Software Restriction for Zero Client Users (AppLocker Group Policy)

Software Restriction for Zero Client Users by Using AppLocker Group Policy

AppLocker Group policy Description:

AppLocker Group Policy for Windows system Applications can be used for restricting User or User Groups from running and installing programs.

Typically, only administrators have the permission to install programs. But green software and other software package do not necessarily need administrators' permission to be installed. So using AppLocker Group policy can directly limit the User from accessing and installing all programs.

AppLocker Group policy Configuration:

Tips:

- AppLocker Group Policy needs to be used in conjunction with User Account Control (**UAC**). Please refer to *User Account Control Guide* to turn on **UAC.**
- Before setting up AppLocker, please standardize the program installation path, be sure to install the required programs in **C: \ Program Files** or **C: \ Program Files (x86)** path. As **Program Files folder** is a kind of system file, which requires the administrator permission to make changes.
- Recommended operating systems: **Windows 7 (Ultimate, Enterprise**), **Windows 8.1 Enterprise**, **Windows 10 Enterprise**, **Server 2008R2 Standard**, **Datacenter, Server 2012R2 (Standard, Datacenter), Server 2016 (Standard, Datacenter).**

Environment of This Guide

- **System:**

Windows 7 x64 Ultimate;

- **Disk partitions:**

C disk - system & software partition
D disk- public partition
E disk – private partition

The following guide applies to the above mentioned environment, configuration steps may vary depending on your actual application environment.

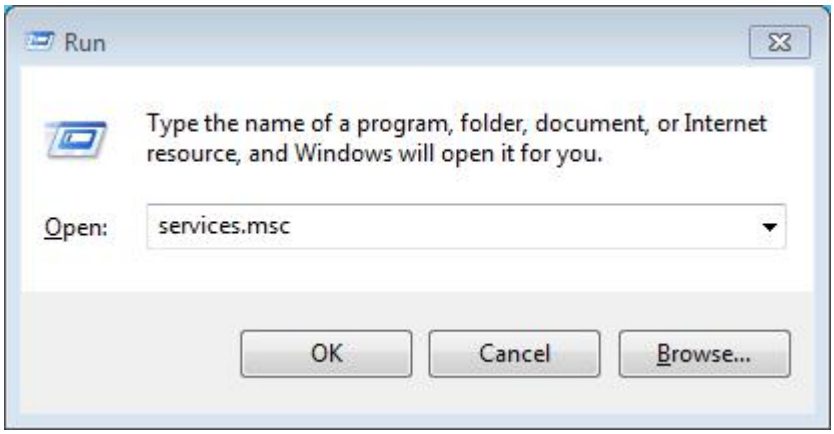
Content

AppLocker Quick Configuration Steps

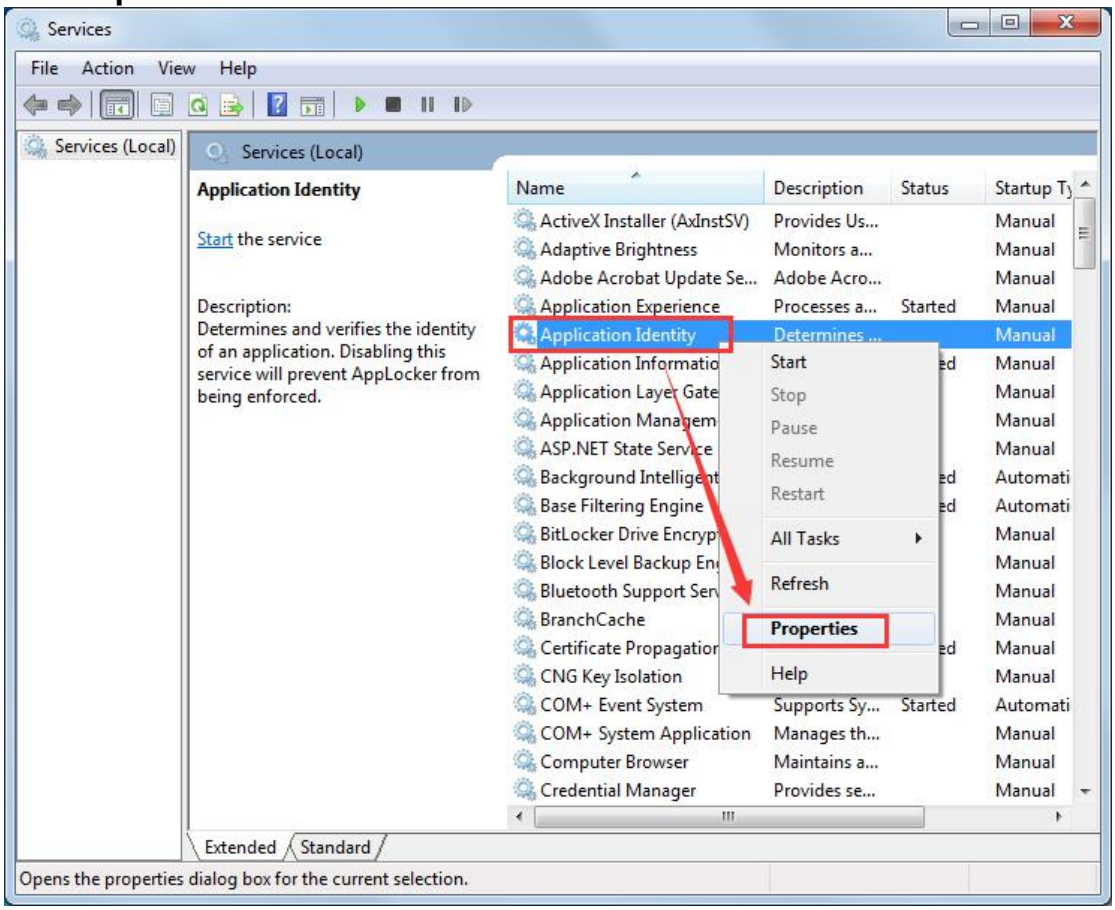
1) Enter **Service**, set the **Application Identity** startup type to **automatic**
2) Enter the **local Group Policy Editor →AppLocker**
3) **Executable rules→ Windows installer rules→ and script specifications create default rules**
4) **AppLocker** open **Configuration rules**
5) Restart the host, Then the AppLocker settings will take effect.

AppLocker Detailed Configuration Steps

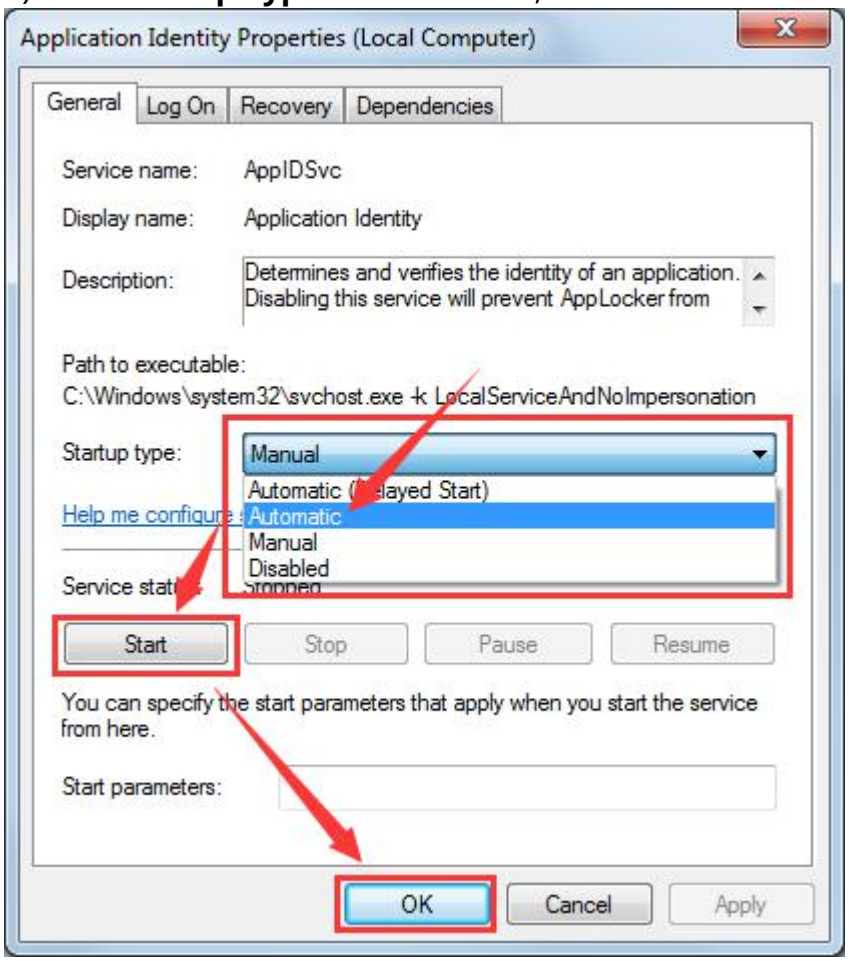
1) Logon to the host system with the administrator account, run **services.msc**



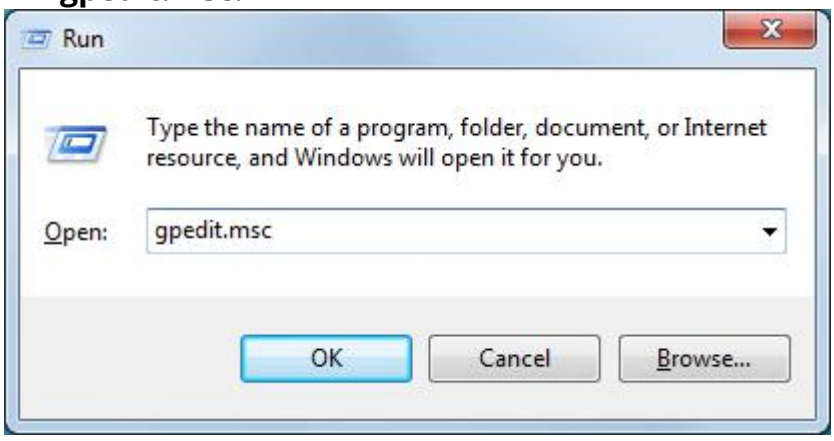
2) Enter **services**, right-click on **Application Identity** and select **Properties.**



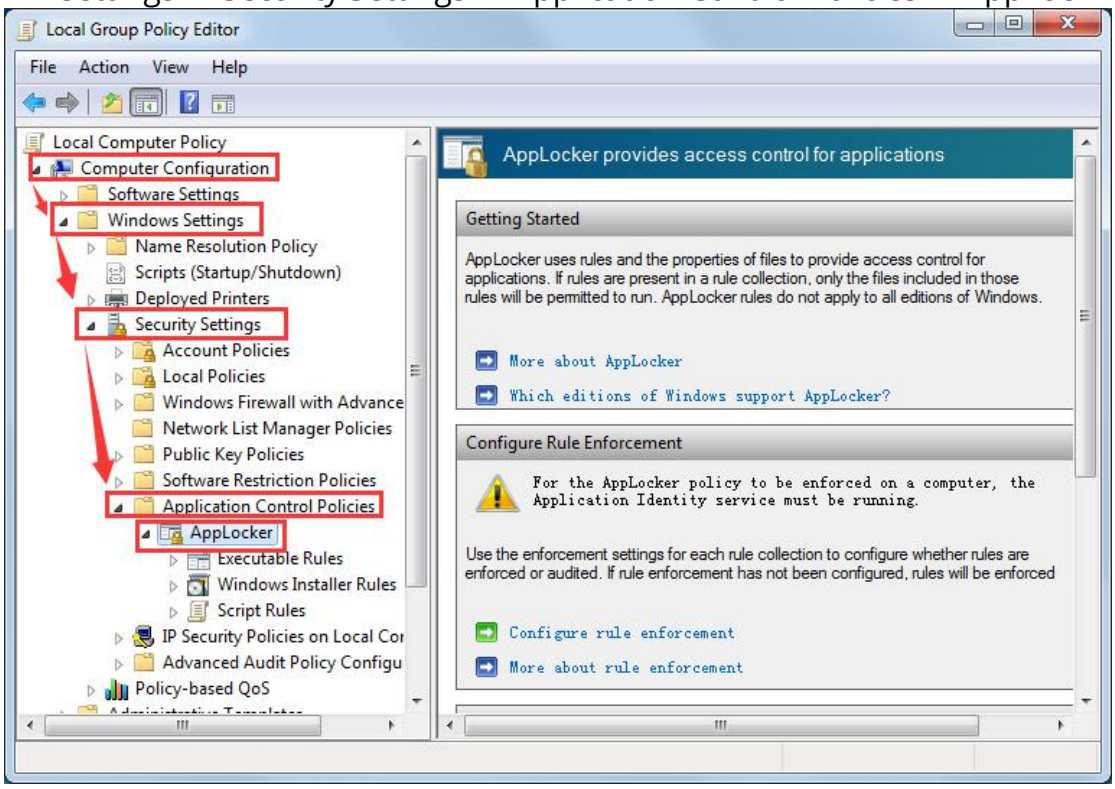
3) Set **Startup Type** to **Automatic**, and **start** the service then click **OK.**



