



How - To Guide

Install Netsurion Open XDR and Change Audit Sensors for Windows

Publication Date:

October 09, 2023

Abstract

The Netsurion Open XDR sensor for Windows deployment processes are described in detail in this manual for the 9.4 and above. The Netsurion Open XDR sensor for Windows can be deployed using Active Directory Group Policy, Command Line and User Interface.

The purpose of this document is to provide step-by-step instructions to deploy the Netsurion Open XDR sensor using various methods and understand the deployment procedure.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Audience

Netsurion Open XDR system administrators who wish to deploy the Netsurion Open XDR sensor for Windows and Change Audit sensor.

Table of Contents

1	Overview.....	4
2	Prerequisite.....	5
3	Software Requirement	5
4	Resource Requirement	6
5	Preparing Netsurion Open XDR Sensor MSI Installer Package for Deployment	6
6	Deploying via Command Prompt.....	6
6.1	GUI and Silent Installation Parameters.....	6
6.2	MSI Installation via GUI without Agent.ini.....	10
6.3	MSI Installation via Silent mode without Agent.ini	18
7	Deploying through Agent.ini File.....	20
7.1	MSI Installation via GUI Mode	20
7.2	MSI Installation via Silent Mode	24
8	Deploying via Group Policy	26
8.1	Preparing Agent.ini File with Configuration Settings	26
8.2	Creating a Network Share.....	29
8.3	Assigning Systems to New Organization Unit	37
8.4	Launching Group Policy Management Console.....	38
8.5	Creating Group Policy Object in Active Directory for Software Deployment	39
8.6	Verifying Installation	48
8.7	Uninstalling Netsurion Open XDR Sensor via GPO.....	49
8.8	Limitation for Group Policy Installation.....	50
9	Uninstallation of Netsurion Sensor via Control Panel	51

1 Overview

The Netsurion Open XDR sensor for Windows is the front-line security component on the Netsurion Open XDR platform which provides detailed visibility into your network. The Open XDR sensor facilitates understanding what software and services are installed, how they are configured, and if there are any potential vulnerabilities and active threats executed against them. The sensor collects and normalizes logs, monitors your network, and collects information about your assets and IT environment.

The Netsurion Open XDR sensor delivers the following essential capabilities:

- Log collection.
- Scans for authenticated assets.
- Scans for unauthenticated asset discovery.
- High-degree monitoring of application log files, TCP/UDP network activities, and USB devices.
- Observes network traffic non-intrusively to identify hosts.
- Software install/uninstall.
- Finds services start/stop.
- Sends events with guaranteed delivery via TCP mode.
- Monitor files and registry changes on the system.
- Monitor/ terminate suspicious activity.
- Provides immediate visibility into the attacks against your systems.
- Syslog relay.

2 Prerequisite

Before deploying Windows sensor, it is essential to set up a few things as detailed below,

- Ensure that the Netsurion Open XDR manager is running during the installation process.
- All target systems must have access to Network Share where the Open XDR sensor MSI files are stored.
- Domain systems must have at least Read access on the Network Share where the Open XDR sensor MSI files are stored.
- If the sensor is deployed via Command Line interface and UI, then it must be uninstalled from the **Control Panel**.
- .NET Framework 3.5 or above must be installed as per the system requirement to use all features of the Open XDR sensor. Restart the system after installing .NET 3.5 or above.
- It is recommended to install the Open XDR sensor and Change Audit sensor either by command line, System Manager or by group policy.
- Restart the target system(s) after configuring the software deployment policy to complete the installation.

Note:

If you uninstall the latest MSI package via the Netsurion Open XDR console, both the Open XDR sensor and Change Audit sensor will be uninstalled.

3 Software Requirement

Windows Server	2022, 2019, 2016, 2012 R2
Windows	11, 10
Microsoft .NET Framework 3.5 and above	

Note:

Versions other than those listed above are not supported.

4 Resource Requirement




Minimum Configuration			Resource Utilization (in a typical environment)		
CORE	RAM	DISK	CPU		MEMORY
			AVG	MAX	
4	8 GB	200 MB	1-2 %	10 %	50 MB

5 Preparing Netsurion Open XDR Sensor MSI Installer Package for Deployment

Before the deployment, it is required to extract the MSI files to a suitable folder. Perform the following procedures outlined below.

