How to Configure AppLocker

Task. Configure AppLocker.

Purpose. AppLocker controls the execution of software programs and can help prevent policy violations, malware infections, etc. This How-To creates a default AppLocker ruleset with one exception: access to PowerShell. The end result is Domain Admins will be able to invoke PowerShell and PowerShell ISE while Domain Users will not.

Conditions. You have domain administrator privileges and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

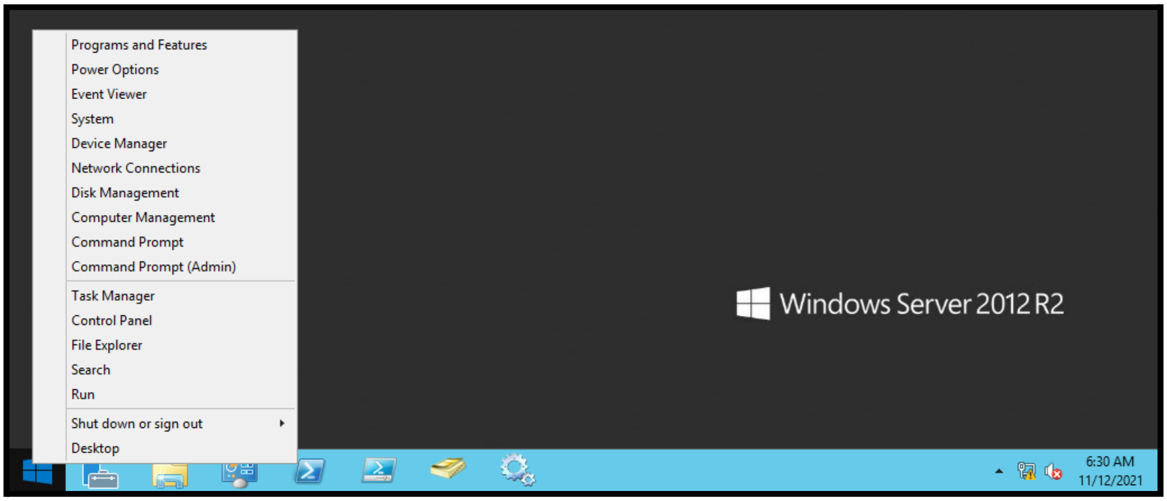
Standard. You were able to configure AppLocker and restrict access to PowerShell.

CIS Critical Security Controls

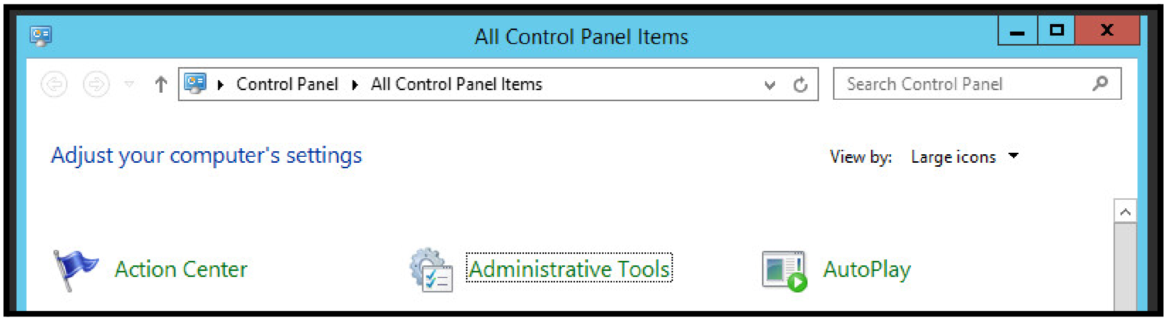
- Control: 2 - Inventory and Control of Software Assets
- Sub-Control: 2.7 - Utilize Application Whitelisting

