

ALTERNATE INSTALLATION METHODS

Method 1:

Group Policy application deployment

Active directory based administrators may choose to leverage existing capabilities within AD to deploy software packaged to the systems under their administration over doing individual installations. This is done using the same AD Group Policy tools that would be used to control any other system settings they may be managing. To do this you would use the Group Policy Management Console, or GPMC or other options that may be available to manage GP under AD.

To complete this process you must create a distribution point within the network on the domain accessible by all hosts on the network you need to deploy the software to.

Step 1: Create a shared folder on one of the domain controllers and upload the downloadable application file to the folder.

In this example I have created a shared folder on one of the domain controllers called "Software" and uploaded the EDR application/service to this location. This can be used for any of the downloadable applications/services such as Patch Management, Backup, or EDR.



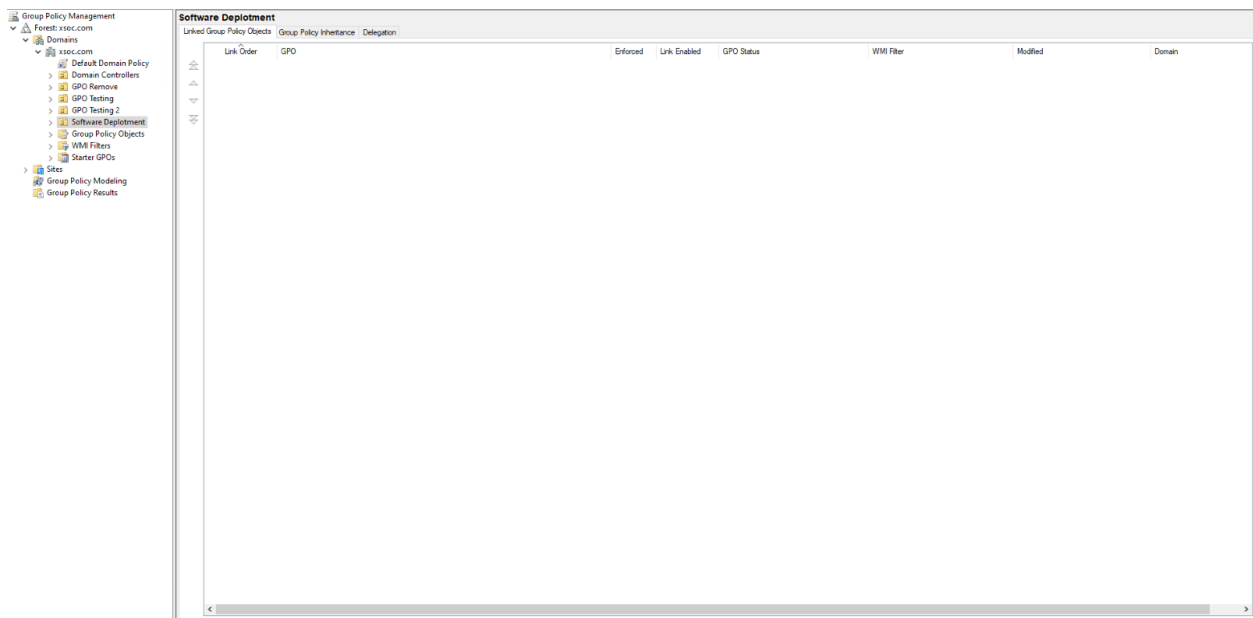
Setup.MBEndpointAgent.x64.msi

4/28/2023 8:21 PM

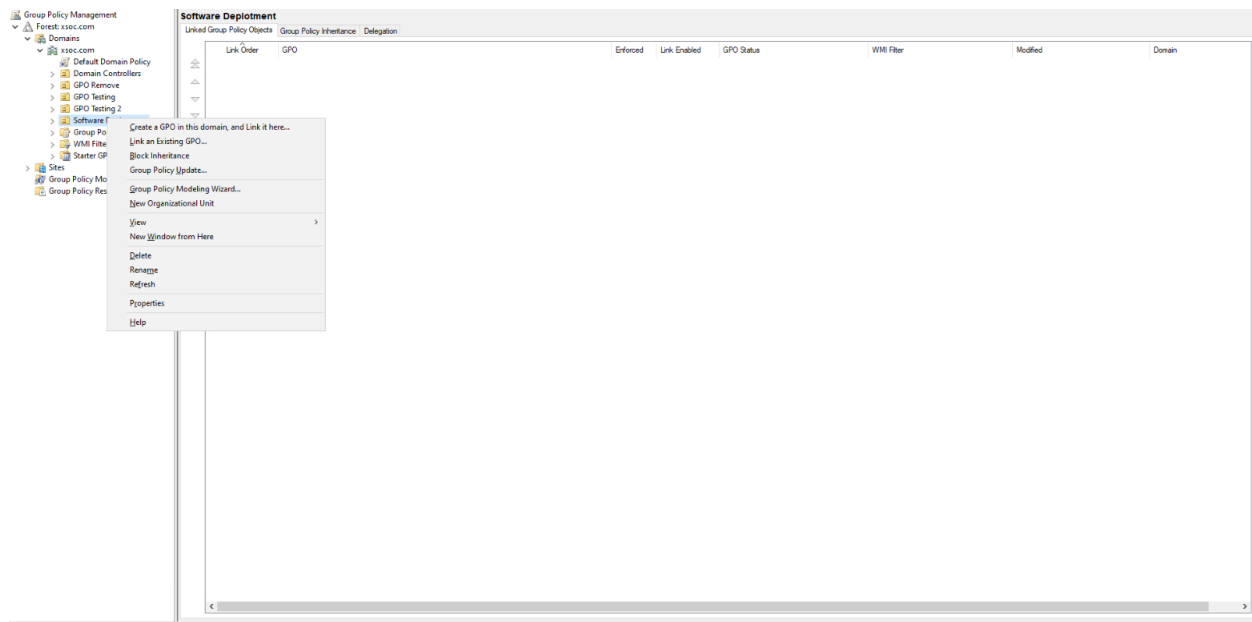
Windows Installer ...