For Netsurion Open XDR 9.4 and above,

1. Download the MSI package (MSI 9.4 is considered in this example in AgentMSI_94.zip) from the location provided by Netsurion Open XDR support team.
2. Extract the **AgentMSI_94.zip** file to the AgentMSI_94\ folder.

Name	Date modified	Type	Size
 Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
 EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
 ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

6 Deploying via Command Prompt

Run the executable MSI Installer with the administrative privilege.

6.1 GUI and Silent Installation Parameters

Argument	Description
EA	Selection of the Windows sensor feature from the Command line. 1 - Installation of the Open XDR sensor feature is selected. 0 - The Windows sensor feature is not selected for installation.

Argument	Description
CA	Selection of the Change Audit feature from the Command line. 1 - Installation of Change Audit feature is selected. 0 - Change Audit Feature is not selected for installation.
CUSTOMCONFIG	0 - Enterprise configuration file in UDP mode. 2 - Customer Existing etacfg.ini. 3 - Enterprise Configuration file in TCP mode. 4 - Enterprise anomalous audit configuration file in TCP mode.
INSTALLDIR (For GUI) INSTALLPATH (For Silent)	Custom Installation directory path
EM	Enterprise Manager name
EP	Enterprise port
CM	Change Audit Manager name
IR	Remedial Actions 1 - Predefined scripts will be placed in the EventTracker\Agent\Script folder.
LS	License Server
LP	License Port
DW	Deploy WinSCP feature. 1 – It will get installed 0 – It will not get installed
SC	shortcut 1 - shortcut enable 0 - means disable
MIN_GUI	Minimal GUI 1 - Minimal GUI enable 0 - Full GUI wizard.

Argument	Description
IS_SUFFIX	<p>Enable Suffix</p> <p>2 - enable (Location Name window will not appear) (any configuration)</p> <p>1 - enable (GUI will contain control to take input as suffix)</p> <p>0 - disable (no extra GUI control)</p>
SUFFIX	Suffix string
SUPPORT_CONTACTS	Support details
PIP	<p>Protection IP</p> <p>If the user provides PIP, the FQDN or the Hostname needs to be added here.</p> <p>When the FQDN or the Hostname is provided, the “protect_flag” is enabled and provided IP will appear in “protect_ip” field.</p>
PKG_UID	Package UID
Agent.ini	<p>Agent.ini</p> <p>0 - Command prompt installation (It won't consider Agent.ini details)</p> <p>1 - Considers Agent.ini filled details</p>

Note:

The Open XDR sensor and Change Audit sensor features are installed by default.

Mandatory Parameters

Parameter	Default Value
EM	Mandatory Parameter

Default values:

Parameters	Default Value
EA	1

Parameters	Default Value
CA	1
CUSTOMCONFIG	0
**INSTALLDIR (For GUI mode)	Custom installation path
**INSTALLPATH (For Silent mode)	Custom installation path
EP	14505
CM	default value EM name
IR	1 (Remedial Action scripts are deployed in the Agent directory) For etacfg.ini (Remedial action is disabled)
LS	default value EM name
LP	14503
SC	0
IS_SUFFIX	0
SUFFIX	exists if IS_SUFFIX=1 , please provide the suffix name
DW	0
MIN_GUI	0
AGENTINI	0
PKG_UID	NIL

Note:




If the user wants MAC address as Suffix, then the **SUFFIX** = "<MAC%>".

Note:

If there is space in the attribute values in command line, then the user must pass those values in double quotes ("").