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

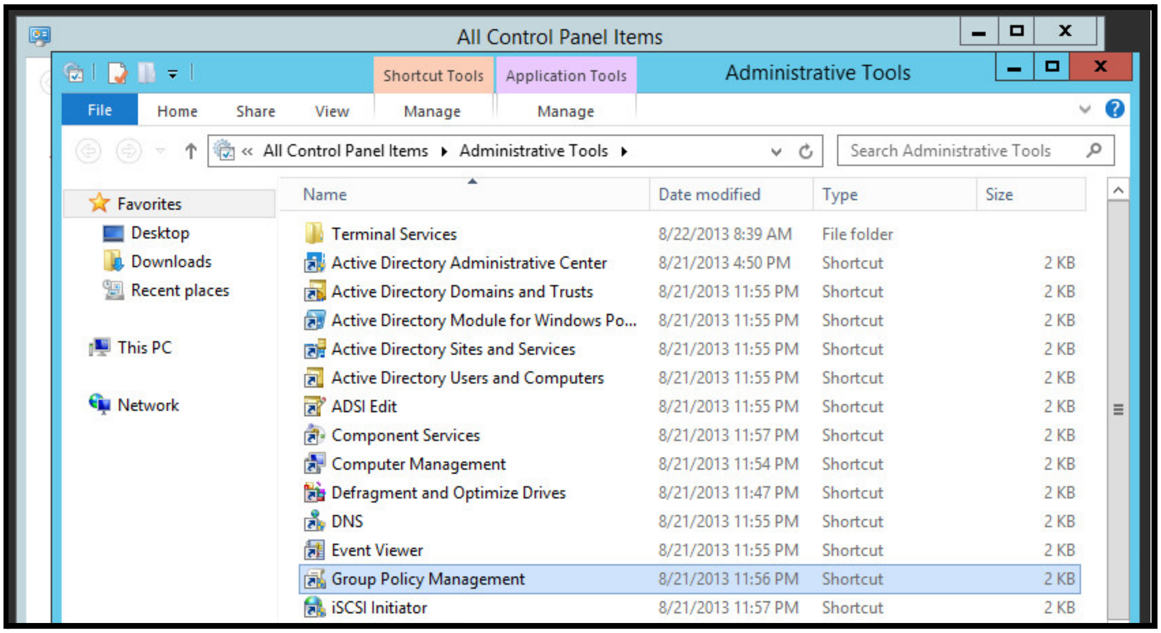
Step 2. Right-click on the Windows icon in the bottom-left corner and select “Control Panel.”



Step 3. Click-on “Administrative Tools.”

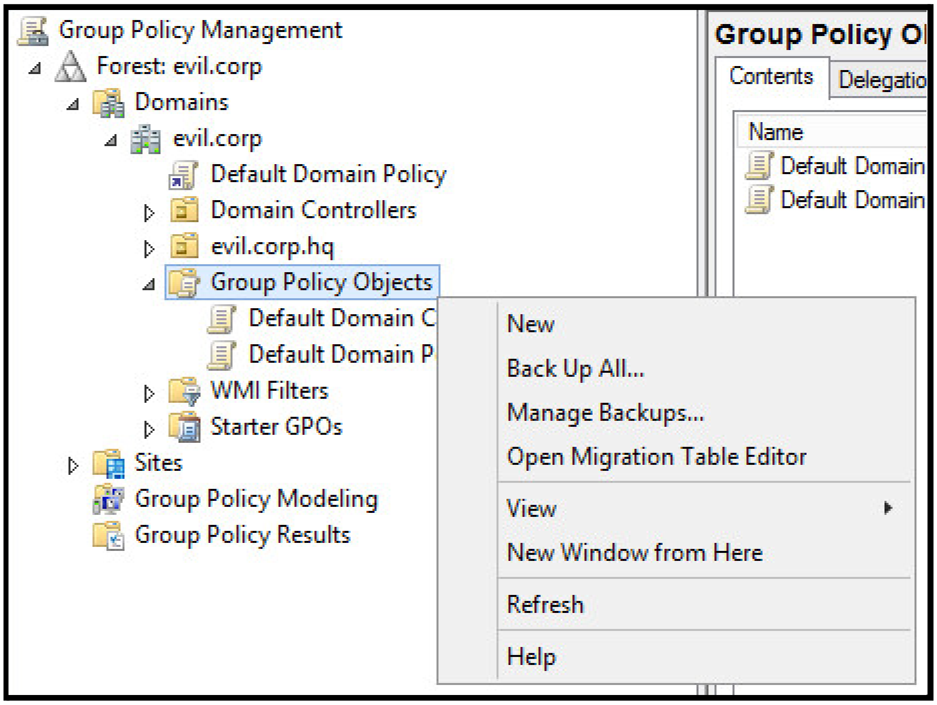


Step 4. Double-click “Group Policy Management.”