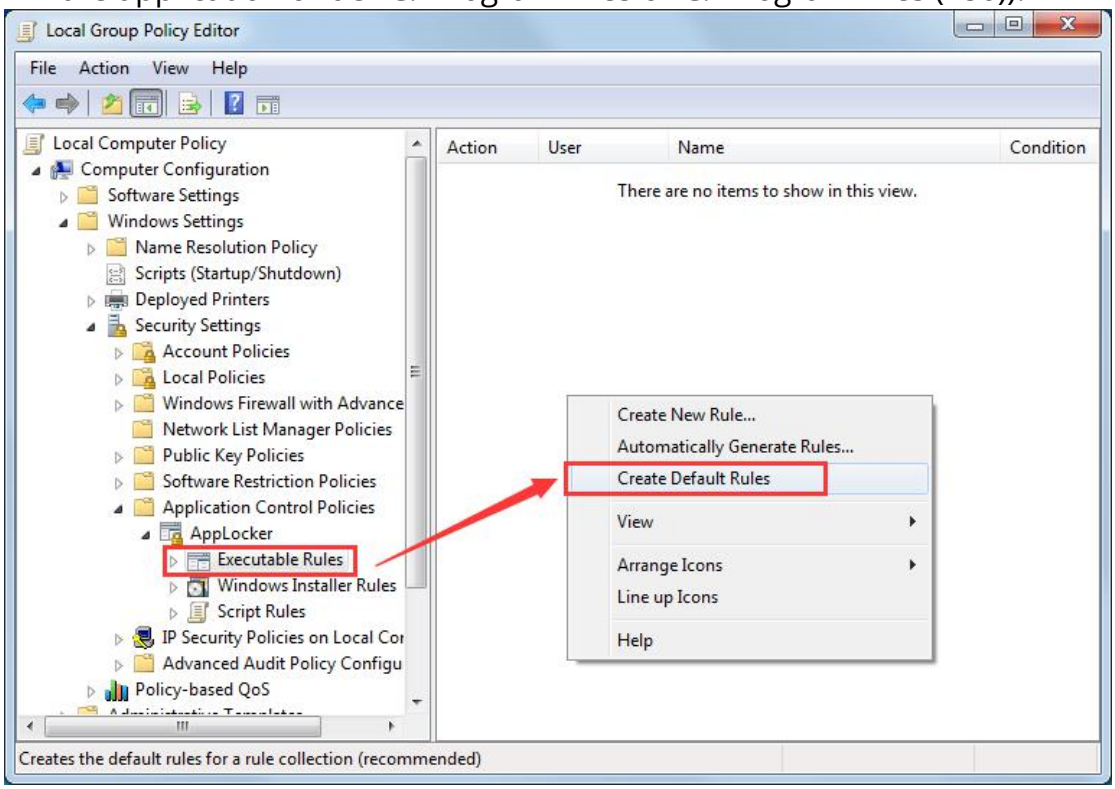
4) Logon to the host system with the administrator account, run **gpedit.msc.**



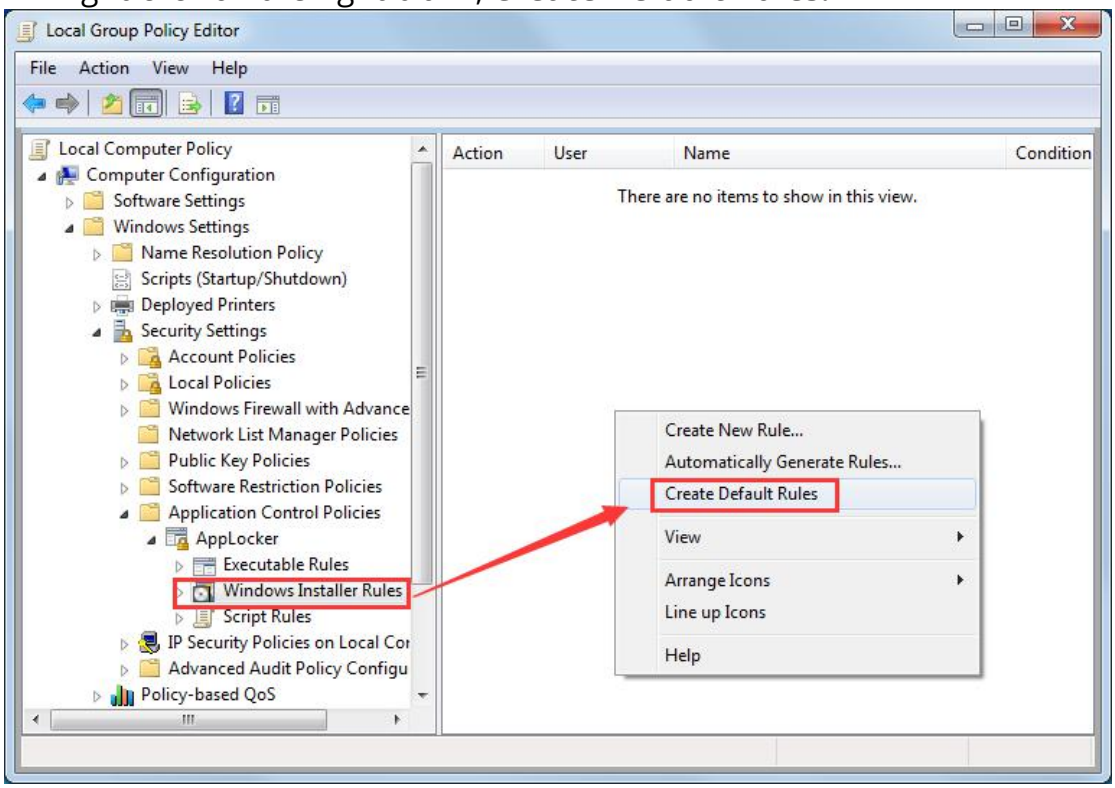
5) On **Local Group Policy Editor** open **AppLocker** through the path of Local Computer Policy -> Computer Configurations -> Windows settings -> Security Settings -> Application Control Policies -> AppLock



6) On **Local Group Policy Editor**, select the **Executable Rules**, right-click the right blank, **Create Default Rules** (default rule: user can only run the application under C:\Program Files or C:\Program Files (x86)).

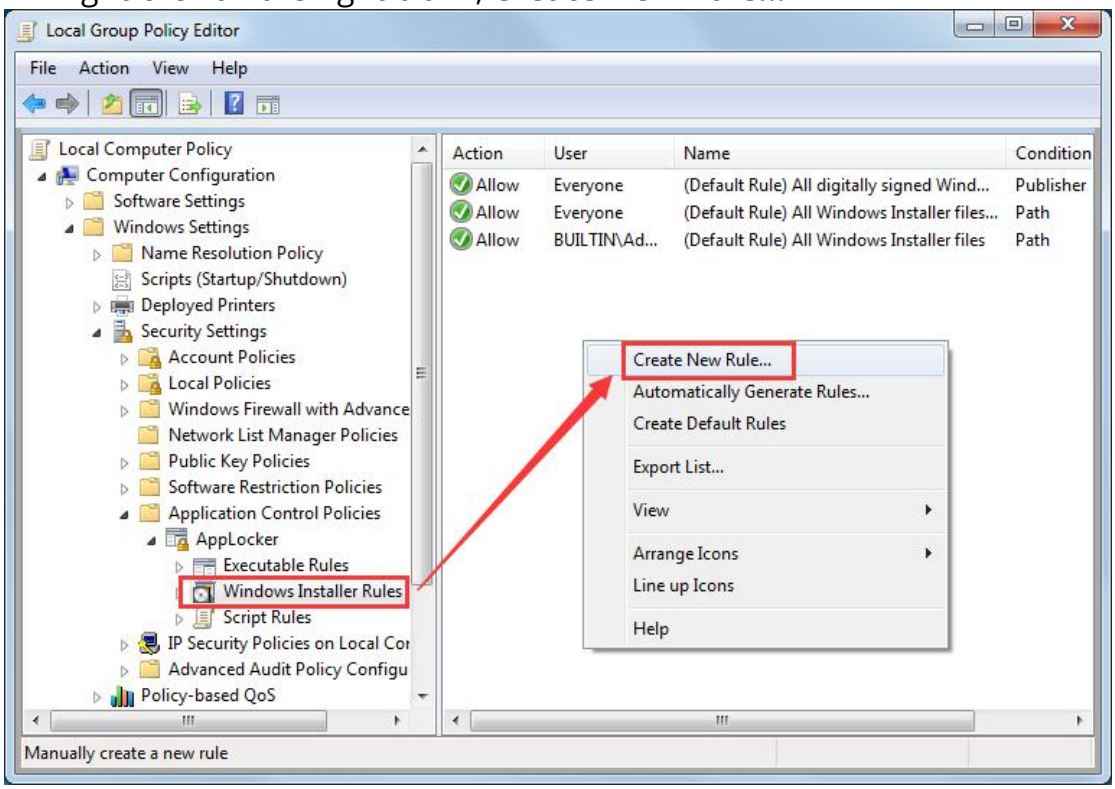


7) On **Local Group Policy Editor**, select the **Windows Installer Rules**, right-click on the right blank, **Create Default Rules.**

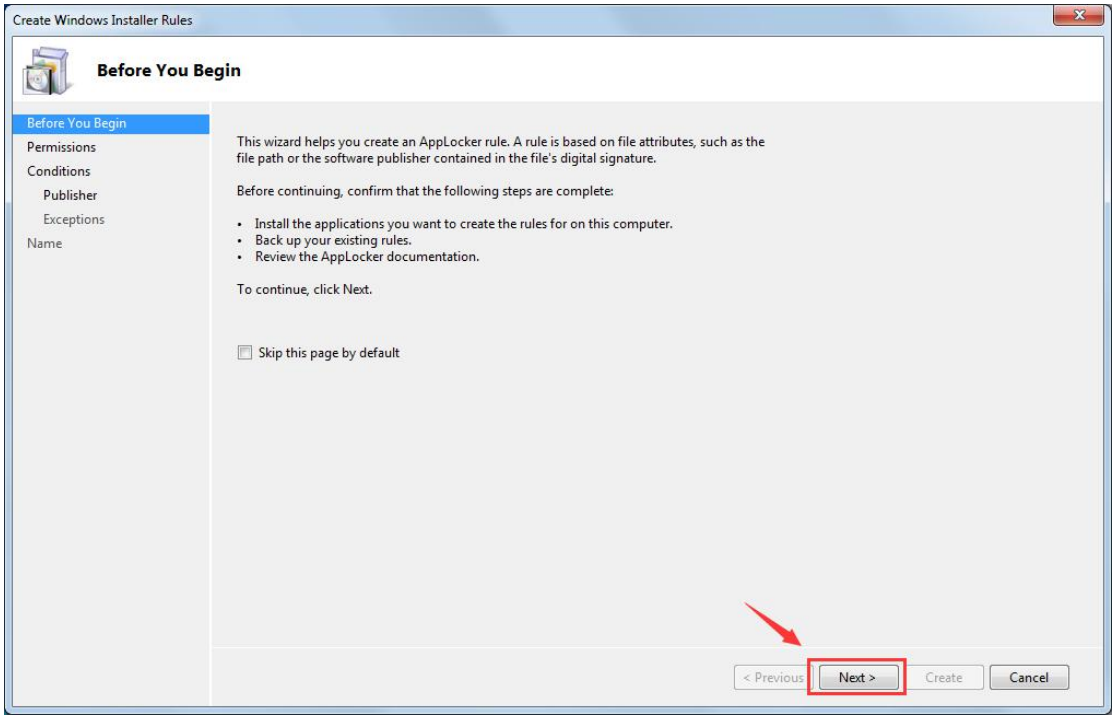


Note: If you want to prevent users from installing programs more effectively, please follow steps 8-20 and manually set all disk installation restriction.

