

Lab 8.9.8 AppLocker Whitelisting on a Windows Domain Controller

From TestOut CompTIA Security+ Course

In this lab I will be whitelisting applications through AD Policy on a Windows Domain Controller. Once these whitelists are applied, they will be applied throughout all machines in the domain.]

The scenario for this lab is as follows:

“You are the IT security administrator for a small corporate network. You are increasing network security by implementing application whitelisting.

Your first step is to prevent applications not located in the operating system directory or the program files directory from running on your computers. In addition, the call center application used by the support team runs from C:\CallCenter\CallStart.exe and must be allowed to run. You also want any future versions of the call center application to run without changing any settings.

In this lab, your task is to configure AppLocker in the default domain policy as follows:

- **Create the default rules.**
 - Allow all files located in the Program Files folder.
 - Allow all files located in the Windows folder.
- **Configure a publisher rule that will allow future updates from the same vendor.**
- **Allow the Support group to run the call center software found in C:\CallCenter\CallStart.exe.”**

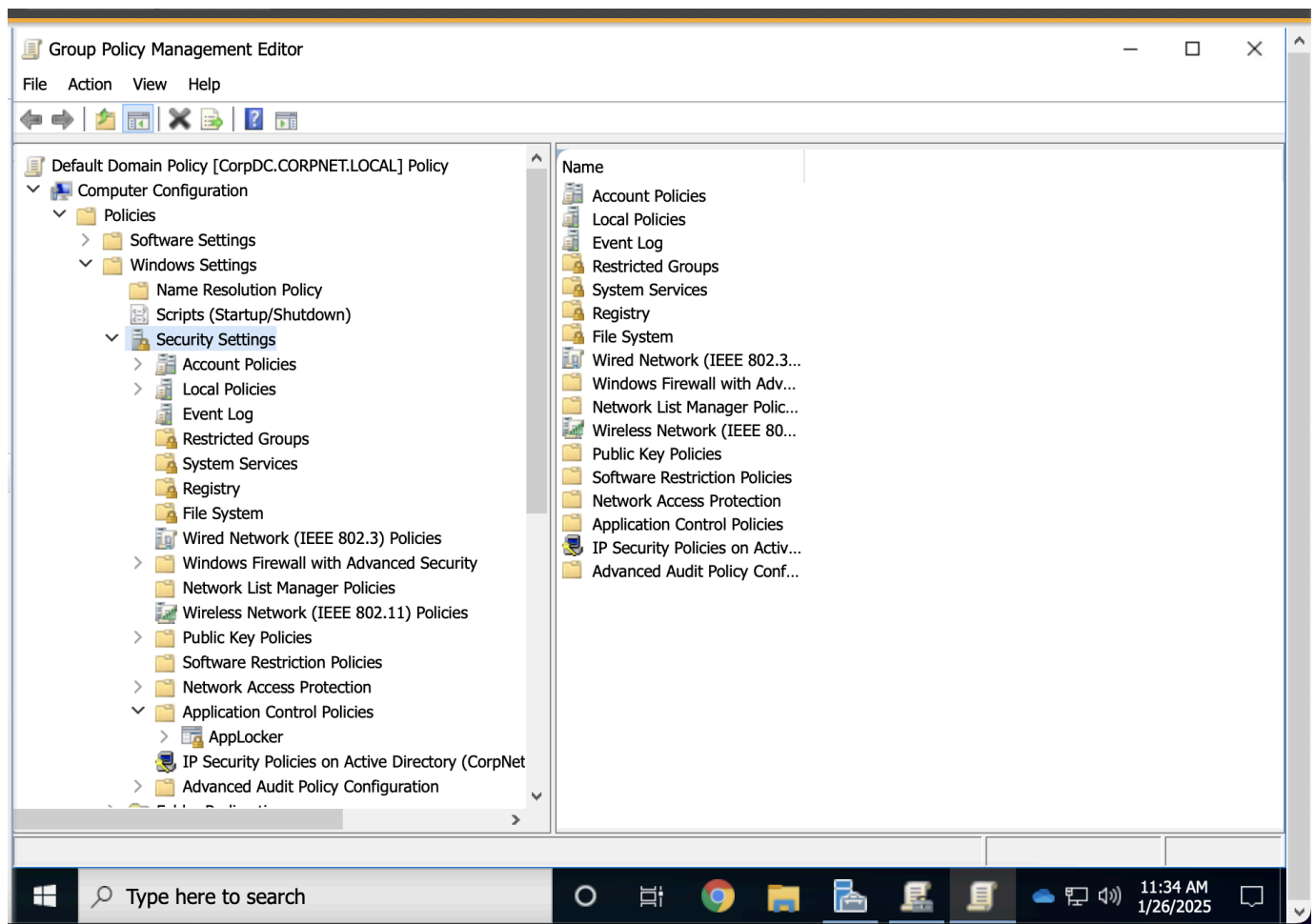
In order to implement AppLocker in the domain, I will need to login to the Domain Controller and open **Server Manager**.

