Contents

[Lab - Set up DC 1](#_Toc141113957)

[Prerequisite: 1](#_Toc141113958)

[\*\*Step 1: Promote your server to a Domain Controller\*\* 3](#_Toc141113959)

[\*\*Step 2: Configure the new Domain Controller\*\* 3](#_Toc141113960)

[\*\*Step 3: Add computers to the domain\*\* 4](#_Toc141113961)

[\*\*Step 4: Create and configure Group Policy Objects (GPOs) for mass deployment of MSI packages\*\* 7](#_Toc141113962)

[4.1 UNC file share guide 7](#_Toc141113963)

[4.2 General GPO Guide to install normal MSI (Details in Method 2) 8](#_Toc141113964)

[Install Method 1 - Use Scheduled task to run bat file 10](#_Toc141113965)

[Stage 1 - Share the BAT with client PCs 10](#_Toc141113966)

[Stage 2 - Deploy GPO to run Scheduled task 10](#_Toc141113967)

[Troubleshoot: 13](#_Toc141113968)

[Install Method 2 - Customize MSI & Install via GPO 15](#_Toc141113969)

Lab - Set up DC

Wednesday, July 12, 2023

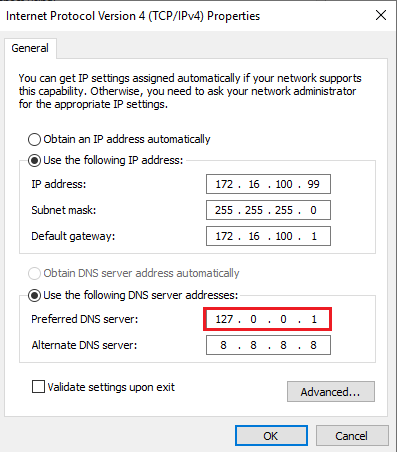
5:13 PM

To build a Domain Controller (DC) and use it to control other computers, you need to follow these steps:

## Prerequisite:

Static IP needs to be set on DC.

The Primary DNS server of DC needs to be DC itself (It will Config automatically).



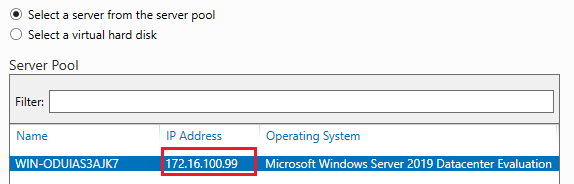
## \*\*Step 1: Promote your server to a Domain Controller\*\*

After installing the Windows Server operating system, you need to promote your server to a Domain Controller. To do this, follow these steps:

1. Open the 'Server Manager' by clicking on the icon in the taskbar or searching through the Start menu.

2. Click on 'Add roles and features'. Proceed to select the target machine to configure.

[Before proceed make sure IP is correct]



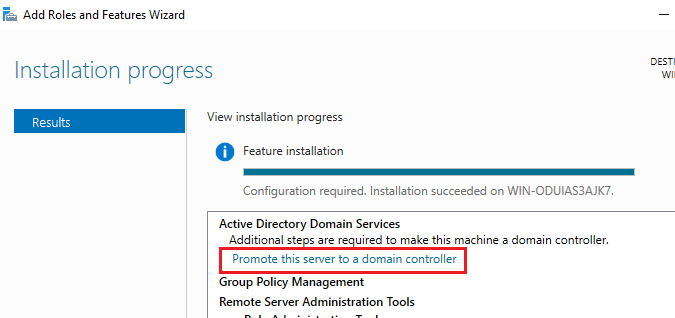
3. In the 'Add Roles and Features Wizard', click 'Next' until you reach the 'Server Roles' page.

4. Check the box for '**Active Directory Domain Services**' and confirm any additional feature installations when prompted.

5. Click 'Next' and follow the wizard until you reach the 'Confirmation' page, then click 'Install'.

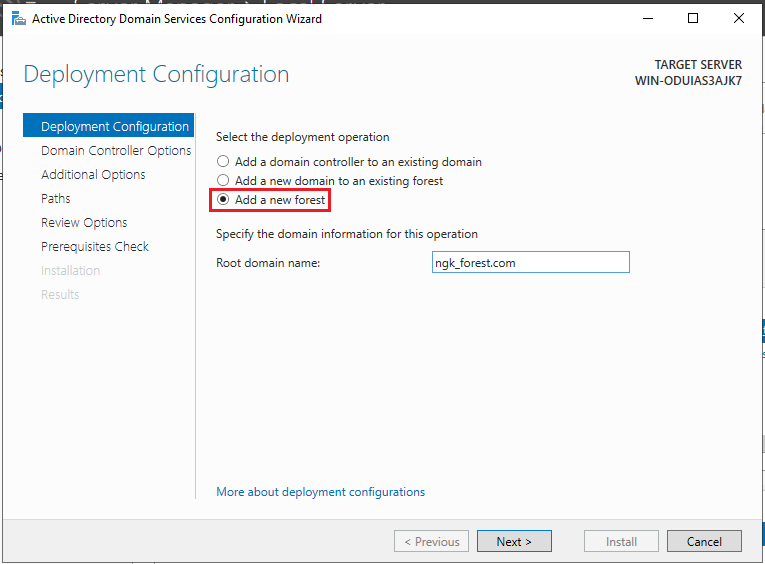
6. Once the installation is complete, click on the 'Promote this server to a domain controller' link in the 'Results' page.

Then, **'Active Directory Domain Services Configuration Wizard'** will pop out.



## \*\*Step 2: Configure the new Domain Controller\*\*

1. In the **'Active Directory Domain Services Configuration Wizard'**, choose 'Add a new forest' and enter your desired root domain name (e.g., example.com).

