Set up Sysmon

1.) Download Sysmon from https://download.sysinternals.com/files/Sysmon.zip
The below PowerShell commands can be used to accomplish this task when executed on a Primary Domain Controller

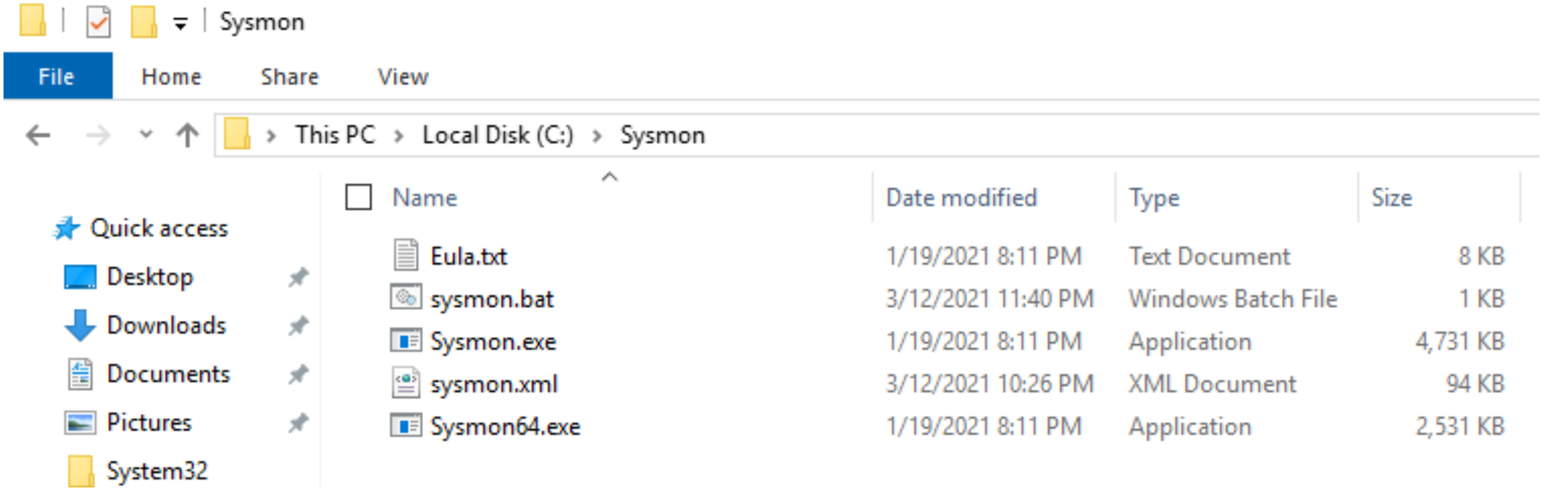
```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
(New-Object -TypeName System.Net.WebClient).downloadFile("https://download.sysinternals.com/files/Sysmon.zip", "$env:USERPROFILE\Downloads\Sysmon.zip")
Expand-Archive -Path "$env:USERPROFILE\Downloads\Sysmon.zip" -Destination "C:\Sysmon\"
```

2.) The above commands will extract the downloaded **sysmon.zip** file to **C:\Sysmon**
We next need a **sysmon.bat** file that will be added to group policy to install the sysmon logging on domain joined devices.
We also need a **sysmon.xml** file that contains a sysmon logging configuration

This **sysmon.bat** file can be downloaded and modified to fit your environment using the below commands
NOTE: We are also creating a network share with these commands to host the sysmon install files and disabling SMBv1 for security reasons

```
$DomainObj = [System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain()
$PrimaryDC = ($DomainObj.PdcRoleOwner).Name
$Domain = $DomainObj.Forest.Name
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Sysmon/sysmon.xml" -OutFile "C:\Sysmon\sysmon.xml"
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Sysmon/sysmon.bat" -OutFile "C:\Sysmon\sysmon.bat"
(Get-Content -Path "C:\Sysmon\sysmon.bat") -Replace "DomainControllerHostname", "$PrimaryDC" -Replace "NETLOGON", "Sysmon" | Set-Content -Path "C:\Sysmon\sysmon.bat"
New-SmbShare -Name "Sysmon" -Path "C:\Sysmon" -FullAccess "$Domain\Domain Admins","Administrators" -ChangeAccess "Users"
Set-SmbServerConfiguration -EnableSMB1Protocol $False -Force
Set-SmbServerConfiguration -EnableSMB2Protocol $True -Force
```

SCREENSHOT EVIDENCE OF DIRECTORY CONTENTS

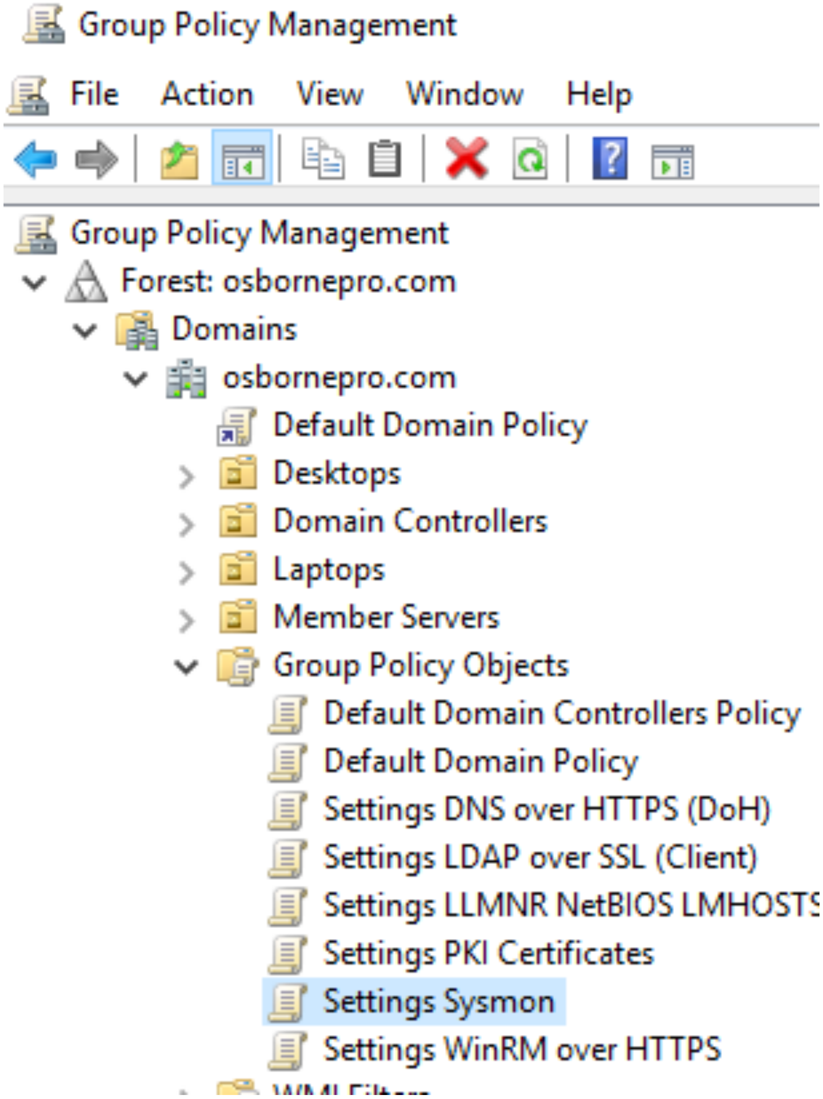


Name	Date modified	Type	Size
Eula.txt	1/19/2021 8:11 PM	Text Document	8 KB
sysmon.bat	3/12/2021 11:40 PM	Windows Batch File	1 KB
Sysmon.exe	1/19/2021 8:11 PM	Application	4,731 KB
sysmon.xml	3/12/2021 10:26 PM	XML Document	94 KB
Sysmon64.exe	1/19/2021 8:11 PM	Application	2,531 KB

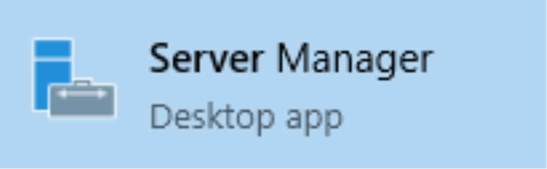
3.) With the above all done on our primary domain controller we can create a blank group policy template to edit for Sysmon
This can be done with the below command

```
New-GPO -Name "Settings Sysmon" -Domain $Domain -
Comment "Group policy object used to get sysmon installed on domain joined devices"
```

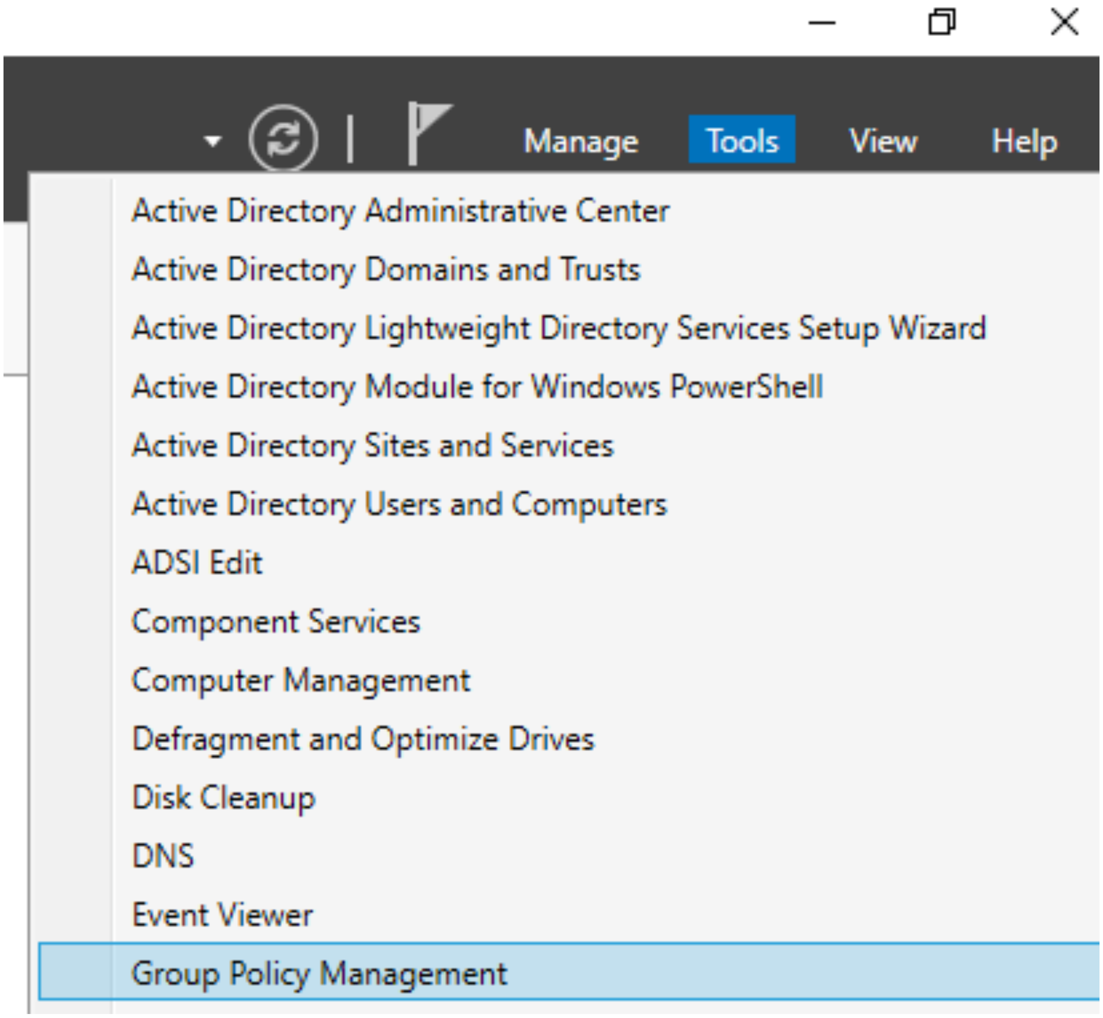
SCREENSHOT EIVDENCE OF CREATED GPO



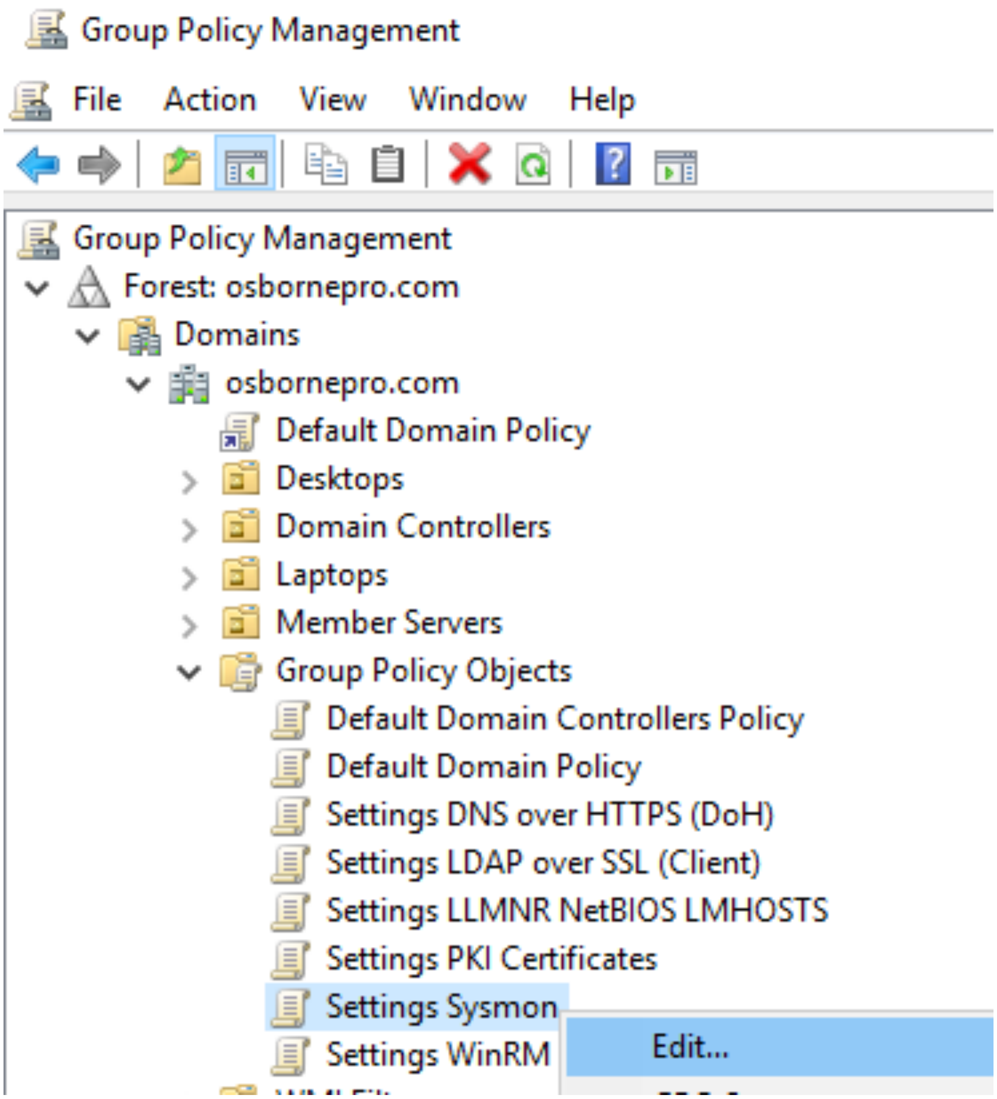
4.) Now we are going to modify that policy so it first creates a Startup script
Open Server Manager



