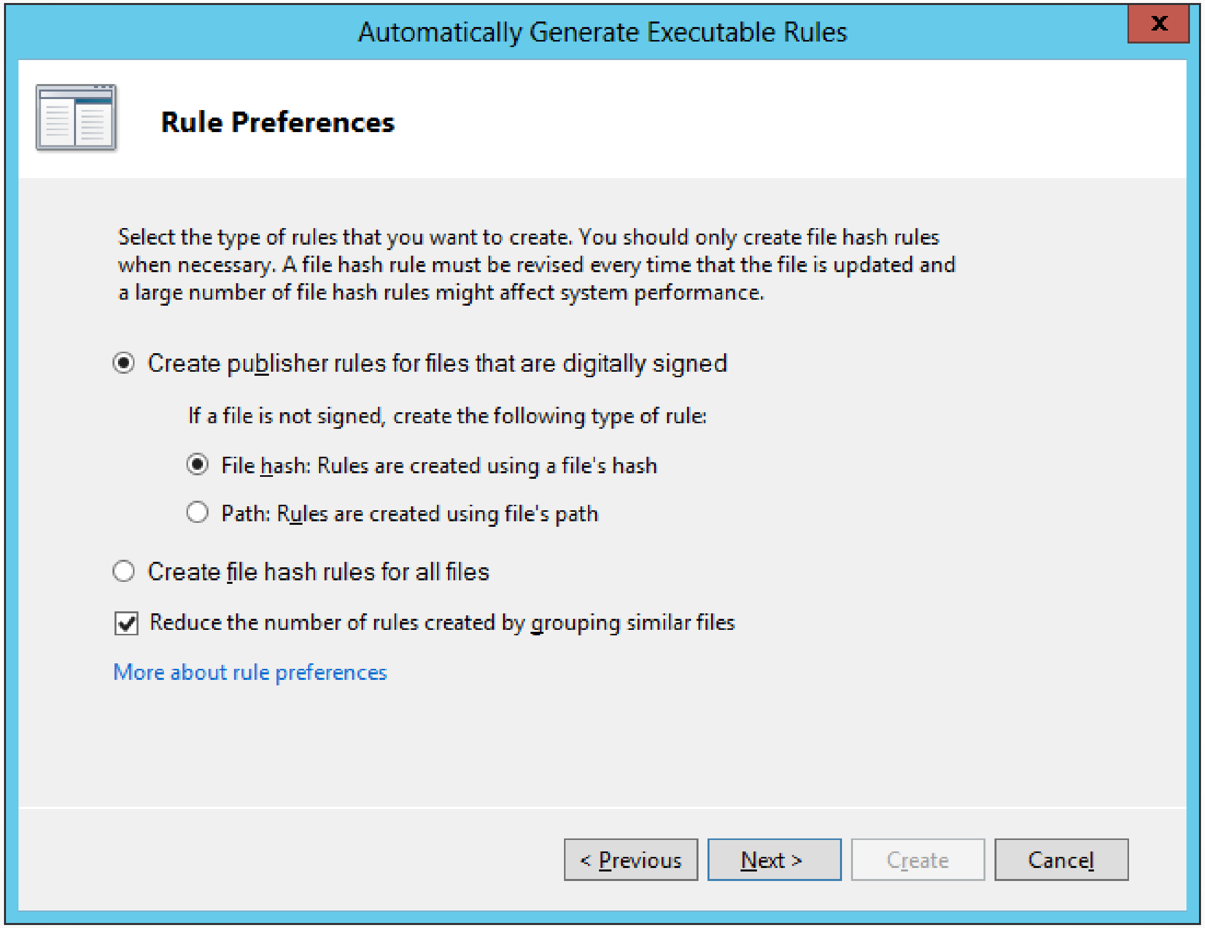
User or security group that the rules will apply to: Everyone

Folder that contains the files to be analyzed: C:\Program Files

Name to identify this set of rules: Program Files

The Automatically Generate Executable Rules Wizard

Creating Rules Automatically



Automatically Generate Executable Rules

Rule Preferences

Select the type of rules that you want to create. You should only create file hash rules when necessary. A file hash rule must be revised every time that the file is updated and a large number of file hash rules might affect system performance.

● Create publisher rules for files that are digitally signed

If a file is not signed, create the following type of rule:

● File hash: Rules are created using a file's hash

○ Path: Rules are created using file's path

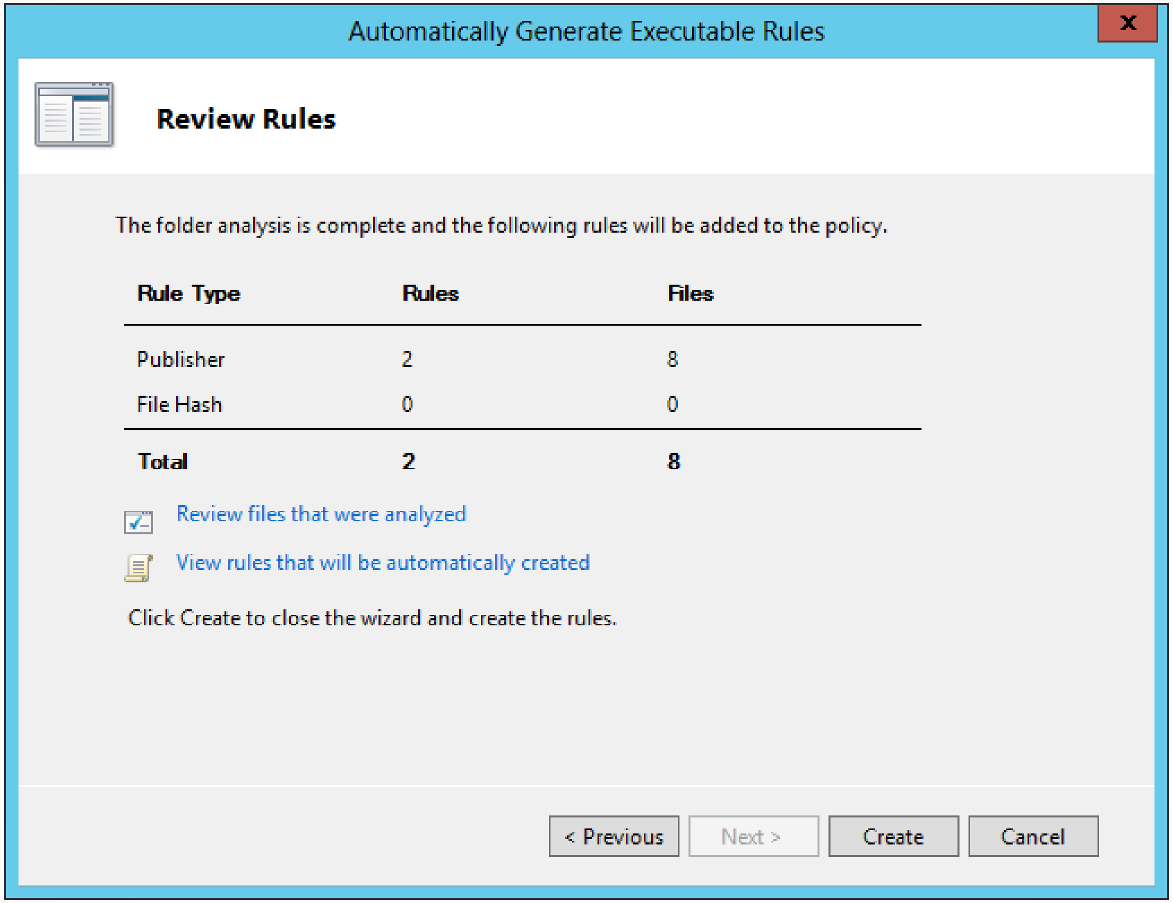
○ Create file hash rules for all files

☑ Reduce the number of rules created by grouping similar files

More about rule preferences

The Rule Preferences page of the Automatically Generate Executable Rules Wizard

Creating Rules Automatically



Review Rules

The folder analysis is complete and the following rules will be added to the policy.

Rule Type	Rules	Files
Publisher	2	8
File Hash	0	0
Total	**2**	**8**

Review files that were analyzed

View rules that will be automatically created

Click Create to close the wizard and create the rules.

The Review Rules page of the Automatically Generate Executable Rules Wizard

Creating Rules Manually

- You can also create rules manually, by using a wizard-based interface.
- The wizard prompts you for the following:
  - **Action:** Specifies whether you want to allow or deny the user or group access to the resource. In AppLocker, explicit deny rules always override allow rules.
  - **User or group:** Specifies the name of the user or group to which the policy should apply.
  - **Conditions:** Specifies whether you want to create a publisher, path, or file hash rule. The wizard generates an additional page for whichever option you select, enabling you to configure its parameters.
  - **Exceptions:** Enables you to specify exceptions to the rule you create, using any of the three conditions: publisher, path, or file hash.

Lesson Summary

- You can use Group Policy to deploy new software on your network and remove or repair software originally deployed by a GPO from your network.
- The Windows Installer service supports three types of package files: .msi files for standard software installation, .mst files for customized software installation, and .msp files for patching .msi files at the time of deployment.
- You must create a shared folder, called a *software distribution point*, to store application installation and package files to be deployed by using Group Policy.
- Software to be deployed using Group Policy can either be Assigned or Published. Assigning software using the User Configuration node of a Group Policy enables the application to be installed when the user accesses the program using the Start menu or an associated file. Publishing an application enables the application to be available through Control Panel.

Lesson Summary

- Software restriction policies enable the software's executable code to be identified and either allowed or disallowed on the network.
- The three Default Security Levels within software restriction policies are Unrestricted, which means all applications function based on user permissions; Disallowed, which means all applications are denied execution regardless of the user permissions; and Basic User, which enables only executables to be run that can be run by normal users.
- Four rule types can be defined within a software restriction policy. They include, in order of precedence, hash, certificate, path, and network zone rules. The security level set on a specific rule supersedes the Default Security Level of the policy.

Lesson Summary

- Software restriction policies are Group Policy settings that enable you to specify the programs that are allowed to run on workstations by creating rules of various types.
- AppLocker enables you to create application restriction rules easily.