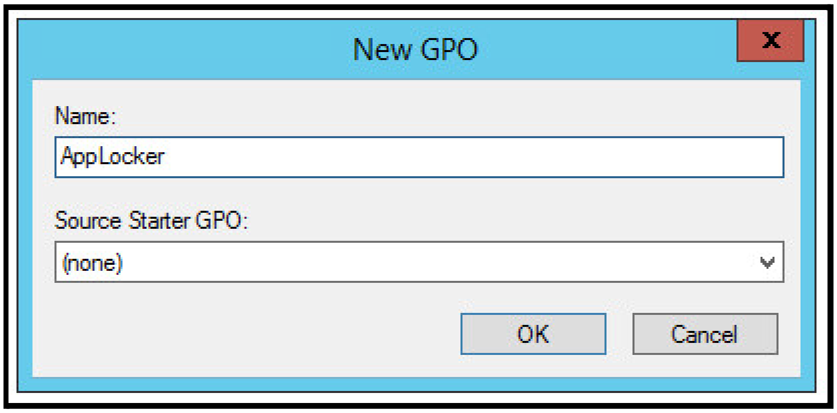
Name	Date modified	Type	Size
Terminal Services	8/22/2013 8:39 AM	File folder	
Active Directory Administrative Center	8/21/2013 4:50 PM	Shortcut	2 KB
Active Directory Domains and Trusts	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Module for Windows Po...	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Sites and Services	8/21/2013 11:55 PM	Shortcut	2 KB
Active Directory Users and Computers	8/21/2013 11:55 PM	Shortcut	2 KB
ADSI Edit	8/21/2013 11:55 PM	Shortcut	2 KB
Component Services	8/21/2013 11:57 PM	Shortcut	2 KB
Computer Management	8/21/2013 11:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/21/2013 11:47 PM	Shortcut	2 KB
DNS	8/21/2013 11:55 PM	Shortcut	2 KB
Event Viewer	8/21/2013 11:55 PM	Shortcut	2 KB
Group Policy Management	8/21/2013 11:56 PM	Shortcut	2 KB
iSCSI Initiator	8/21/2013 11:57 PM	Shortcut	2 KB

Step 5. Right-click the “Group Policy Objects” container and select “New.”



How to Configure AppLocker

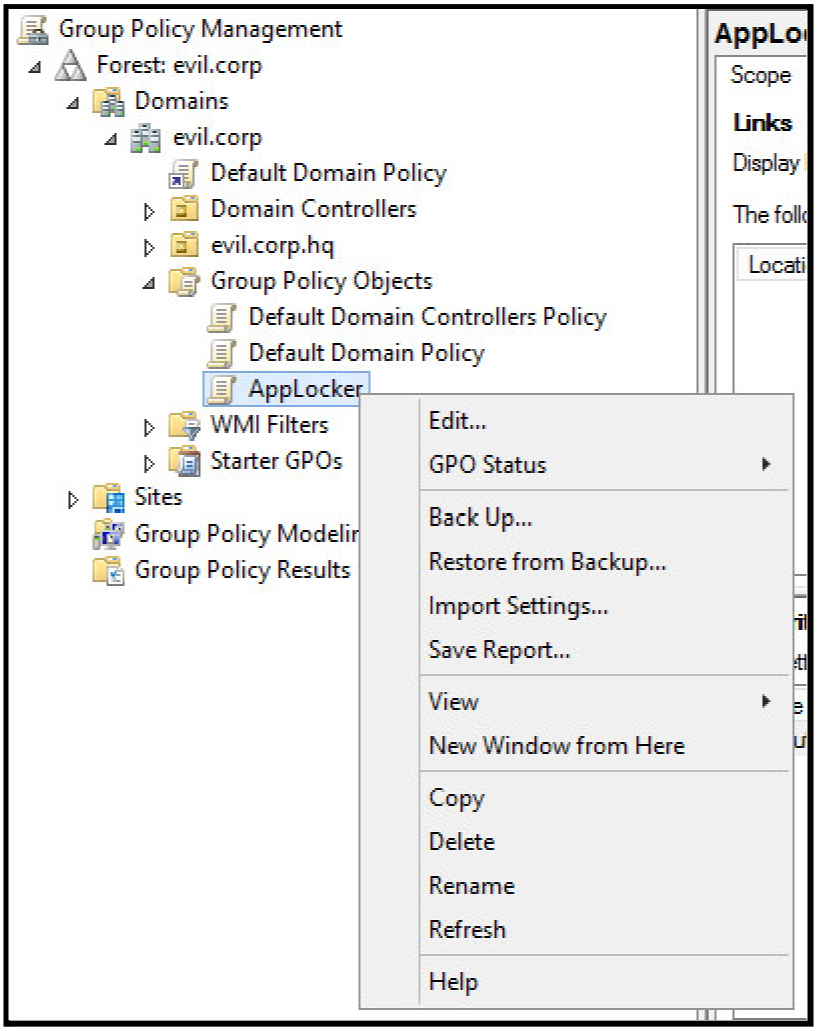
Step 6. Type “AppLocker” in the “Name” field.