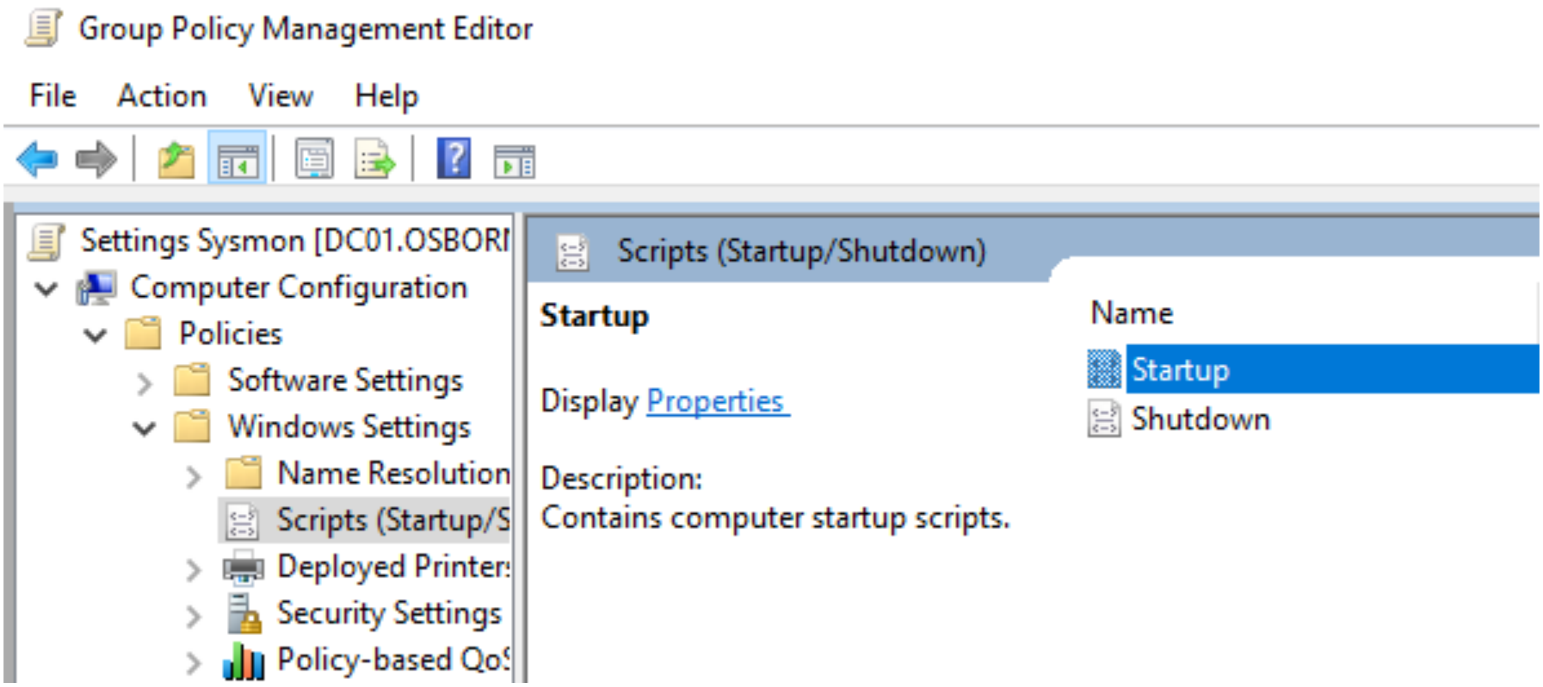
Go to **Tools** > **Group Policy Management**


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Lightweight Directory Services Setup Wizard
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management

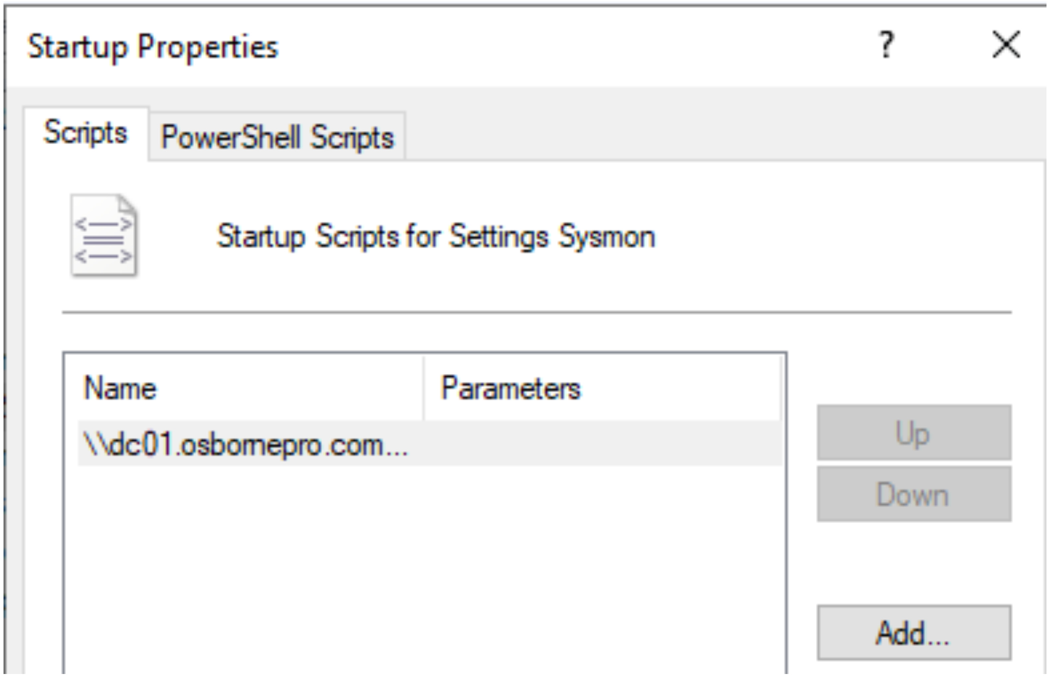
The '**Group Policy Management**' Window will open. Expand '**Forest: $Domain**' > Expand '**Domains**' > Expand '**$Domain**' > Expand '**Group Policy Objects**' > Right click on '**Settings Sysmon**' and select **Edit**



Navigate the dropdowns from '**Computer Management**' > '**Policies**' > '**Windows Settings**' > '**Scripts**' > and Double Click '**Startup**' to open the '**Startup Properties' Window**"



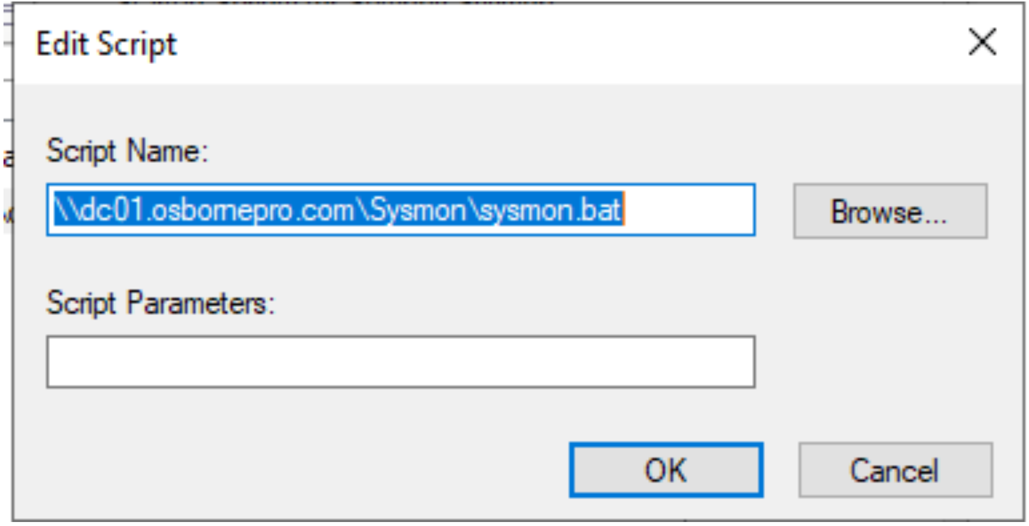
With the 'Scripts' tab selected click the 'Add' button.



Startup Scripts for Settings Sysmon

Name	Parameters
\\dc01.osbornepro.com...	

In the '**Script Name**' text box enter your network share path to sysmon.bat which is most likely '**\\$PrimaryDC.$Domain\Sysmon\sysmon.bat**'. Leave the '**Parameters**' text box blank"



Script Name: \\dc01.osbornepro.com\Sysmon\sysmon.bat

Script Parameters:

Click OK and then click OK again.

Malicious IP Checker GPO Task

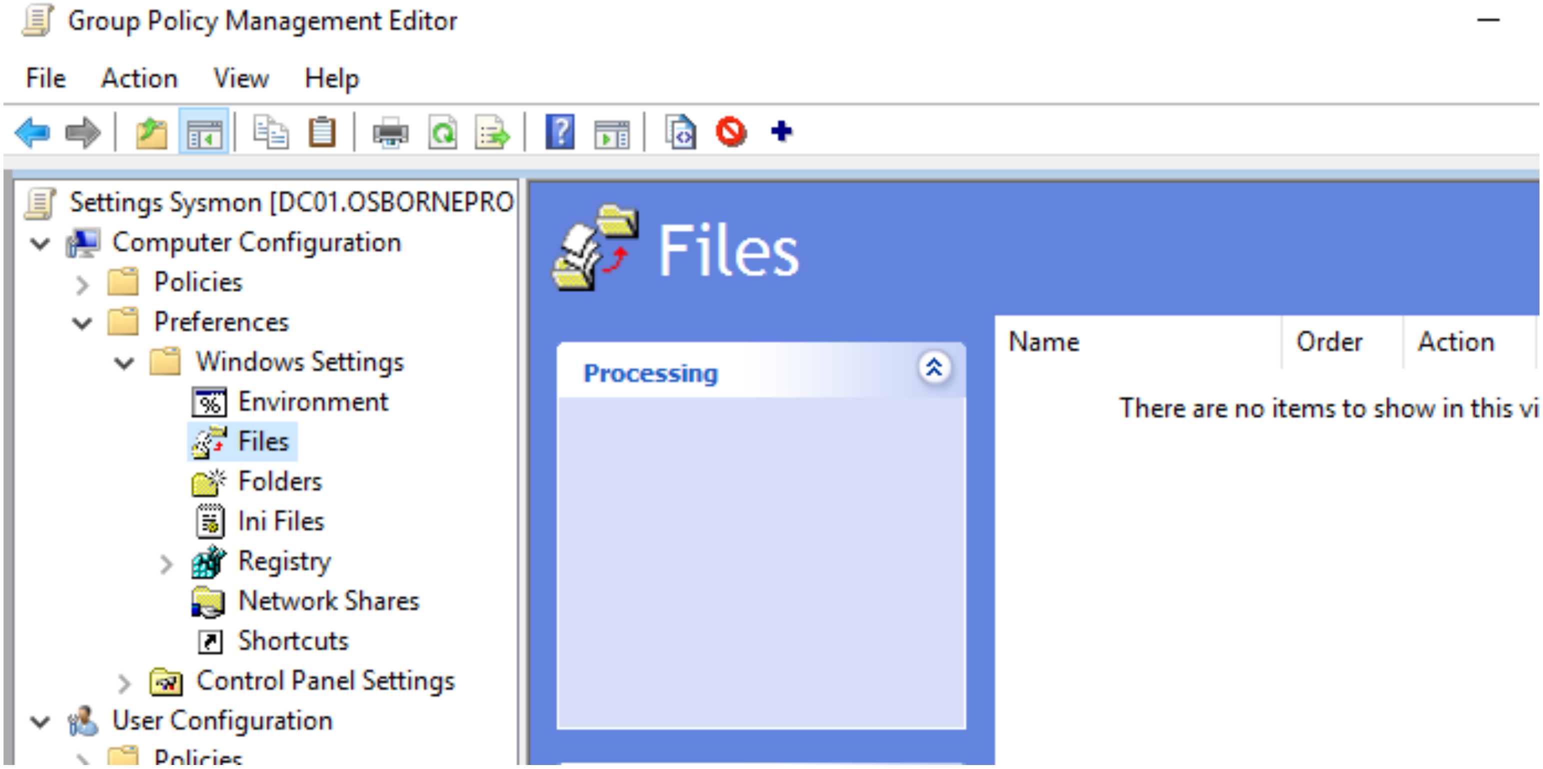
With the '**Group Policy Management Editor**' still open we are now going to cover making a task for Malicious IP Checker

If you have not already, download HashValidator.ps1 to your primary domain controller. This can be done using the below command

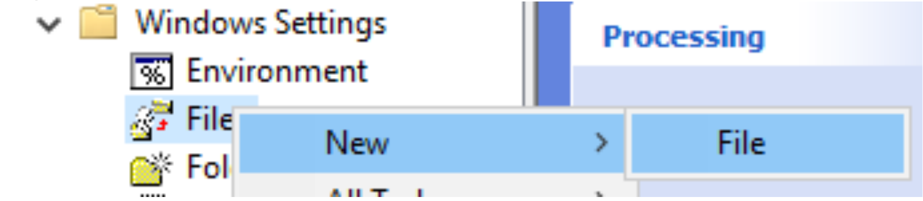
```
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Sysmon/MaliciousIPChecker.ps1" -OutFile "C:\Sysmon\MaliciousIPChecker.ps1"
```

GPO THAT DISTRIBUTES THE MALICIOUS IP CHECKER SCRIPT RUN BY TASK SCHEDULER

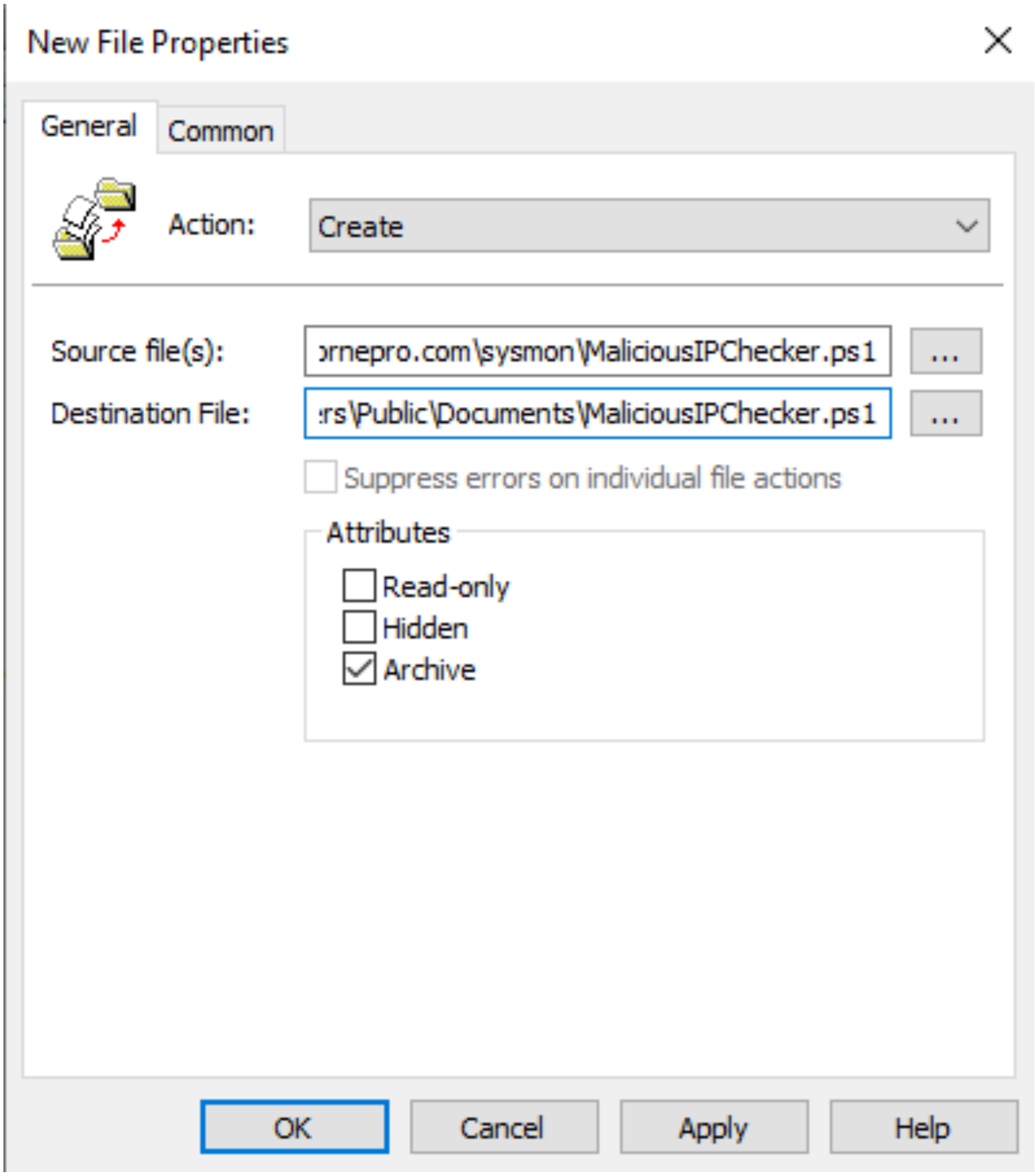
Navigate to '**Computer Configuration**' > '**Preferences**' > '**Windows Settings**' > '**Files**'