Once I'm in **Server Manager**, I'll need to open **Group Policy Management**.

Then, I will expand **Forest > CorpNet.local > Domains > CorpNet.local > Default Domain Policy**. I will need to edit the **Default Domain Policy** by right clicking it and selecting **Edit**.

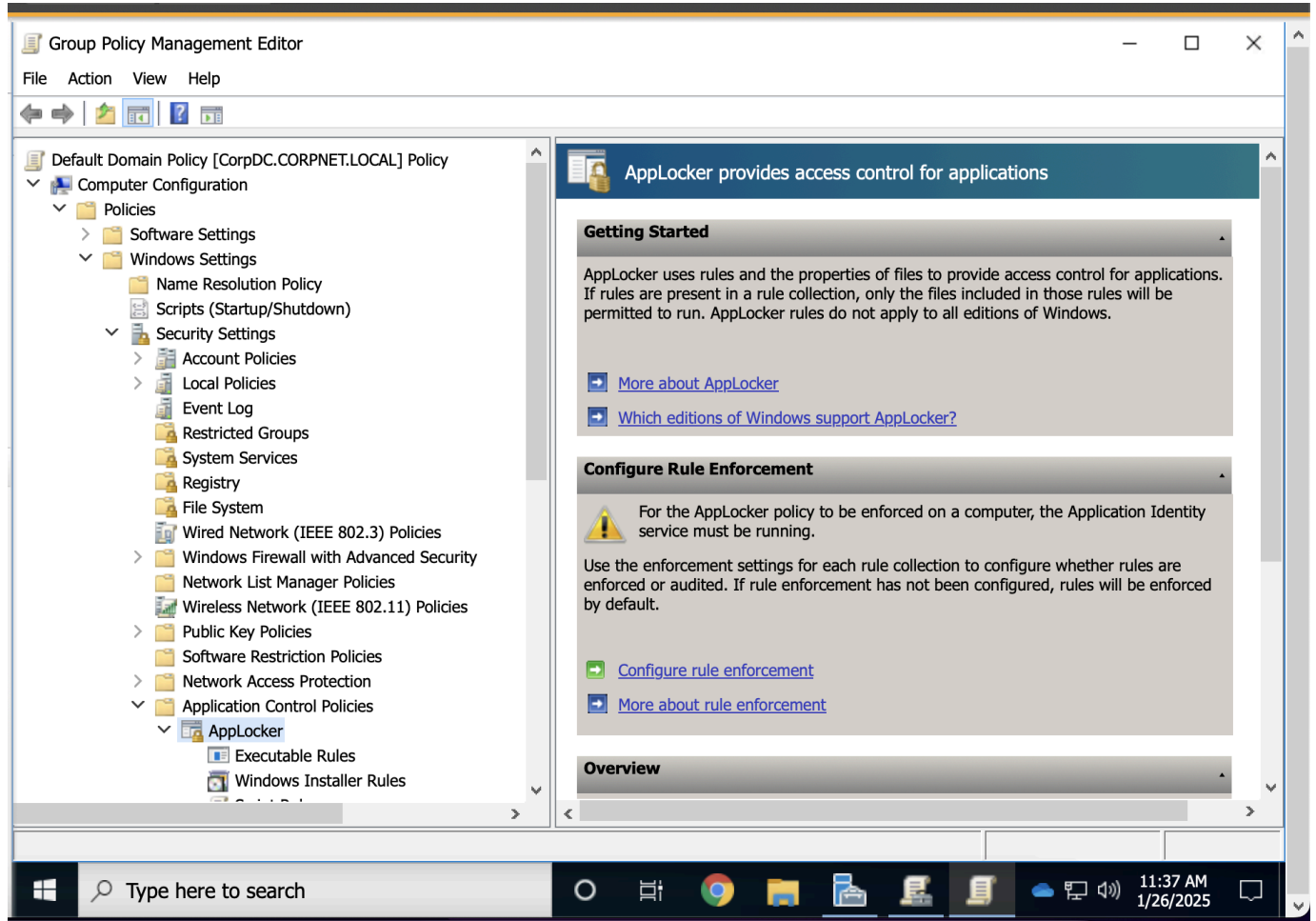
Robert Carpenter
github.com/robertmcarpenter
Sun January 26th 2025