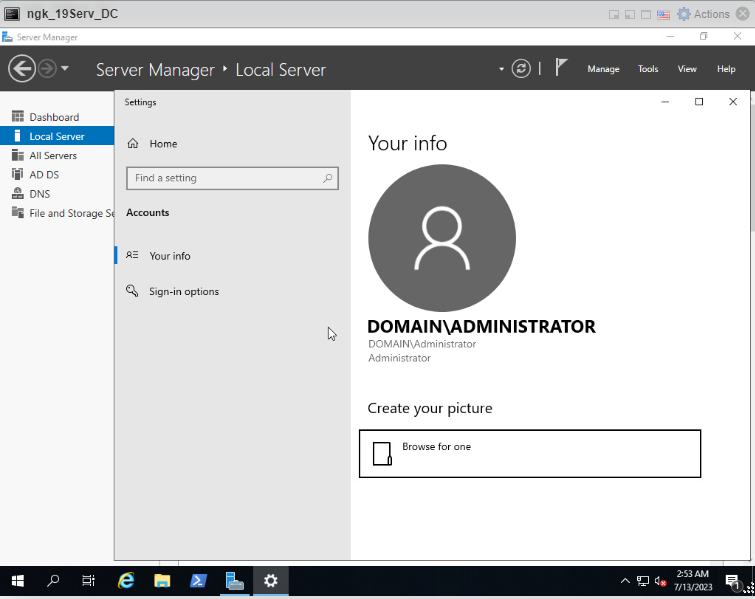


2. Configure the forest and domain functional levels, and then set the Directory Services Restore Mode (DSRM) password.

3. Click 'Next' and follow the wizard to configure the DNS server and NetBIOS domain name. (Keep others default, no need for DNS delegation)

4. Review your settings and click 'Next' to start the prerequisite check. If everything passes, click 'Install'.

After the domain is created, the Domain Controller's username is changed to <DOMAIN NAME>\<username>



## \*\*Step 3: Add computers to the domain\*\*

1. Go to the computer you want to add to the domain.

2. Open the 'System Properties' by right-clicking on 'This PC' or 'My Computer' and selecting 'Properties'.

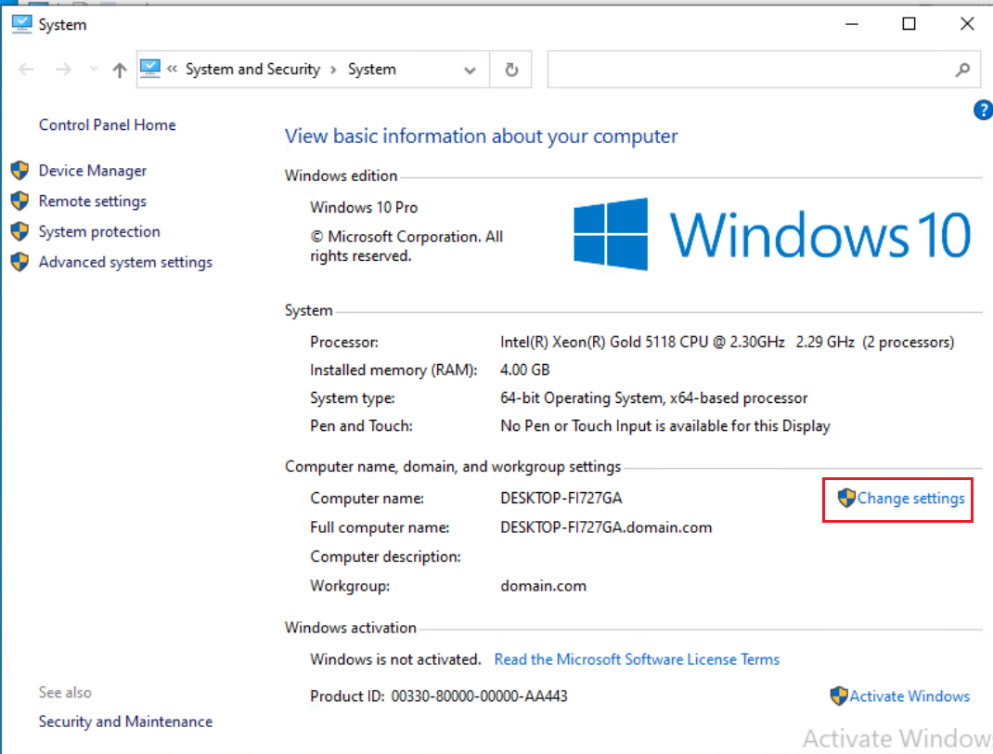
3. Click on 'Change settings' next to the computer name.

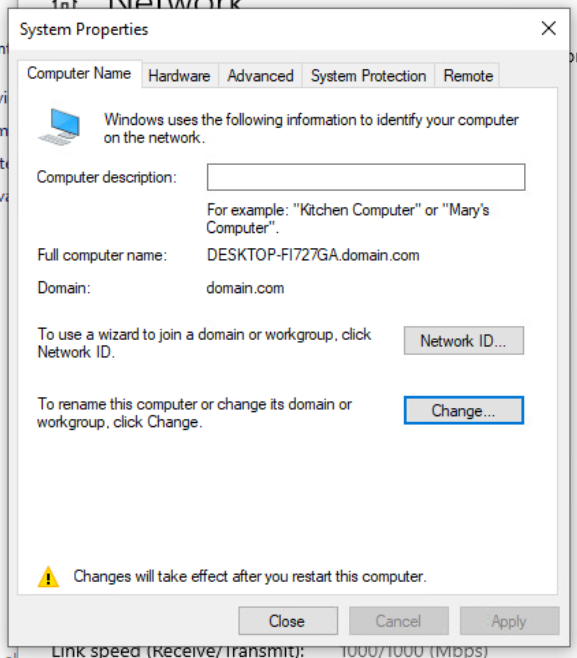
4. In the 'System Properties' window, click the 'Change' button.