Right click '**Files**' and select '**New**' > '**File**'



A "**New File Properties**" window will pop up. Enter the below info
ACTION: Create
SOURCE FILES: \\YourPrimaryDCHere.Domain.com\sysmon\MaliciousIPChecker.ps1
DESTINATION FILES: C:\Users\Public\Documents\MaliciousIPChecker.ps1



Action: Create

Source file(s): ɔrnepro.com\sysmon\MaliciousIPChecker.ps1

Destination File: :rs\Public\Documents\MaliciousIPChecker.ps1

□ Suppress errors on individual file actions

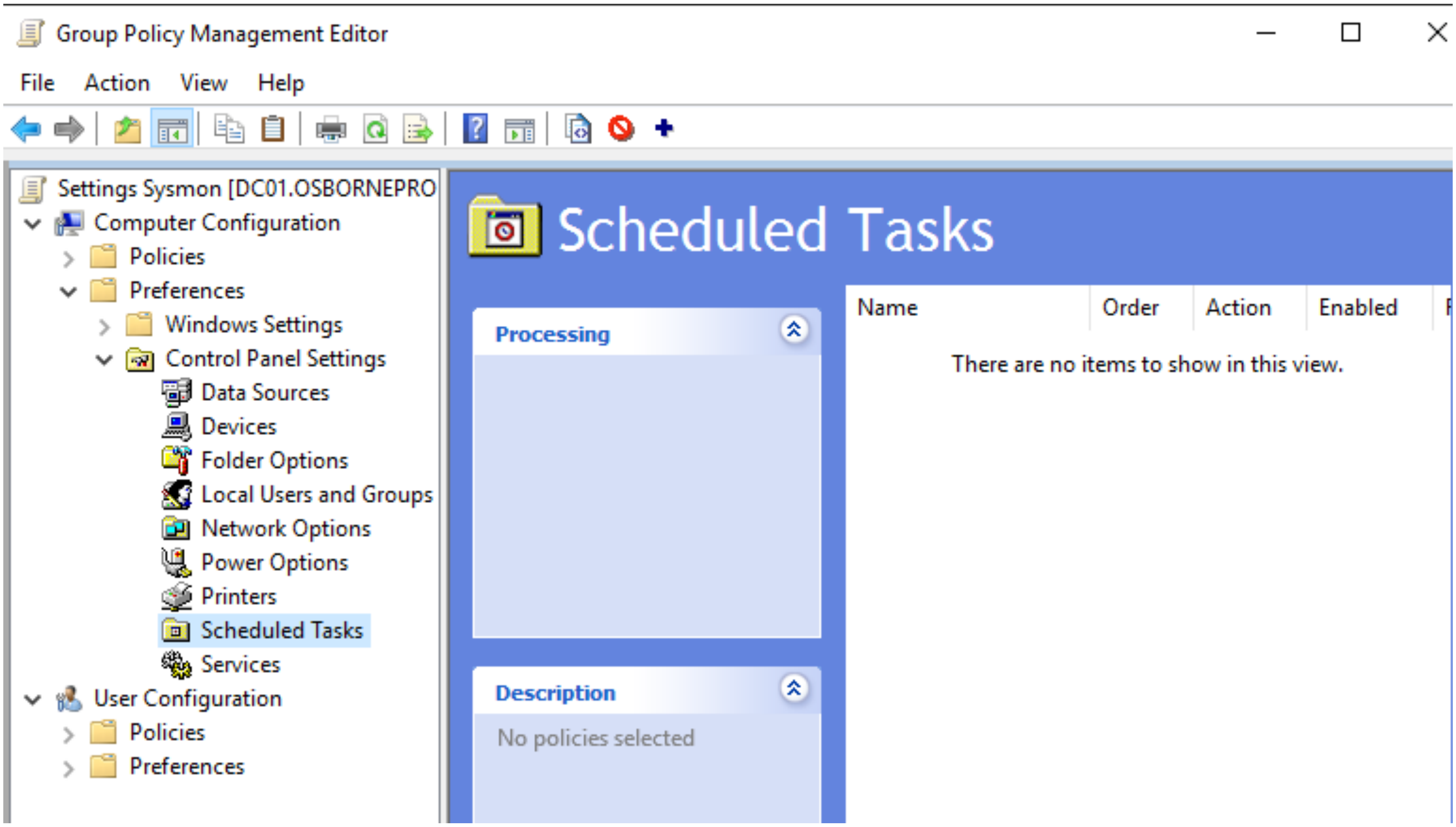
Attributes

□ Read-only
□ Hidden
☑ Archive

Then Click **OK**

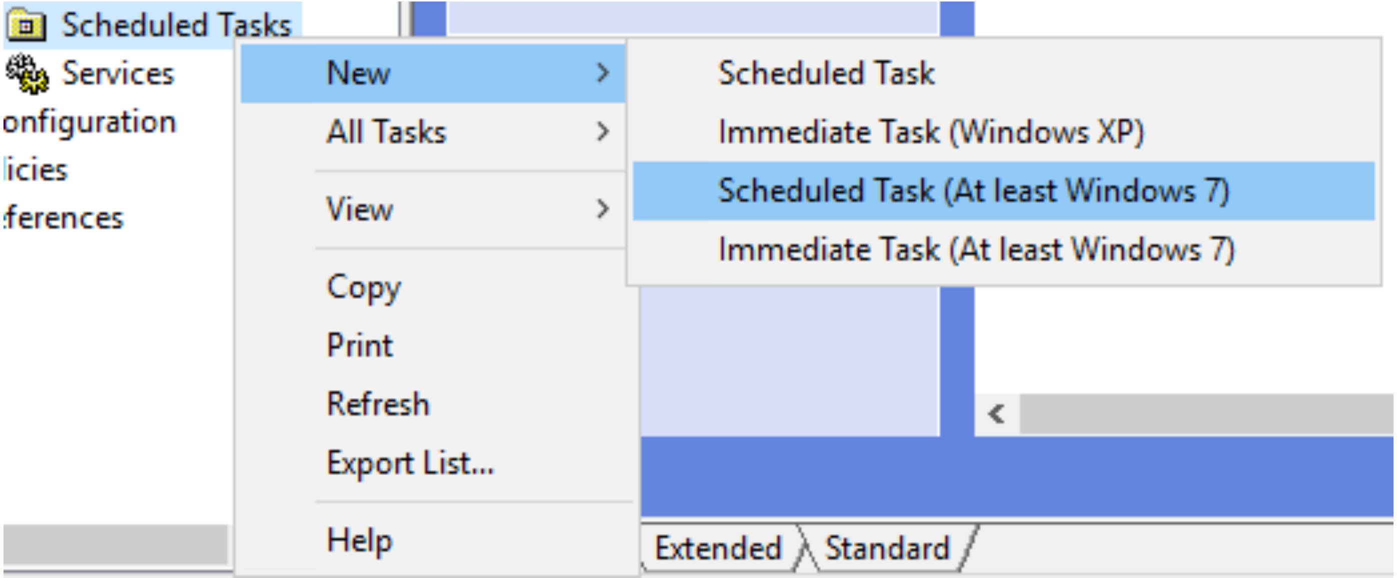
GPO THAT CREATES THE SCHEDULED TASK TO RUN MALICIOUS IP CHECKER

Navigate to '**Computer Configuration**' > '**Preferences**' > '**Control Panel Settings**' > '**Scheduled Tasks**'

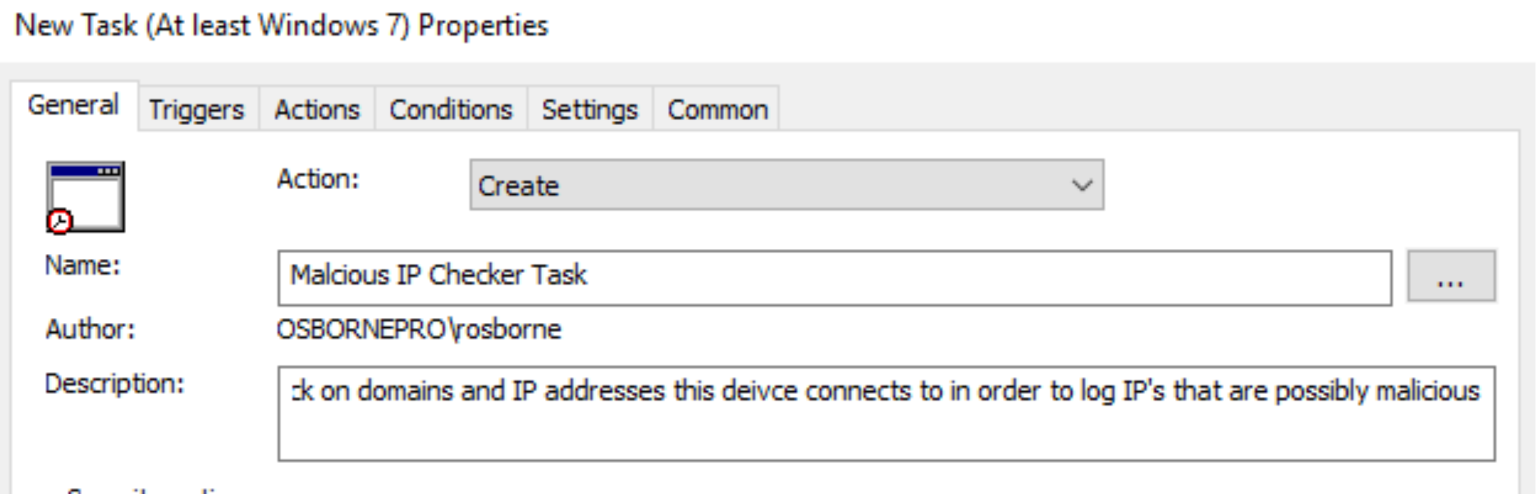


There are no items to show in this view.

Right click on ‘**Scheduled Tasks**’ and select ‘**New**’ > ‘**Scheduled Task (At least Windows 7)**’



Set the below values
ACTION: Create
NAME: Malicious IP Checker Task
DESCRIPTION: Runs a check on domains and IP addresses this device connects to in order to log IP's that



New Task (At least Windows 7) Properties

Action: Create

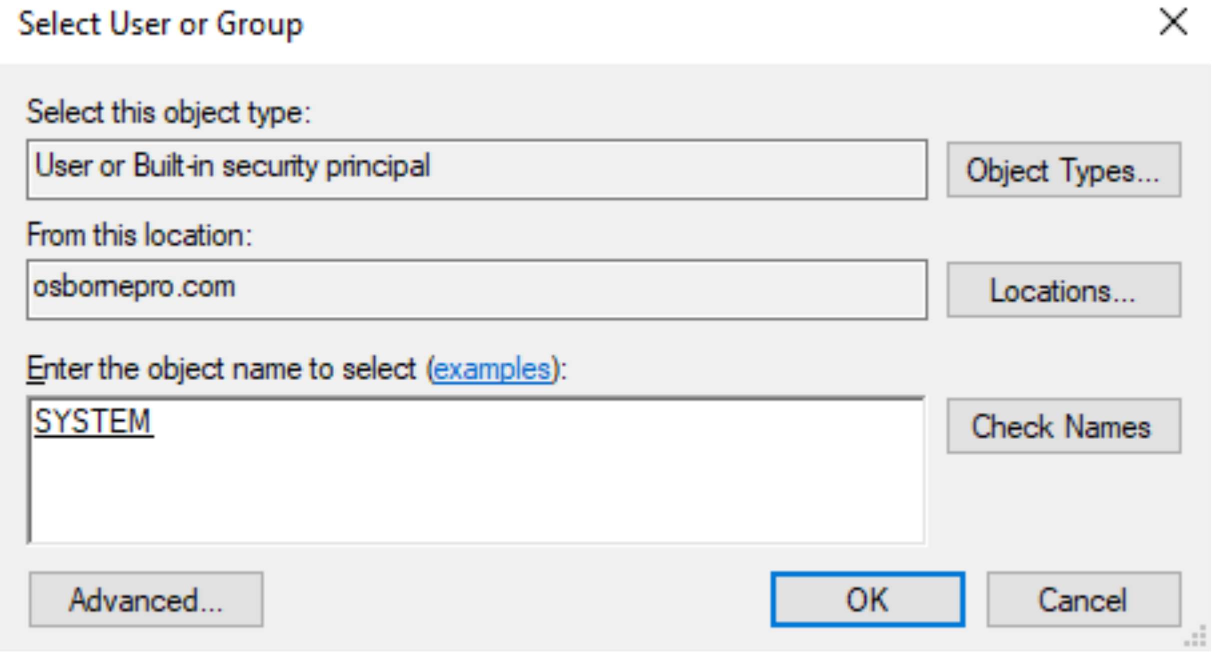
Name: Malcious IP Checker Task

Author: OSBORNEPRO\rosborne

Description: :k on domains and IP addresses this deivce connects to in order to log IP's that are possibly malicious

Click the “Change User or Group” button

In the window that pops up type SYSTEM and click CHECK NAMES then click OK



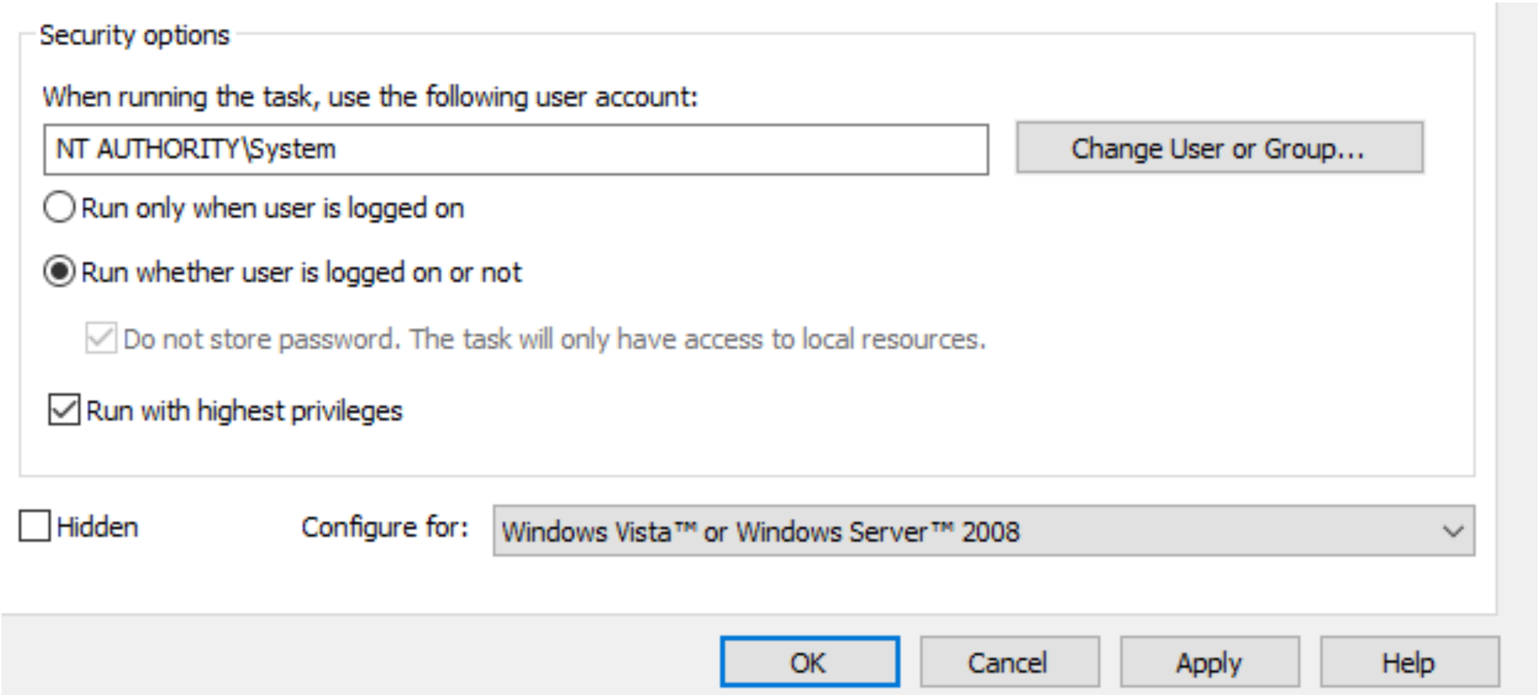
Select User or Group

Select this object type: User or Built-in security principal

From this location: osbornepro.com

Enter the object name to select (examples): SYSTEM

Select the “Run whether user is logged on or not” button
Tick the “Run with highest privileges” button



Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

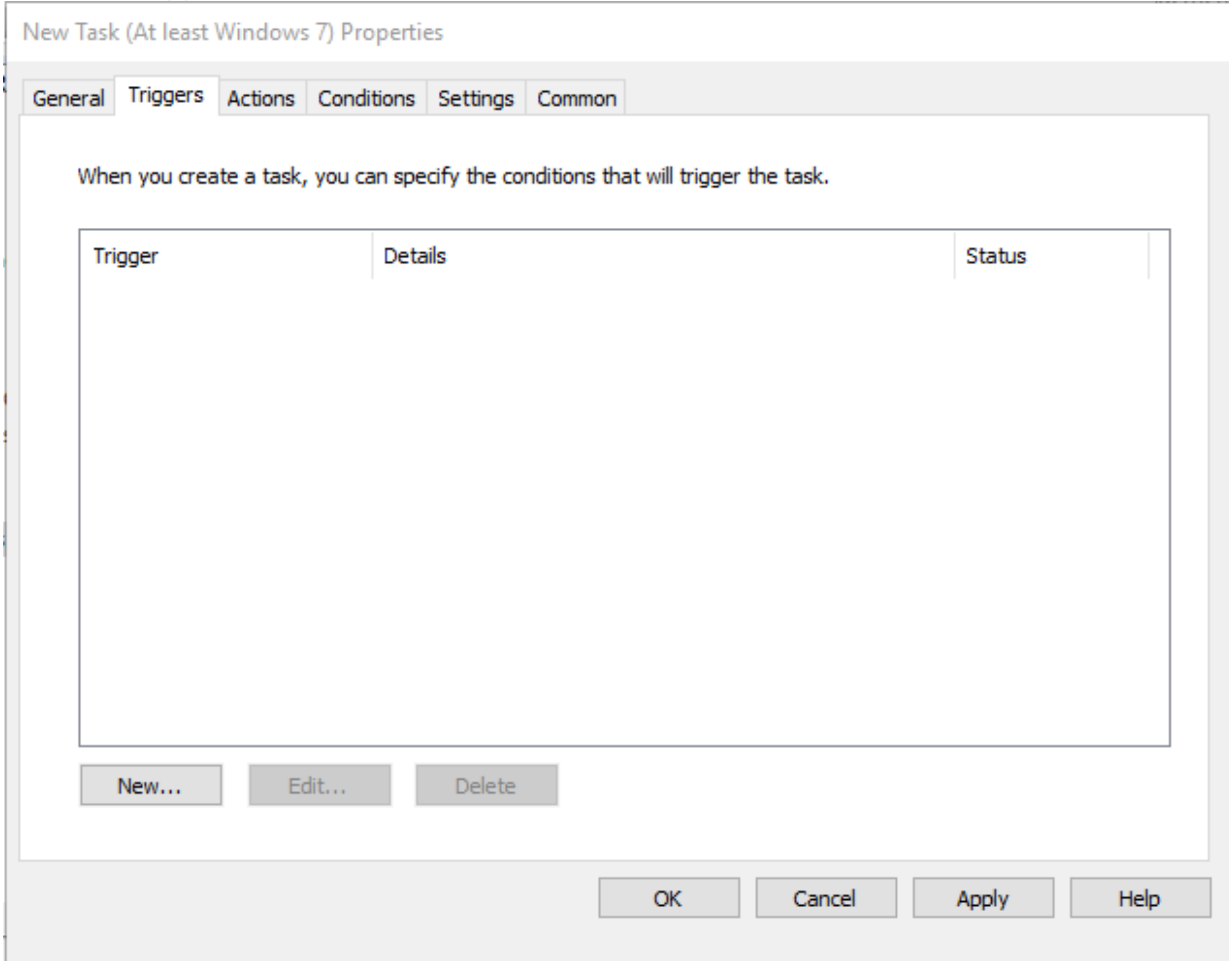
☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™ or Windows Server™ 2008

Under the **Triggers** tab click the **New** button

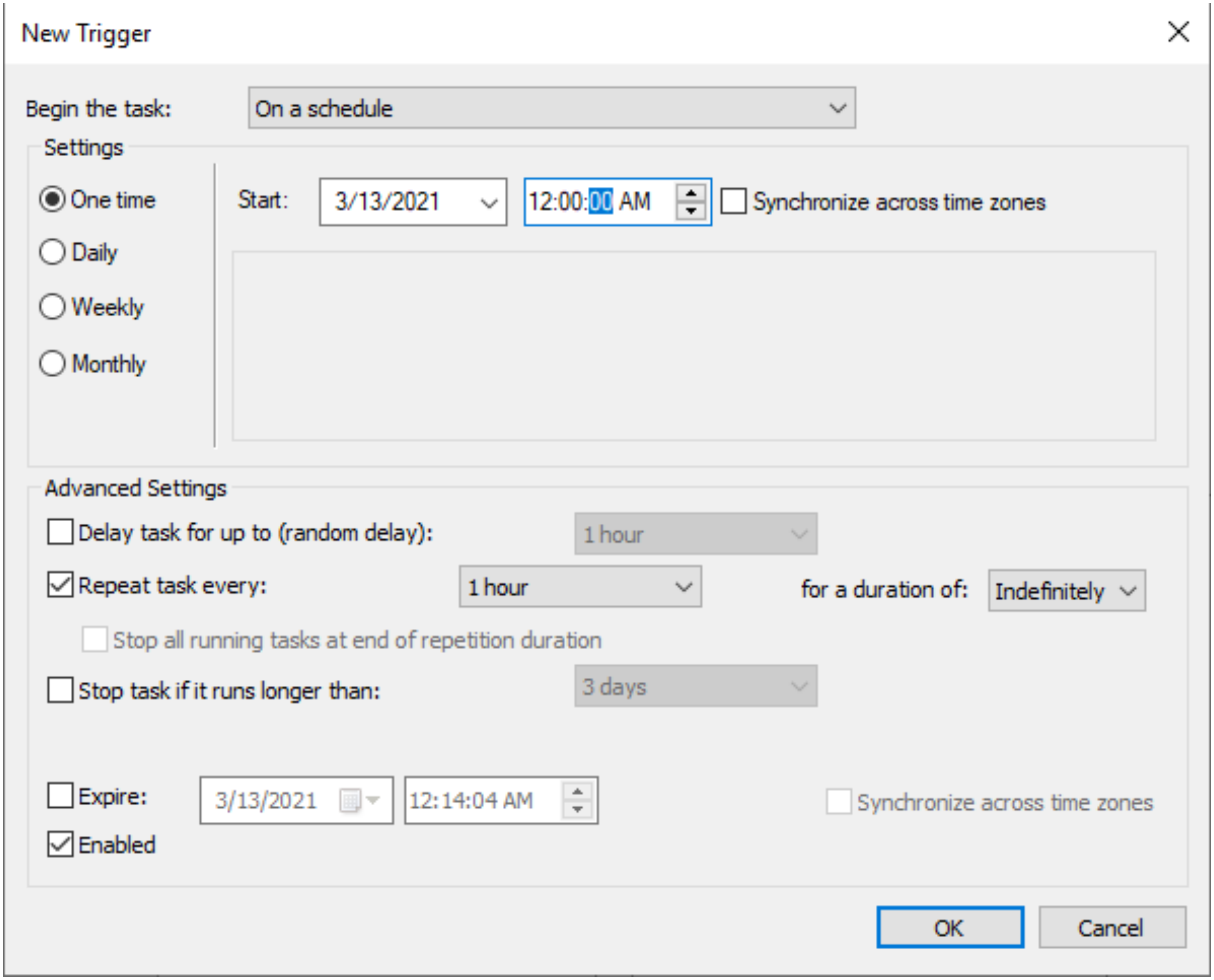


New Task (At least Windows 7) Properties

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status

Set the below values for “On a Schedule” and click OK. This is to run the task once an hour forever



New Trigger

Begin the task: On a schedule

Settings

● One time
○ Daily
○ Weekly
○ Monthly

Start: 3/13/2021 12:00:00 AM □ Synchronize across time zones

Advanced Settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 1 hour for a duration of: Indefinitely

□ Stop all running tasks at end of repetition duration

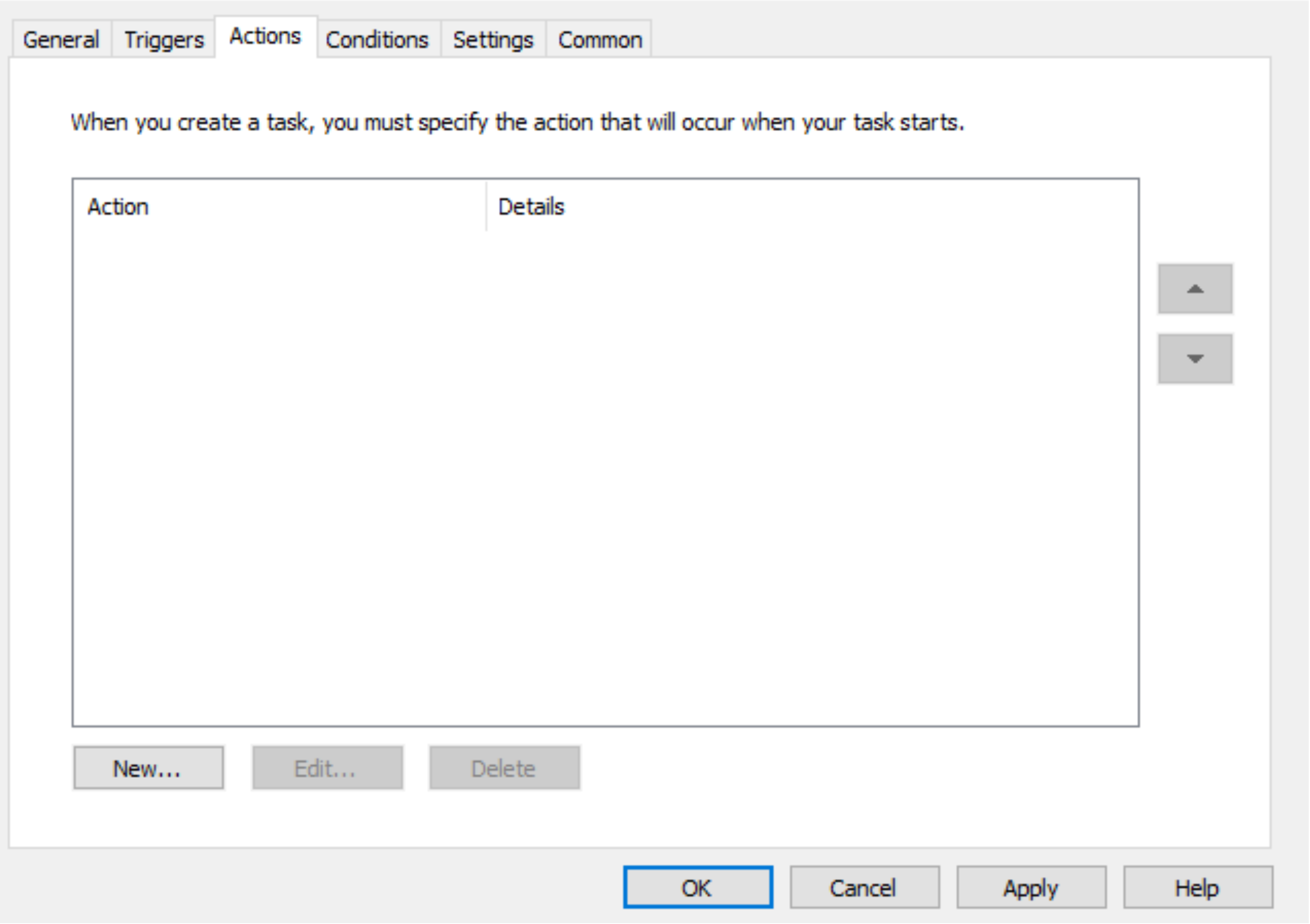
□ Stop task if it runs longer than: 3 days

□ Expire: 3/13/2021 12:14:04 AM □ Synchronize across time zones

☑ Enabled

In the **Actions** tab click the **New** button

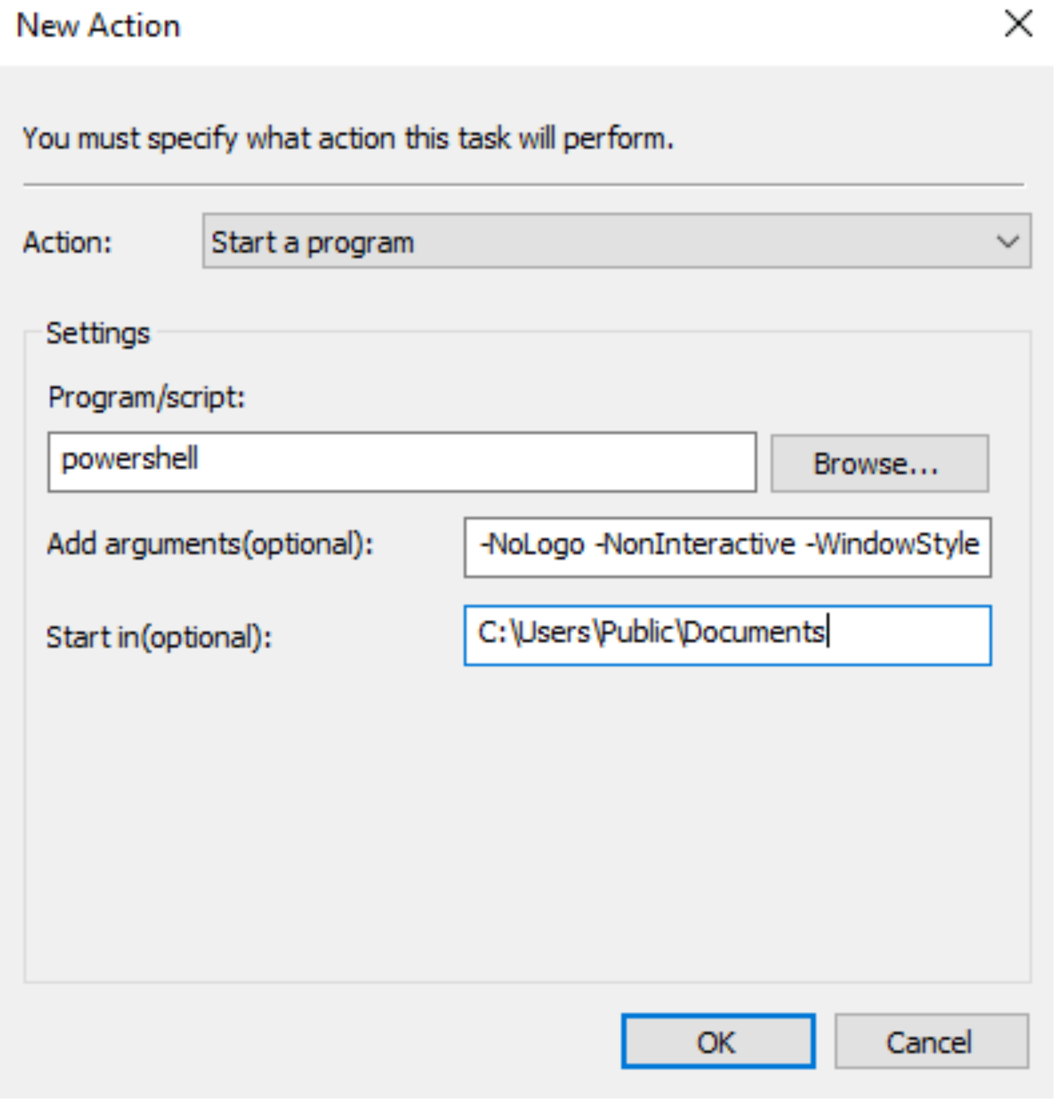
New Task (At least Windows 7) Properties



When you create a task, you must specify the action that will occur when your task starts.

