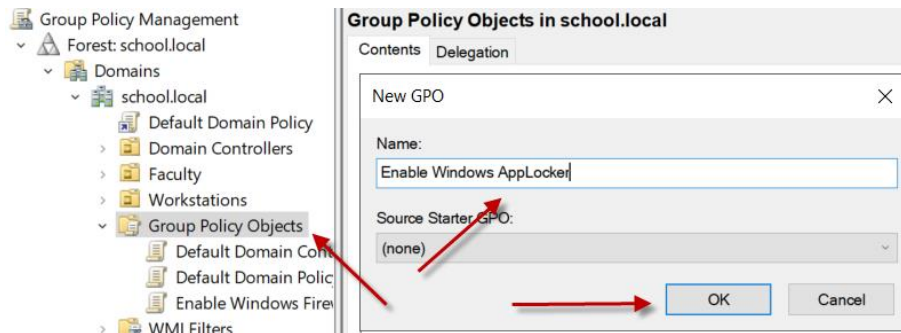


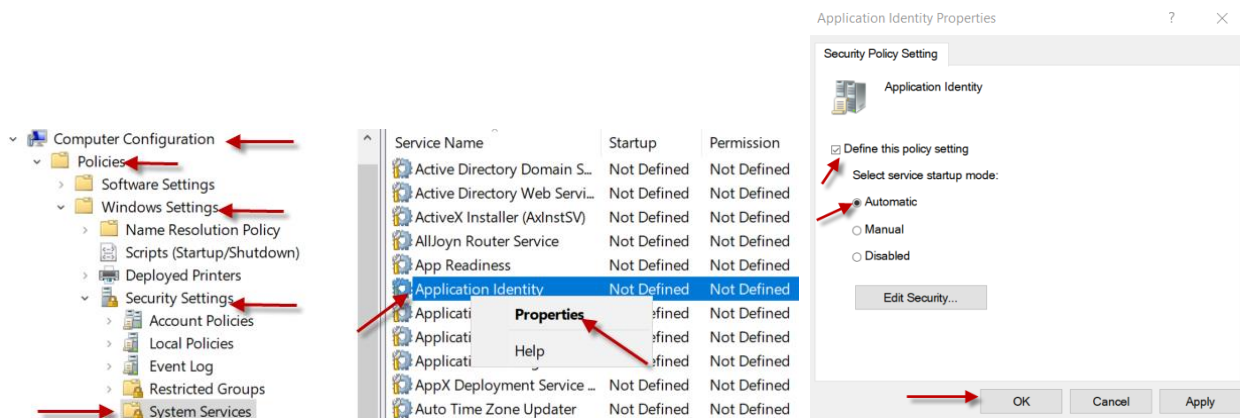
Enable Windows AppLocker via GPO

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

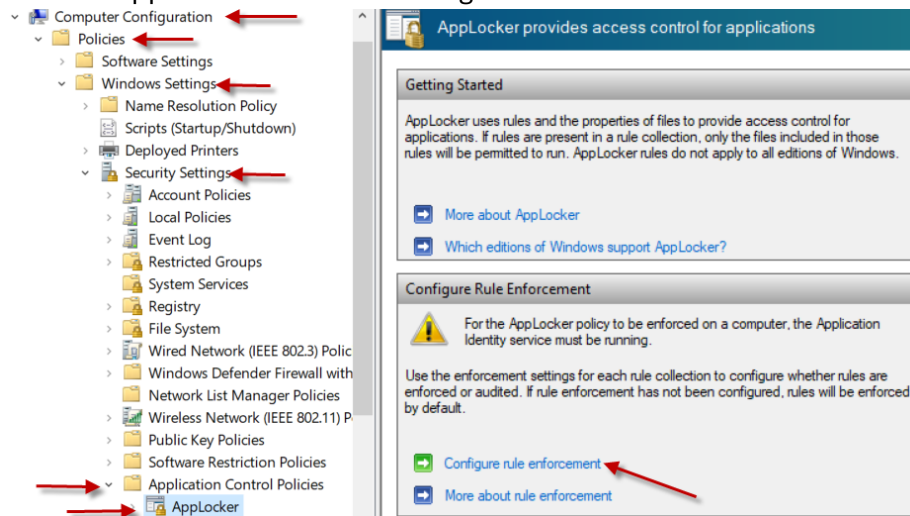


2. Right Click the newly created GPO and select Edit
 - a. Expand Computer Configuration>Policies>Windows Settings>Security Settings>System Services
 - b. Right Click on Application Identity and select Properties
 - c. Check 'Define this policy setting' and set to 'Automatic' click on OK.