22,456 KB

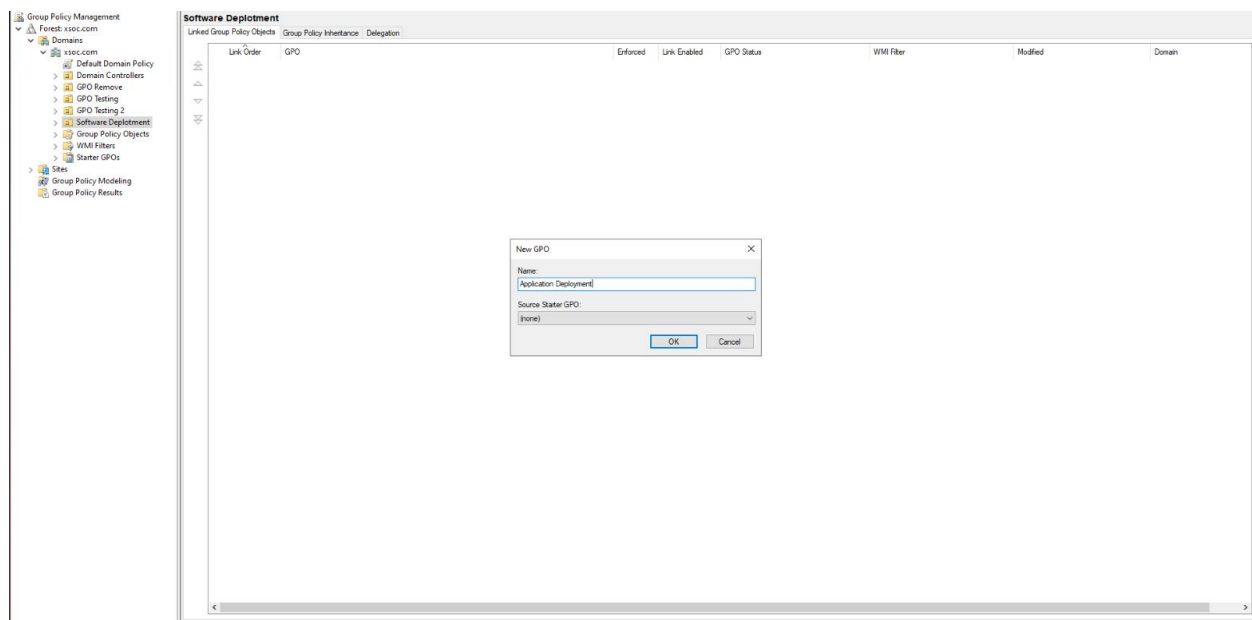
Step 2: Navigate to the Organizational unit (OU) you wish to apply the policy to. In this example screen below I am using the OU named “software Deployment”.



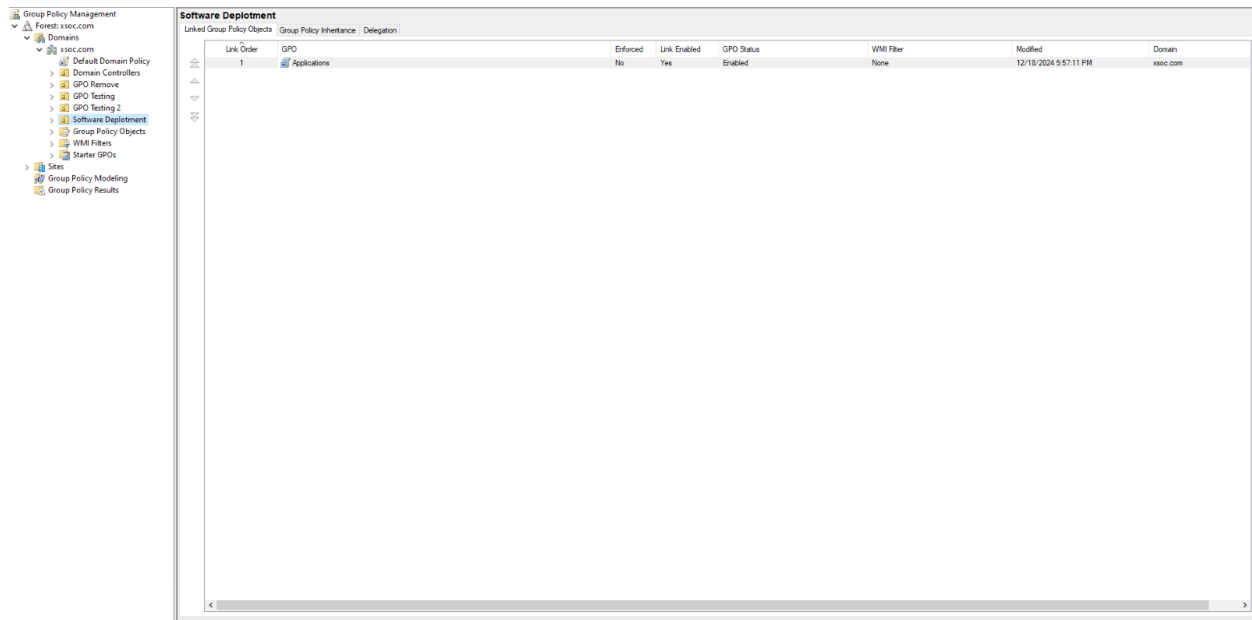
Step 3: Right click the OU and choose the option “Create a GPO in this domain and link it here” to create and apply a GP to the selected OU.