Action	Details

Set the following values and click **OK**
ACTION: Start a program
PROGRAM/SCRIPT: powershell
ADD ARGUMENTS: -NoLogo -NonInteractive -WindowStyle Hidden .\MaliciousIPChecker.ps1
START IN: C:\Users\Public\Downloads



New Action

You must specify what action this task will perform.

Action: Start a program

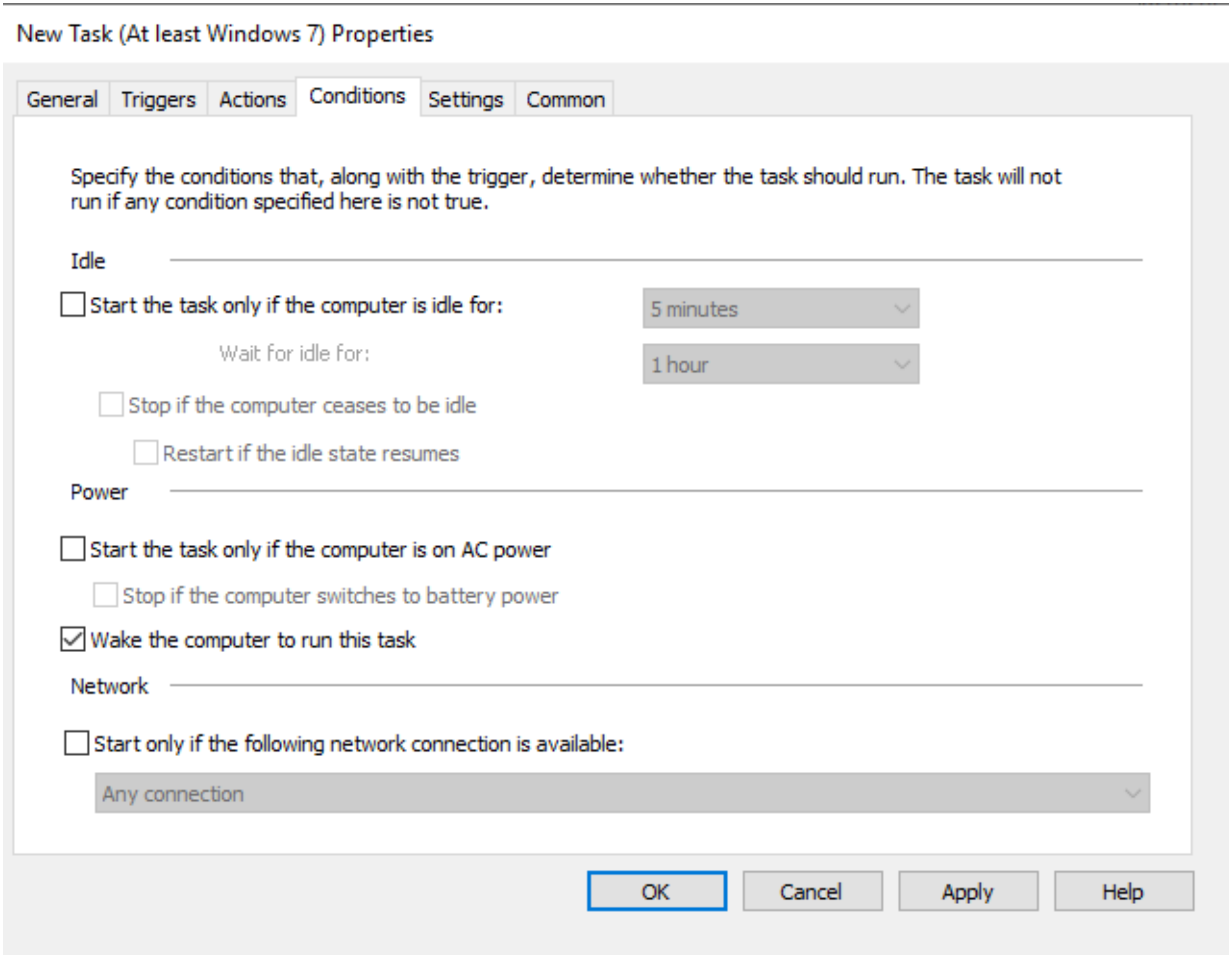
Settings

Program/script: powershell

Add arguments(optional): -NoLogo -NonInteractive -WindowStyle

Start in(optional): C:\Users\Public\Documents

Under the **Conditions** tab select “**Wake the Computer to run this task**”



Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 5 minutes

Wait for idle for: 1 hour

□ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

□ Start the task only if the computer is on AC power

□ Stop if the computer switches to battery power

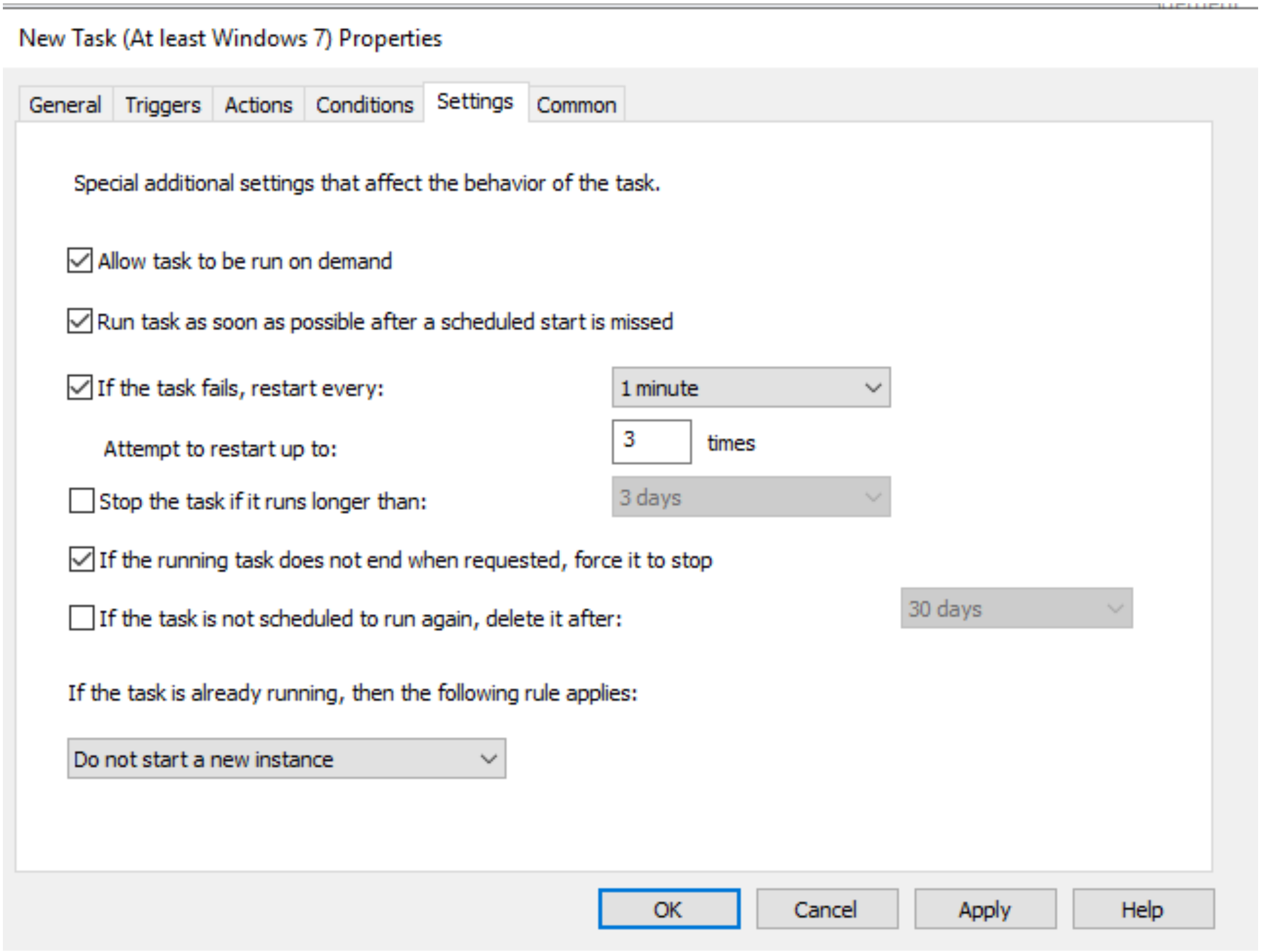
☑ Wake the computer to run this task

Network

□ Start only if the following network connection is available:

Any connection

Under the **Settings** tab select the below values
- Allow task to be run on demand
- Run task as soon as possible after a scheduled start is missed
- If the task fails restart every 1 minute up to 3 times
- If the running task does not end when requested force it to stop
- Do not start a new instance



Special additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☑ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

□ Stop the task if it runs longer than: 3 days

☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

Then click **OK**

Hash Validator GPO Task

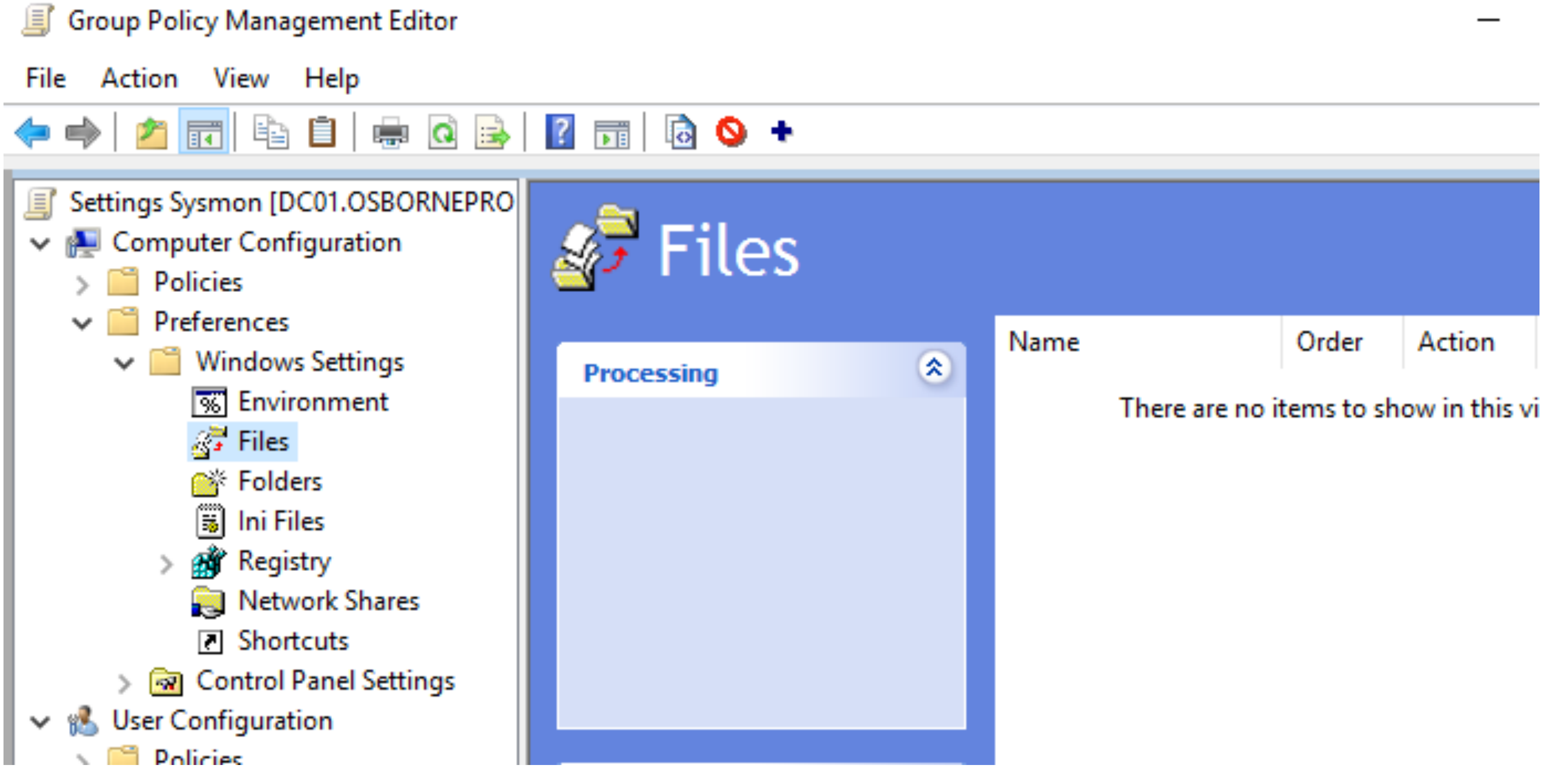
With the ‘**Group Policy Management Editor**’ still open we are now going to cover making a task for Malicious IP Checker

If you have not already, download HashValidator.ps1 to your primary domain controller. This can be done using the below command

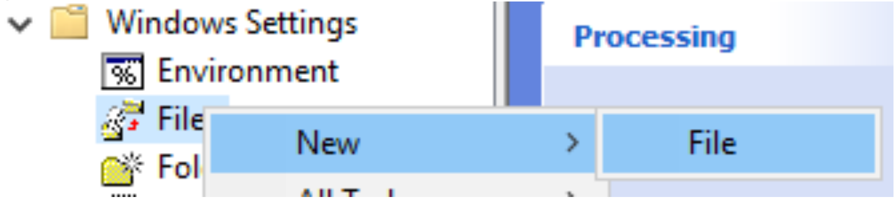
```
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/tobor88/BTPS-SecPack/master/Sysmon/HashValidator.ps1" -OutFile "C:\Sysmon\HashValidator.ps1"
```

GPO THAT DISTRIBUTES THE MALICIOUS IP CHECKER SCRIPT RUN BY TASK SCHEDULER

Navigate to ‘**Computer Configuration**’ > ‘**Preferences**’ > ‘**Windows Settings**’ > ‘**Files**’

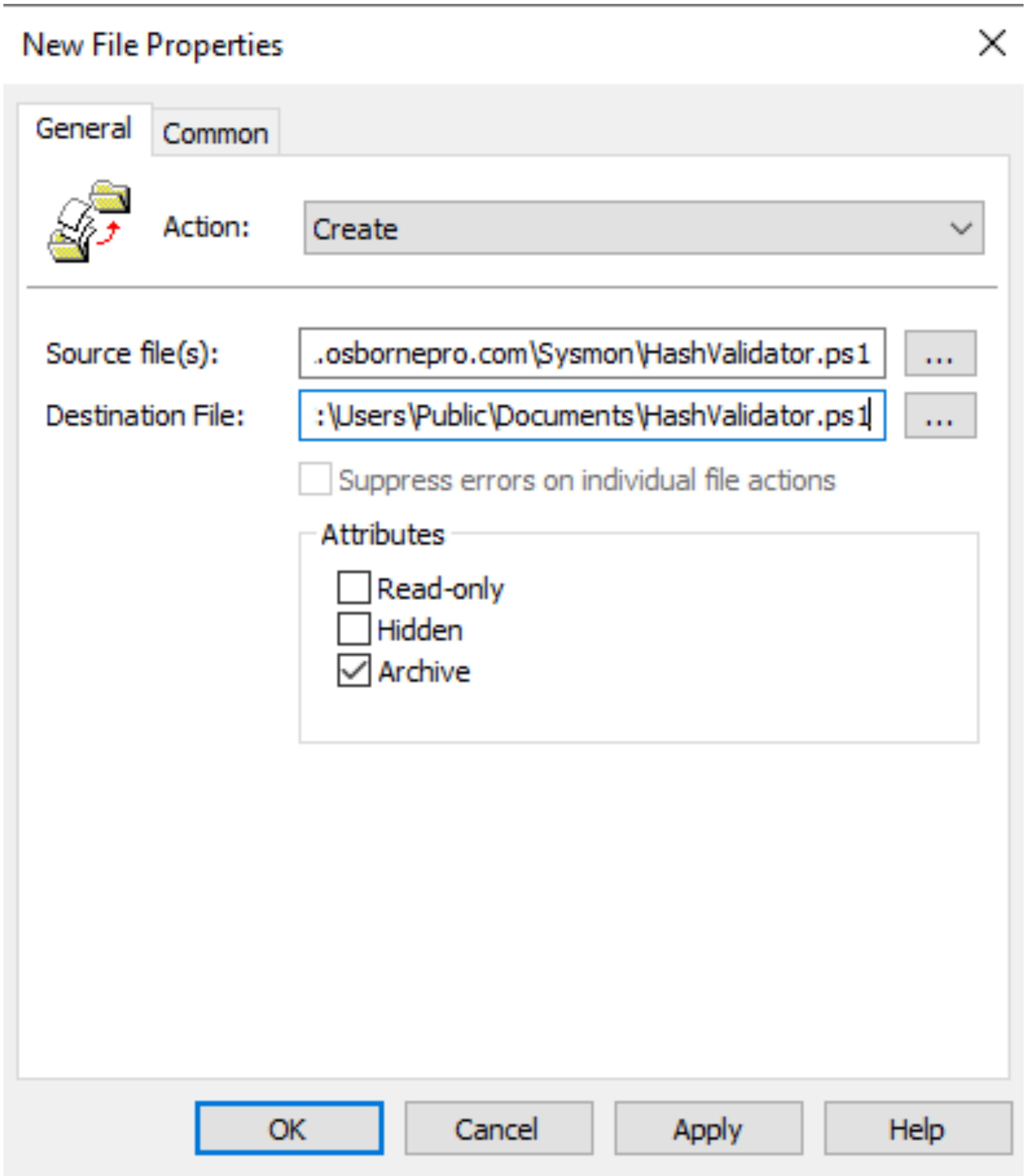


Right click '**Files**' and select ‘**New**’ > ‘**File**’