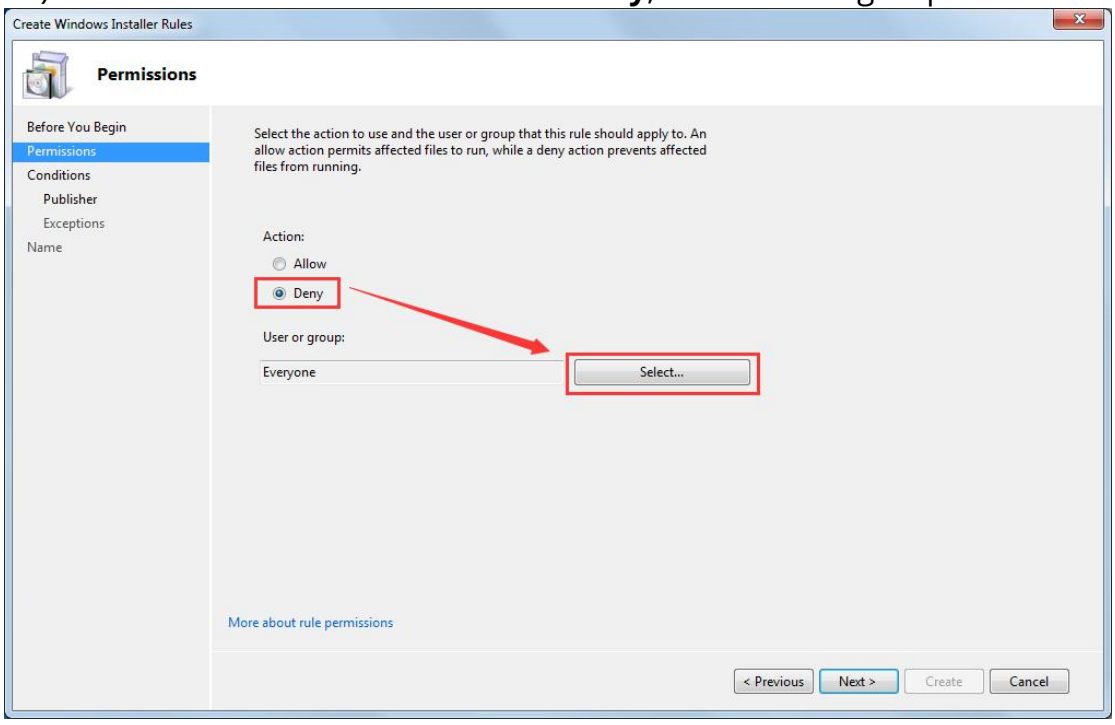
8) On **Local Group Policy Editor** Select **Windows Installer Rules**, right-click on the right blank, **Create New Rule...**



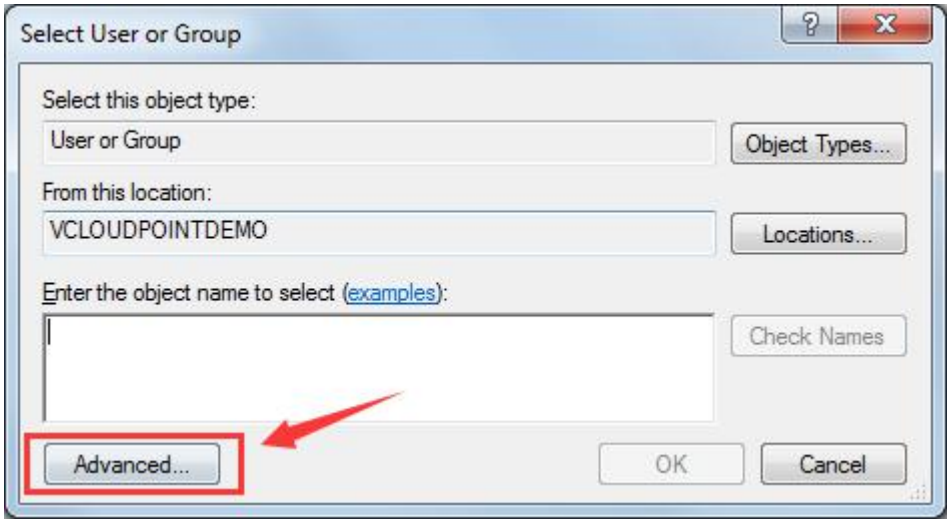
9) **Next>**



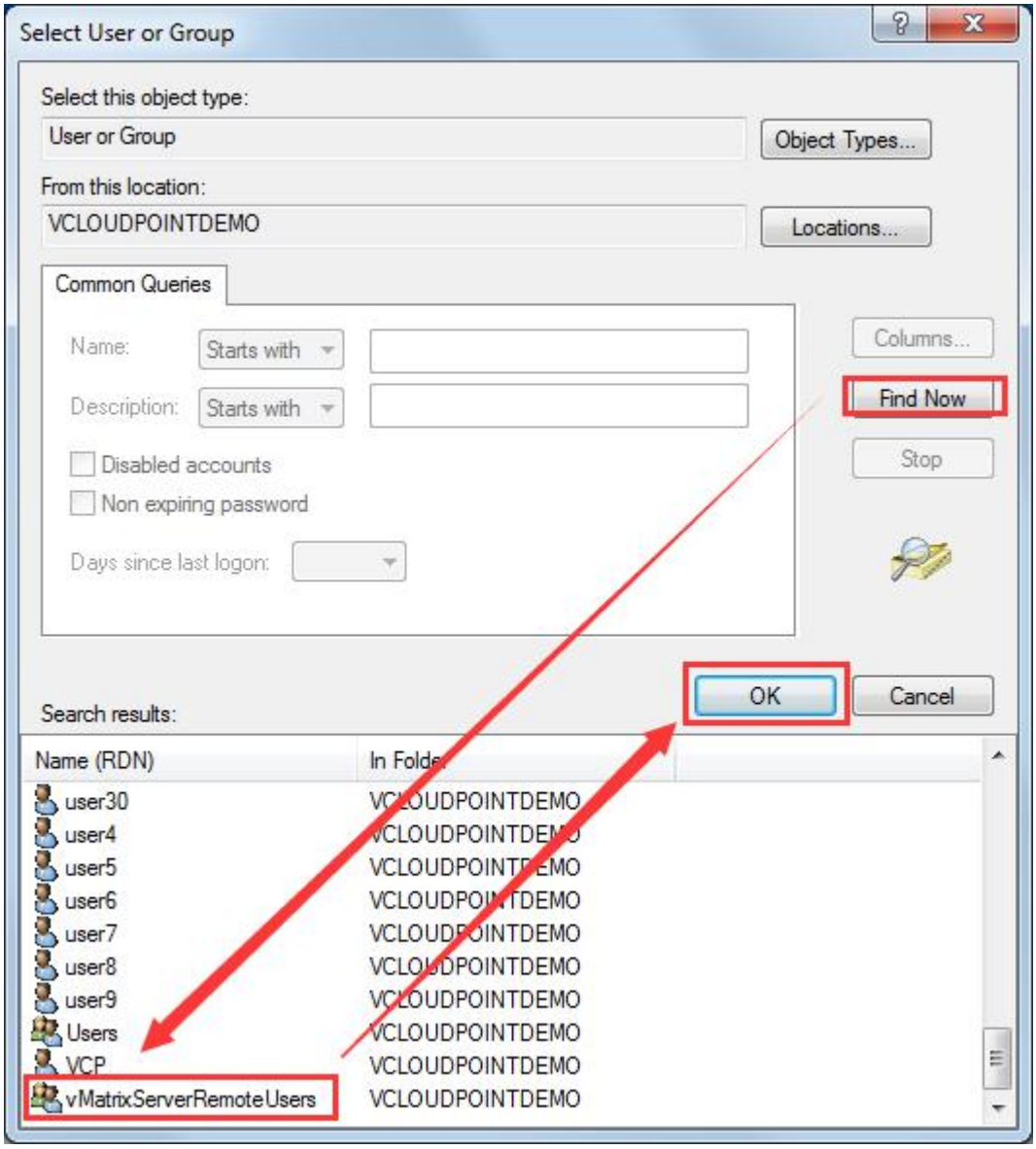
10) On **Create Executable Rules** Select **Deny**, and **select** a group.



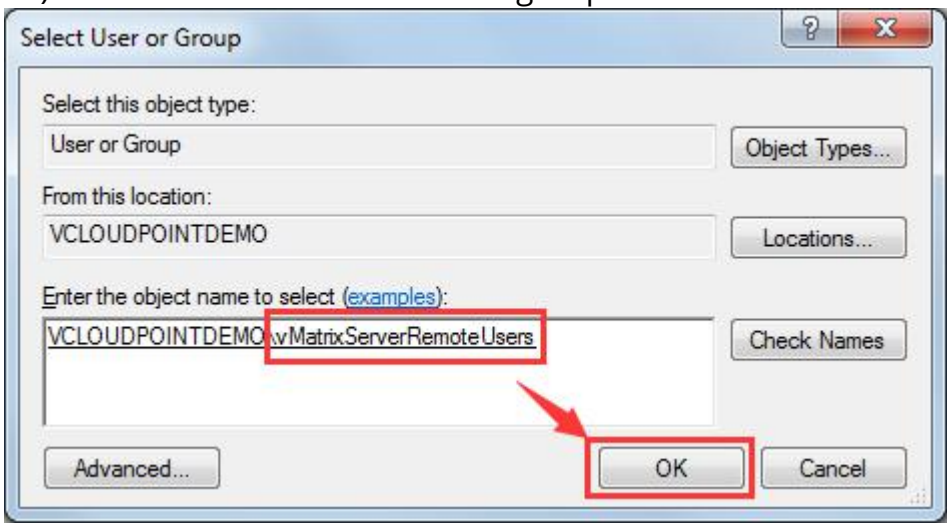
11) Click **Advanced.**



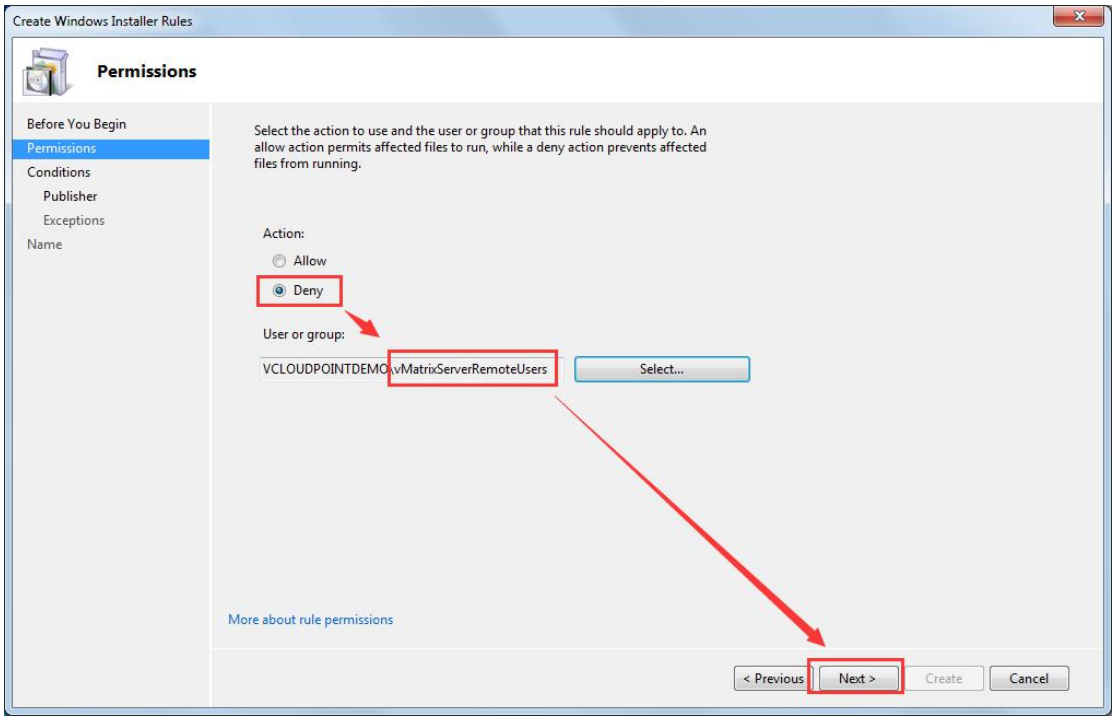
12) Click **Find Now**, select **vMatrixServerRemoteUsers**, and click **OK.**



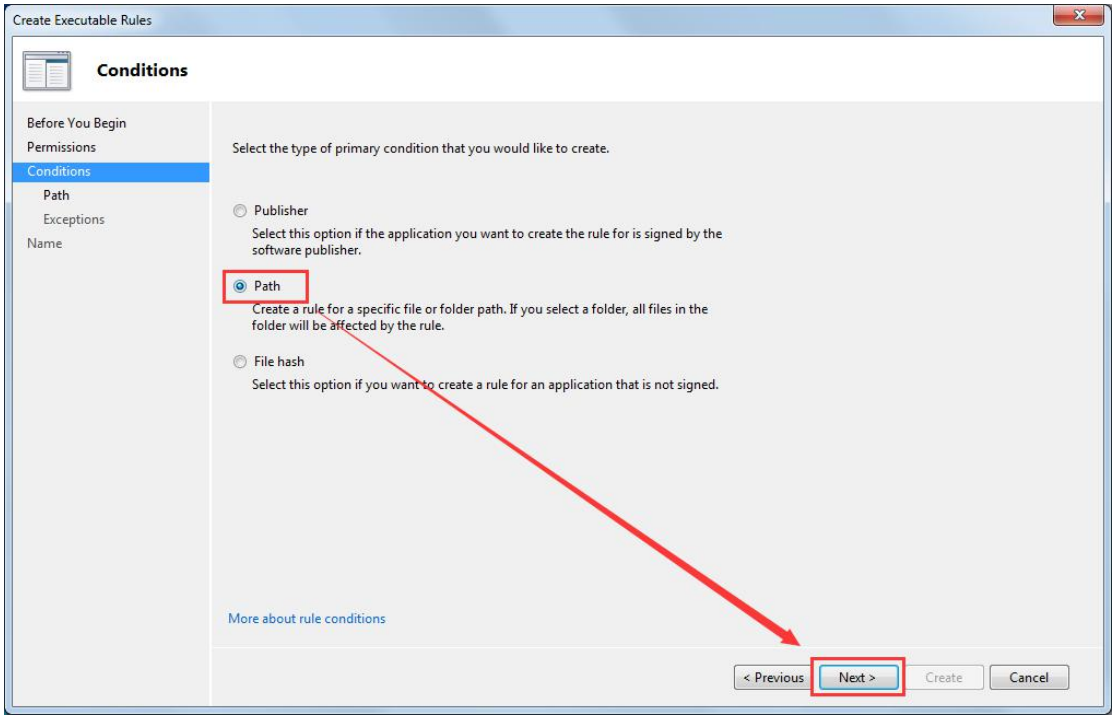
13) Reconfirm the selection of the group and click **OK.**