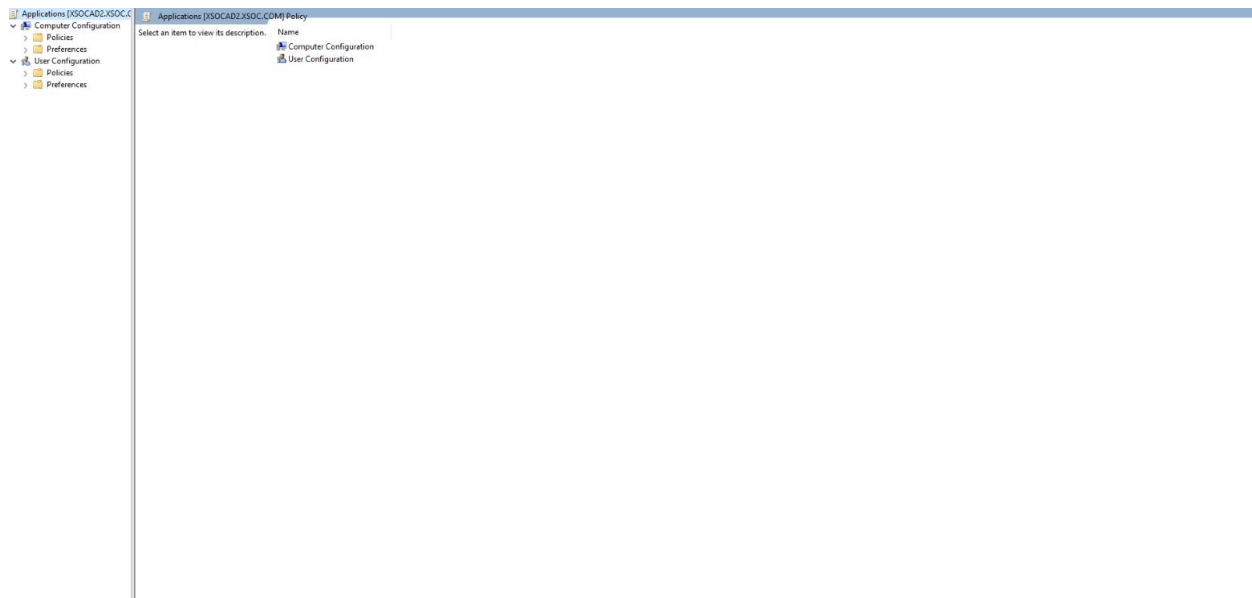
Step 4: In the pop up dialog box give the group policy a descriptive name of your choice, in the example below I have chosen “Applications”.



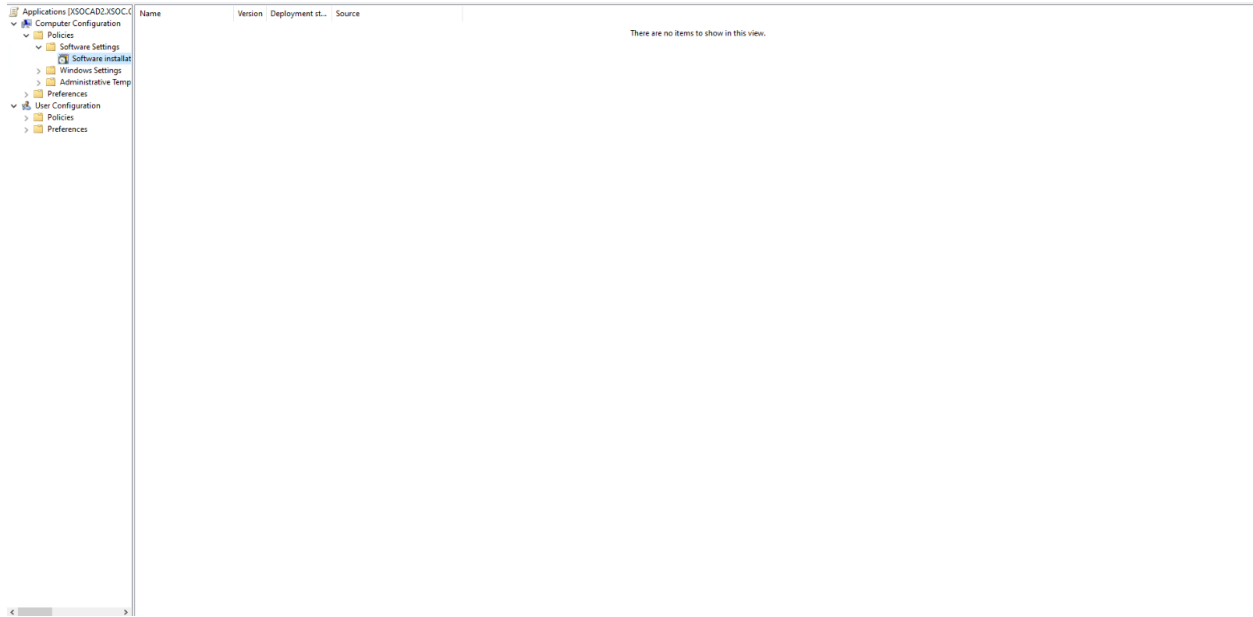
The newly created GPO will then appear in the list on the right-hand side of the window.



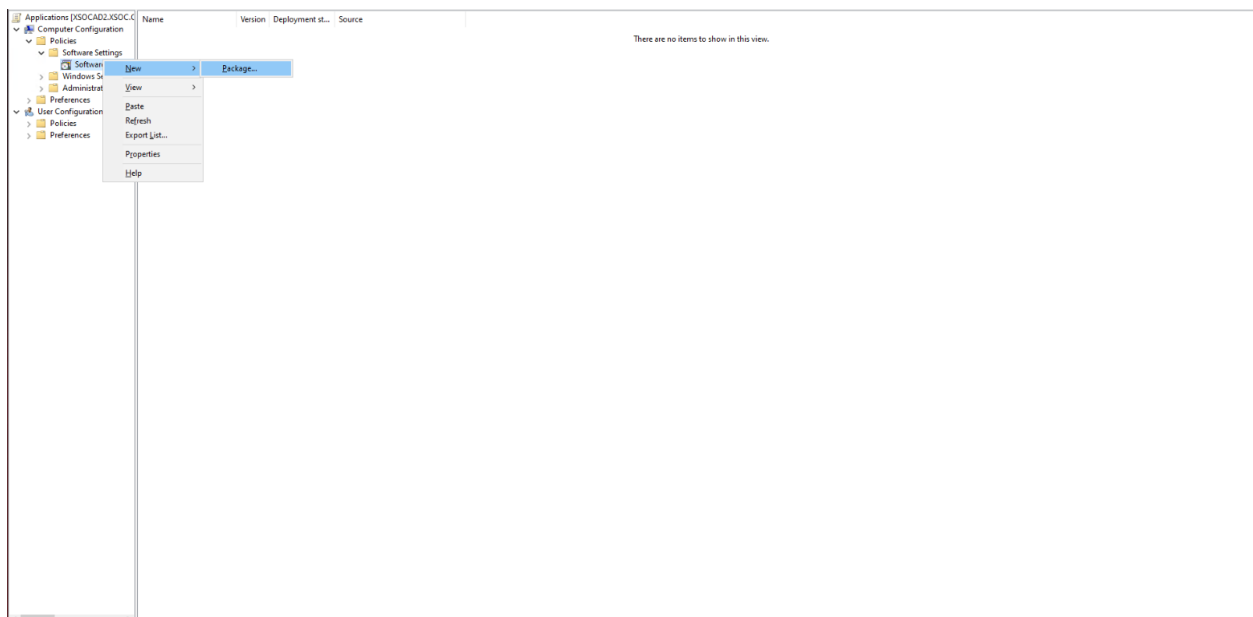
Step 5: Now we will create the setting necessary to assign the software packages we wish this policy to deploy. In this example we will use the software distribution point created earlier in this document To set this up you must edit the GPO created in the prior steps by right clicking it and choosing “edit” which will result in the following screen as a pop up.