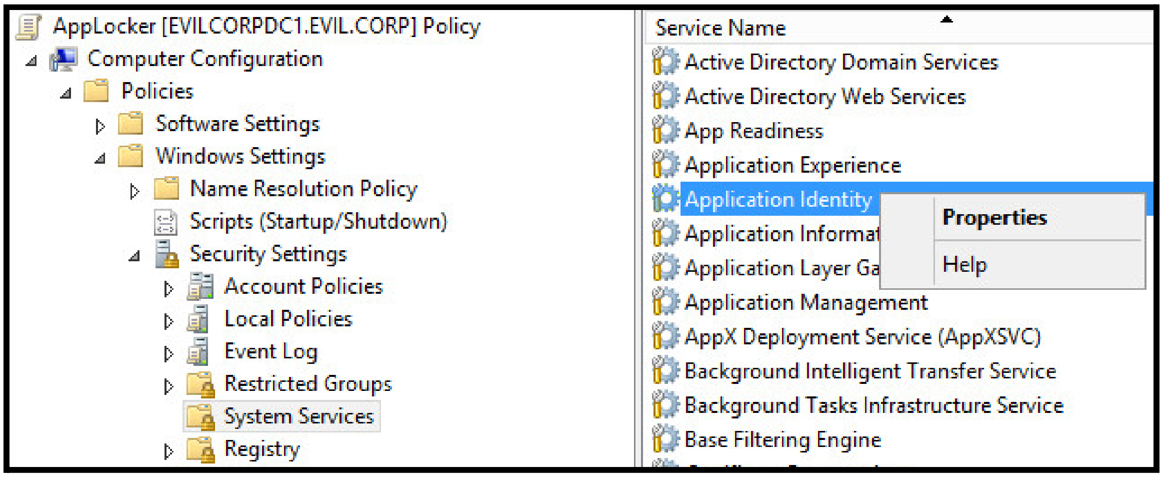
Name:
AppLocker

Source Starter GPO:
(none)

Step 7. Right-click the GPO you created and select “Edit.”



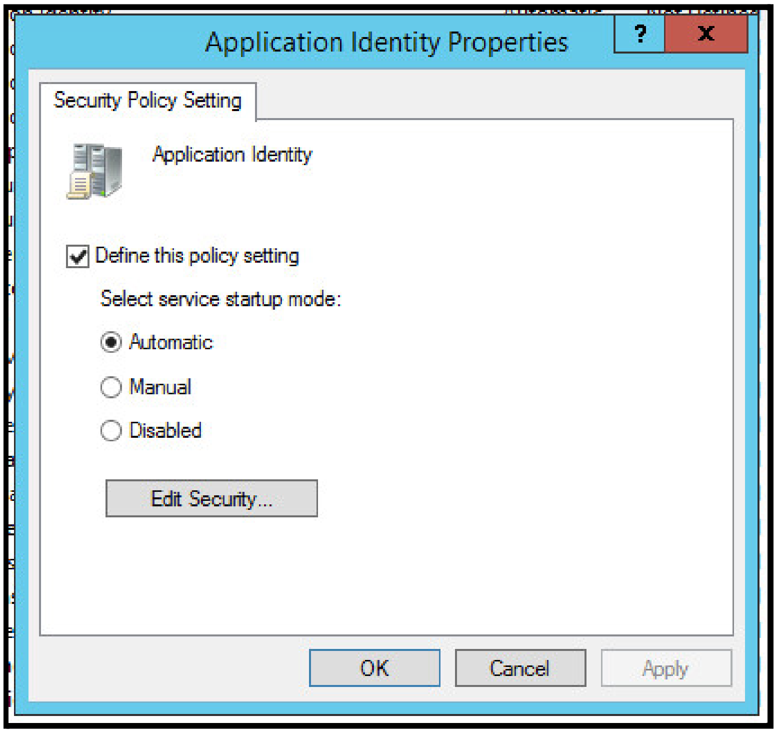
Step 8. With the GPO open, navigate to the following path: “Computer Configuration” > “Policies” > “Windows Settings” > “Security Settings” > “System Services.” Right-click “Application Identity” and select “Properties.”



AppLocker [EVILCORPDC1.EVIL.CORP] Policy
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry

Service Name
- Active Directory Domain Services
- Active Directory Web Services
- App Readiness
- Application Experience
- Application Identity
- Application Informat
- Application Layer Ga
- Application Management
- AppX Deployment Service (AppXSVC)
- Background Intelligent Transfer Service
- Background Tasks Infrastructure Service
- Base Filtering Engine

Step 9. Click “Define this policy setting,” select “Automatic,” click “Apply,” and click “OK.”