6.2 MSI Installation via GUI without Agent.ini

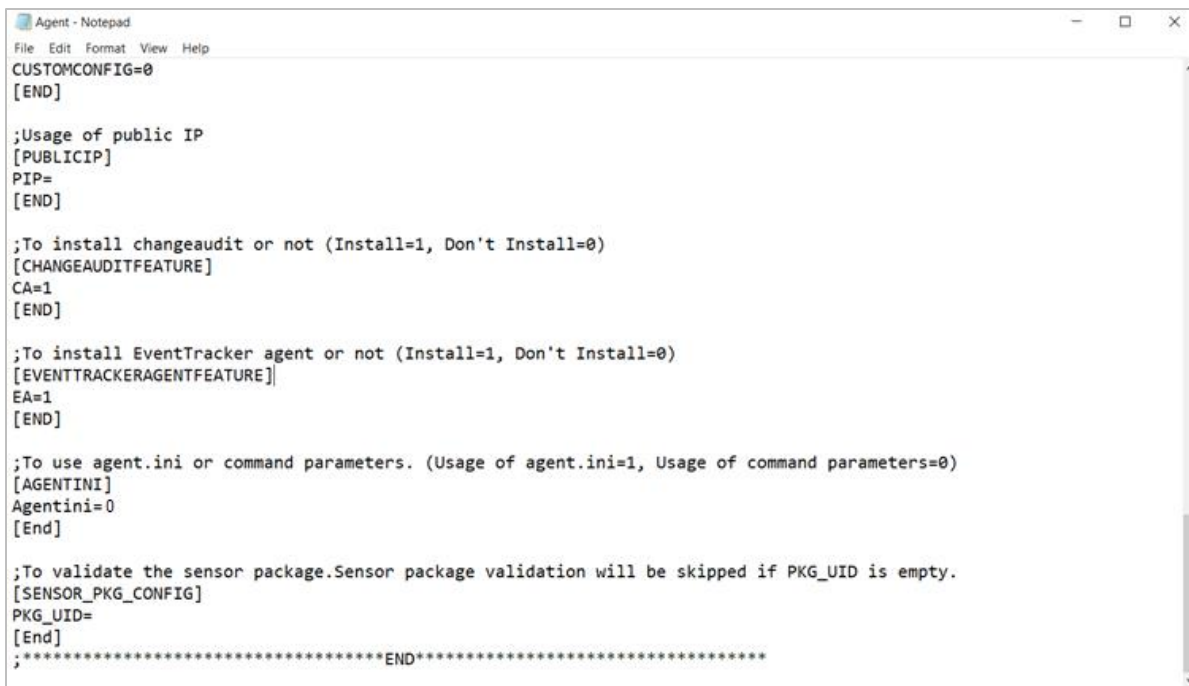
1. Extract the **MSI Package** which contains the following files as shown in the below image.

Name	Date modified	Type	Size
 Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
 EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
 ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

2. Open the **Agent.ini** file and ensure the value for **Agentini=0**.

Note:

By default, the value for **Agentini** is 0.



```

Agent - Notepad
File Edit Format View Help
CUSTOMCONFIG=0
[END]

;Usage of public IP
[PUBLICICIP]
PIP=
[END]

;To install changeaudit or not (Install=1, Don't Install=0)
[CHANGEAUDITFEATURE]
CA=1
[END]

;To install EventTracker agent or not (Install=1, Don't Install=0)
[EVENTTRACKERAGENTFEATURE]
EA=1
[END]

;To use agent.ini or command parameters. (Usage of agent.ini=1, Usage of command parameters=0)
[AGENTINI]
Agentini=0
[End]

;To validate the sensor package.Sensor package validation will be skipped if PKG_UID is empty.
[SENSOR_PKG_CONFIG]
PKG_UID=
[End]
;*****END*****

```

Note:

Refer the parameter abbreviation specified in the [GUI and Silent Installation Parameters](#) section for more details.

If the EA and CA field are not specified with any details, by default it will install the Open XDR sensor and the Change Audit sensor.

If the user wants to install only the Open XDR sensor, then the value for CA must be **0** and vice-versa.