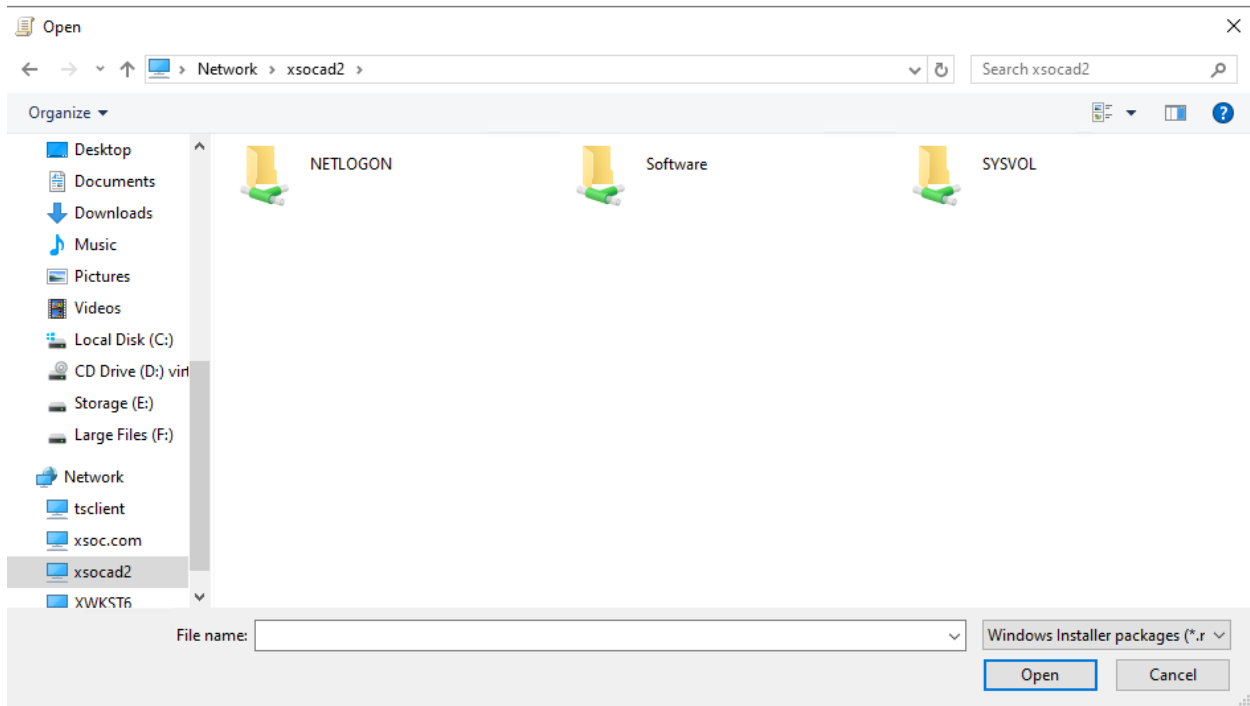
Step 6: To Assign the package we will expand the “computer Configuration” section of the policy and then the Software Setting” to find the “Software Installation” option.



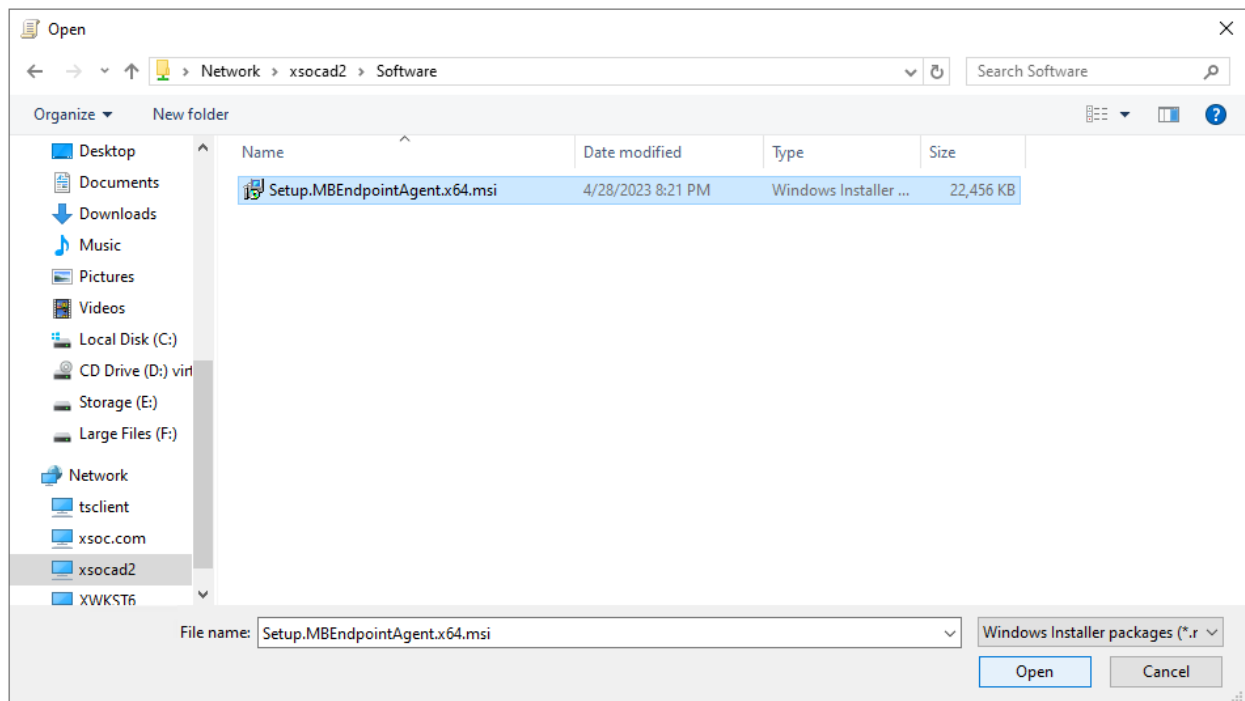
Step 7: Right clicking on the “Software Installation” option you will select the “New” and then “Package” option.