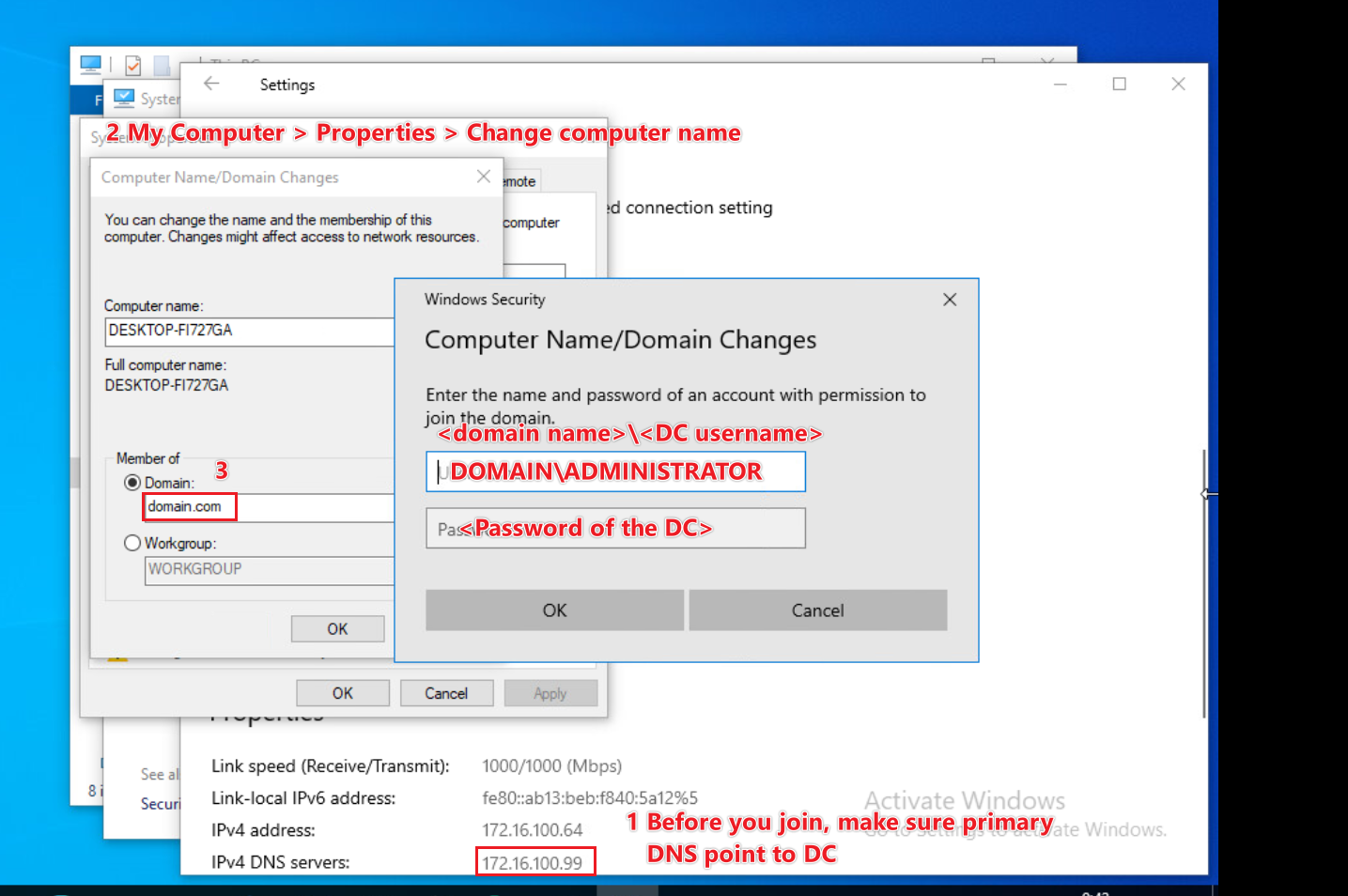
5. Enter the domain name you created earlier and click 'OK'.

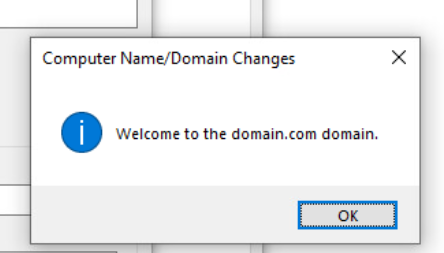
6. You will be prompted to enter the domain administrator's username and password. After entering the credentials, click 'OK'.

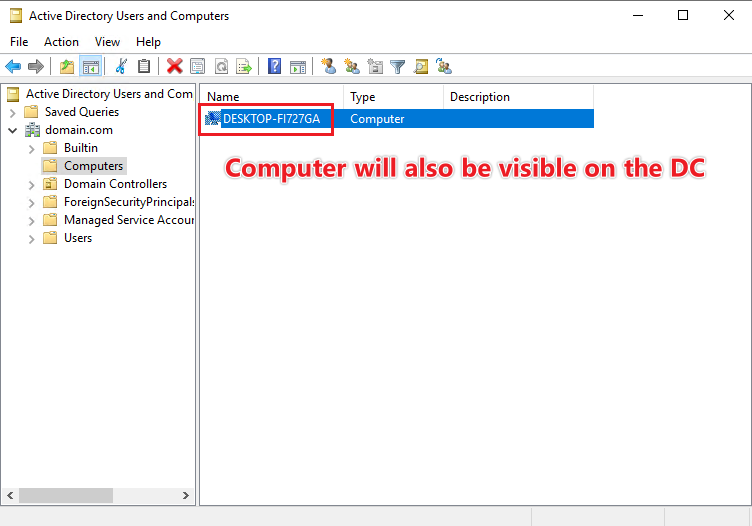
7. Restart the computer to apply the changes.