A “**New File Properties**” window will pop up. Enter the below info

ACTION: Create
SOURCE FILES: \\YourPrimaryDCHere.Domain.com\sysmon\HashValidator.ps1
DESTINATION FILES: C:\Users\Public\Documents\HashValidator.ps1



New File Properties

Action: Create

Source file(s): .osbornepro.com\Sysmon\HashValidator.ps1

Destination File: :\Users\Public\Documents\HashValidator.ps1

☐ Suppress errors on individual file actions

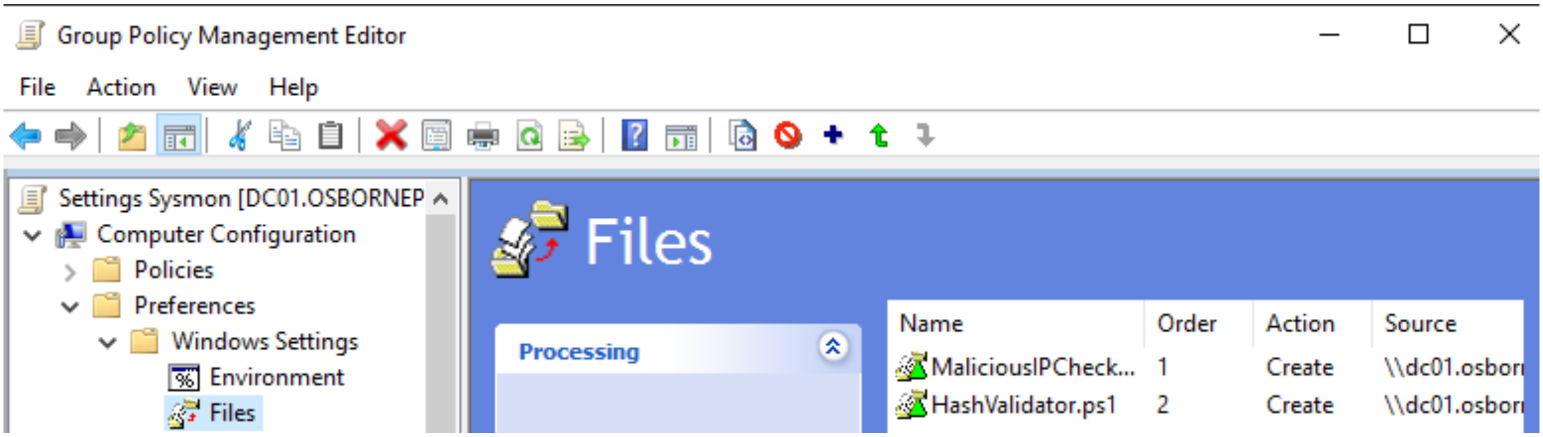
Attributes

☐ Read-only

☐ Hidden

☑ Archive

Then Click **OK**



Group Policy Management Editor

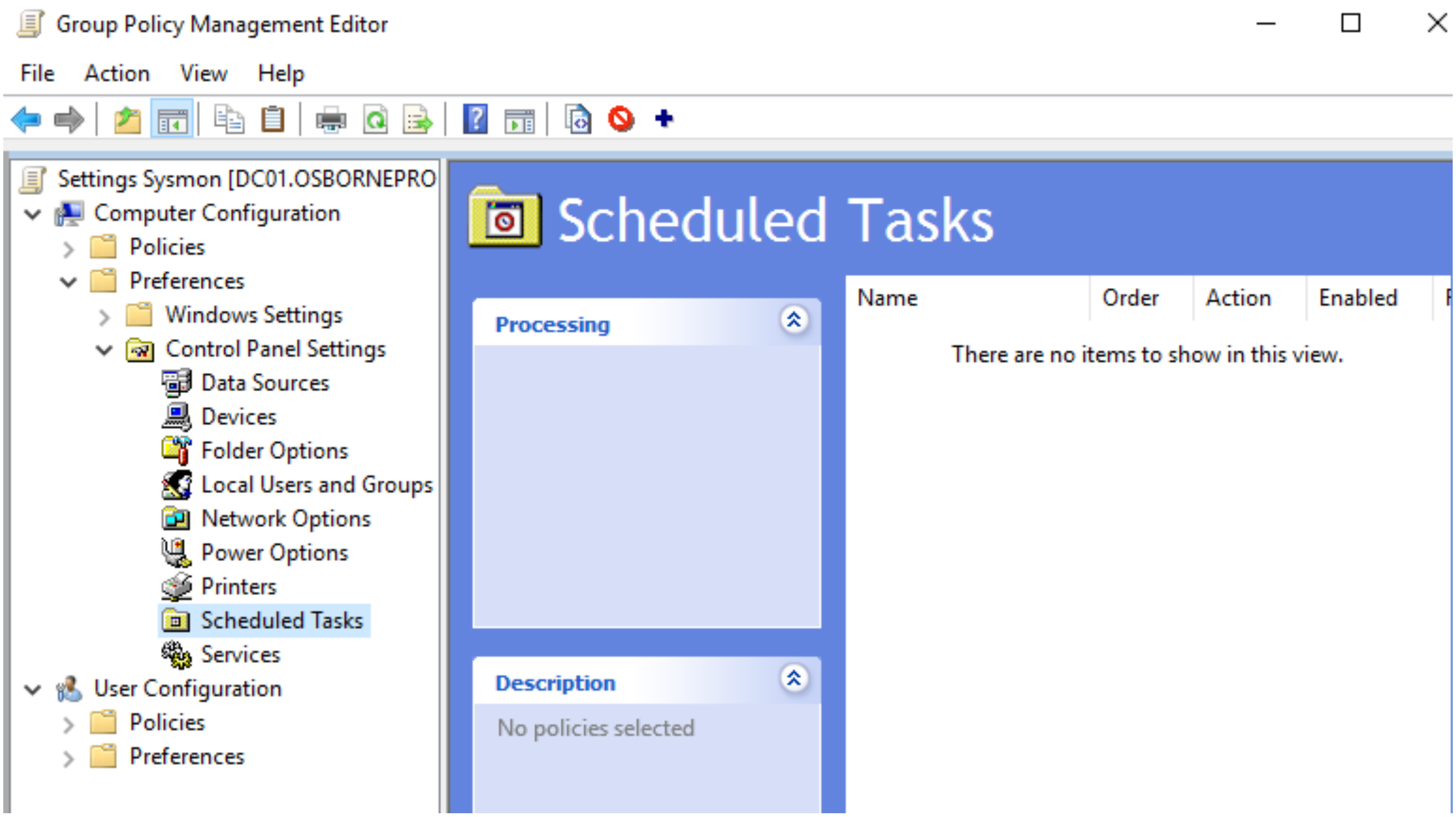
Settings Sysmon [DC01.OSBORNEP
Computer Configuration
Policies
Preferences
Windows Settings
Environment
Files

Name	Order	Action	Source
MaliciousIPCheck...	1	Create	\\dc01.osbor
HashValidator.ps1	2	Create	\\dc01.osbor

GPO THAT CREATES THE SCHEDULED TASK TO RUN MALICIOUS IP CHECKER

Navigate to ‘**Computer Configuration**’ > ‘**Preferences**’ > ‘**Control Panel Settings**’ > ‘**Scheduled**

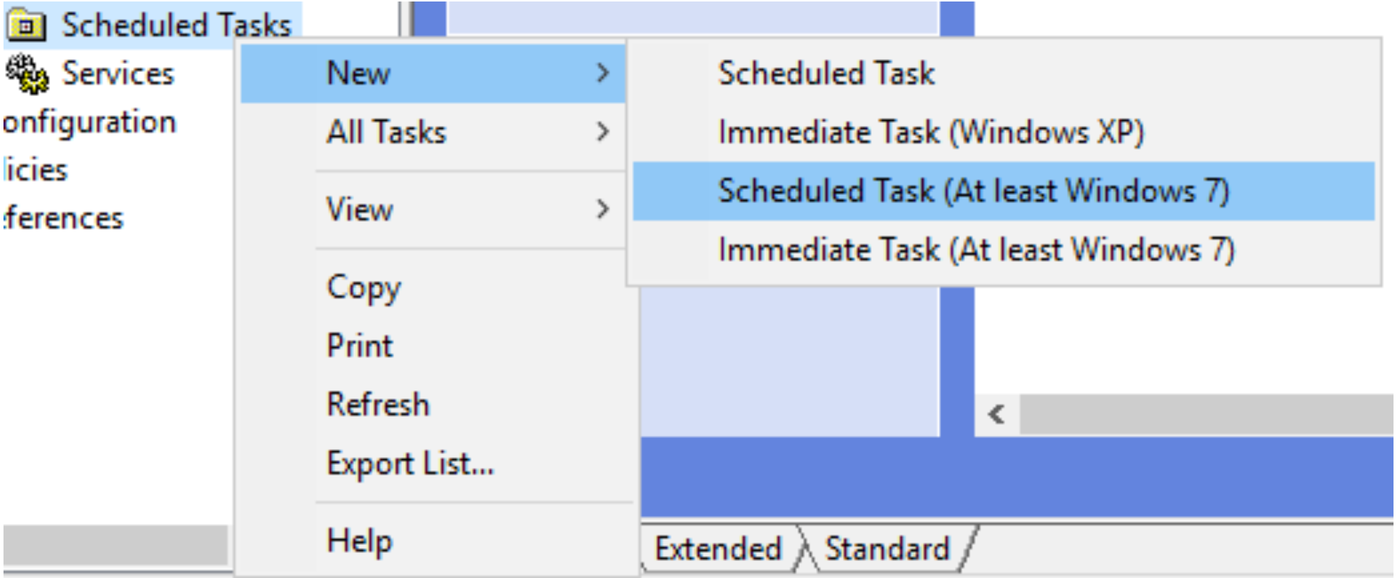
Tasks’



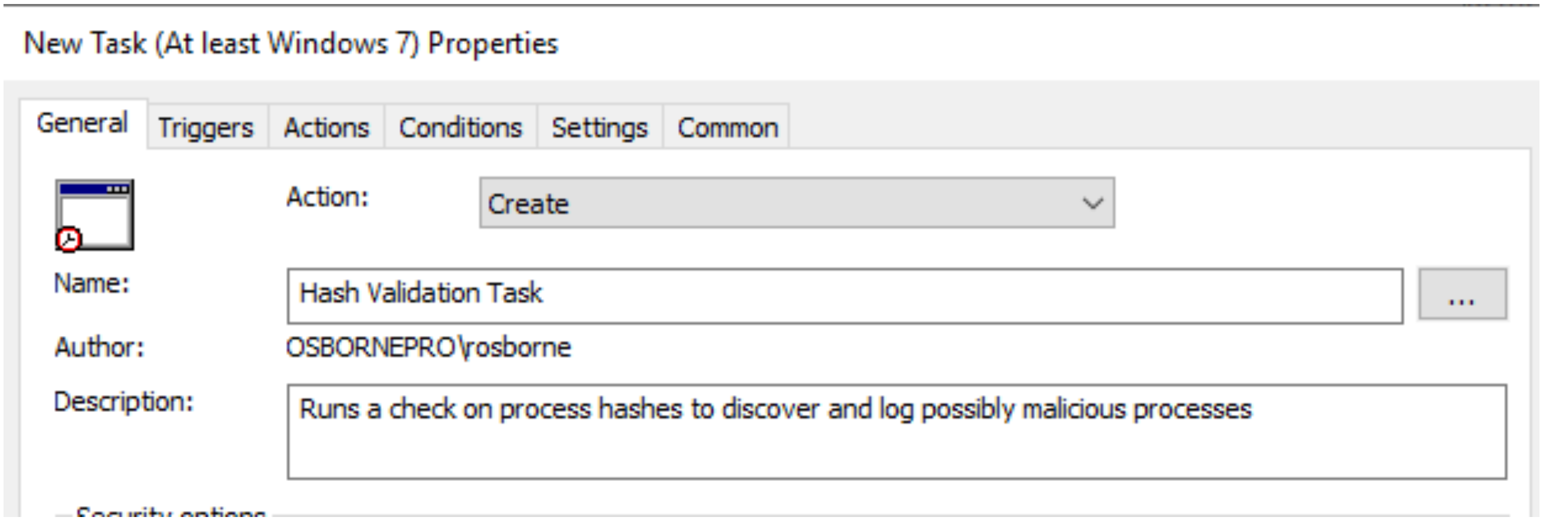
There are no items to show in this view.

