## Enable Windows AppLocker via GPO

AppLocker requires the Application Identity service to be running. We will configure that service to start automatically.

- 1. Open Group Policy Management
  - a. Expand Domain and Right Click on Group Policy Objects
  - b. Select New
  - c. Name: Enable Windows AppLocker



- 2. Right Click the newly created GPO and select Edit
  - a. Expand Computer Configuration>Policies>Windows Settings>Security Settings>System Services
  - b. Right Click on Application Identity and select Properties
  - c. Check 'Define this policy setting' and set to 'Automatic' click on OK.

				Application Identity Properties	?	$\times$
				Security Policy Setting		
				Application Identity		
- 🛃 Computer Configuration 🔶 🔹 🔹	Service Name	Startup	Permission	□ Define this policy setting		
Policies	Active Directory Domain S	Not Defined	Not Defined	Select service startup mode:		
Software Settings	Active Directory Web Servi	Not Defined	Not Defined	Automatic		
Name Resolution Policy	ActiveX Installer (AxInstSV)	Not Defined	Not Defined	Manual		
Scripts (Startup/Shutdown)	AllJoyn Router Service	Not Defined	Not Defined			
> En Deployed Printers	App Readiness	Not Defined	Not Defined	Obsabled		
Security Settings	Application Identity	Not Defined	Not Defined	Edit Security		
> 🖹 Account Policies	Applicati Properties	fined	Not Defined			
> 🛃 Local Policies	Applicati	fined	Not Defined			
> 📅 Event Log	Applicati Help	fined	Not Defined			
> 🔀 Restricted Groups	AppX Deployment Service	Not Defined	Not Defined			
System Services	🙀 Auto Time Zone Updater	Not Defined	Not Defined	OK Cancel	Ар	ply

- 3. Next we will configure AppLocker
  - a. In the same GPO, Expand Computer Configuration>Policies>Windows Settings>Security Settings>Application Control Rules

b. Click on AppLocker then click 'Configure rule enforcement'



×

c. Check all of the boxes and click OK

AppLocker Properties

Enforcement Advanced	
Specify whether AppLocker rules are enforced for each collection.	rule
Executable rules:	
Enforce rules	$\sim$
Windows Installer rules:	
Enforce rules	~
Script rules: Configured	
Enforce rules	~
Packaged app Rules: ☑ Configured	
Enforce rules	~
More about rule enforcement	
OK Cancel	Apply

d. Expand AppLocker and Right Click on 'Executable Rules' Select 'Create Default Rules'



- e. You will see the 3 default rules created:
  - i. Allow Everyone All files located in the Program Files folder (Allows members of the Everyone group to run applications that are located in the Program Files folder.)
  - ii. Allow Everyone All files located in the Windows folder (Allows members of the Everyone group to run applications that are located in the Windows folder.)
  - iii. Allow Administrators All files (Allows members of the local Administrators group to run all applications.)
- f. Do the same 'Create Default Rules' for the following:
  - i. Windows Installer Rules
  - ii. Script Rules
  - iii. Packaged app Rules
    - Application Control Policies
       AppLocker
       Executable Rules
       Windows Installer Rules
       Script Rules
       Packaged app Rules

Create New Rule... Automatically Generate Rules...

Create Default Rules

4. Link the Enable Windows AppLocker GPO to your Workstations OU (I highly recommend testing this on a small amount of machines before deploying everywhere)

Select GPO

- a. In Group Policy Management, browse to your desired Workstations OU
- b. Right Click and select 'Link an Existing GPO'
- c. Select 'Enable Windows AppLocker' and click OK

Group Policy Management	Workstations Linked Group Policy Objects	Look in this domain: school.local ~ Group Policy objects:
<ul> <li>Domains</li> <li>school.local</li> <li>Default Domain Policy</li> <li>Domain Controllers</li> <li>Faculty</li> <li>Workstations</li> </ul>	Link Örder	Name Default Domain Controllers Policy Default Domain Policy Enable Windows AppLocker Enable Windows Firewall
<ul> <li>Enable Wi</li> <li>Group Policy</li> <li>Link a</li> <li>Default D</li> <li>Default D</li> <li>Enable Wi</li> <li>Group</li> </ul>	te a GPO in this domain, and l an Existing GPO. (Inheritance p Policy Update	OK Cancel