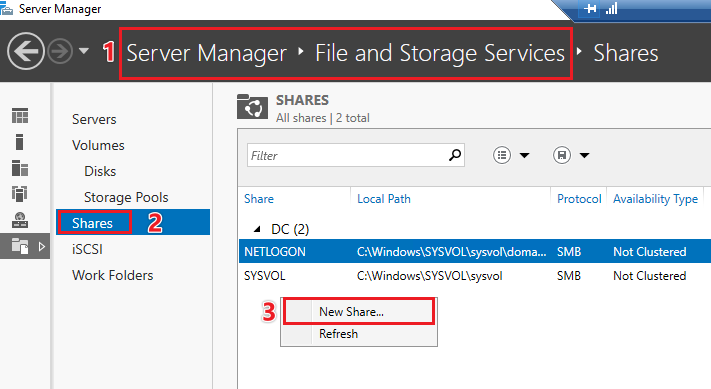




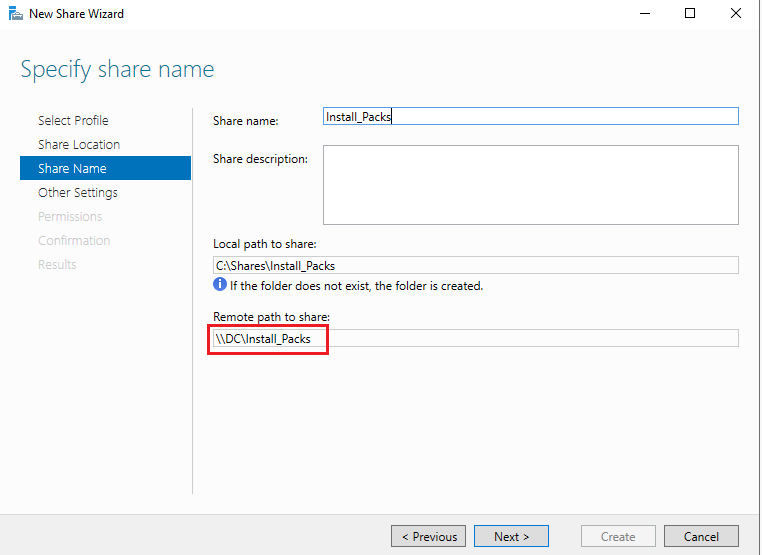


## \*\*Step 4: Create and configure Group Policy Objects (GPOs) for mass deployment of MSI packages\*\*

### 4.1 UNC file share guide

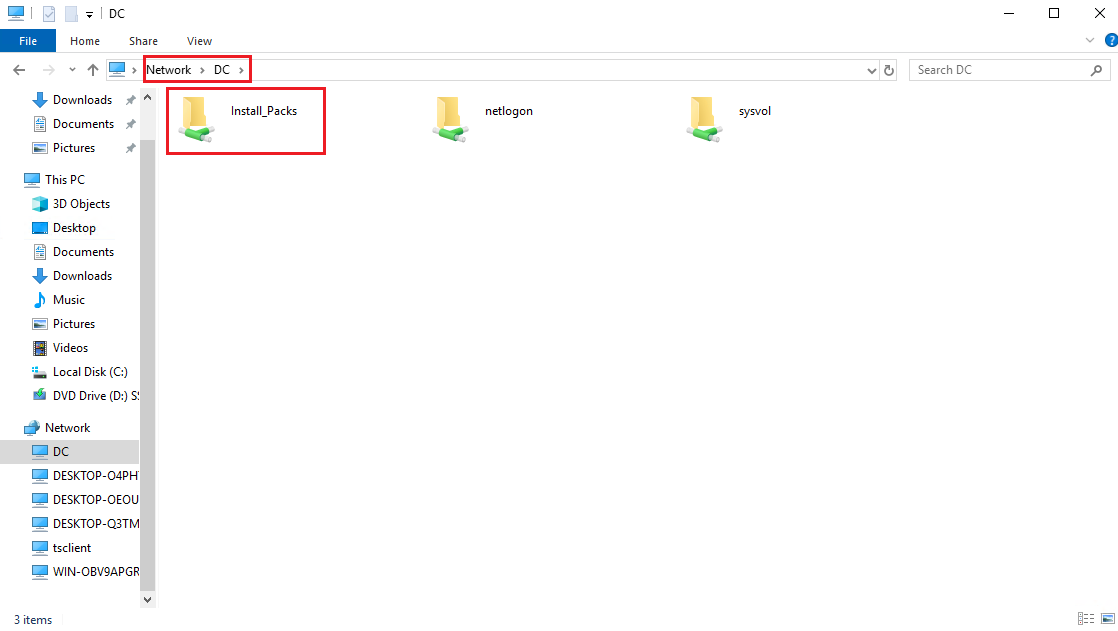


Profile: SMB - quick for windows



**Permissions: Make sure the intended end users have permissions. You may add the pricipal "Everyone" for convenience.**

When finished, you can use the UNC path to locate your share.

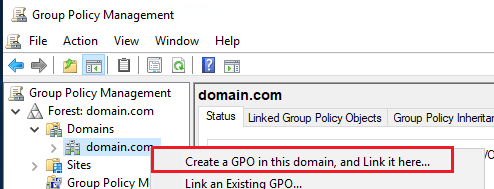


\\ is called the UNC prefix. It is applicable for all UNC paths

### 4.2 General GPO Guide to install normal MSI (Details in Method 2)

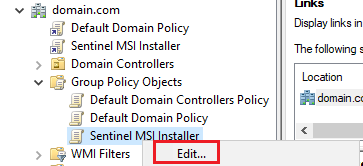
1. On the Domain Controller, open the 'Group Policy Management' console by searching for it in the Start menu.

2. Right-click on your domain and select 'Create a GPO in this domain, and Link it here…'.



3. Name the new GPO and click 'OK'.

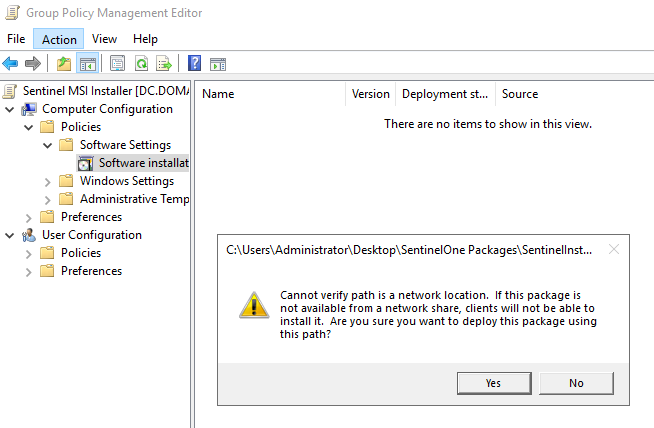
4. Right-click on the newly created GPO and select 'Edit' to open the 'Group Policy Management Editor' console.



5. Navigate to 'Computer Configuration > Policies > Software Installation'.

6. Right-click on 'Software Installation' and select 'New > Package'.

If local path is selected, the following prompt will be shown:



7. Enter the UNC path (e.g., `\\fileserver\share\software\example.msi`) for the MSI package you want to deploy. You can use a shared folder on the file server or a network-attached storage (NAS) device to store the MSI files.

8. Choose the deployment method ('Assigned', 'Published', or 'Advanced') and click 'OK'.

\*\*Step 5: Configure the security filtering for the GPO\*\* (Optional)

1. In the 'Group Policy Management' console, select the GPO you created earlier.

2. In the 'Security Filtering' section, remove the default 'Authenticated Users' group.

3. Click the 'Add' button and select the desired security groups or individual computers to which you want the GPO to apply.