No policies selected

Right click on ‘**Scheduled Tasks**’ and select ‘**New**’ > ‘**Scheduled Task (At least Windows 7)**’



Set the below values
ACTION: Create
NAME: Hash Validation Task
DESCRIPTION: Runs a check on process hashes to discover and log possibly malicious processes


New Task (At least Windows 7) Properties

Action: Create

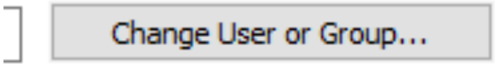
Name: Hash Validation Task

Author: OSBORNEPRO\rosborne

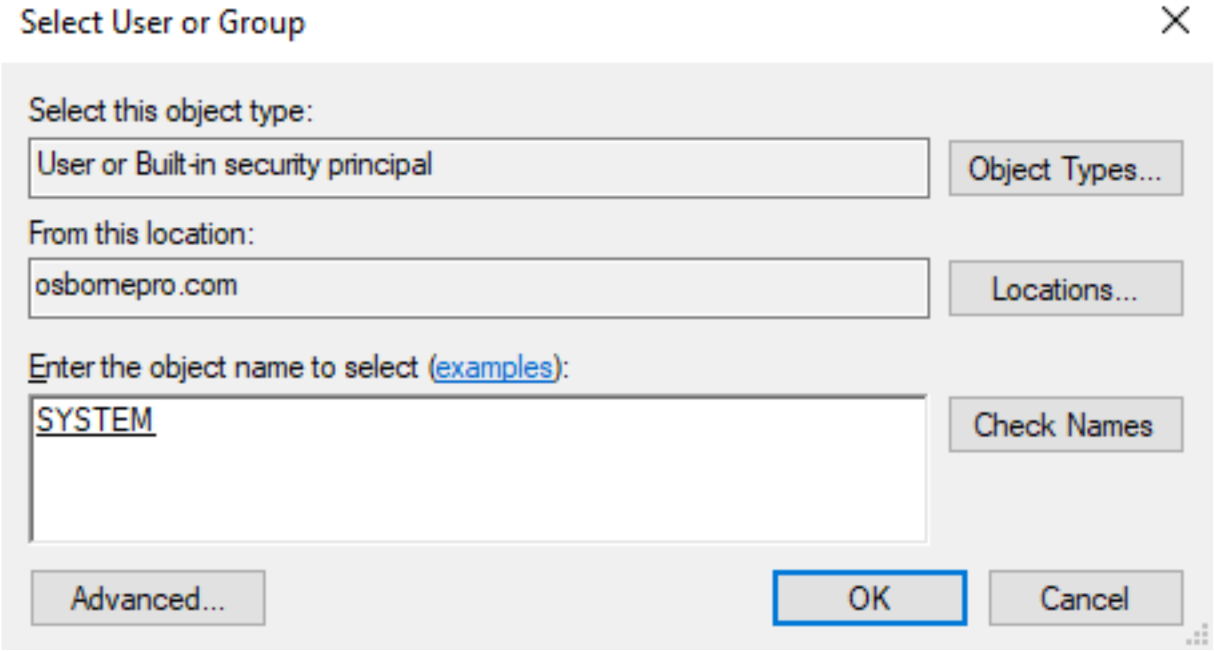
Description: Runs a check on process hashes to discover and log possibly malicious processes

Security options

Click the “Change User or Group” button



In the window that pops up type SYSTEM and click CHECK NAMES then click OK

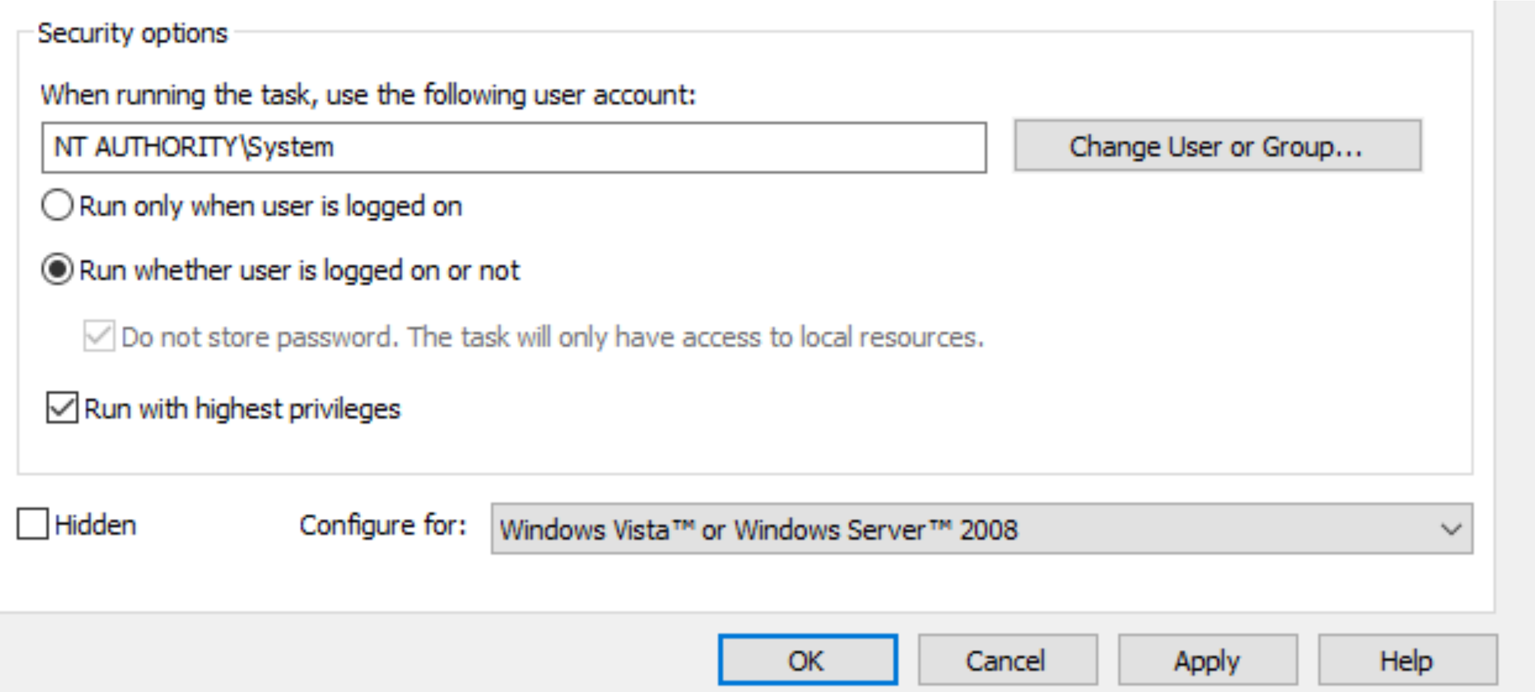

Select User or Group

Select this object type: User or Built-in security principal

From this location: osbornepro.com

Enter the object name to select (examples): SYSTEM

Select the “Run whether user is logged on or not” button
Tick the “Run with highest privileges” button



Security options

When running the task, use the following user account:

NT AUTHORITY\System

○ Run only when user is logged on

● Run whether user is logged on or not

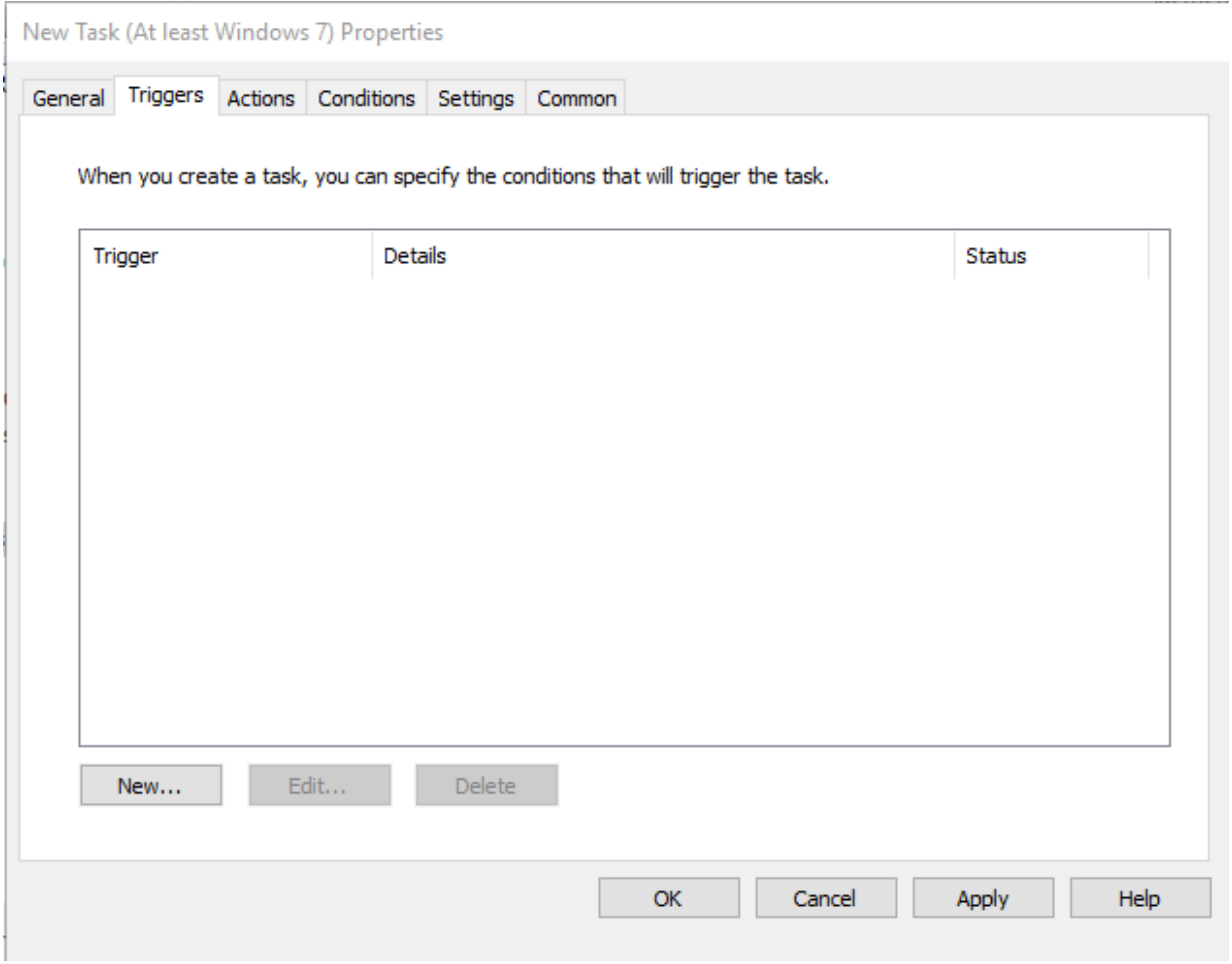
☑ Do not store password. The task will only have access to local resources.

☑ Run with highest privileges

□ Hidden

Configure for: Windows Vista™ or Windows Server™ 2008

Under the **Triggers** tab click the **New** button

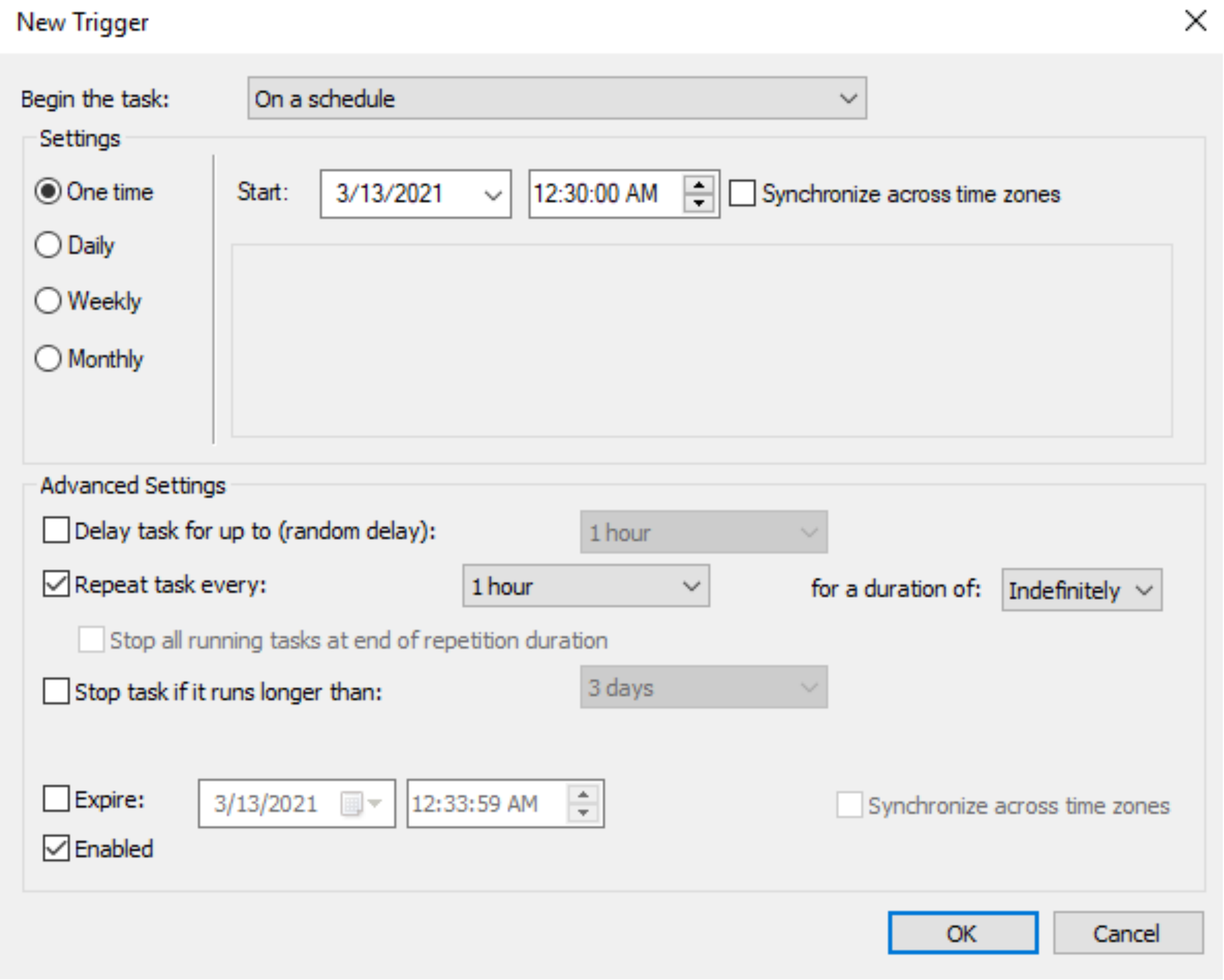


New Task (At least Windows 7) Properties

When you create a task, you can specify the conditions that will trigger the task.

Trigger	Details	Status

Set the below values for “On a Schedule” and click OK. This is to run the task once an hour forever



New Trigger

Begin the task: On a schedule

Settings

● One time
○ Daily
○ Weekly
○ Monthly

Start: 3/13/2021 12:30:00 AM □ Synchronize across time zones

Advanced Settings

□ Delay task for up to (random delay): 1 hour

☑ Repeat task every: 1 hour for a duration of: Indefinitely

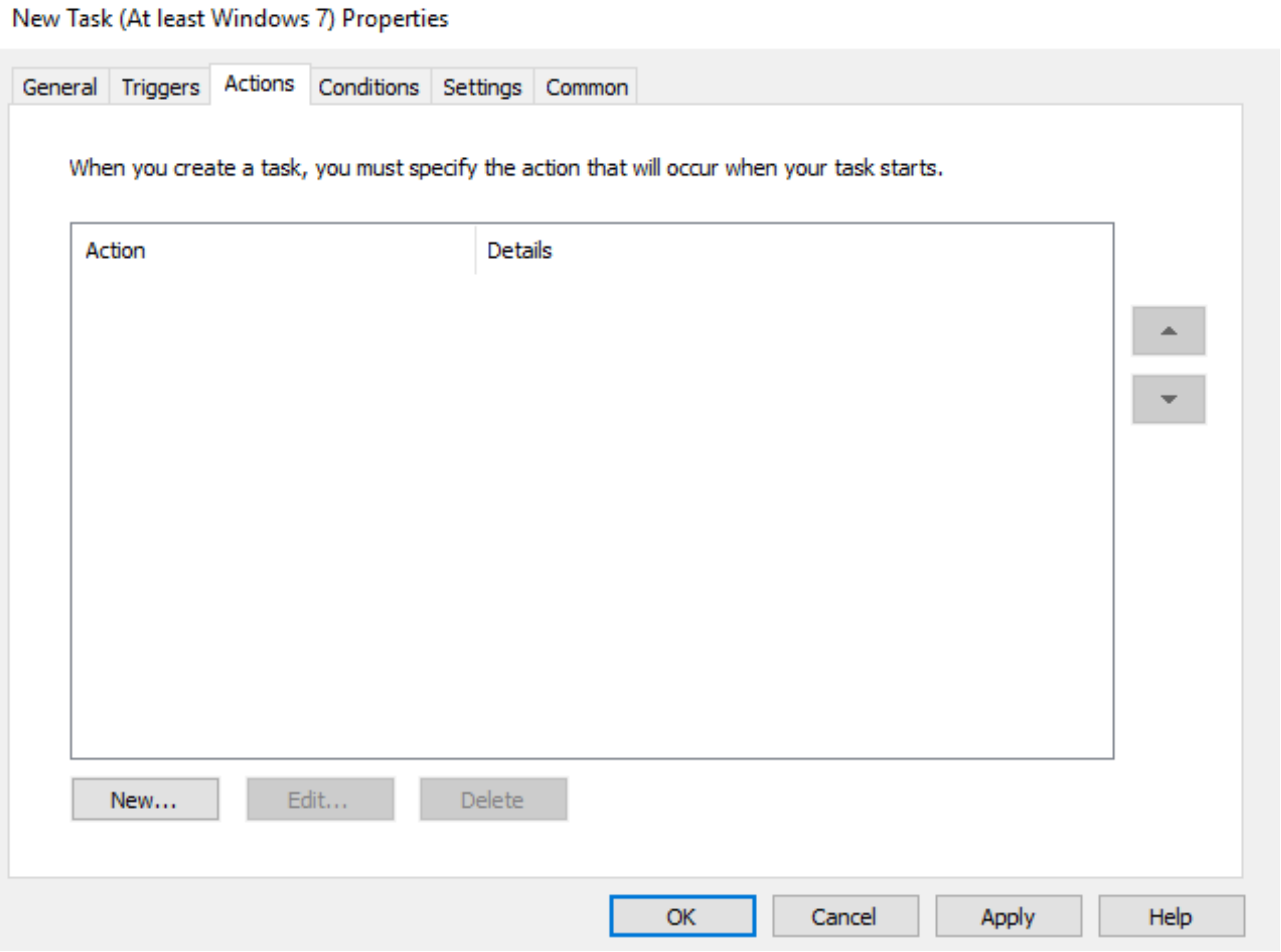
□ Stop all running tasks at end of repetition duration