Application Identity Properties

Security Policy Setting

Application Identity

☑ Define this policy setting

Select service startup mode:

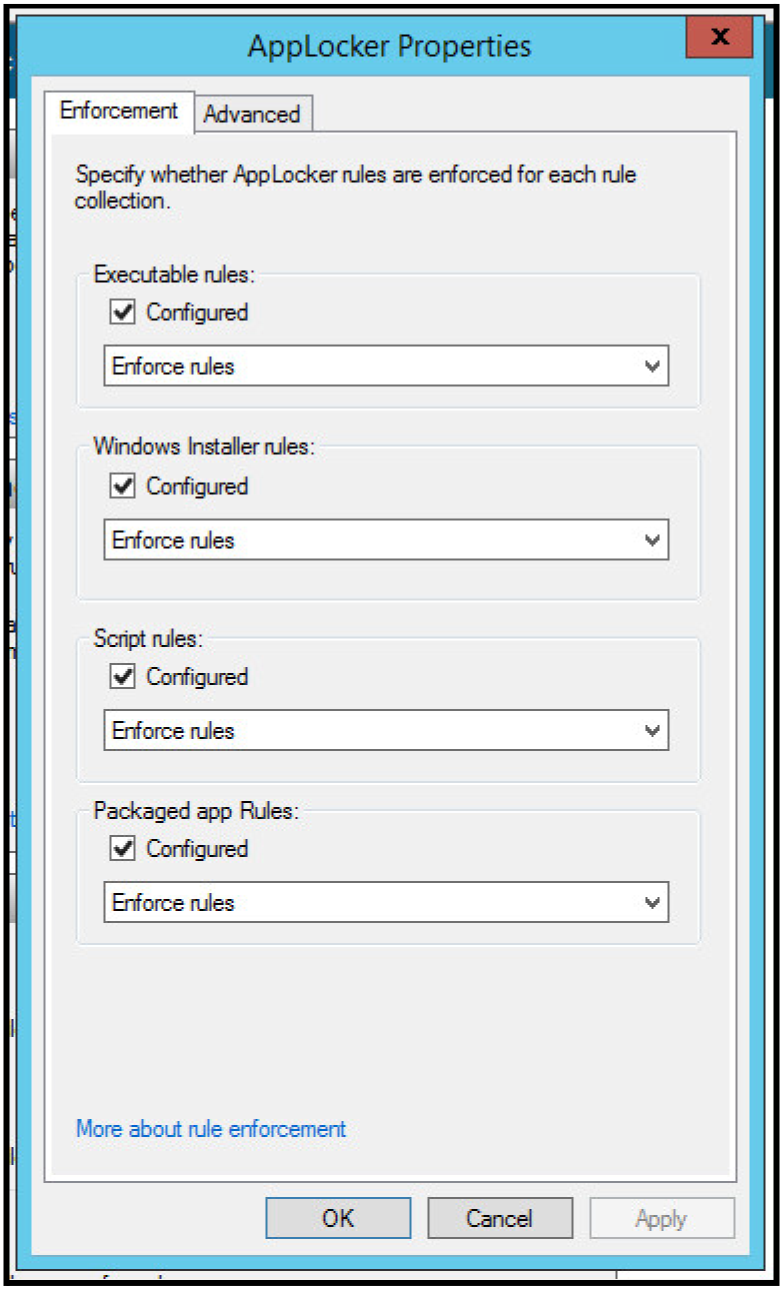
● Automatic

○ Manual

○ Disabled

How to Configure AppLocker

Step 10. With the same GPO still open, navigate to the following path: “Computer Configuration” > “Windows Settings” > “Security Settings” > “Application Control Policies” > “AppLocker.” Click “Configure rule enforcement.” After the “AppLocker Properties” window opens, click select “Configured” and “Enforce rules” for all four rule collections. Click “Apply” and click “OK.”