\*\*Step 6: Force a Group Policy update\*\*

To apply the GPO immediately, you can force a Group Policy update on the target computers:

1. Open the 'Command Prompt' with administrative privileges on the target computers.

2. Enter the following command: `gpupdate /force`

3. Restart the computers if prompted.

Now, the MSI packages should be deployed on the target computers according to the GPO settings you configured.

Windows Search service may be disabled

Install Method 1 - Use Scheduled task to run bat file

## Stage 1 - Share the BAT with client PCs

Use your DC to create a Shared folder on your domain network.

Save the install command as .bat (All in one line).

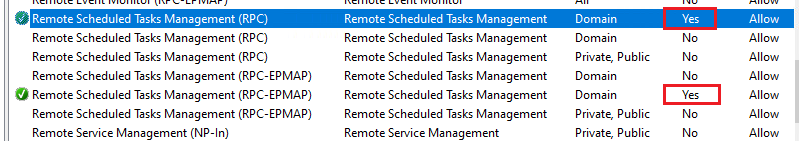
Format: <UNC Path to .msi> SITE\_TOKEN=<site token> /q /norestart

Example:

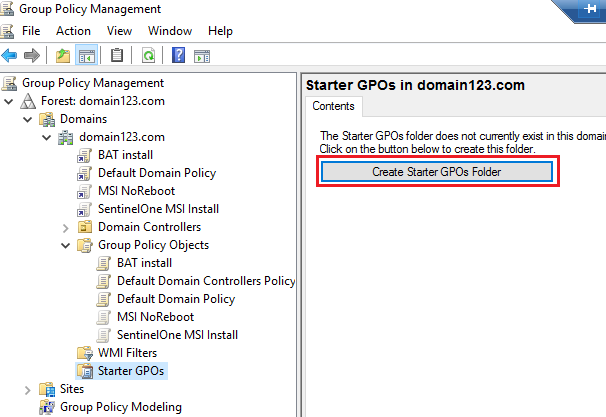
[\\WIN-P9JDN0NHI6B\Install\_Packs\SentinelInstaller\_windows\_64bit\_v22\_3\_5\_887.msi](file://WIN-P9JDN0NHI6B/Install_Packs/SentinelInstaller_windows_64bit_v22_3_5_887.msi) SITE\_TOKEN=eyJ1cmwiOiAiaHR0cHM6Ly9hcG5lMS0xMTAxLW5mci5zZW50aW5lbG9uZS5uZXQiLCAic2l0ZV9rZXkiOiAiMzc4YzI0YjhhNDE5ZG888888 /q /norestart

Make sure the intended users can access BAT & MSI giving them the Read & Execute permissions.

## Stage 2 - Deploy GPO to run Scheduled task

* 1. Firewall requirements checking: **The two Firewall Allow rules (as shown below) must be enabled on the client computers. You may check this in their Windows Defender Firewall with Advanced Security (Firewall advanced settings).**

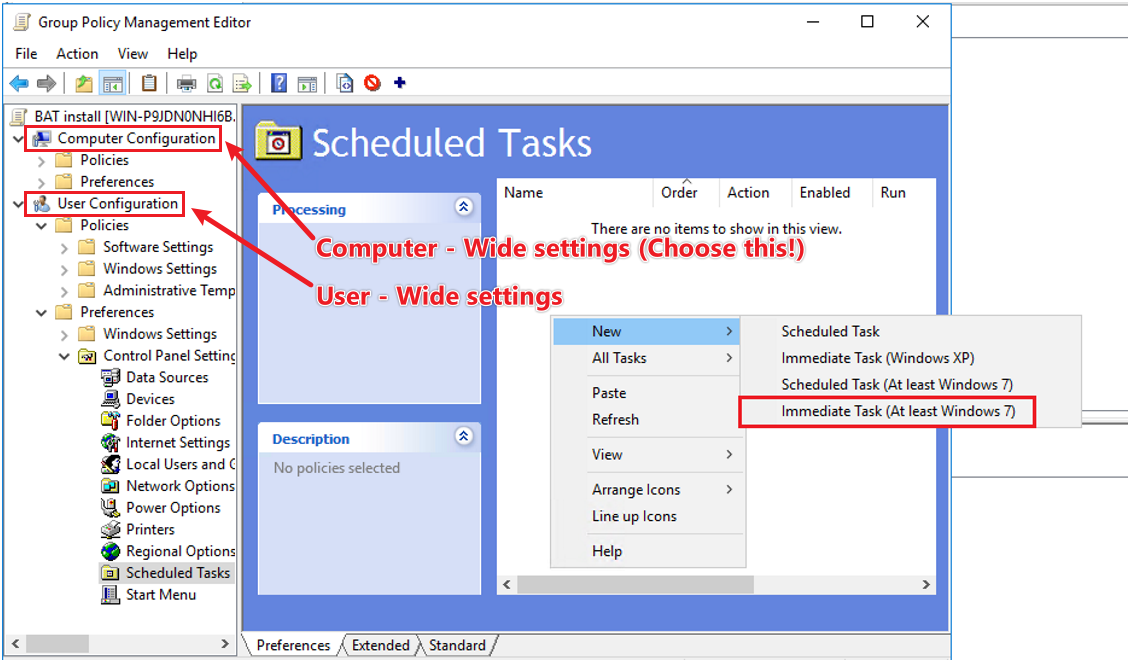
**If not enabled,** Use the starter GPO “Group Policy Remote Update Firewall Ports” to enable necessary firewall ports. We need it to run scheduled task remotely.