Clicking that opens **Group Policy Management Editor**. In order to implement AppLocker I will need to configure it under **Computer Management**. This is because we want ALL machines in this domain to respect the AppLocker policy I am about to implement - no matter what user they are.

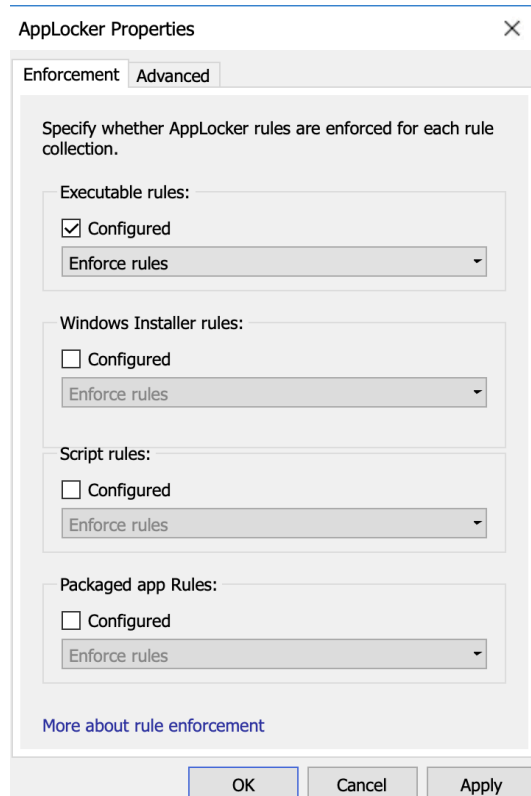


Inside **GPME** , I will navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Application Control Policies** .

To configure the rule I will click **Configure Rule Enforcement**.



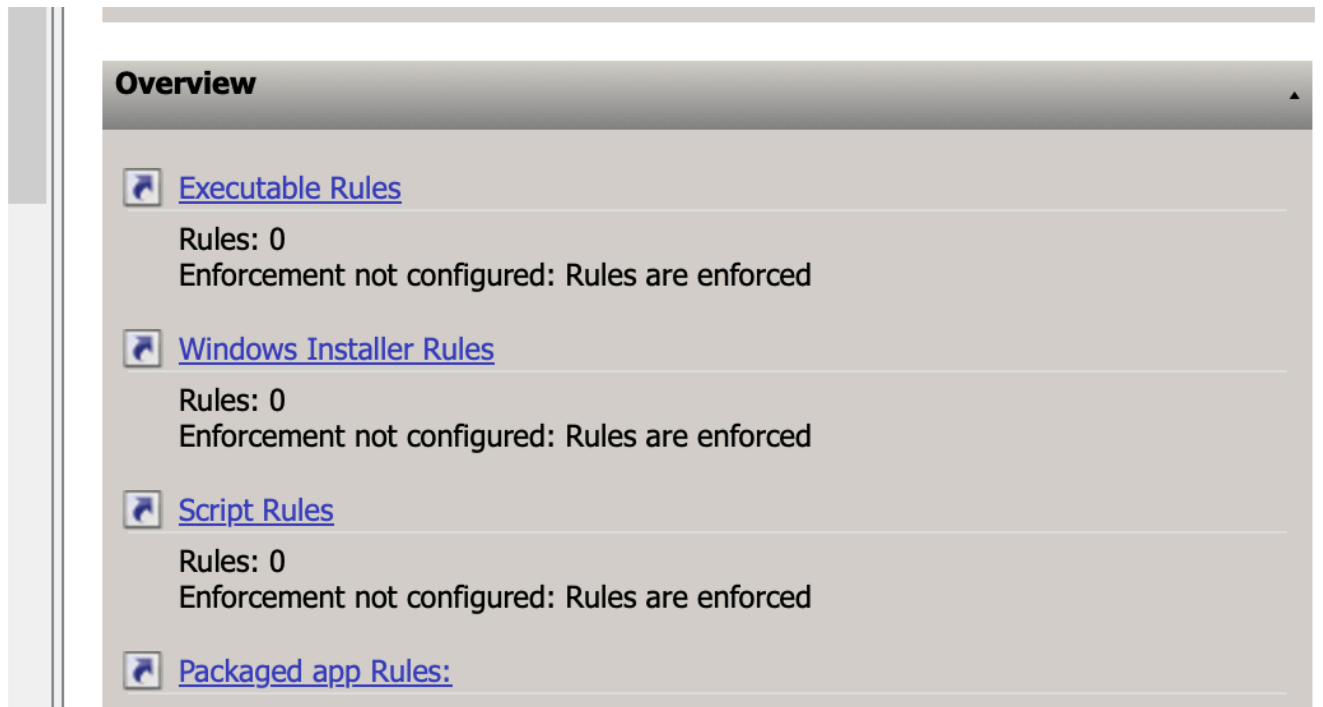
Once the Window opens I will click the checkbox under **Executable Rules**.