AppLocker Properties

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured
Enforce rules

Windows Installer rules:
☑ Configured
Enforce rules

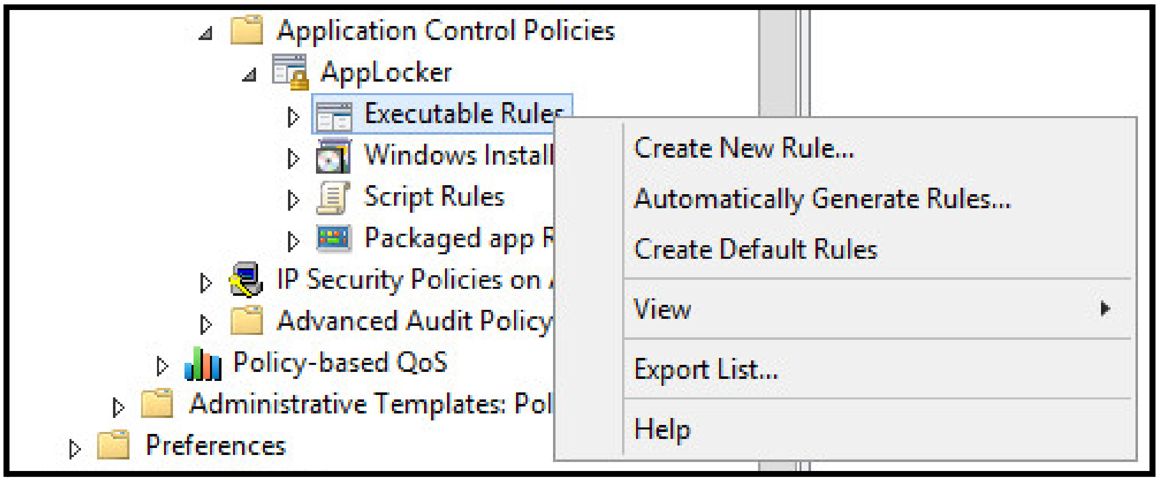
Script rules:
☑ Configured
Enforce rules

Packaged app Rules:
☑ Configured
Enforce rules

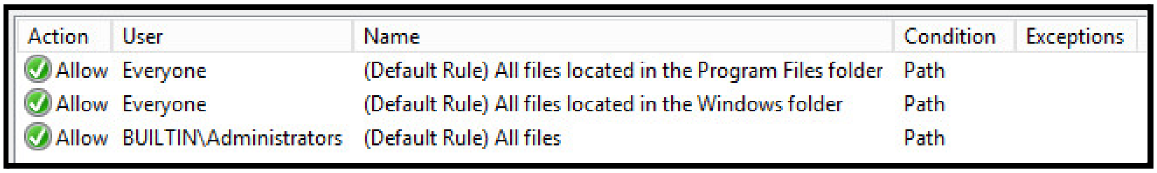
More about rule enforcement

How to Configure AppLocker

Step 11. With the same GPO still open, navigate to the following path: “Computer Configuration” > “Windows Settings” > “Security Settings” > “Application Control Policies” > “AppLocker.” Right-click “Executable Rules” and select “Create Default Rules…”

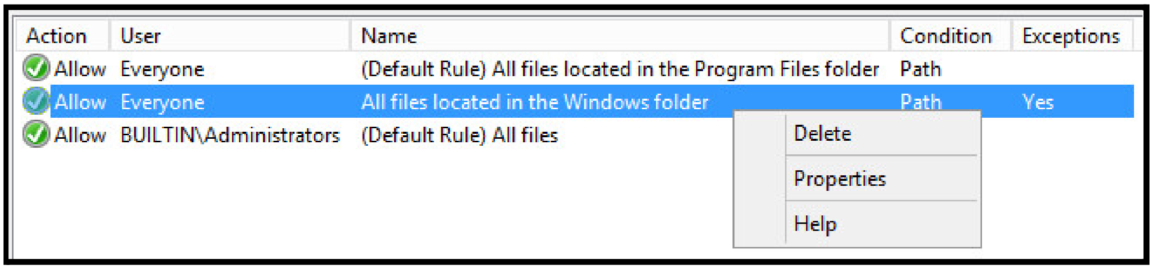


Once complete, your point of view should look like the screenshot below.