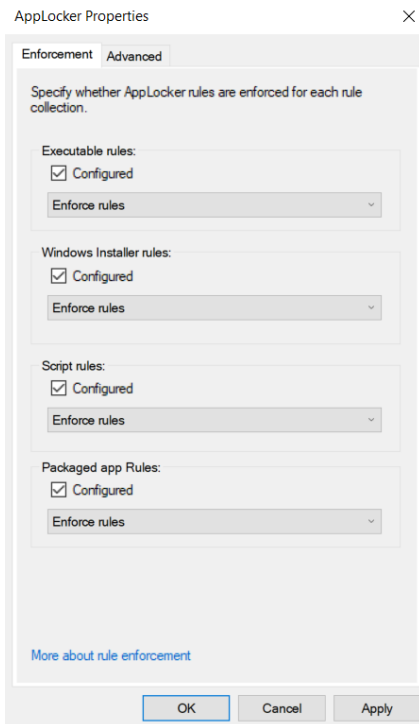


3. Next we will configure AppLocker
 - a. In the same GPO, Expand Computer Configuration>Policies>Windows Settings>Security Settings>Application Control Rules

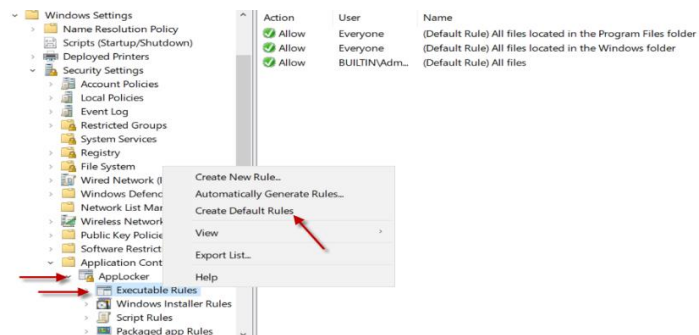
b. Click on AppLocker then click 'Configure rule enforcement'



c. Check all of the boxes and click OK



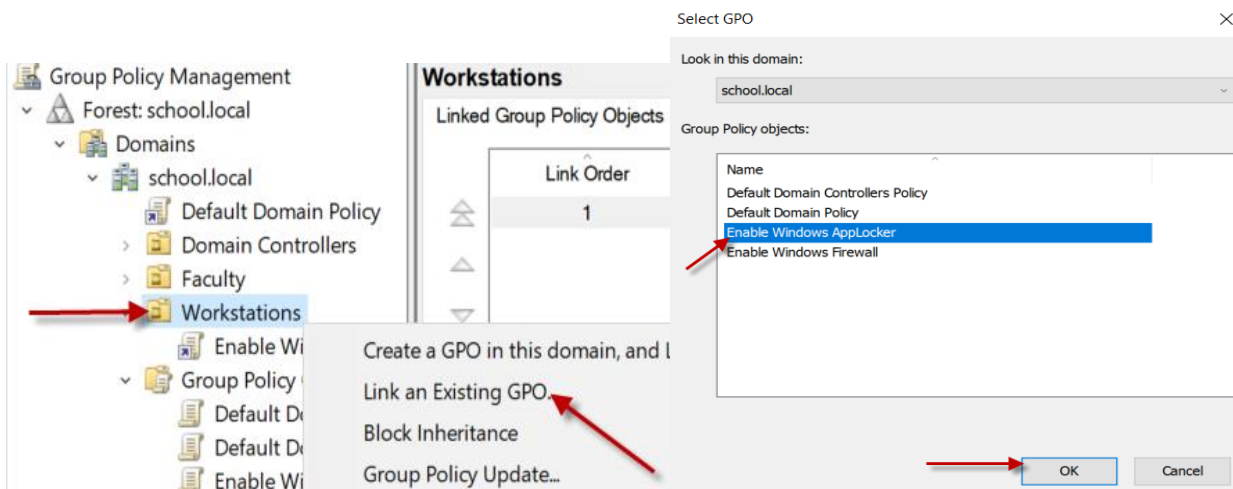
d. Expand AppLocker and Right Click on 'Executable Rules' Select 'Create Default Rules'