This is because the Lab wants me to allow a specific in-house application located under C:\CallCenter\CallStart.exe. I will also need to generate the default rules for AppLocker to allow system processes to run.

I must also restrict the **CallStart.exe** executable to only allow the **Support** group of this Domain to run it. No other users outside the **Support group** should be allowed to run it and if they do, they will be blocked by AppLocker. To quickly recap, my tasks are:

- **Create the default rules.**
 - **Allow all files located in the Program Files folder.**
 - **Allow all files located in the Windows folder.**
- **Configure a publisher rule that will allow future updates from the same vendor.**
- **Allow the Support group to run the call center software found in C:\CallCenter\CallStart.exe.**




After clicking Enforce rules, I'll navigate back to the previous window and select **Executable Rules** (shown above).

This opens up a wizard to set up the rule.

Sun January 26th 2025

Create Executable Rules ✕

 **Before You Begin**

Before You Begin

Permissions

Conditions

Publisher

Exceptions

Name

This wizard helps you create an AppLocker rule. A rule is based on file attributes, such as the file path or the software publisher contained in the file's digital signature.

Before continuing, confirm that the following steps are complete:

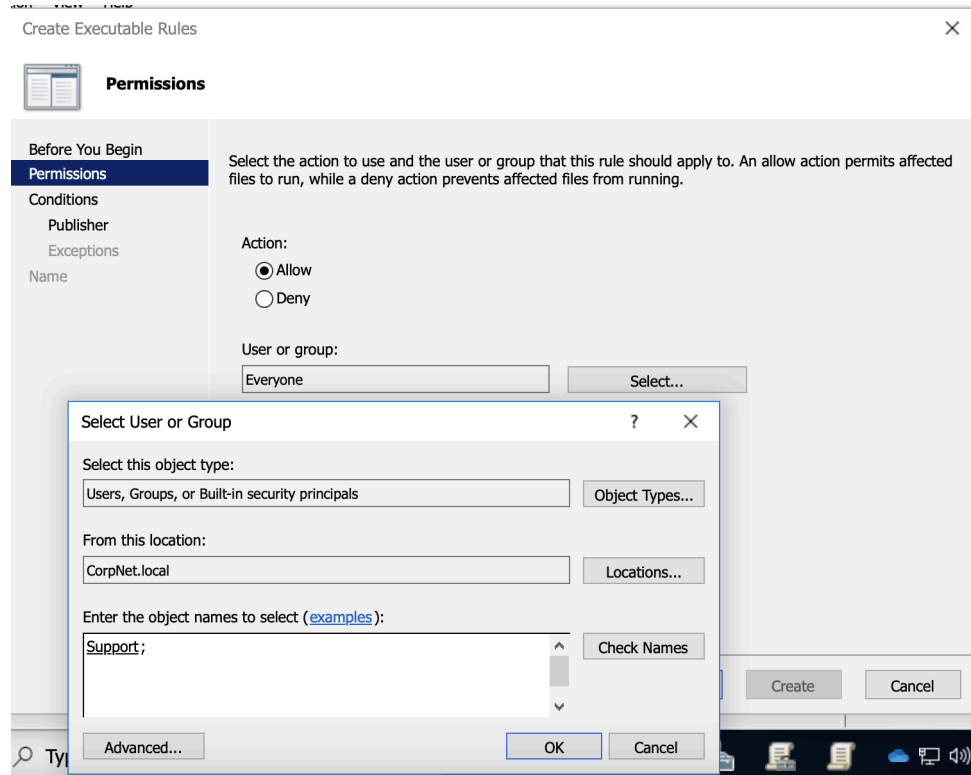
- Install the applications you want to create the rules for on this computer.
- Back up your existing rules.
- Review the AppLocker documentation.