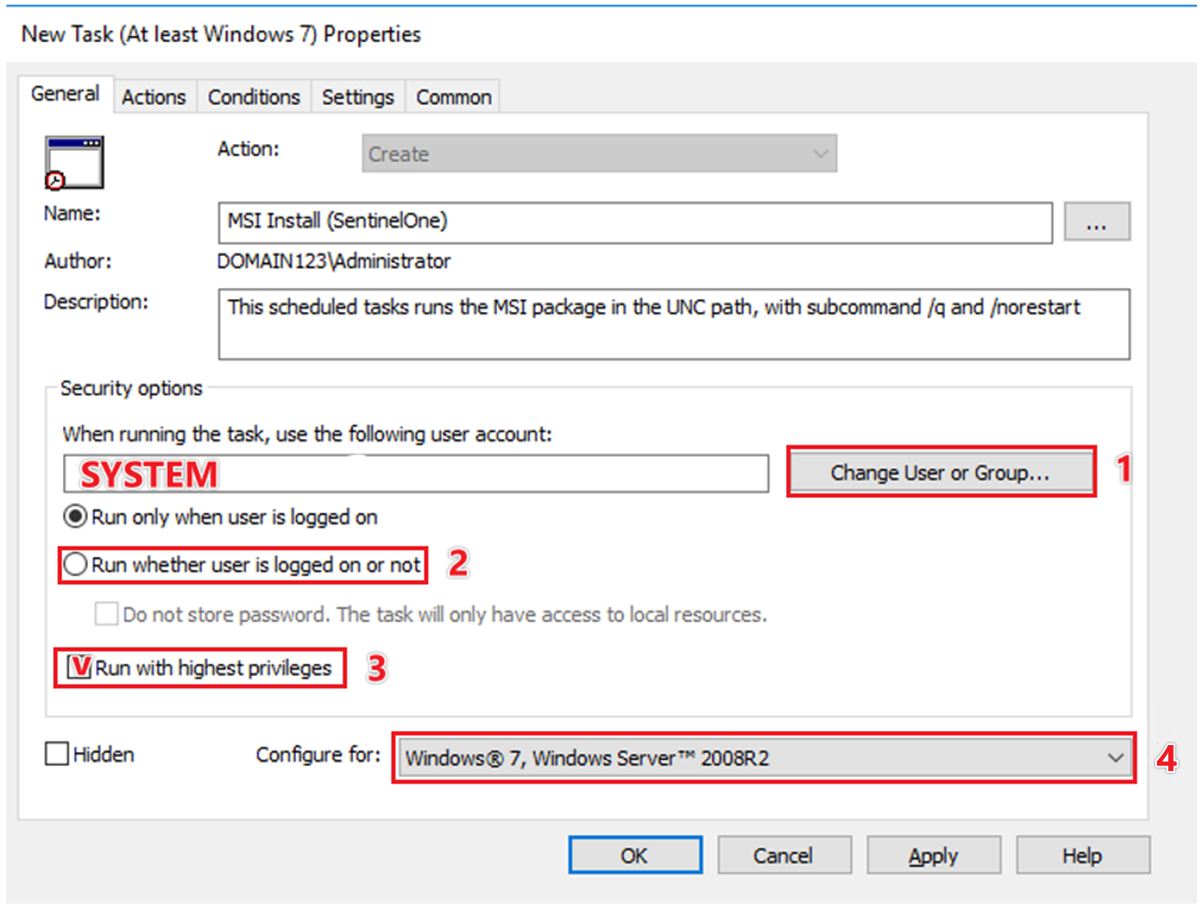
* 1. On the DC, go to Group Policy management.

Create a GPO and link it to domain/OU. The domain/OU need to contain the machines that will be installed SentinelOne.

* 1. Edit the GPO. Go to **Computer Configuration** - Preferences - Control Panel Settings.

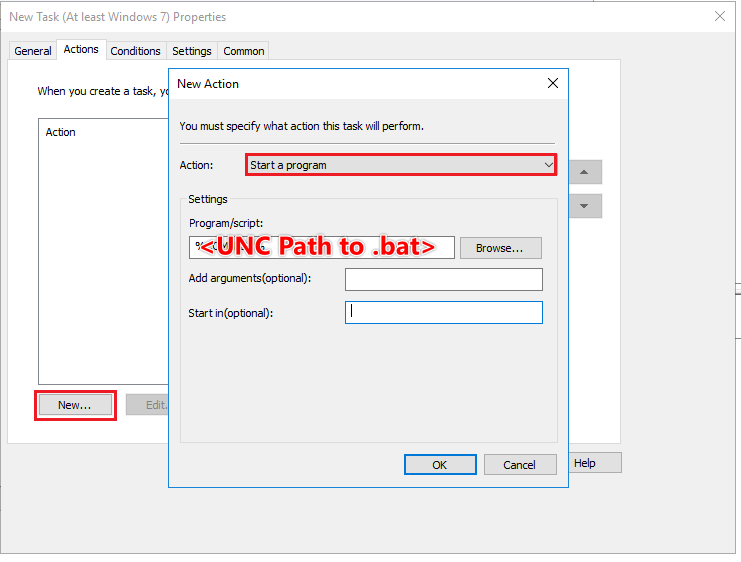


* 1. Scheduled Tasks - New - Immediate Task (At least Windows 7)
     1. General - Security options - Change User or Group
     2. Type "SYSTEM"
     3. Check Names - OK
        1. Note: SYSTEM stands for the user account “NT AUTHORITY\SYSTEM” that will be running the task.
     4. Tick Run whether user is logged on or not and tick Run with highest privileges(Y)



* 1. Go to Action Tab, add New action.

Directly paste the UNC path in "Program/Script".



Then, click on OK and click on OK of the outer-layer window to save changes to the Task Scheduler.

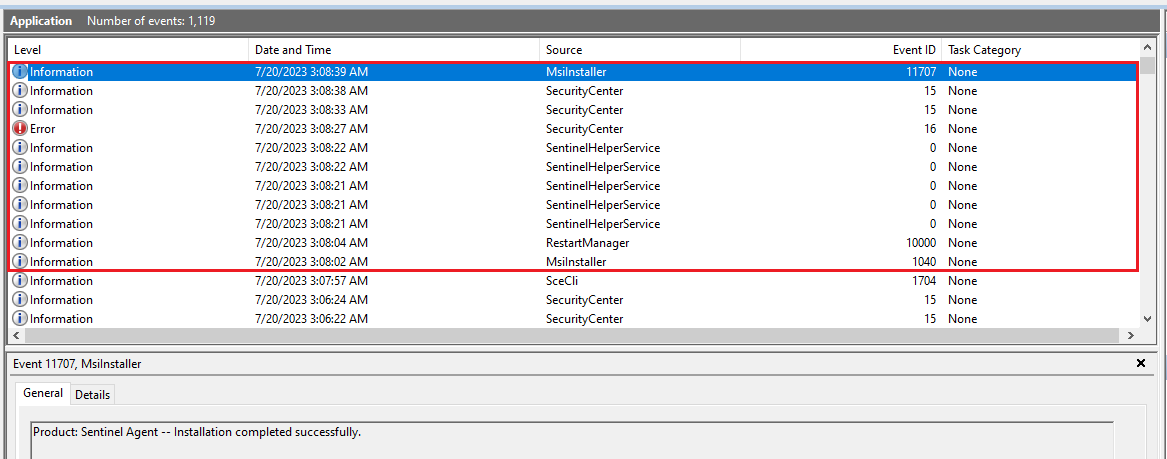
**Never configure "Send a message" Action or "Send an e-mail" Action, as they are depreciated features and will cause the scheduled task to fail.**

* 1. Lastly, you may optionally run gpupdate /force on the client PC to make it quicker.