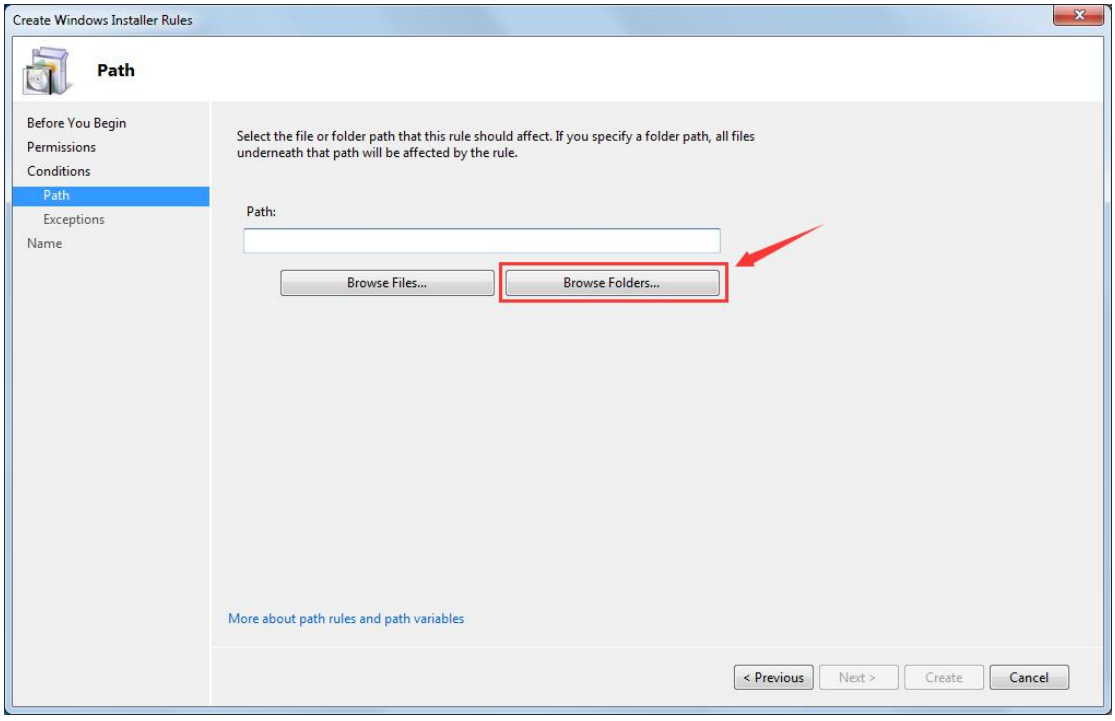
14) On **Create installer rules** select **Permission** Confirm the **Deny**, then click **Next.**



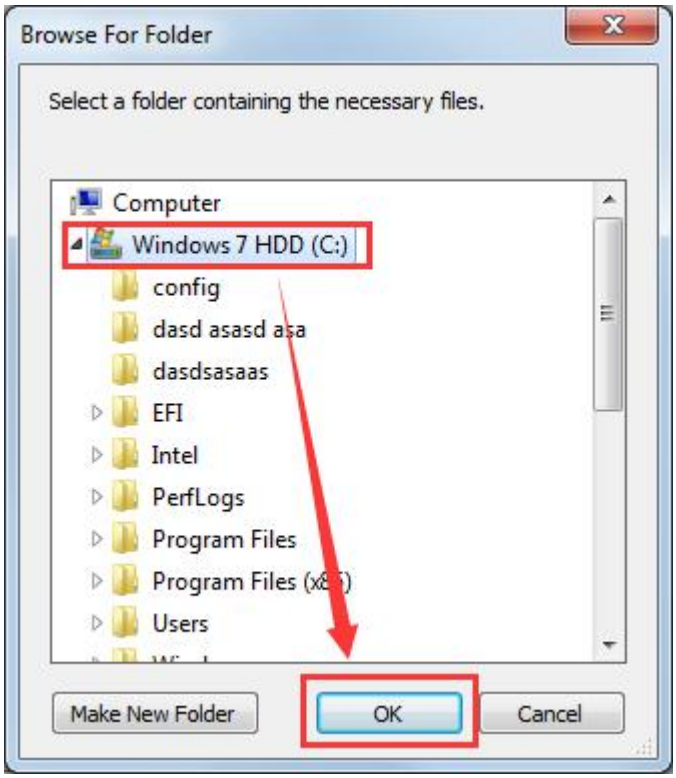
15) On **Create installer rules** Select **Path**, **Next>.**



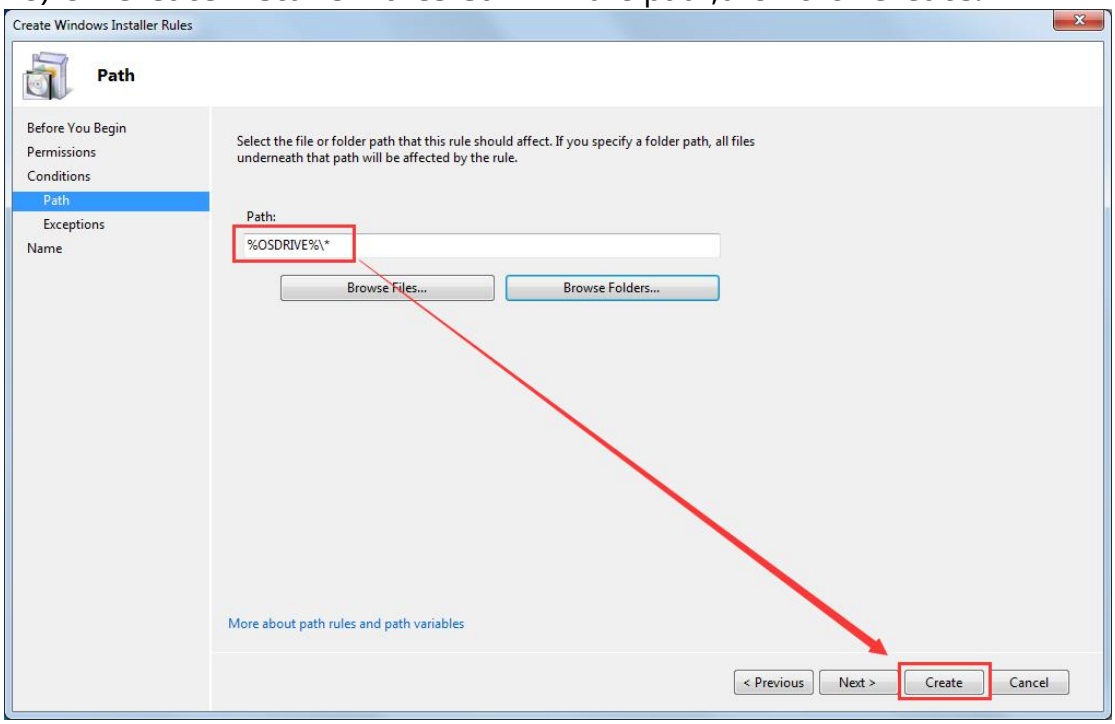
16) On **Create installer rules** Select **Browse Folders…**



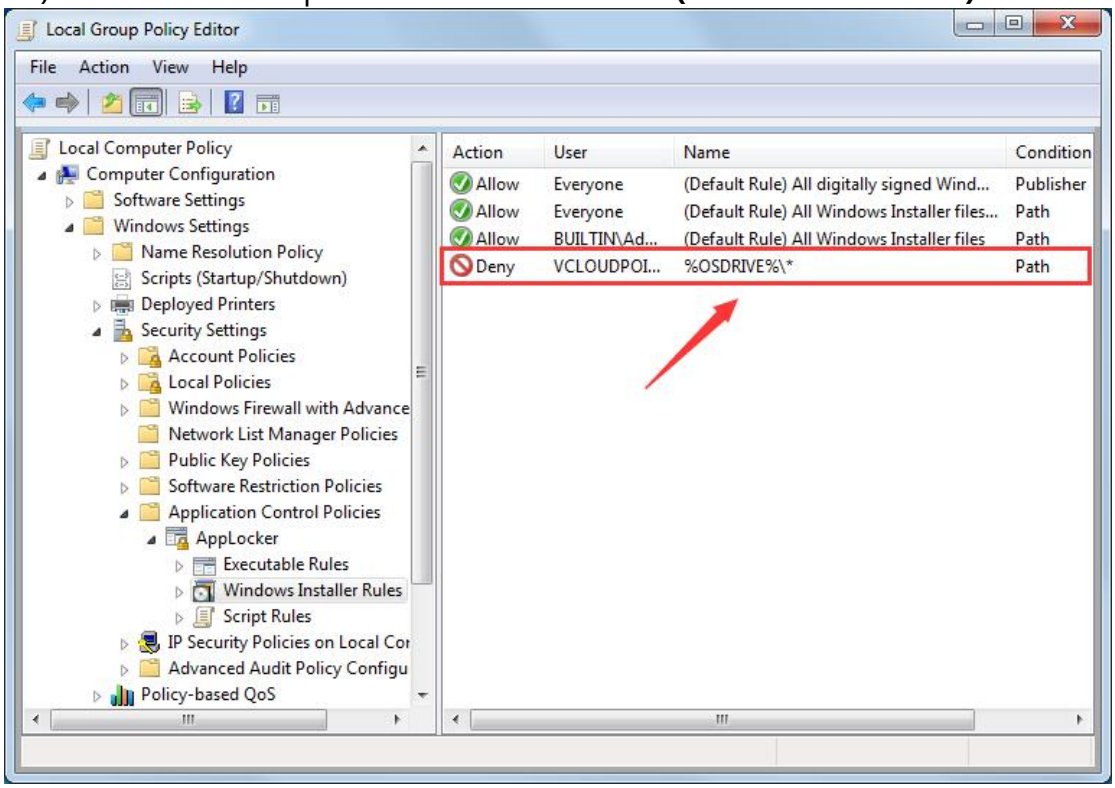
17) Select **Disk(C:)**, limit the user to install the software in **disk C**, then click **OK.**