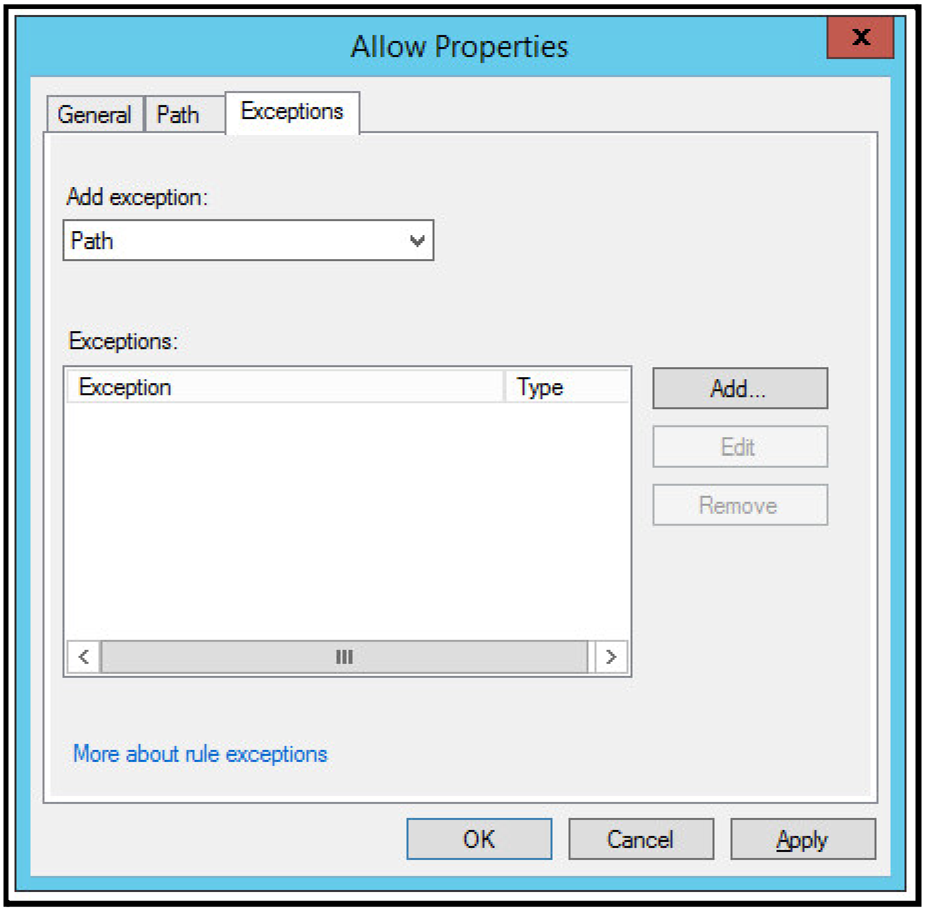
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

Step 12. Right-click the rule named “All files located in the Windows folder” and select “Properties.”



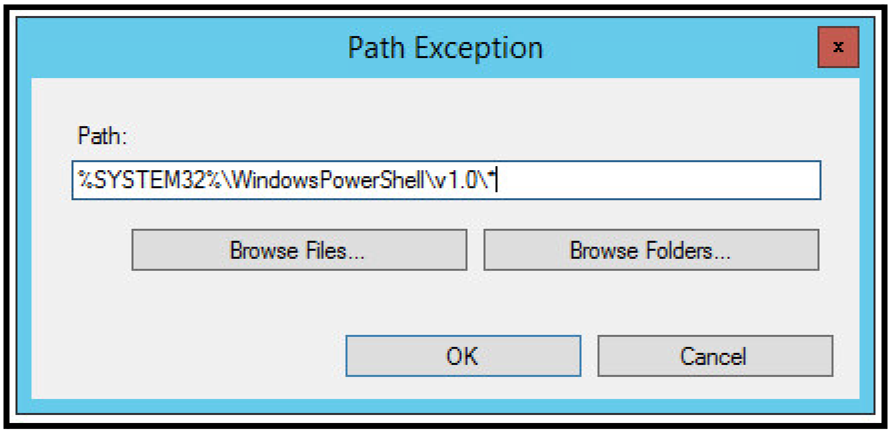
Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
Allow	Everyone	All files located in the Windows folder	Path	Yes
Allow	BUILTIN\Administrators	(Default Rule) All files		

Step 13. Click the “Exceptions” tab. Select “Path” in the “Add exception” drop-down menu.