Troubleshoot:

Log is checkable at Event viewer - Application

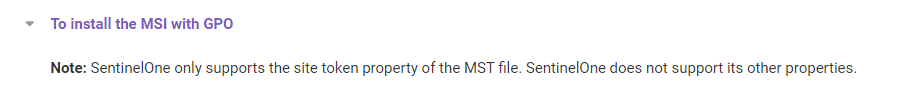
The MSI Installer log is at C:\Windows\Temp. If not found, check %temp%.

Event log example of a successful install:

Install Method 2 - Customize MSI & Install via GPO

Tuesday, July 18, 2023

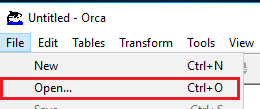
2:41 PM

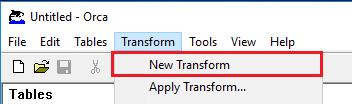


Download Orca from [Windows SDK components for Windows Installer developers - Win32 apps | Microsoft Learn](https://learn.microsoft.com/en-us/windows/win32/msi/platform-sdk-components-for-windows-installer-developers)

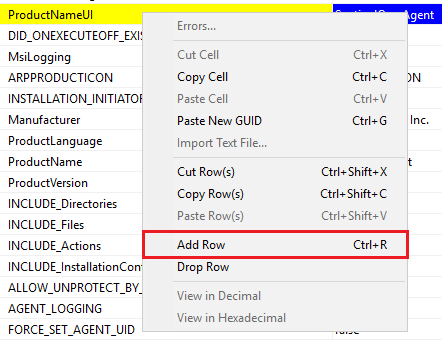
Choose MSI Tools when running the Windows SDK installer.

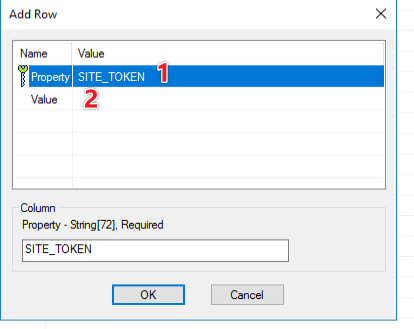
Save Transform as a separate file





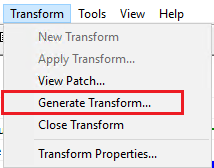
On the left, go to "Properties". Add the SITE\_TOKEN as a new row.







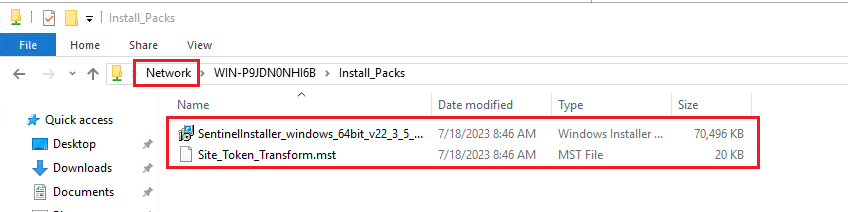
Then



Validate by:

* 1. Open Orca
  2. Drag MSI to Orca window
  3. Drag MST to Orca window, and see if the Site token is present on "Properties".

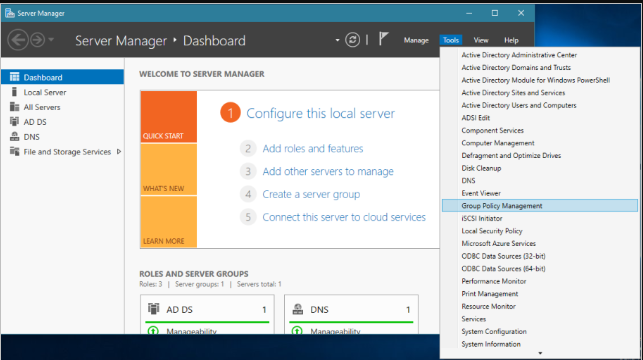
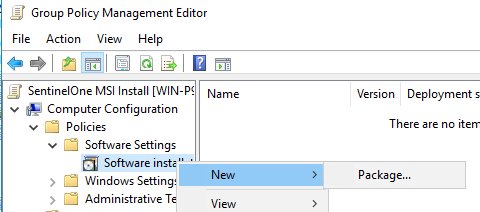
Lastly, put the two files into the UNC shared path