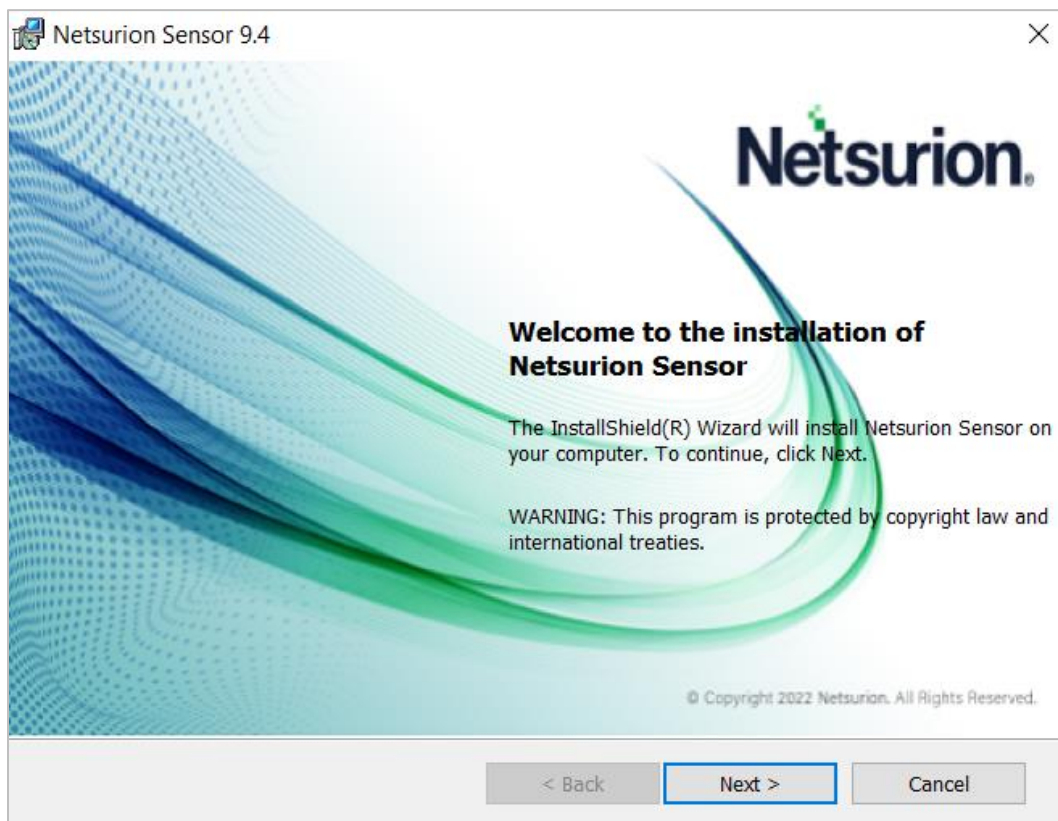
3. After making the necessary changes, save the **Agent.ini** file.
4. Then, launch the Command prompt as **“Run as Administrator”**.