18) On **Create installer rules** Confirm the path,then click **Create.**

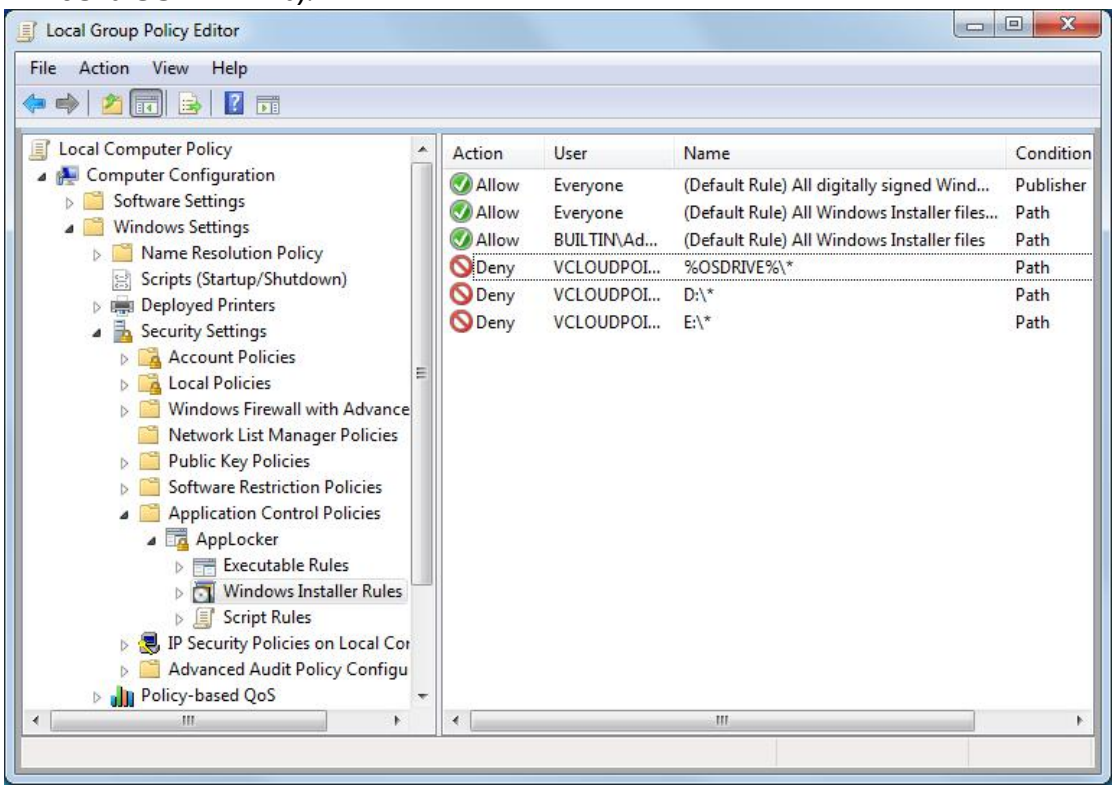


19) You can see the path has been restricted **(C for %OSDRIVE%).**

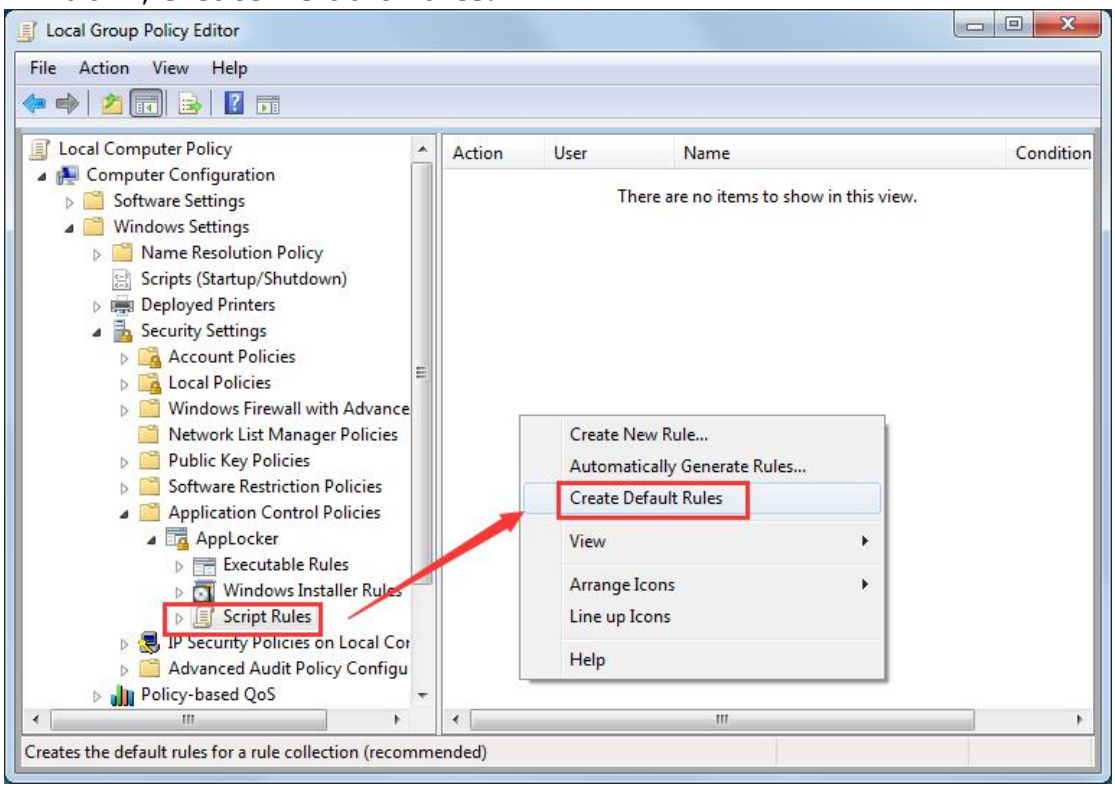


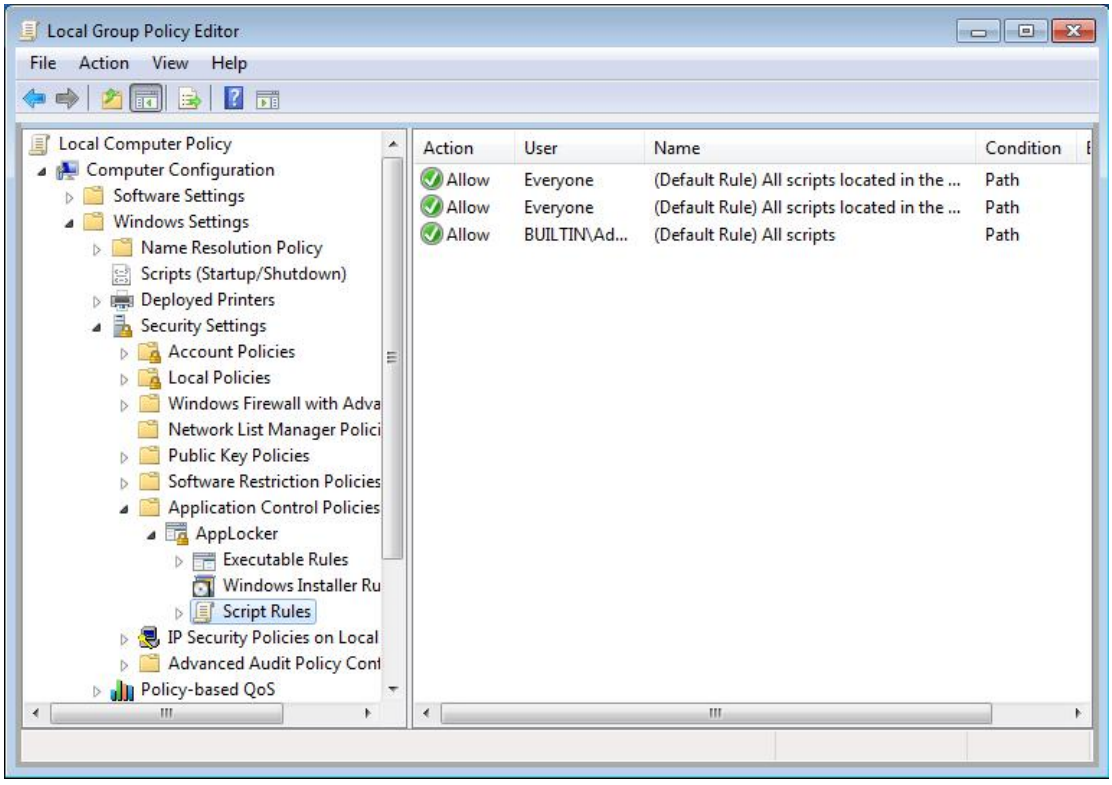
In the same way, add other disks (public disk, private disk...) to the restriction list, which can limit the user to install the software under other disks.

20) All three Disk have been added to restriction list and (**C drive** appears as**% OSDRIVE%**).

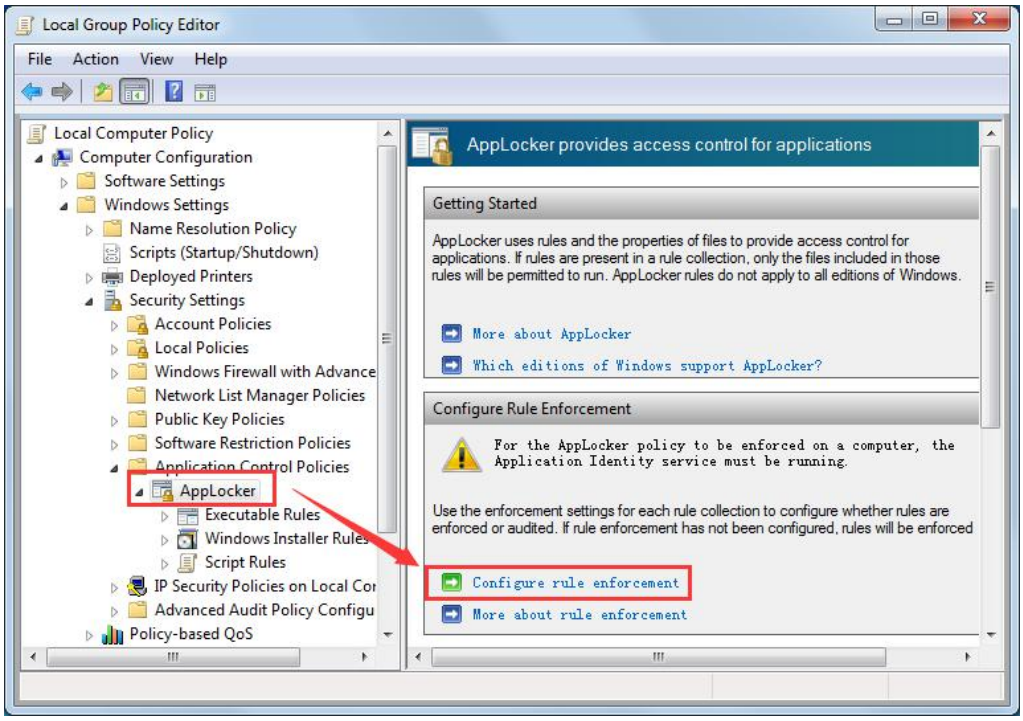


21) On **local group policy editor** Select **Script Rules**, right-click the right blank, **Create Default Rules.**

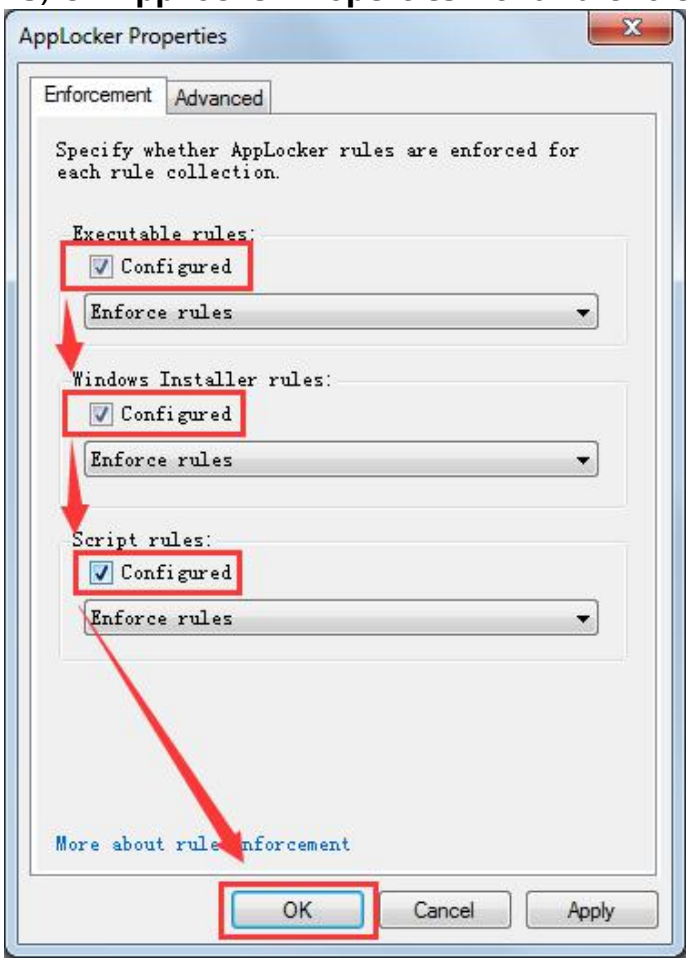




22) On **local group policy editor**, select **AppLocker**, click **Configure rule enforcement.**



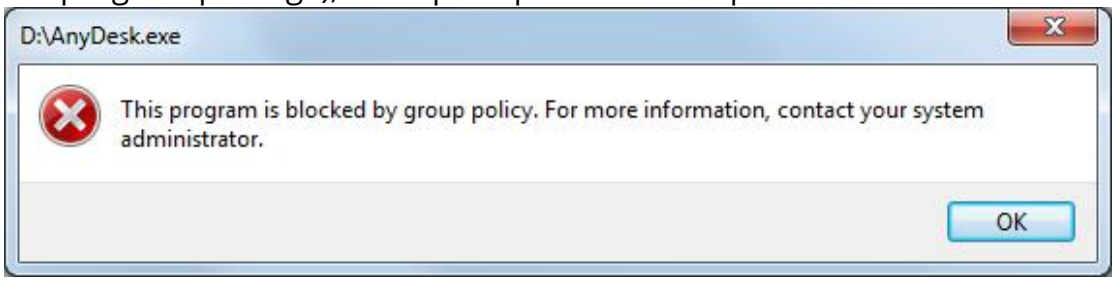
23) On **AppLocker Properties** Tick all the rules then click **OK.**



24) AppLocker Setup complete, restart the host.

Test:

- login a user at a vCloudPoint Zero Client, run the software that need to be used to see they run normally or not.
- When opening .exe file (program installation package or green program package), it will prompt and fail to open.

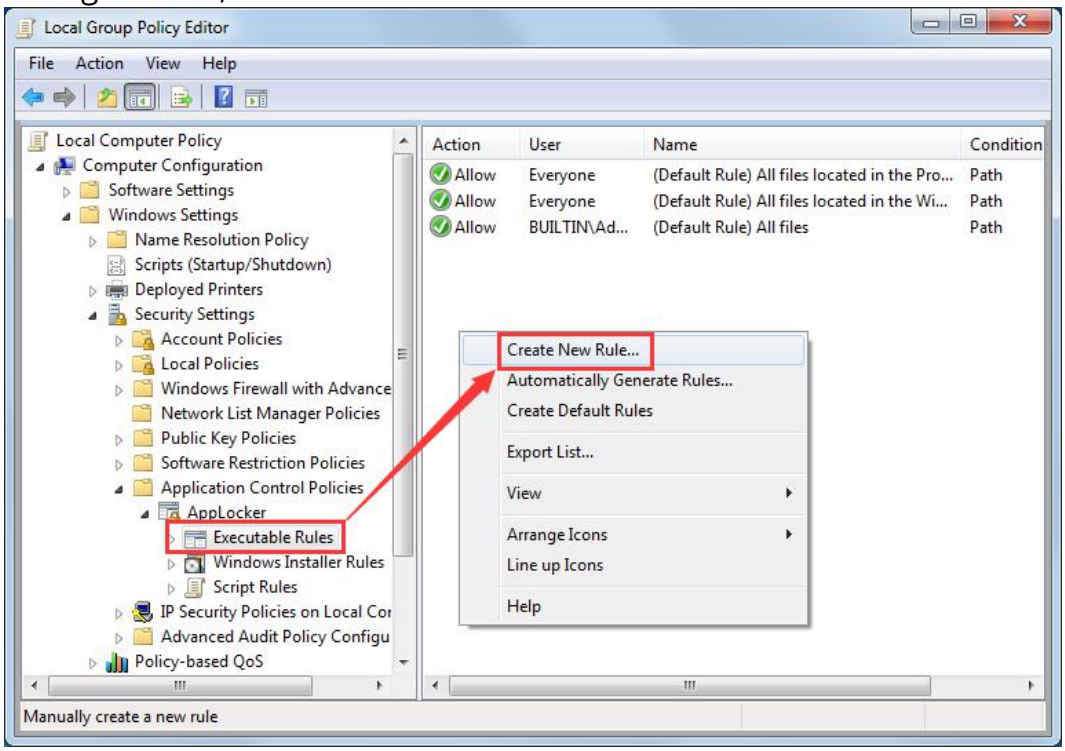


Tips: Users can only open program shortcut on the user's desktop, please do not put.exe files on the user's desktop.