To continue, click Next.

☐ Skip this page by default

Clicking **Next** brings up the **Permissions** window. Here, I can enter the **Support** group and select **Allow**.

Robert Carpenter
github.com/robertmcarpenter
Sun January 26th 2025

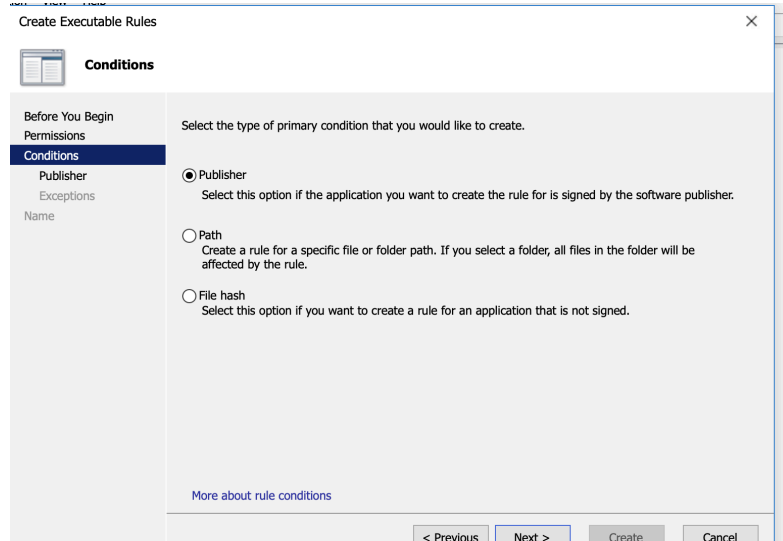


Clicking **next** after entering the group , brings me to the next page which is asking how I would like to configure the .exe in question. I can go by a specific software **Publisher, File Path, or File Hash**. IN this case, the lab asks me to restrict based on the software **publisher**. I will select that and hit next.