5. Change the directory to **AgentMSI_94**.
6. Provide the following command with the required CUSTOMCONFIG value.

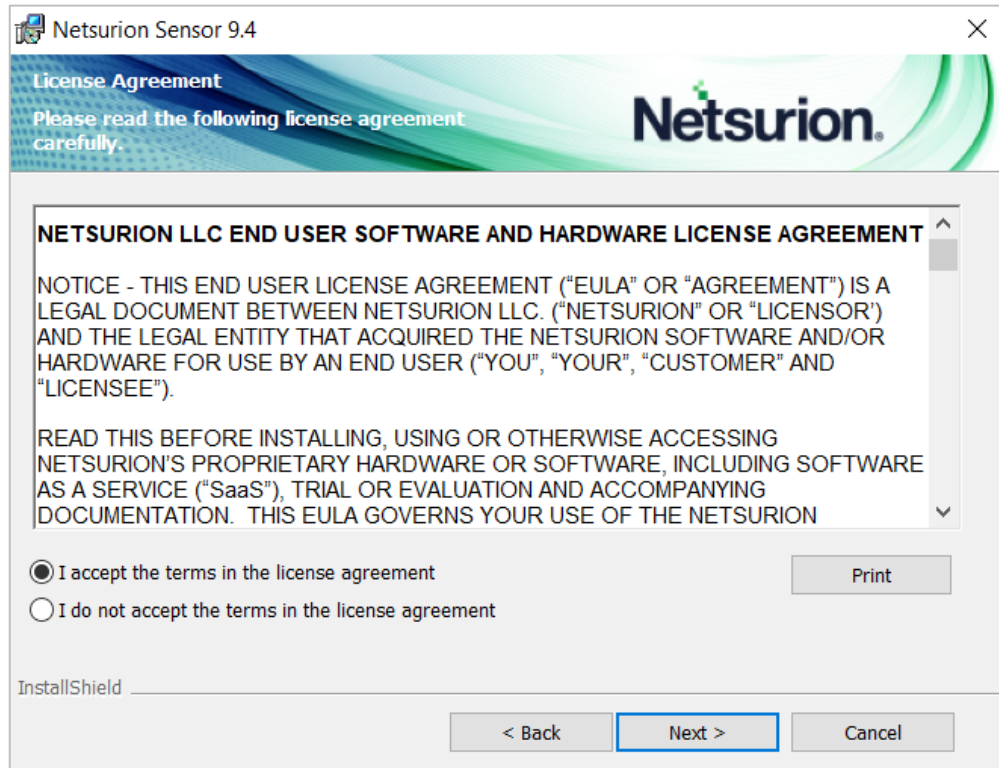
```
EventTrackerSensor.msi EA=1 CA=1 CUSTOMCONFIG=0(or 3/4) EM=Enterprise
Manager name EP=Manager port number CM=Change Audit Manager name IR=1
LS=License server name LP=License port number MIN_GUI=0 IS_SUFFIX=1
SUFFIX=Suffix name SUPPORT_CONTACTS=Contact details
```

```
C:\Users\ [redacted] \AgentMSI_94>EventTrackerSensor.msi EA=
1 CA=1 CUSTOMCONFIG=0 EM=[redacted] EP=14505 CM=[redacted]
IR=1 LS=[redacted] LP=14503 MIN_GUI=0 IS_SUFFIX=1 SUFFIX=MSI
-9.4
```

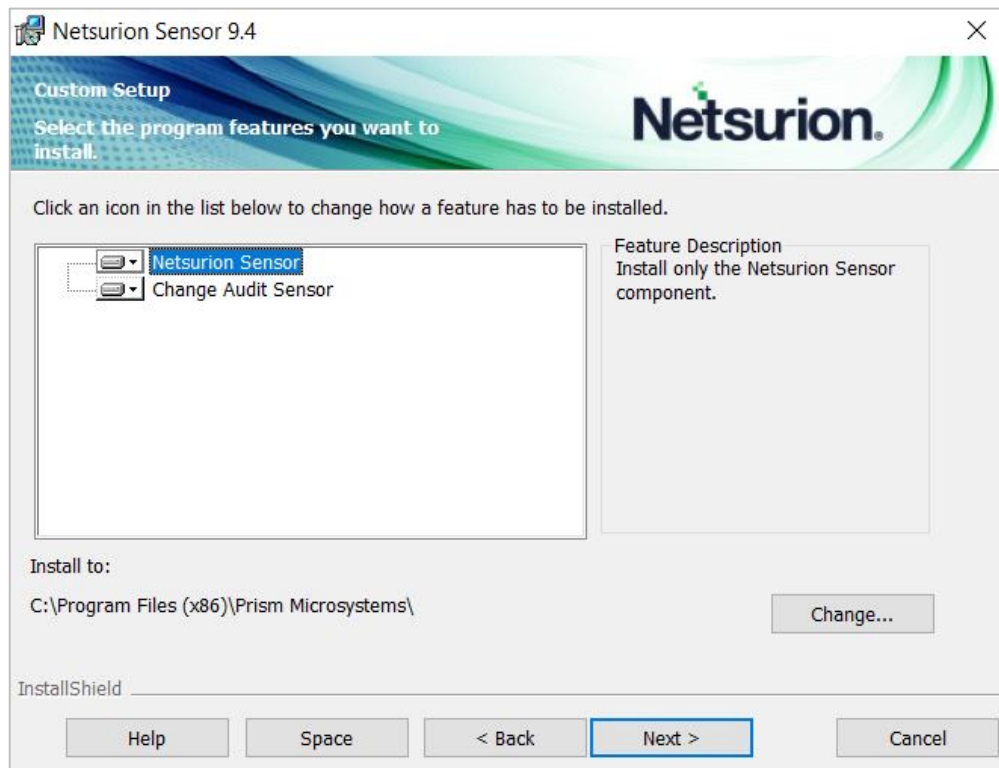
7. Press the **Enter** key after providing the command and **Netsurion Open XDR InstallShield Wizard** interface will appear.
8. Click **Next >** to proceed with the GUI installation.