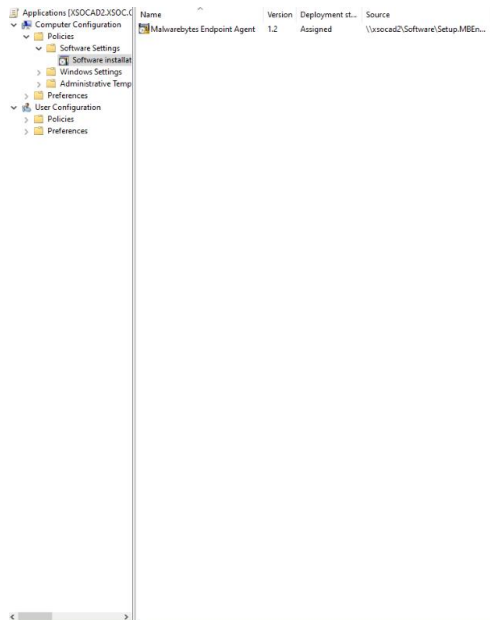
This will bring up a files browser pop up dialog which you will use to navigate to the shared folder hosting the files.



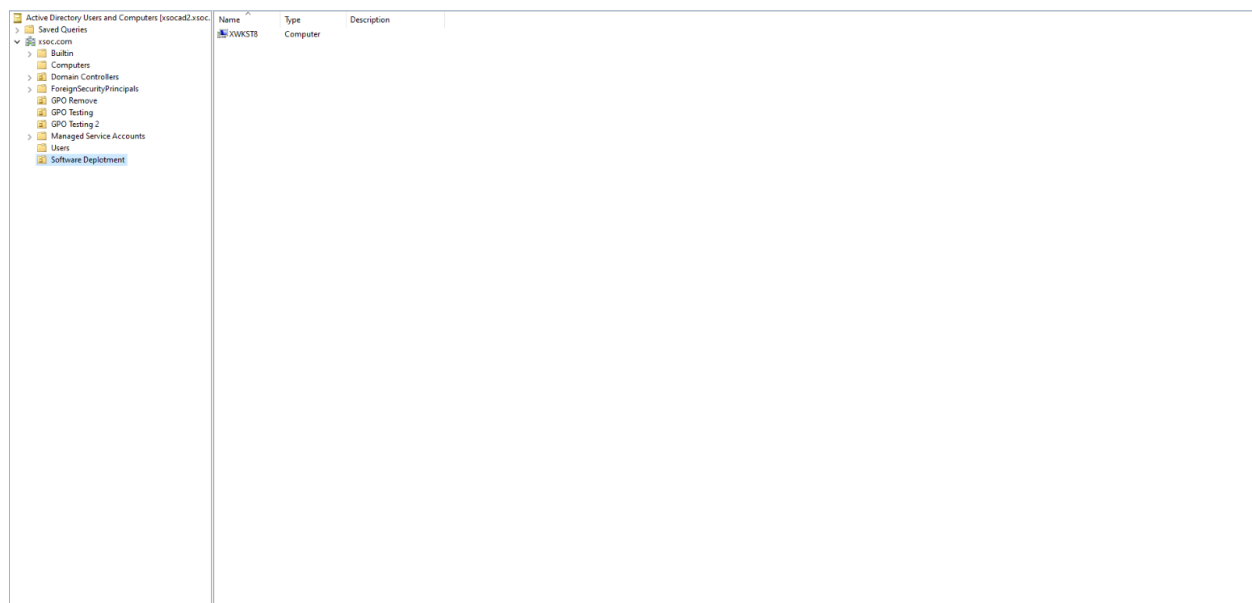
Step 8: Choose the folder, and then the desired package, and click Open in the lower right corner of the window.



You will be given three options upon doing so, Publish, Assign, and Advanced. Publish makes it available but does not automatically install it. Assign will automatically install the package. Advanced allows you to select various options and or modify the deployment as needed. The most common usage of this will be to simply assign it unless you require additional arguments or modifications to be made. For this example we have chosen “Assign” so the package now appears in the policy tab accordingly.



Step 9: All that remains now is to modify the source OU where the policy was created by adding the hosts you wish the application installed to. Drag the desired hosts from their current location in the Active Directory Users and Computers application to the new location.



Step 10: The application will be automatically installed in most cases no later than the following day pending the settings of the domain.

Step 11: Confirm with XeneX when you have completed this by emailing Support@xenexsupport.com.

Step 12: We will get back to you confirming that the hosts have gotten their installations.

Important note:

In Active Directory OUs can of course be nested allowing for you to maintain the settings of the current OU and add the new ones without modifying it. It is important to make sure the hierarchy of nested OUs is correct and do not conflict with each other as they could override each other if the order isn't right. In general the more important settings are higher in the tree structure than lesser ones

Method 2:

Using Scripts to deploy software.