- 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

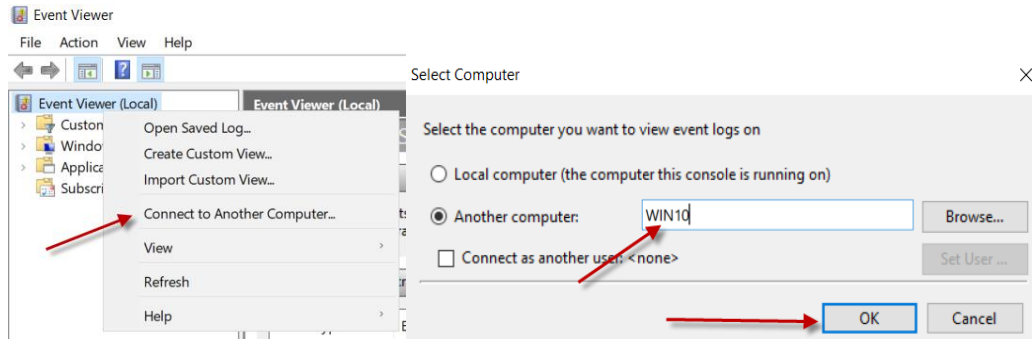


4. Link the Enable Windows AppLocker GPO to your Workstations OU (I highly recommend testing this on a small amount of machines before deploying everywhere)
 - a. In Group Policy Management, browse to your desired Workstations OU
 - b. Right Click and select 'Link an Existing GPO'
 - c. Select 'Enable Windows AppLocker' and click OK

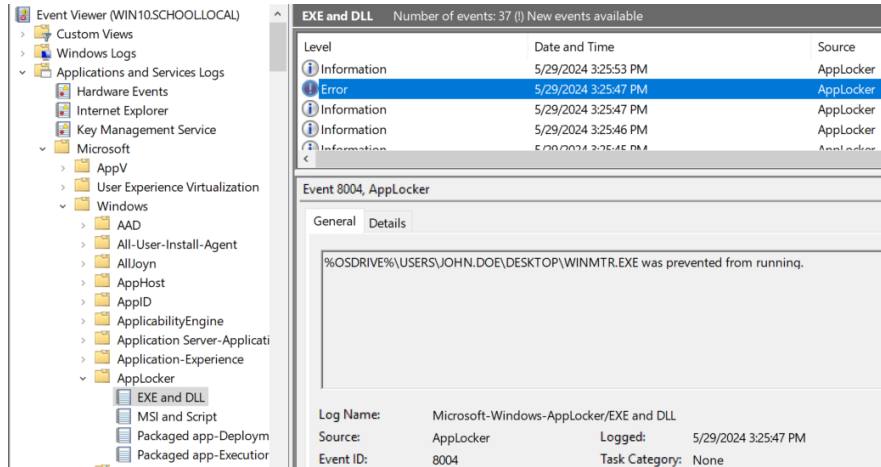


5. Troubleshooting Apps being blocked by AppLocker

- 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)



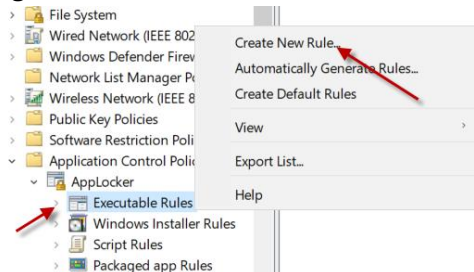
- b. Expand Applications and Services Logs>Microsoft>Windows>AppLocker
- c. Click on EXE and DLL and look for any errors



- 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



- 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.