□ Stop task if it runs longer than: 3 days

□ Expire: 3/13/2021 12:33:59 AM □ Synchronize across time zones

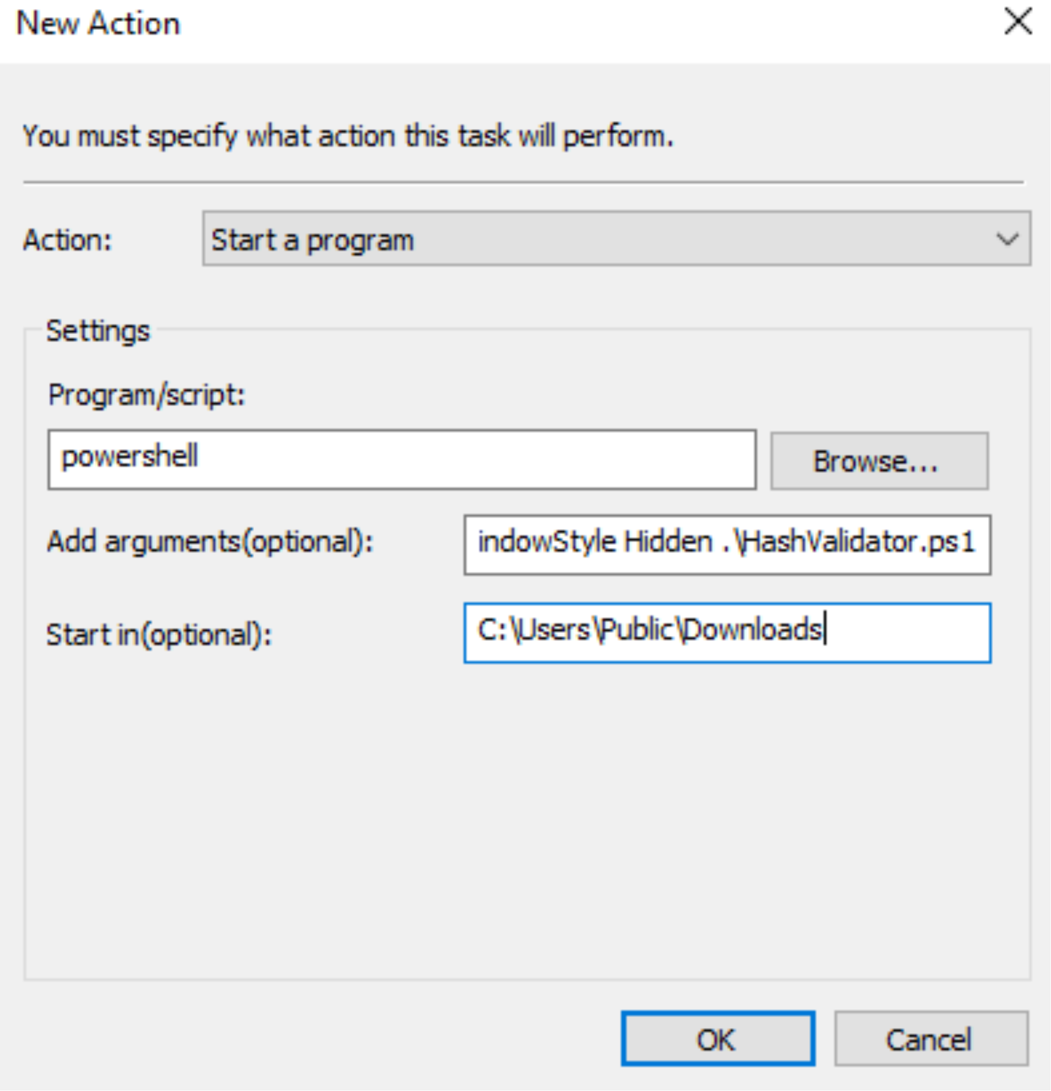
☑ Enabled

In the **Actions** tab click the **New** button



When you create a task, you must specify the action that will occur when your task starts.

Set the following values and click **OK**
ACTION: Start a program
PROGRAM/SCRIPT: powershell
ADD ARGUMENTS: -NoLogo -NonInteractive -WindowStyle Hidden .\HashValidator.ps1
START IN: C:\Users\Public\Downloads


New Action

You must specify what action this task will perform.

Action: Start a program

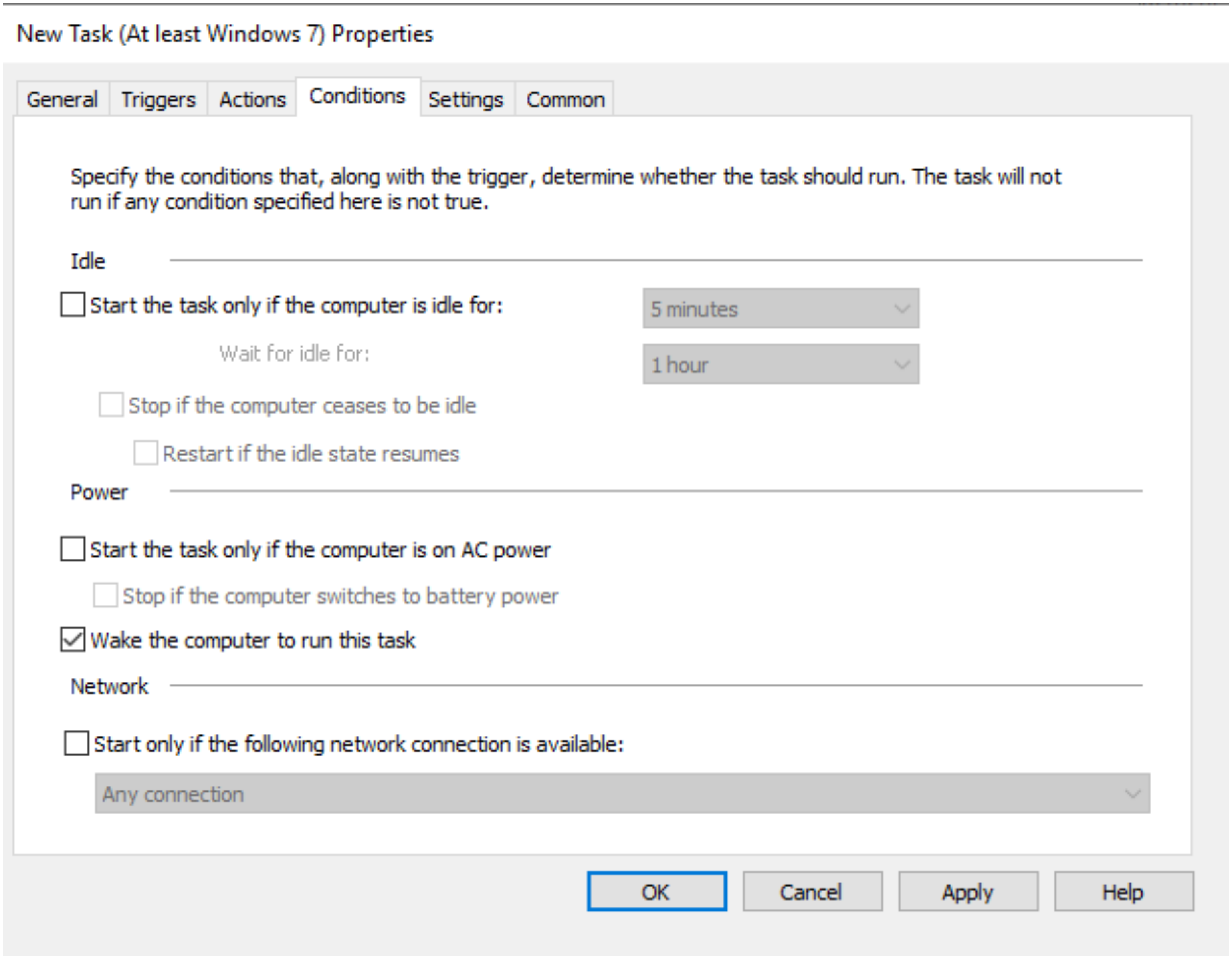
Settings

Program/script: powershell

Add arguments(optional): indowStyle Hidden .\HashValidator.ps1

Start in(optional): C:\Users\Public\Downloads

Under the **Conditions** tab select “**Wake the Computer to run this task**”



Specify the conditions that, along with the trigger, determine whether the task should run. The task will not run if any condition specified here is not true.

Idle

□ Start the task only if the computer is idle for: 5 minutes

Wait for idle for: 1 hour

□ Stop if the computer ceases to be idle

□ Restart if the idle state resumes

Power

□ Start the task only if the computer is on AC power

□ Stop if the computer switches to battery power

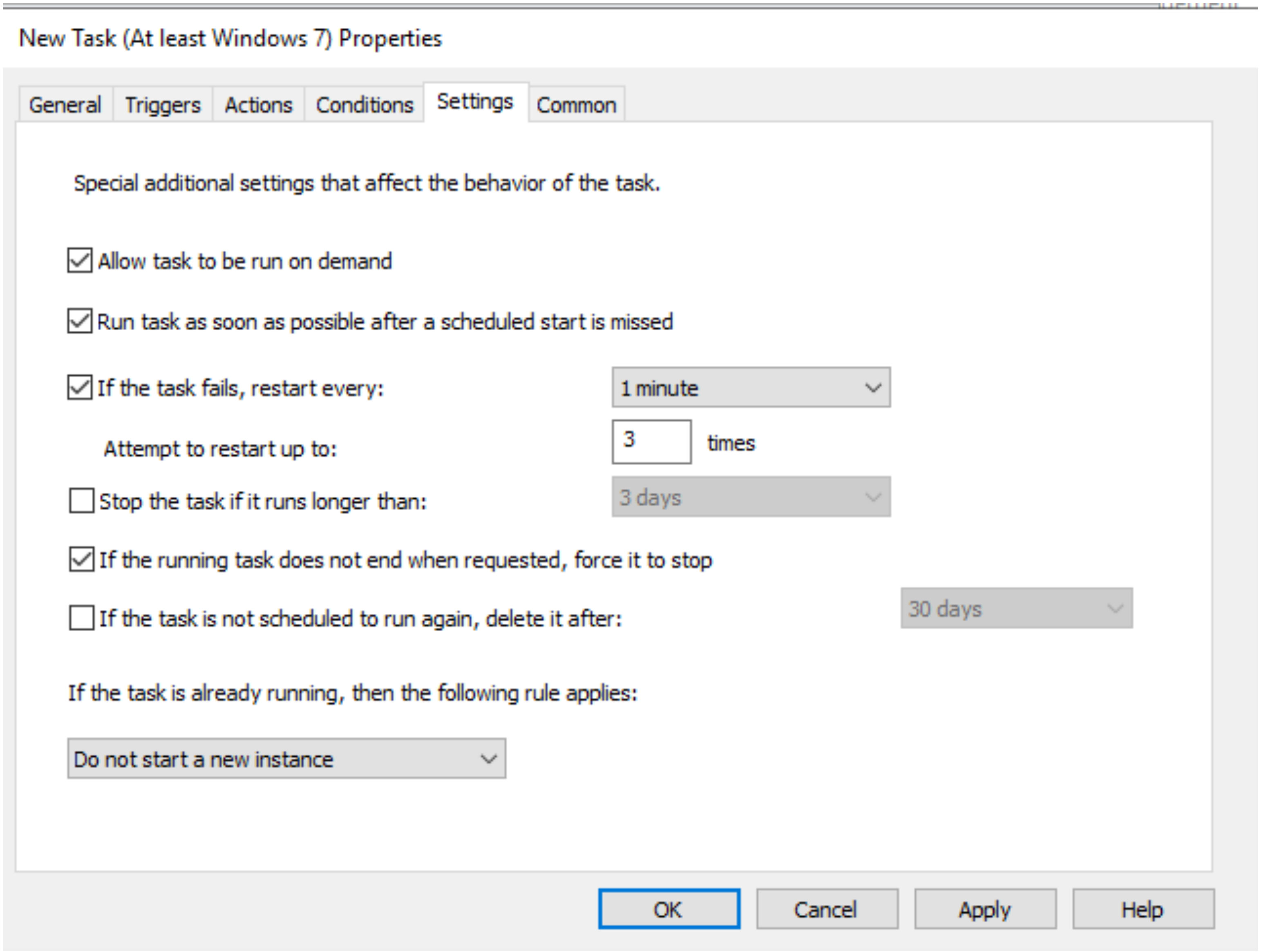
☑ Wake the computer to run this task

Network

□ Start only if the following network connection is available:

Any connection

Under the **Settings** tab select the below values
- Allow task to be run on demand
- Run task as soon as possible after a scheduled start is missed
- If the task fails restart every 1 minute up to 3 times
- If the running task does not end when requested force it to stop
- Do not start a new instance



New Task (At least Windows 7) Properties

Special additional settings that affect the behavior of the task.

☑ Allow task to be run on demand

☑ Run task as soon as possible after a scheduled start is missed

☑ If the task fails, restart every: 1 minute

Attempt to restart up to: 3 times

□ Stop the task if it runs longer than: 3 days

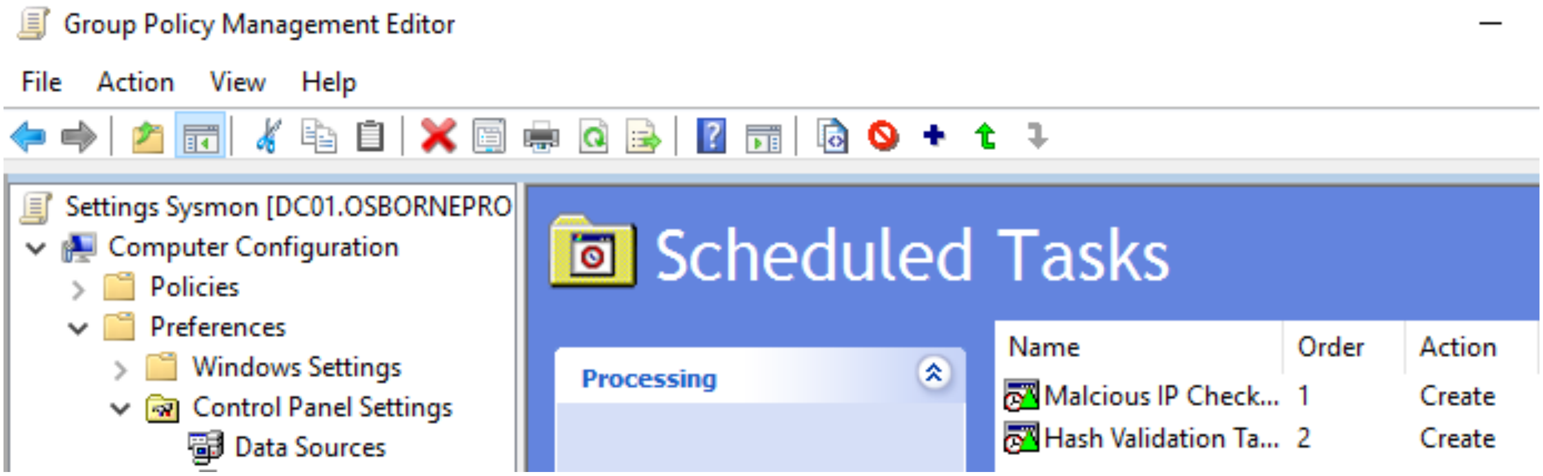
☑ If the running task does not end when requested, force it to stop

□ If the task is not scheduled to run again, delete it after: 30 days

If the task is already running, then the following rule applies:

Do not start a new instance

Then click **OK**



Group Policy Management Editor

Settings Sysmon [DC01.OSBORNEPRO
- Computer Configuration
  - Policies
  - Preferences
    - Windows Settings
    - Control Panel Settings
      - Data Sources

Scheduled Tasks

Name	Order	Action
Malcious IP Check...	1	Create
Hash Validation Ta...	2	Create