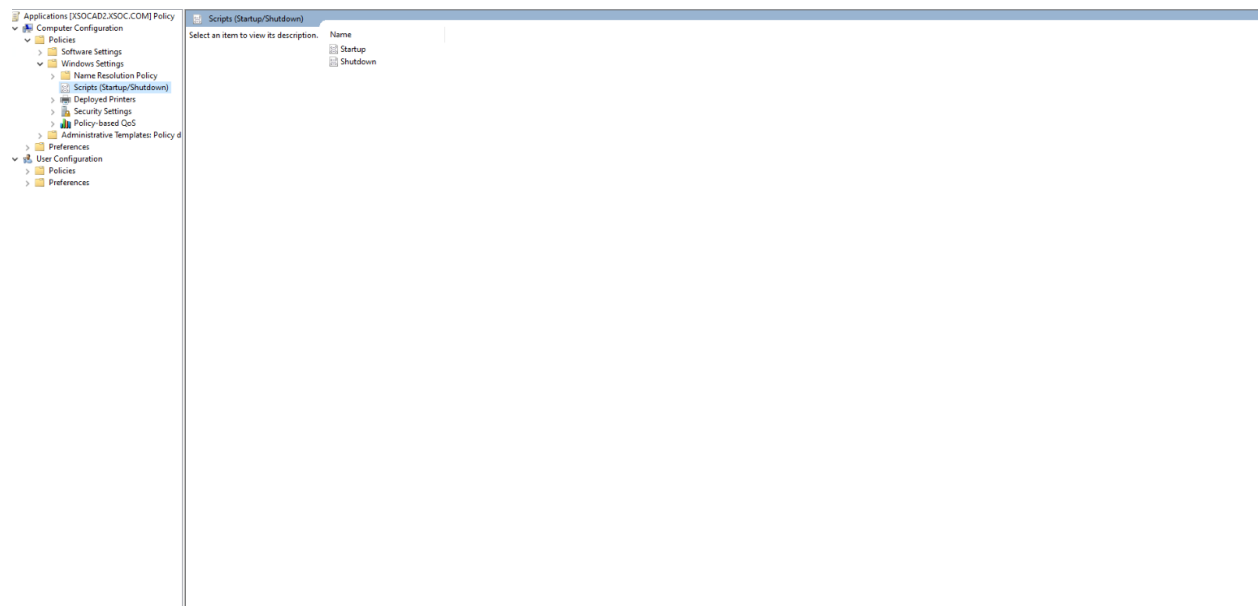
In some cases deploying software is easy, assign the package through group policy as previously discussed and let the automation work as intended. In some cases, however, it isn't that simple. You may require additional arguments, or the format of the file may not be easily compatible with GPO deployment which may require more complication steps to complete the installation. In this case it may be more appropriate to use a script-based install over the more typical *.msi option. To use a powershell *.ps1 type script or other script format to complete this which allows for more advanced options.

Scripting can be used to perform many functions in addition to simply installing an application by command line argument. For example, it can be used to also reach out and download the

files, install them, and start the required services in one step, as opposed to having to do each of the manually.

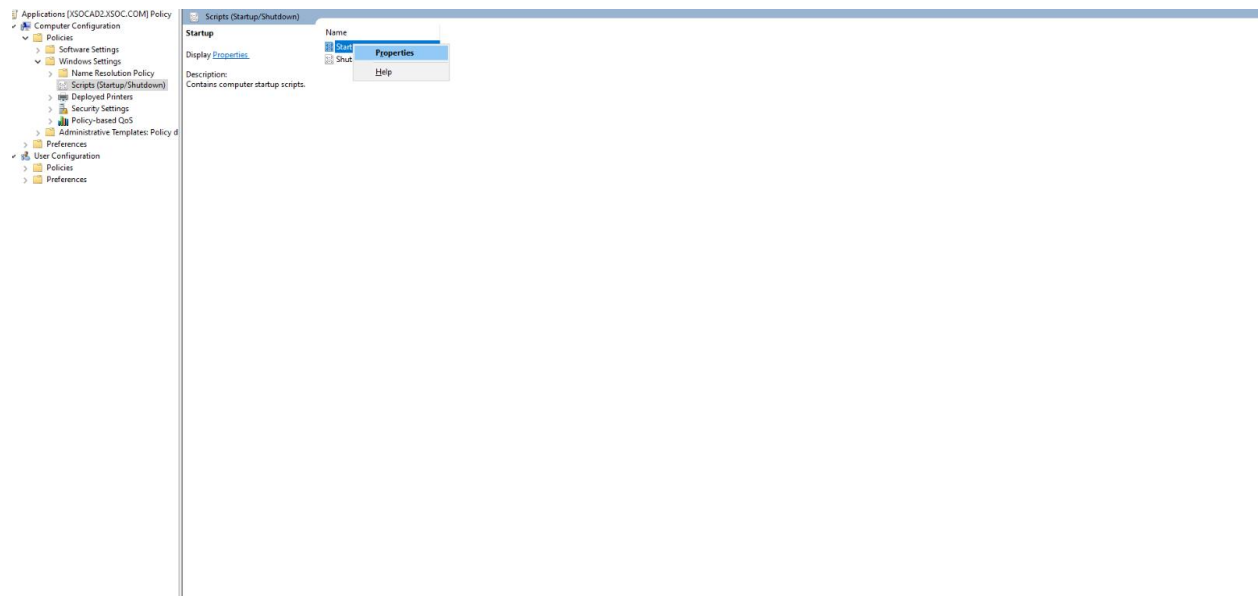
Scripts are typically set to be applied in one of 4 places, Startup, Shutdown, Login, or Logoff. Login and Logoff are typically used for user based settings, Software is assigned to the computer so Startup and Shutdown are the more common options, specifically, Startup.

The primary difference between a GPO MSI install and a script based install is where you configure the policy. The settings can be in the same policy as you might use to deploy a standard MSI package, but in a different section.