Add exception: Path

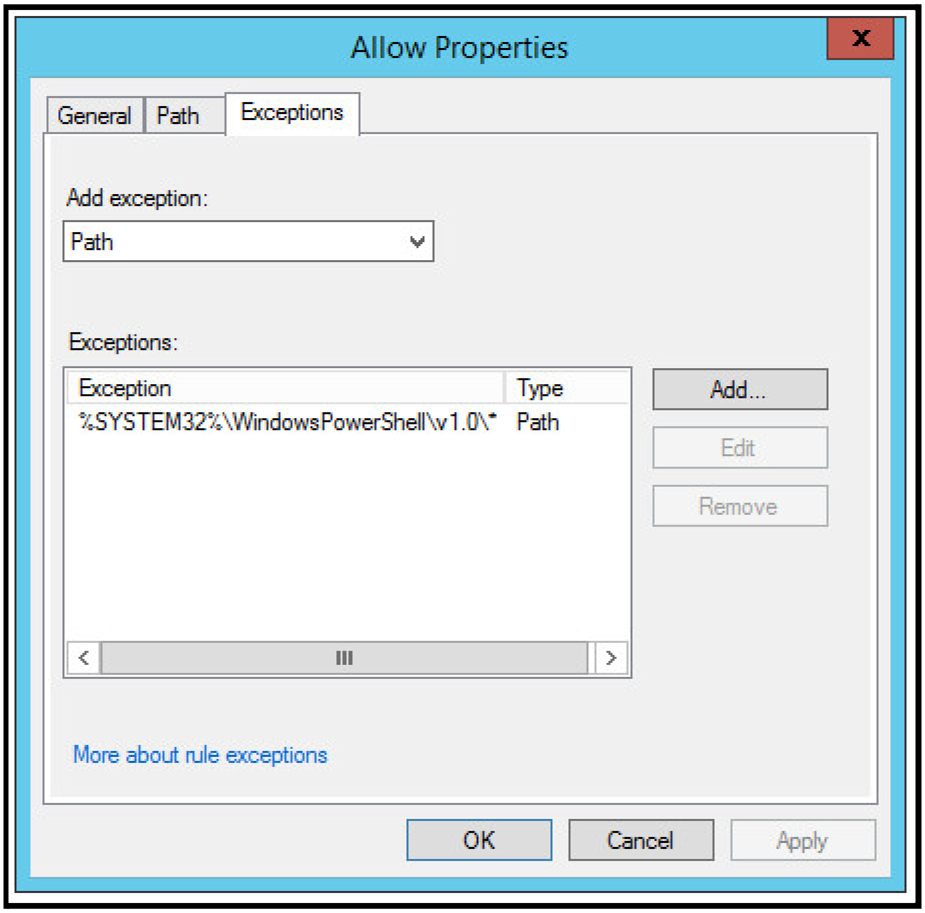
Step 14. Click “Add” and type “%SYSTEM32%\WindowsPowerShell\v1.0\*” in the “Path” field. Click “OK.”



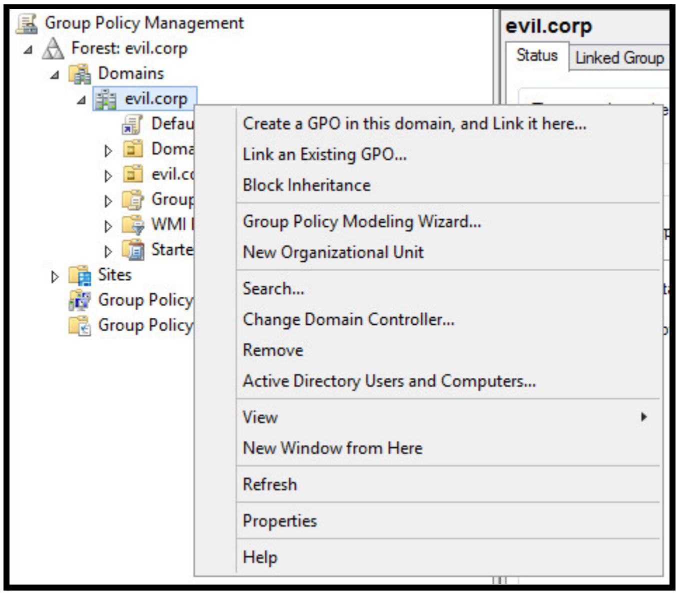
Path: %SYSTEM32%\WindowsPowerShell\v1.0\*

How to Configure AppLocker

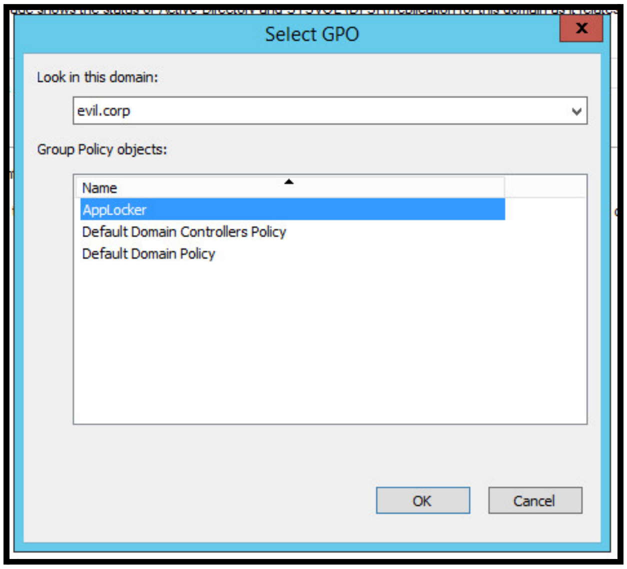
Step 15. Click “Apply,” click “OK,” and close the GPO.



Step 16. Right-click on your domain and select “Link an Existing GPO…”



Step 17. Select the GPO you created and click-on “OK.” Initiate a Group Policy update and reboot on all affected computers.



Look in this domain: evil.corp

Group Policy objects:

Name
AppLocker
Default Domain Controllers Policy
Default Domain Policy