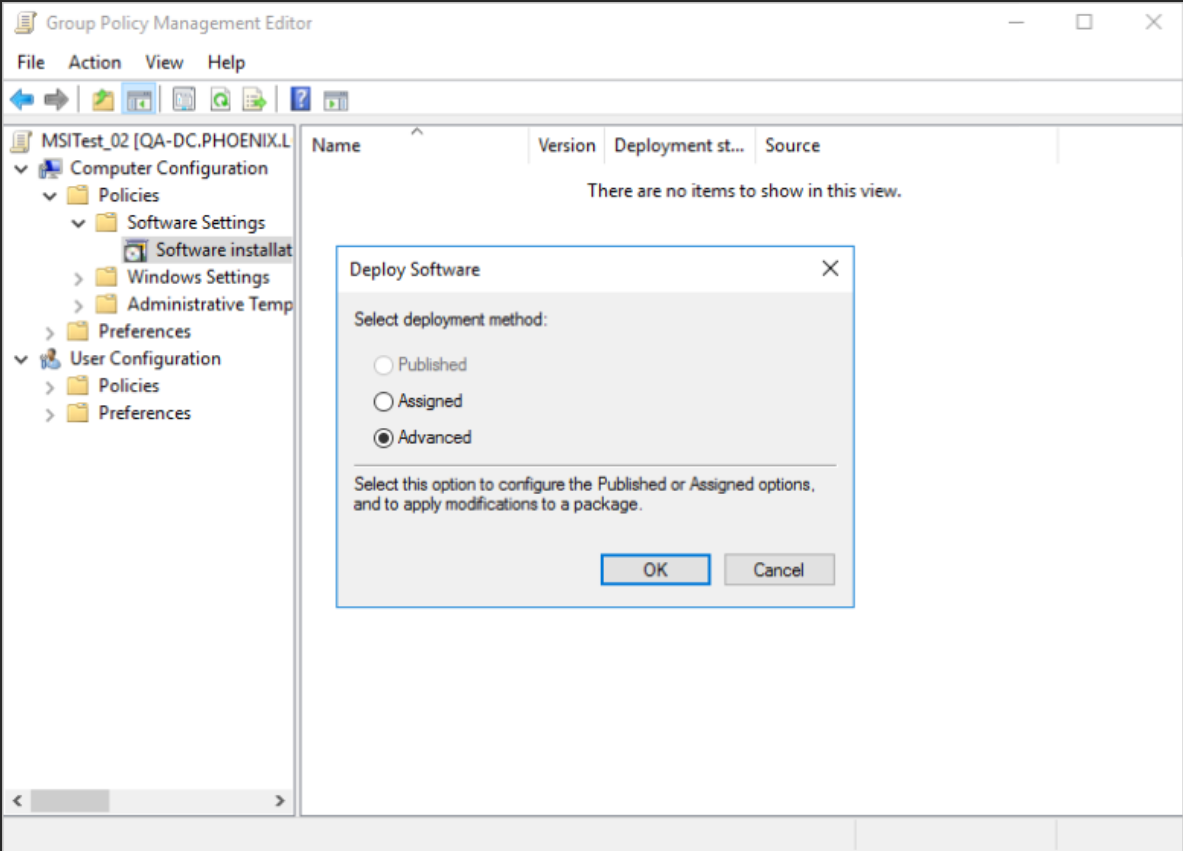


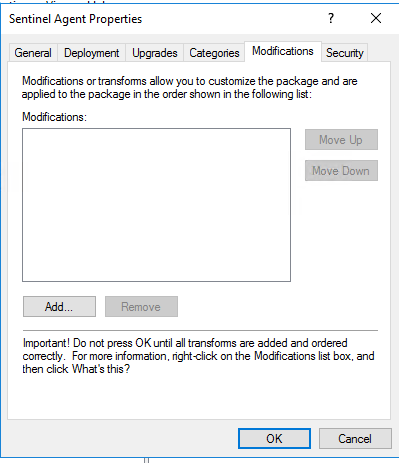
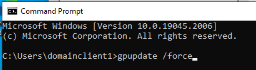
When the two files are ready, proceed to group policy deployment:

[Installing and Upgrading the Windows Agent Using an MSI Package (sentinelone.net)](https://apne1-1101-nfr.sentinelone.net/docs/en/installing-and-upgrading-the-windows-agent-using-an-msi-package.html#UUID-0ea53872-0b42-bcc0-fe94-3a0679d04e82_sidebar-idm4506731721032032436629261566)

Group Policy Deployment

* 1. Save the MST file with the MSI file, in a path that all the target endpoints can access.
  2. From your AD Domain Server > **Server Manager**, click **Tools**> **Group Policy Management**.
  3. 
  4. Right-click the domain and select **Create a GPO in this domain and Link it here**.
  5. In the window that opens, enter a name for the new policy and click **OK**.
  6. In the Group Policy Manager window, right-click the new policy and select **Edit**.
  7. In the window that opens, expand **Computer Configuration** > **Policies**> **Software Settings**. Right-click **Software Settings** and select **New** > **Package**.
  8. 
  9. In the window that opens, select the SentinelOne MSI.
  10. In the Deploy Software window, make sure **Advanced** is selected.

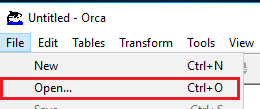


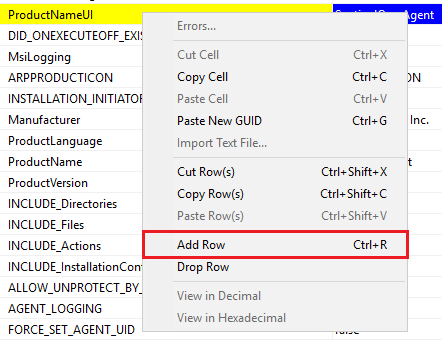
* 1. Click **OK**.  
     Wait for the Sentinel Agent Properties window to open. (~30 secs)
  2. 
  3. Click **Modifications** > **Add**.
  4. Select the MST file. Wait for it to load. Click **OK**.
  5. On the **endpoints**, in cmd, run: gpupdate /force
  6. 
  7. When the policy is updated, end user must enter Y to restart the endpoint!
  8. When the user logs in, see that the Agent is installed.

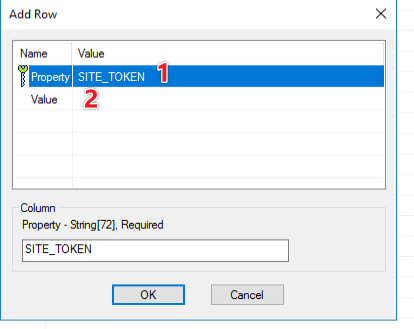
====================

Alternative Method (Does not work on SentinelOne, will cause application signature error)

Alternatively, Save the change into MSI.









Save the change to the file.

References

UNC Path

[\\WIN-P9JDN0NHI6B\Install\_Packs](file://WIN-P9JDN0NHI6B/Install_Packs)

FQDN UNC Path

[\\WIN-P9JDN0NHI6B.domain123.com\Install\_Packs](file://WIN-P9JDN0NHI6B.domain123.com/Install_Packs)

SentinelOne Guide (Need account)

[Installing and Upgrading the Windows Agent Using an MSI Package (sentinelone.net)](https://apne1-1101-nfr.sentinelone.net/docs/en/installing-and-upgrading-the-windows-agent-using-an-msi-package.html#UUID-0ea53872-0b42-bcc0-fe94-3a0679d04e82_sidebar-idm4506731721032032436629261566)