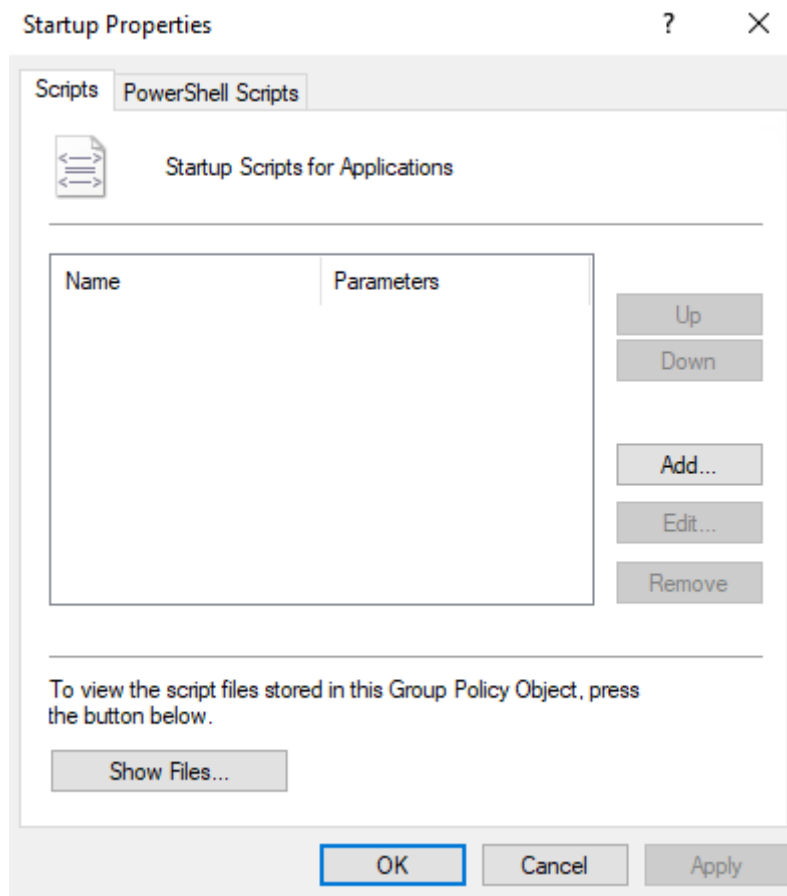


Step 1: As you can see this is still in the “Computer Configuration” section of the GPO but unlike standard MSI deployment which is located in the Computer Configuration – Policies - Software Settings section, the script based options is found under Computer Configuration – Windows Settings – Scripts (Startup/Shutdown). Software deployment is typically done through a startup script as opposed to a shutdown, though sometimes shutdown is better if it required the system to be rebooted after as is often the case in some applications.

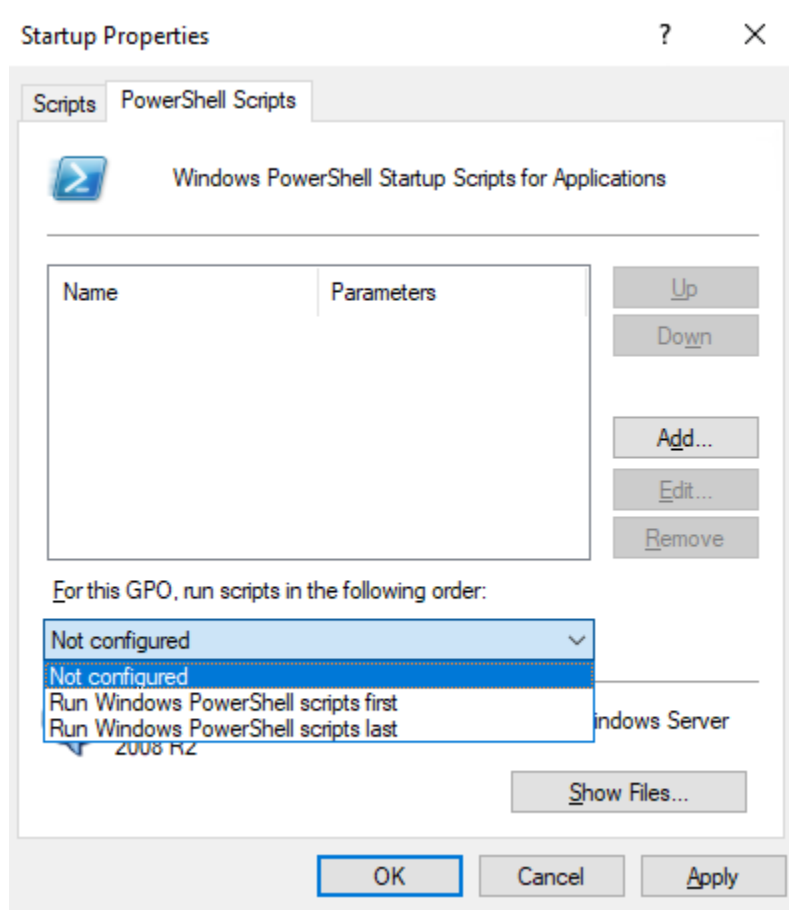
Step 2: To assign the script you right click the intended location, either startup or shutdown, and choose properties



The popup dialog gives you a number of options, to add or remove a script, or to change the script order which controls priority. Note that there is a separate tab for using powershell scripts versus other formats.



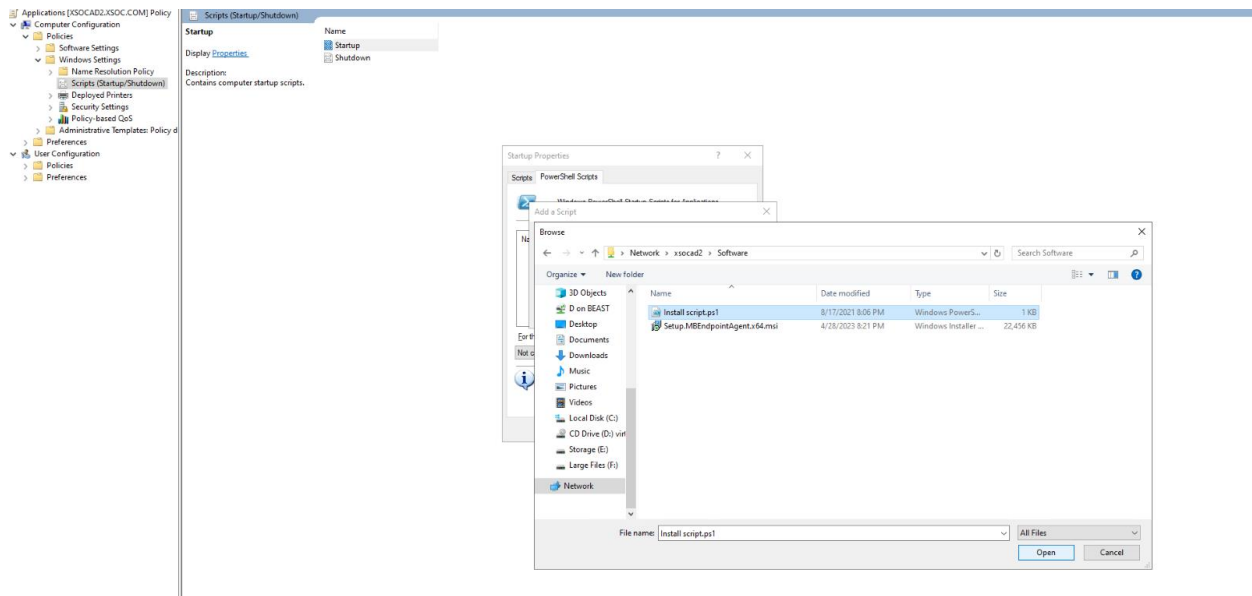
The PowerShell tab has an additional option to control the order, whether to prioritize PS scripts versus other formats. In general, you will want to do this if there are multiple formats of scripts being used.