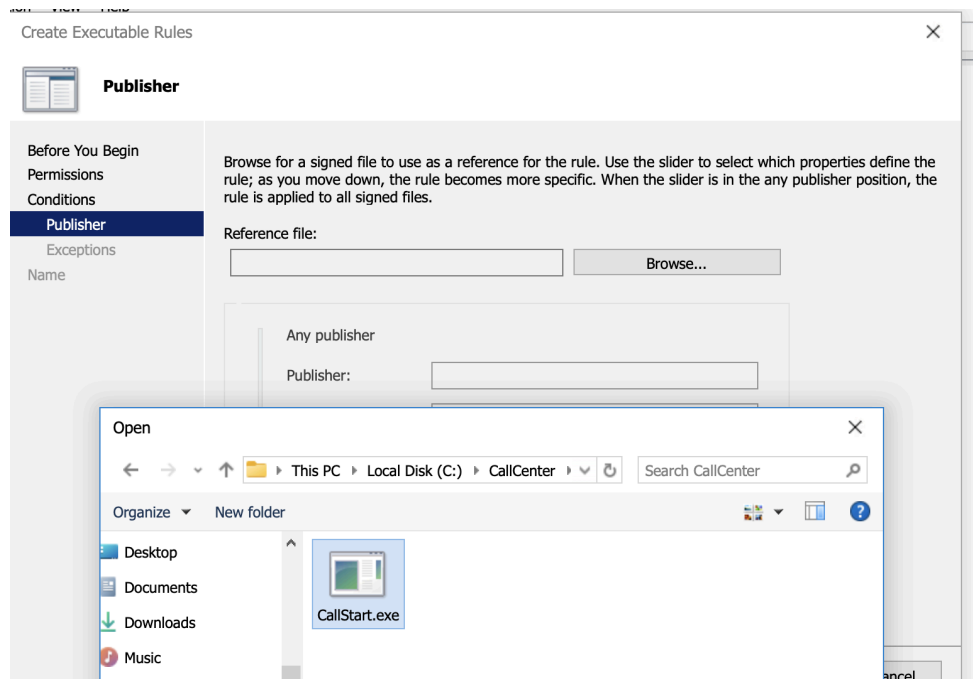
Robert Carpenter

github.com/robertmcarpenter

Sun January 26th 2025

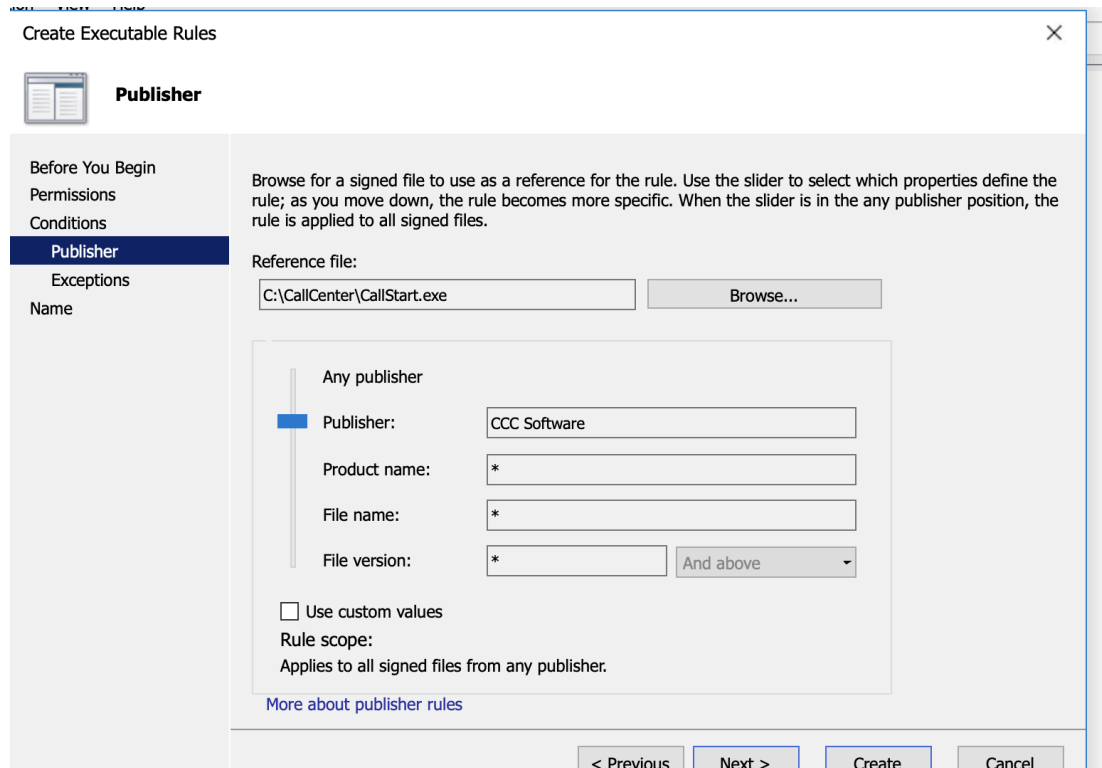


The next window then asks me to give a reference file for it to set a baseline. I will navigate to **C:\CallCenter\CallStart.exe**.