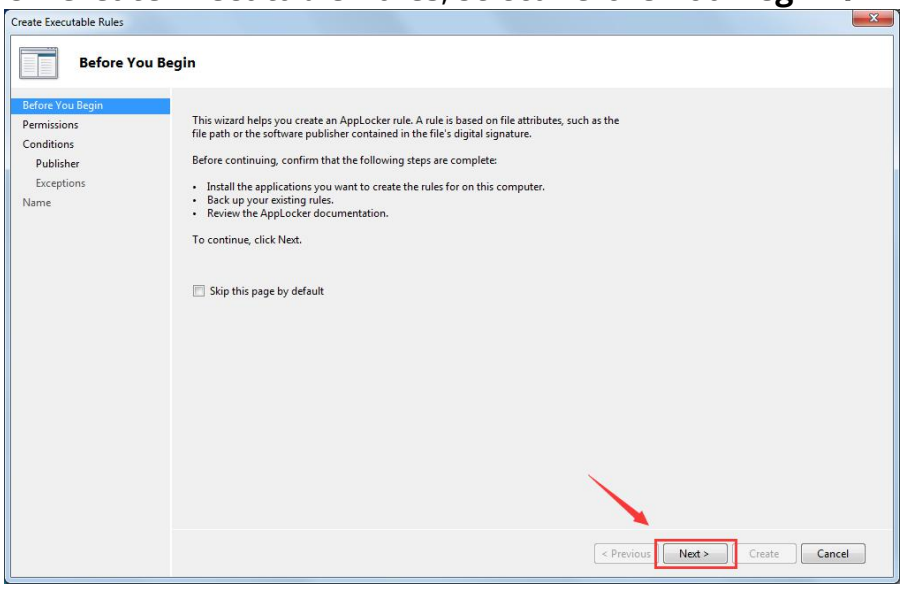
Remark 1: Allow software installation on other directories

If you have software to be installed in other directories but not C:\Program Files and C:\Program Files (x86) (for example, E:\Program Files), follow the following steps to create new rules.

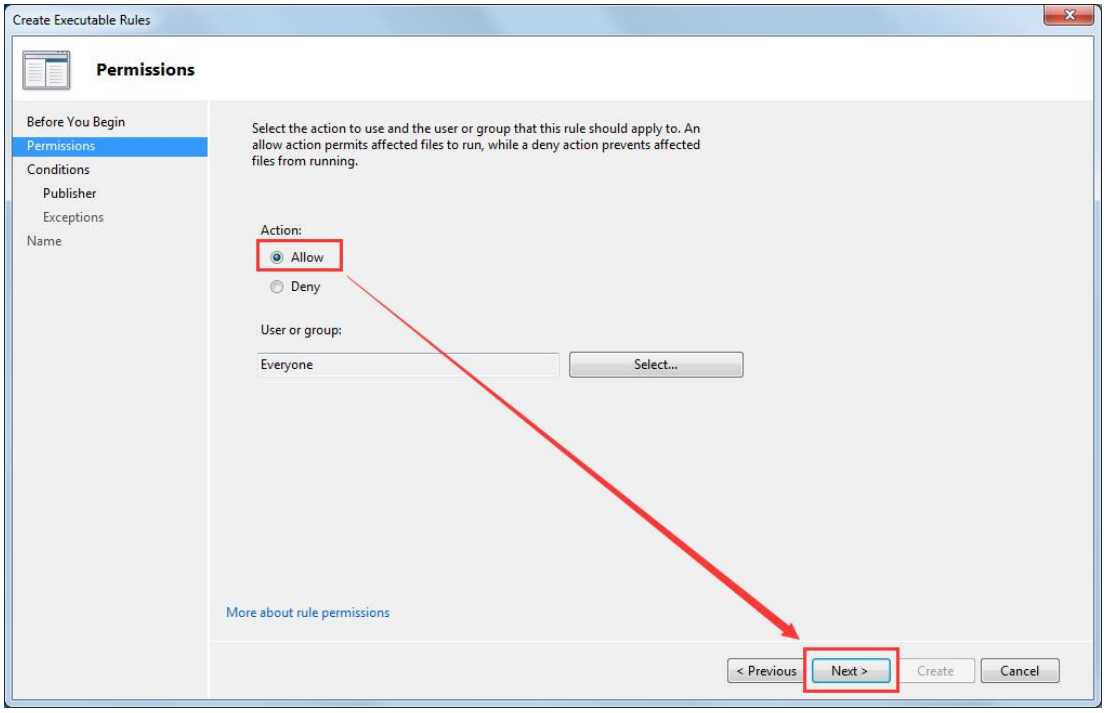
1) On **local group policy editor**, select **Executable Rules**, right-click on right blank, **Create New Rule…**



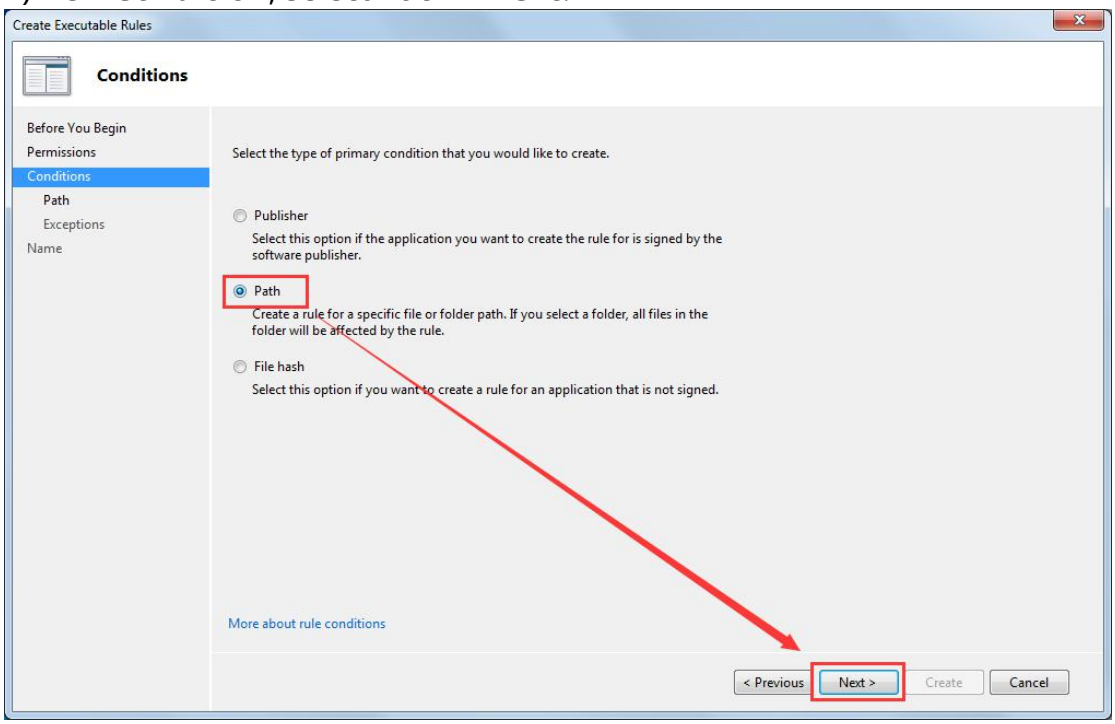
2) On **Create Executable Rules**, select **Before You Begin → Next.**



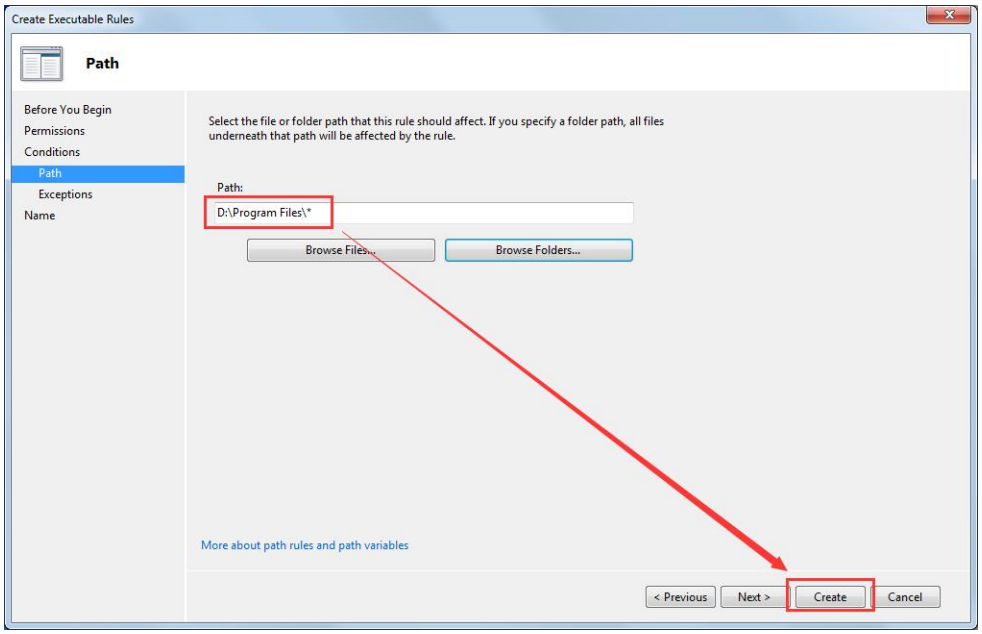
3) **On Permission** select **Allow→ Next**.



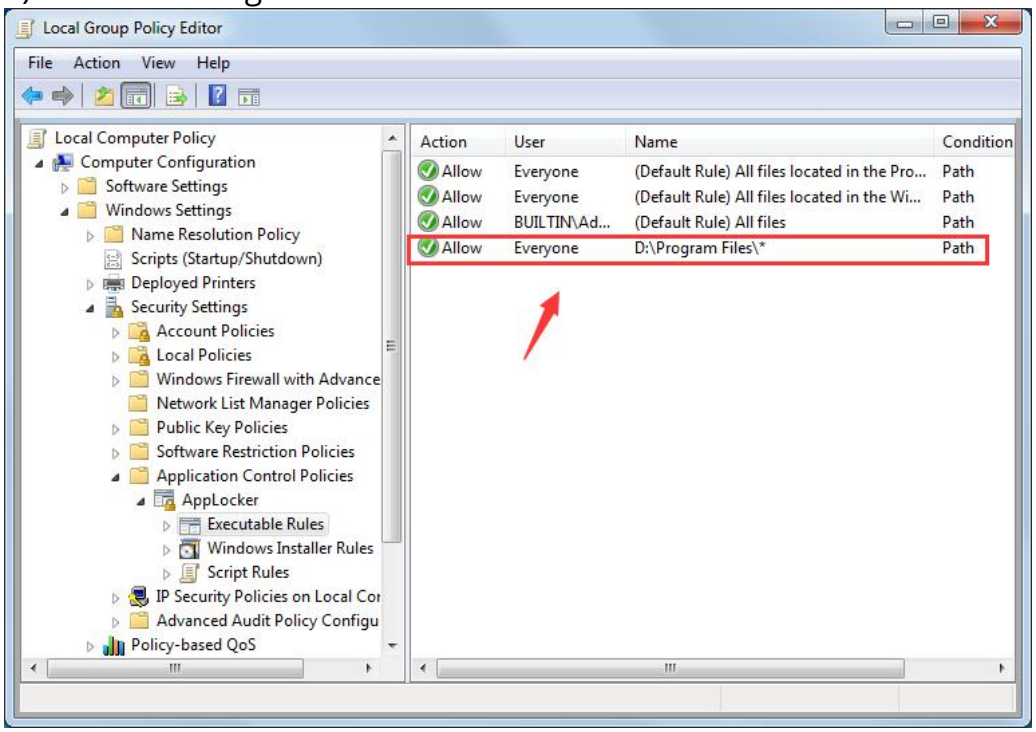
4) On **Condition**, select **Path→Next**.



5) **Path**, select **Browse Folders…** Select the disk (D:) **Program Files** → **Create**.