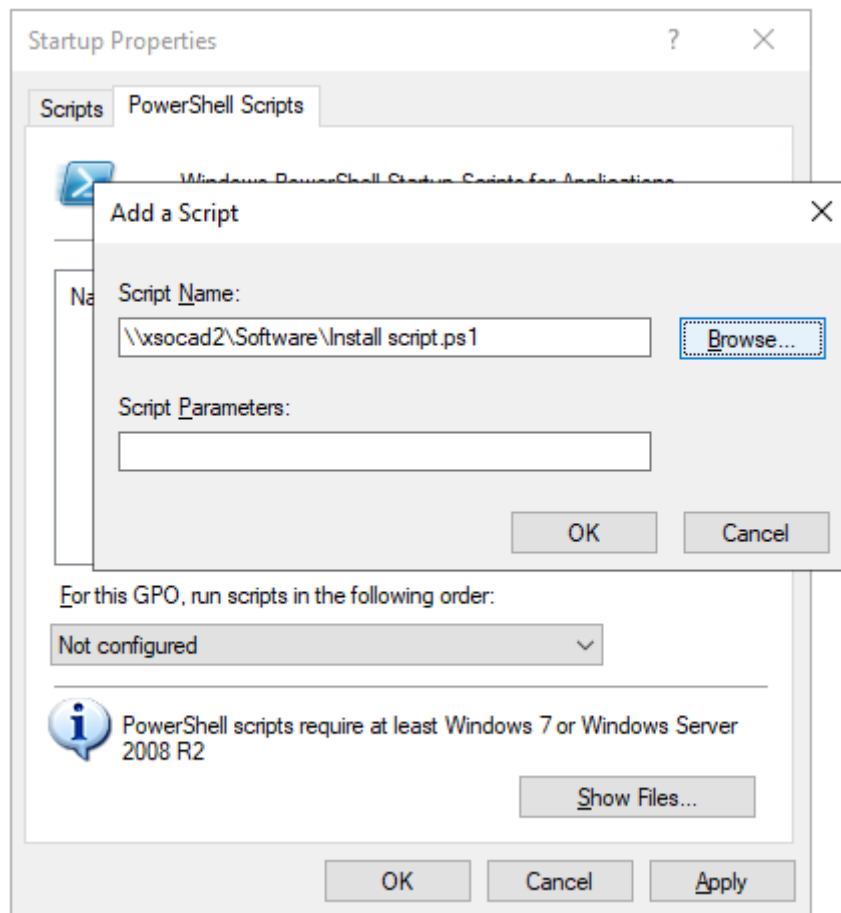
For this example we will be using a powershell script or *.ps1 file

Step 3: To add this, we select the "Add" button on the right-hand side and navigate to the network share hosting the required files.

Step 4: We select the intended scripts and choose the "Open" option in the bottom right corner.

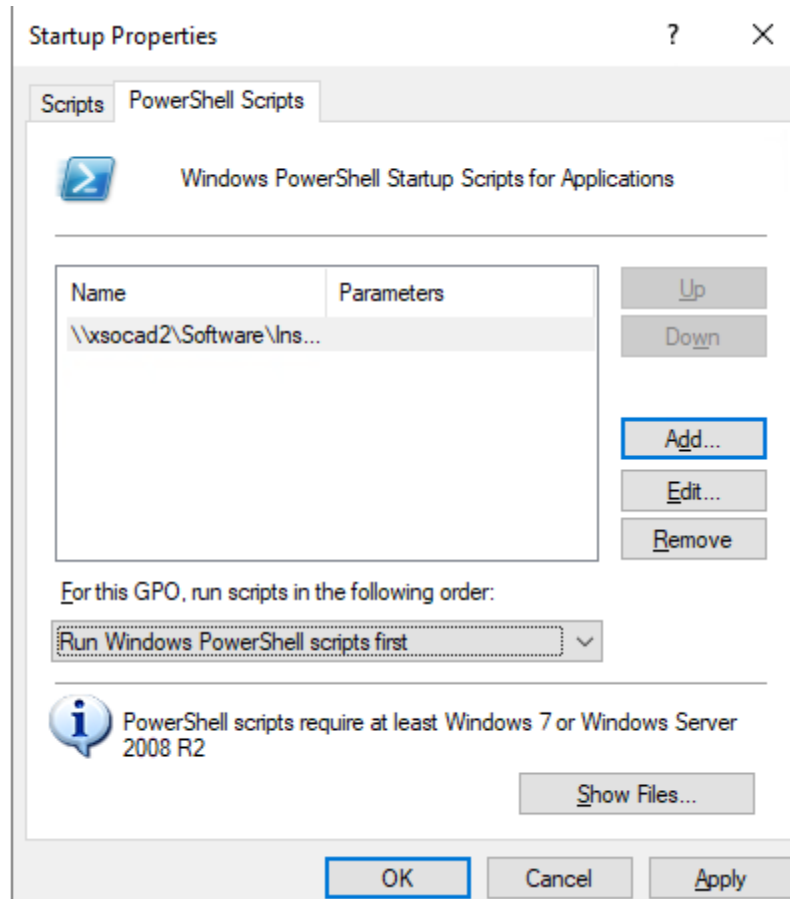


After choosing it you are still given one more opportunity to add any additional requires arguments though in most cases these will be contained within the script.



Step 5: To finalize the choice you select the “OK” button and the script will appear with the properties box.

Step 6: To apply the settings, choose your options on execution order and click OK to apply to the GPO



Step 7: The next time the computer is restarted the policy will apply and the application will be installed based on the settings contained in the script file.

Step 8: Confirm with XeneX when you have completed this by emailing Support@xenexsupport.com.

Step 9: We will get back to you confirming that the hosts have gotten their installations.