- 5. Troubleshooting Apps being blocked by AppLocker
  - a. Open Event Viewer (Either directly on the workstation having the issue, or connect to another computer from Event Viewer on your management PC/Server)

Event Viewer					
File Action View Help	Select (	Computer			×
Event Viewer (Local)     Custon     Open Saved Log.     Windo     Create Custom View     Applice     Import Custom View	vent Viewer (Local) Select v	t the computer you wan	t to view event logs on nputer this console is runn	ing on)	
Connect to Anothe	r Computer t: ()	Another computer:	WIN10		Browse
View Refresh	· · · · · · · · · · · · · · · · · · ·	Connect as another use	n <none></none>	S	et User
Help	,				Cancel

- b. Expand Applications and Services Logs>Microsoft>Windows>AppLocker
- c. Click on EXE and DLL and look for any errors

Event Viewer (WIN10.SCHOOLLOCAL)	EXE and DLL Nu	umber of events: 37 (!) New (	events available		
Custom Views	Level	Date	and Time	S	ource
Applications and Services Logs		5/29	/2024 3:25:53 PM	A	ppLocker
Hardware Events	Error	5/29	/2024 3:25:47 PM	A	ppLocker
Internet Explorer	(i) Information	5/29	/2024 3:25:47 PM	A	ppLocker
Key Management Service	(i) Information	5/29	/2024 3:25:46 PM	A	ppLocker
- Microsoft	Information	E /00	10004 2-0E-4E DNA	٨	nnl ockor
> 🧮 AppV	<				
> User Experience Virtualization	Event 8004, AppLo	cker			
~ 🛄 Windows		7			
> 🧮 AAD	General Details				
> 🧮 All-User-Install-Agent					
> 🧮 AllJoyn	%OSDRIVE%\U	SERS\JOHN.DOE\DESKTOP	\WINMTR.EXE was pre	vented from running.	
> 🦲 AppHost					
> 🦲 AppID					
> 🧮 ApplicabilityEngine					
> 🧮 Application Server-Applicati					
Application-Experience					
<ul> <li>AppLocker</li> </ul>					
EXE and DLL					
MSI and Script	Log Name:	Microsoft-Windows-A	pLocker/EXE and DLL		
Packaged app-Deploym	Source:	AppLocker	Logged:	5/29/2024 3:25:47 PM	
Packaged app-Execution	Event ID:	8004	Task Category:	None	

- d. Note the path and EXE that was being blocked. You can add this as an exception in the Enable Windows AppLocker GPO. *You can use \* in place of the username to apply to all users*
- 6. Unblocking Apps being blocked by AppLocker
  - a. Open Group Policy Management and edit your Enable Windows AppLocker GPO
  - b. Expand Computer Configuration>Policies>Windows Settings>Security Settings>Application Control Rules>AppLocker
  - c. Right Click on Executable Rules and select Create New Rule

<ul> <li>File System</li> <li>Wired Network (IEEE 802</li> </ul>	Create New Rule
<ul> <li>Windows Defender Firev</li> <li>Network List Manager P</li> <li>Wireless Network (IEEE 8</li> </ul>	Automatically Generate Rules Create Default Rules
<ul> <li>Public Key Policies</li> <li>Software Restriction Poli</li> </ul>	View
Application Control Polic	Export List
<ul> <li>AppLocker</li> <li>Executable Rules</li> </ul>	Help
🦯 🛐 Windows Installer R	ules
> 🧾 Script Rules	
Packaged app Rules	

- d. Click Next on the Before You Begin page
- e. On the permissions page, leave Action set to 'Allow'

- f. User or group, leave 'Everyone' if you want this rule to apply to everyone, or select your desired user or group. Click Next
- g. There are 3 Conditions you can select from to unblock: Publisher, Path, File hash.
  - i. Publisher: Select this option if the application you want to create the rule for is signed by the software publisher.
  - ii. Path: Create a rule for a specific file or folder path. If you select a folder, all files in the folder will be affected by the rule.
  - iii. File hash: Select this option if you want to create a rule for an application that is not signed.
- h. In this example I am going to choose 'File hash'. This will allow the file to run from any saved location.
  - i. Click Browse Files
  - ii. Browse to the path of the desired file and click Open
  - iii. Enter a name to identify this rule and click Create
- i. Confirm that application is now able to successfully open.