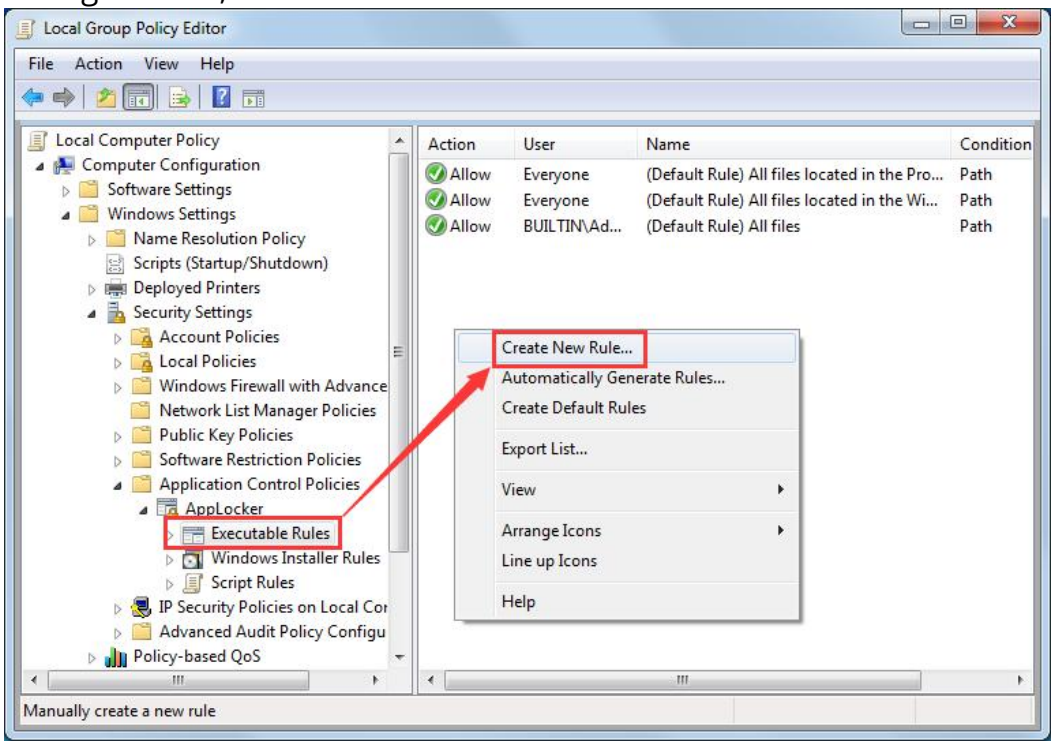
6) After creating the new allowable custom rules will be shown.



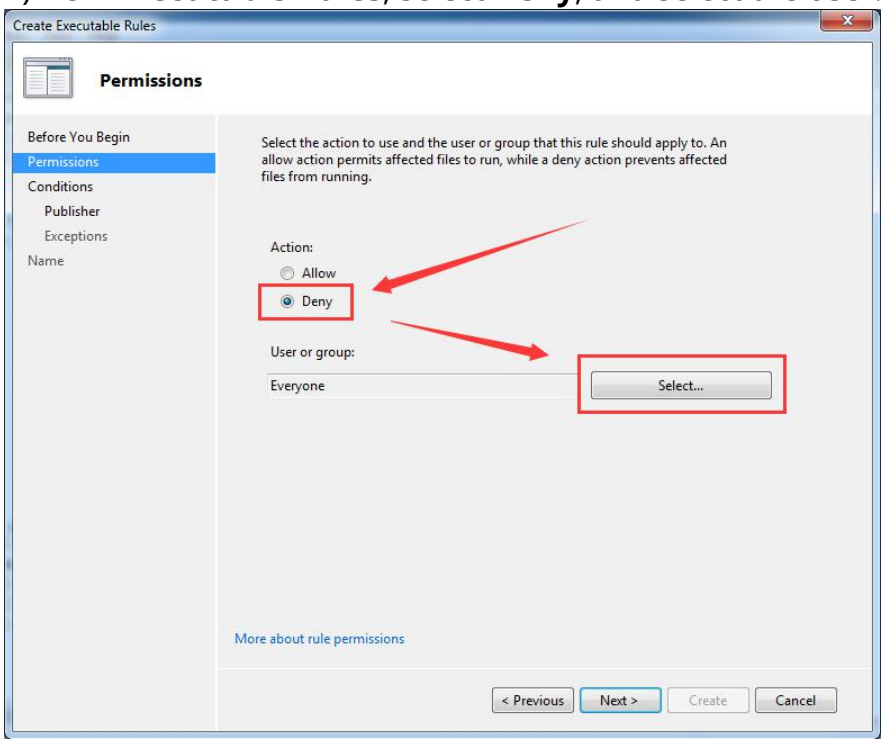
Remark 2: Restrict a user from using a software

If a user (for example, user1) is required to be restricted from using a software, a denial rule should be created in the **Executable Rules**.

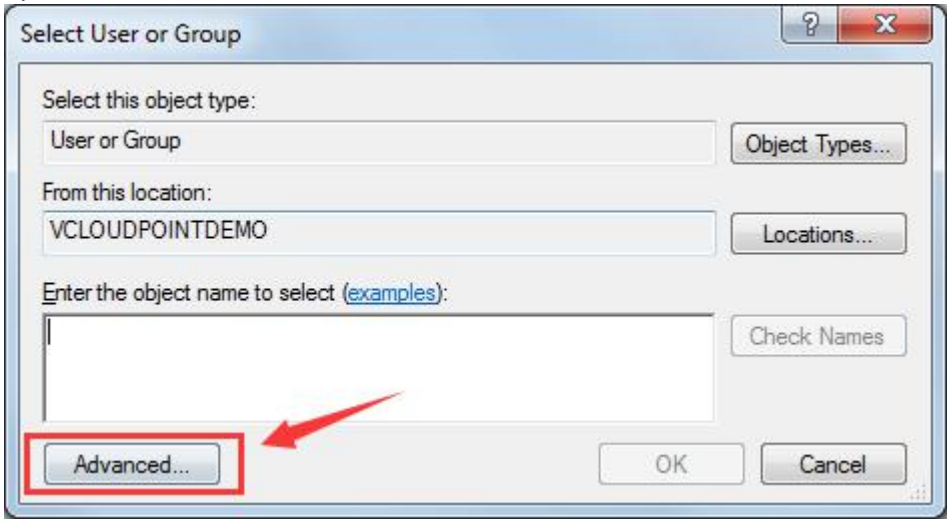
1) On **local group policy editor** Select **Executable Rules**, right-click the right blank, **Create New Rule...**



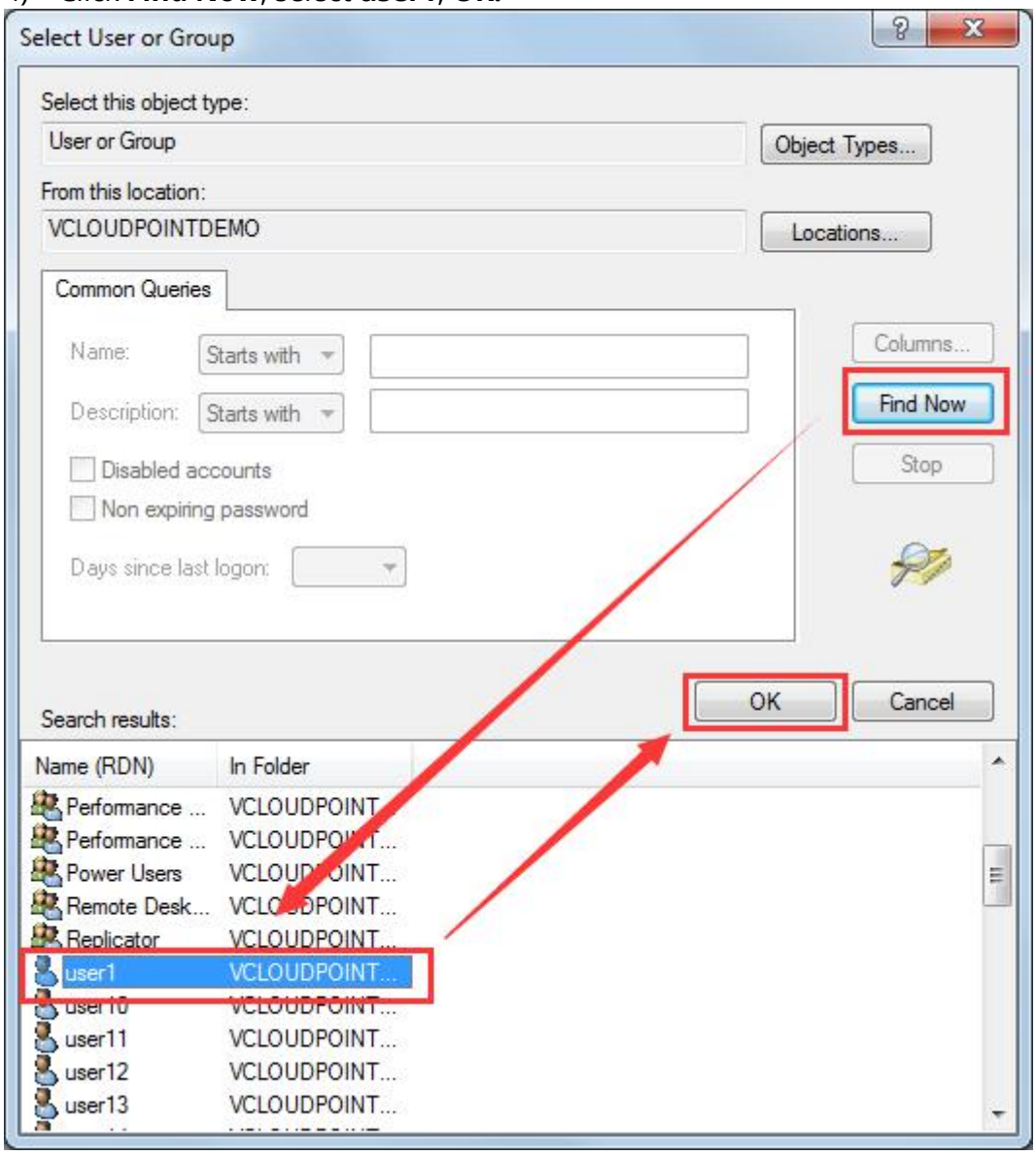
2) On **Executable Rules**, select **Deny**, and select the user.



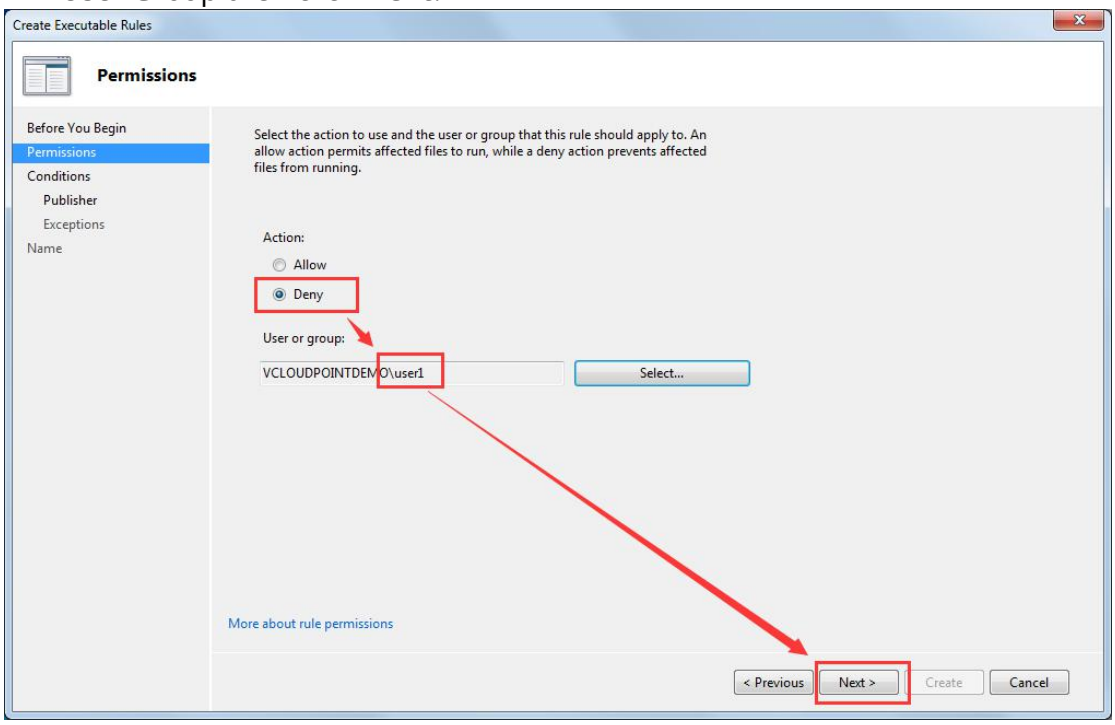
3) Click **Advanced.**



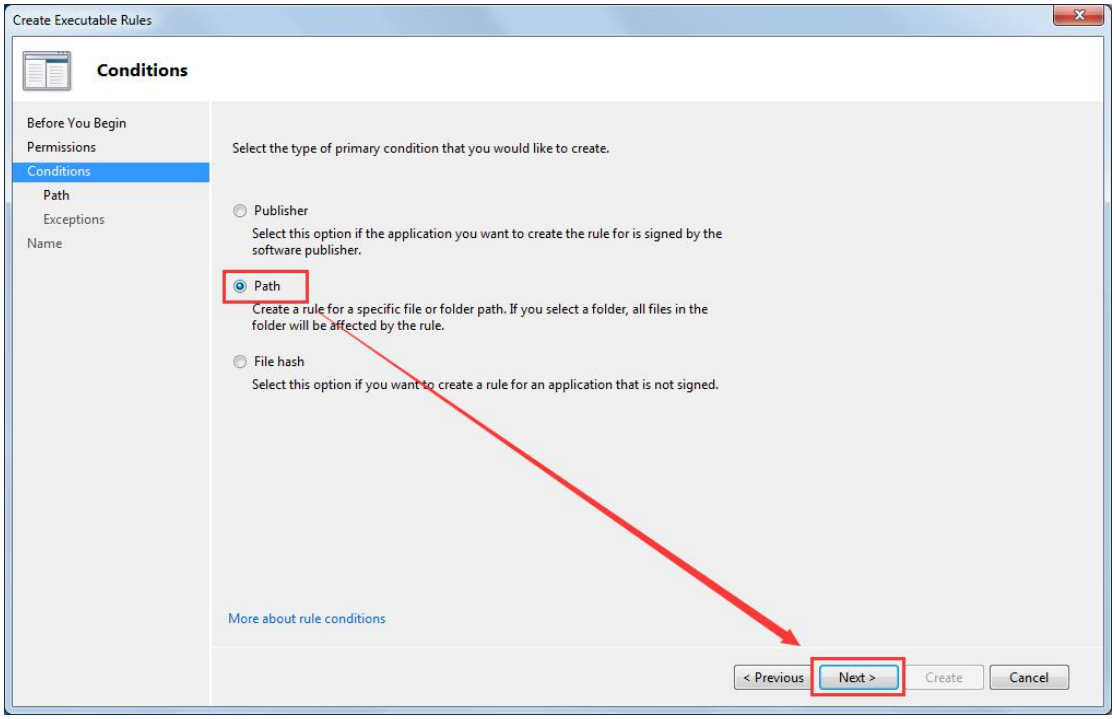
4) Click **Find Now**, select **user1**, **OK.**