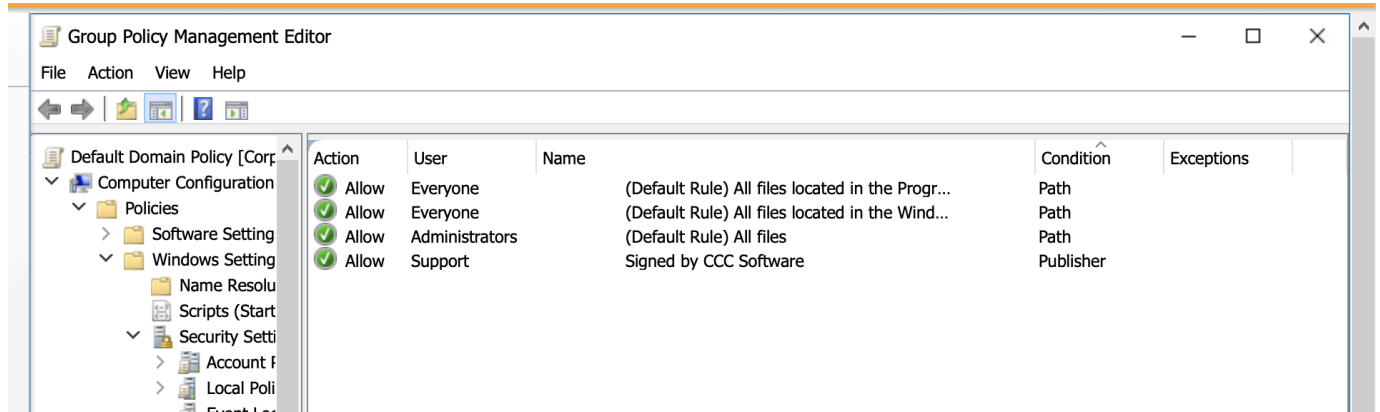
Then I will drag the slider up to **Publisher**. When I do that, I notice that the fields below it turn into the character ' * '. This is a wildcard and tells the system to allow

whatever is in that field. We are only worried if the software publisher is CCC Software.



After going through this Window I will click **Create** and accept the default name. A dialog box appears asking if I would like to create the default rules. I will click Yes and then review the rules just created in the right manu pane.

Robert Carpenter
github.com/robertmcarpenter
Sun January 26th 2025



As you can see the default rules were added which allow all files within the core Windows folders to run. We need this in order for everyday system .exes to run that are necessary for Windows.

Below the default rules I see the **Publisher** rule I created for the **Support** group.

This means my AppLocker policy is being applied.

This now concludes this lab!

Robert Carpenter
github.com/robertmcarpenter
Sun January 26th 2025

The screenshot shows a web browser window displaying a TestOut lab report. The browser's address bar shows the URL `labsimapp.testout.com/v6_0_659/simwindow.html?c2ltRGVmVXJl`. The page has a dark theme with a 'TestOut' logo in the top left. The main content area is titled 'Lab Report' and shows a score of '3/3 (100%)' with a full orange progress bar. The 'Time Spent' is '2:32:16'. Below the score is a 'TASK SUMMARY' section with 'Required Actions' listed as three items, each with a green checkmark: 'Create the default rules' (with a 'Show Details' link), 'Allow the Support group to run the call center software', and 'Configure a publisher rule to allow for future updates from the same vendor'. The background of the browser window shows a 'Group Policy Management Editor' interface with a 'Scenario' panel on the left containing instructions about AppLocker whitelisting. The Windows taskbar at the bottom shows the search bar and system clock indicating 1:44 PM on 1/26/2025.

Learning Platform | CompTIA

Building A Floor 1 CorpDC

Check Answers

Scenario

You are the IT security administrator for a small corporate network. You are increasing network security by implementing application whitelisting.

Your first step is to prevent applications not located in the operating system directory or the program files directory from running on your computers. In addition, the call center application used by the support team runs from C:\CallCenter\CallStart.exe and must be allowed to run. You also want any future versions of the call center application to run without changing any settings.

In this lab, your task is to configure AppLocker in the default domain policy as follows:

- Create the default rules.
 - Allow all files located in the Program Files folder.
 - Allow all files located in the Windows folder.
- Configure a publisher rule that will allow future updates from the same vendor.
- Allow the Support group to run the call center software found in C:\CallCenter\CallStart.exe.

Group Policy Management Editor

File Action View Help

Lab Report

Time Spent: 2:32:16

Score: 3/3 (100%)

TASK SUMMARY

Required Actions

- ✓ Create the default rules [Show Details](#)
- ✓ Allow the Support group to run the call center software
- ✓ Configure a publisher rule to allow for future updates from the same vendor

Condition Exceptions

Path

Path

Path

Publisher

Type here to search

1:44 PM 1/26/2025