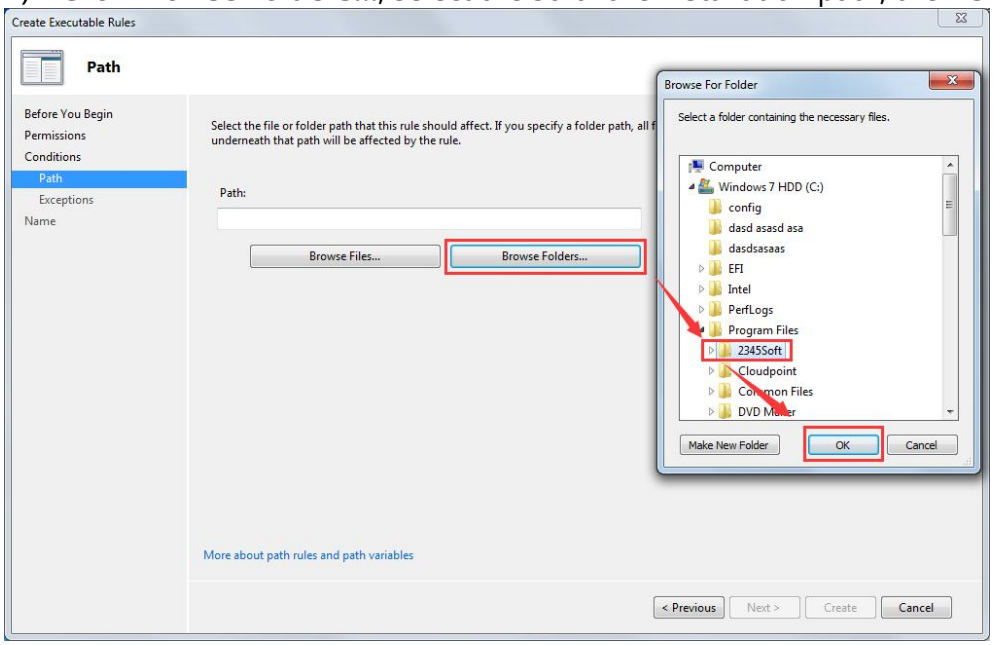
5) On **Create Executable Rules,** select **Permission→ Deny**, confirm User or User Group then click **Next**.



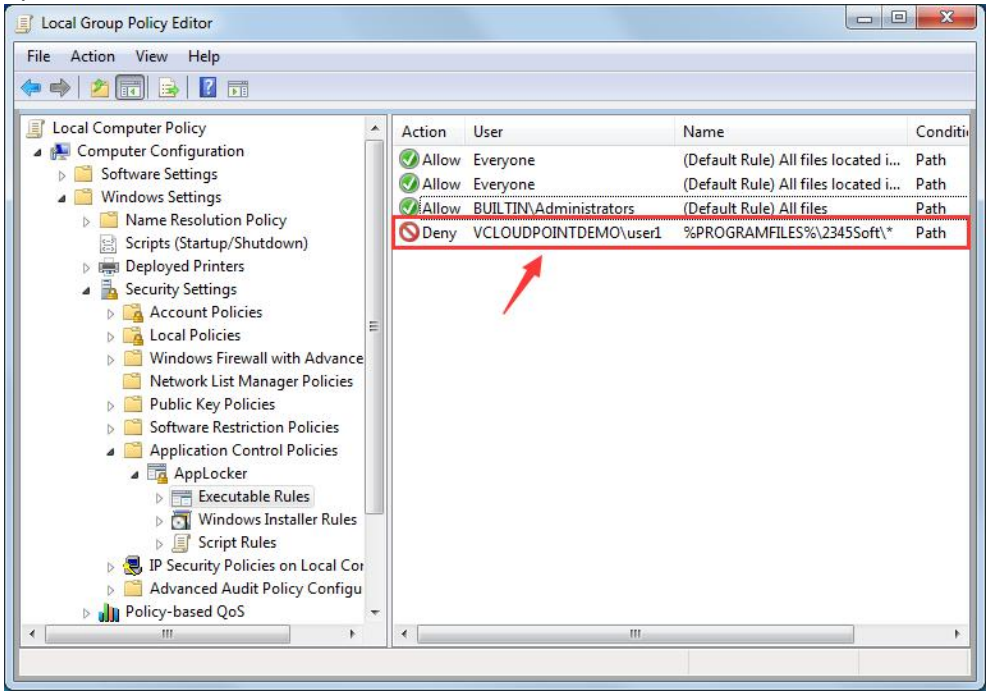
6) On **Create Executable Rules**, select **Condition**, select **Path**, click **Next**.



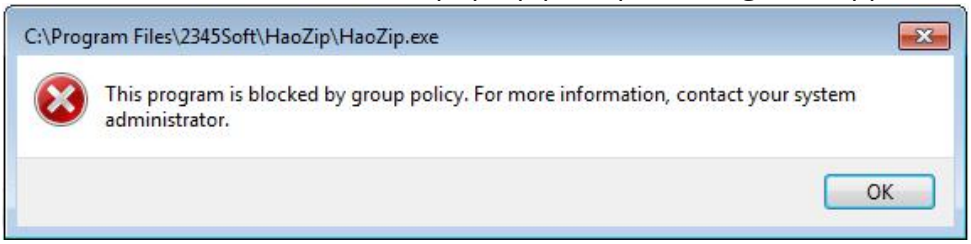
7) Click **Browse Folders…**, select the software installation path, then **Create.**



8) A denial rule has been added.



9) When User1 runs the file, a pop-up prompt message will appear.

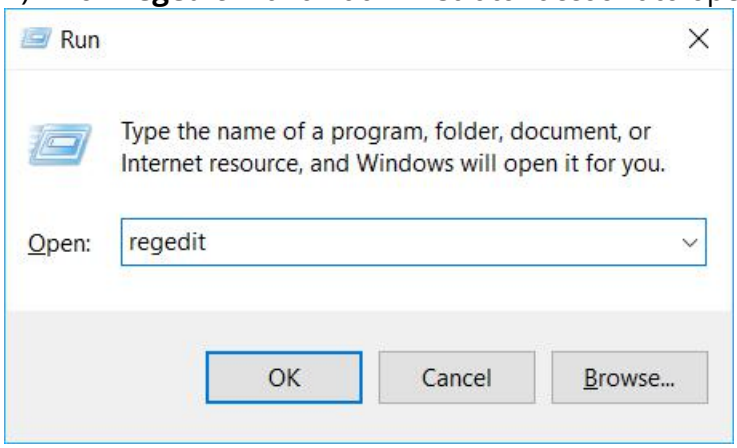


10) If you need to restrict some users, you can first create a user group, add these users to the user group, and then restrict the user group.

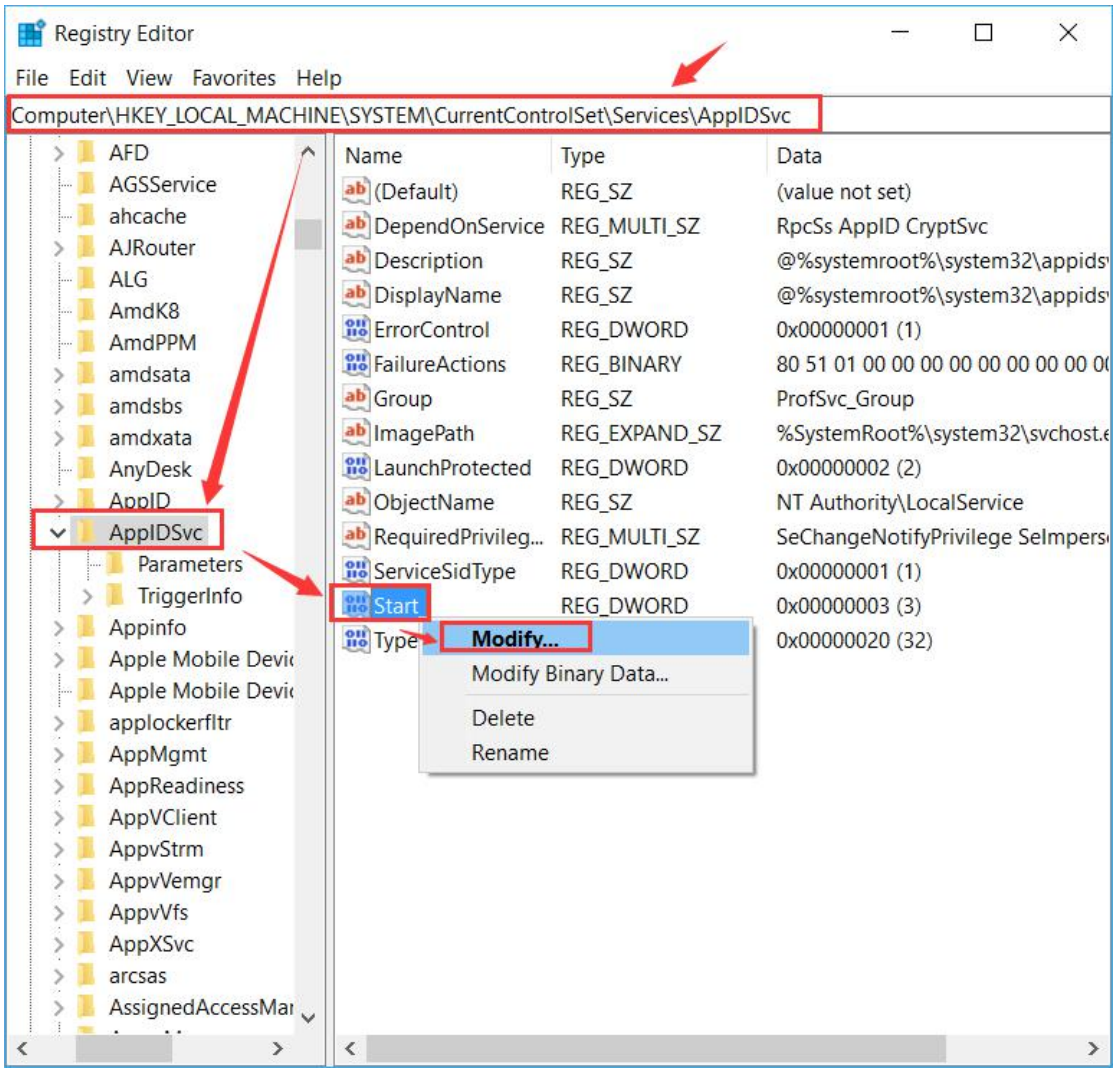
Remark 3: Enable Application Identity service in Windows 10/ Server 2016

In Windows 10/Server 2016, Application Identity service cannot be set automatic startup at the **Services** console but the **Registry**.

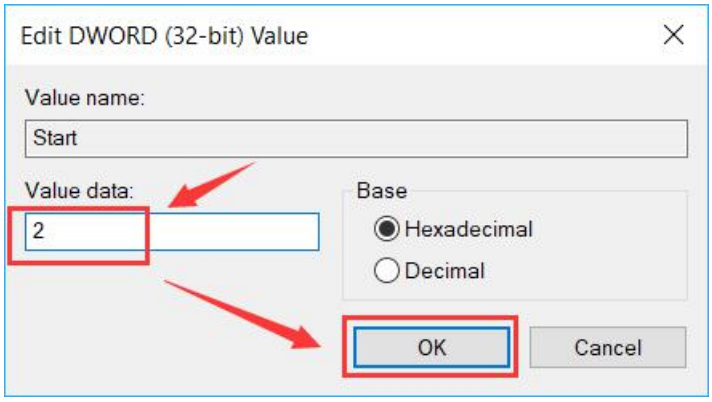
1) Run **regedit** with an administrator account to open the Registry Editor.



2) Find **AppIDSvc**, right click **Start** to **modify** the value (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppIDSvc)



3) Modify the value to be **2**, press **Enter**.



4) The configuration of Application Identity service automatic startup is done.