9. Read the **License Agreement** and select the option *'I accept the terms in the license agreement'*, and then click **Next >** to proceed.



10. In **Custom Setup**, select Netsurion Sensor and (or) Change Audit Sensor based on the requirement.



- In **Custom Setup**, click the folder  icon to select the required installation option.

	This feature will be installed on local hard drive.
	This feature, and all subfeatures, will be installed on local hard drive.
	This feature will not be available.

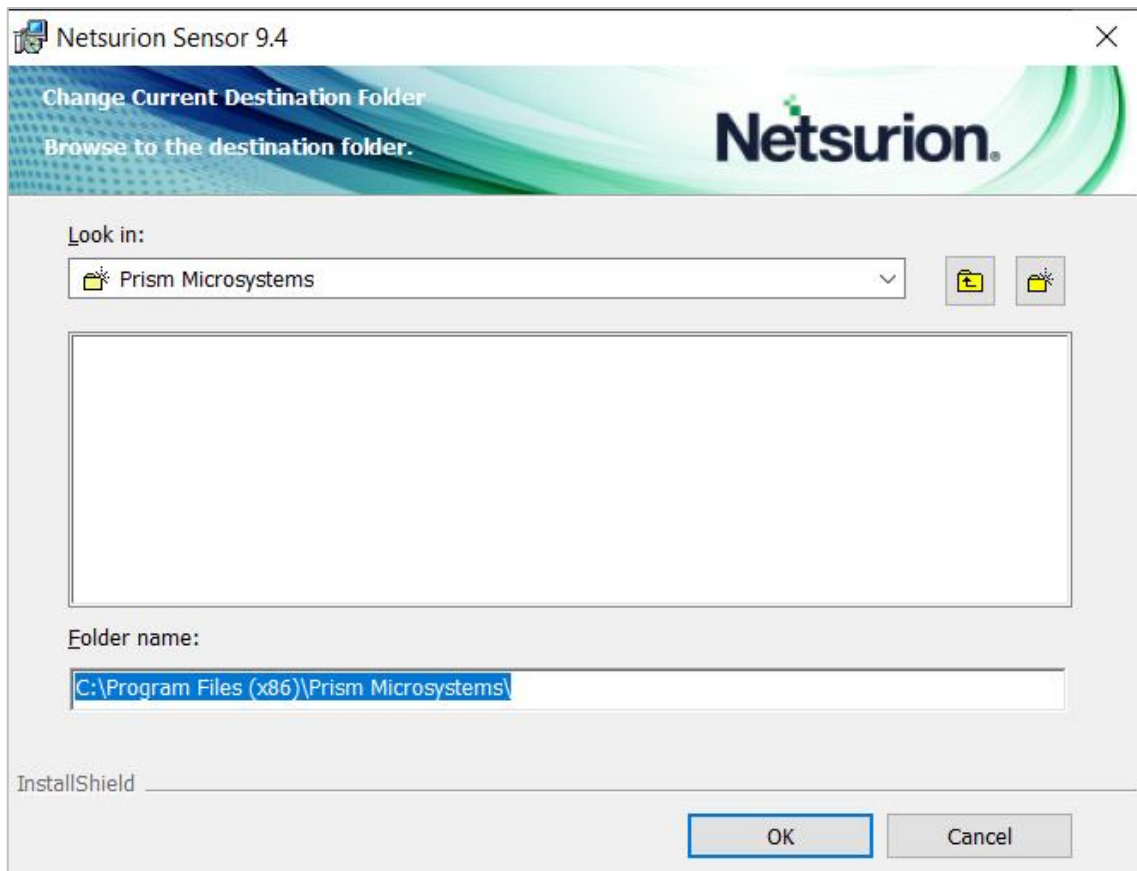
Note:

Select ***'This feature will be installed on local hard drive'*** option to install only the sensor without including its sub features. (OR),

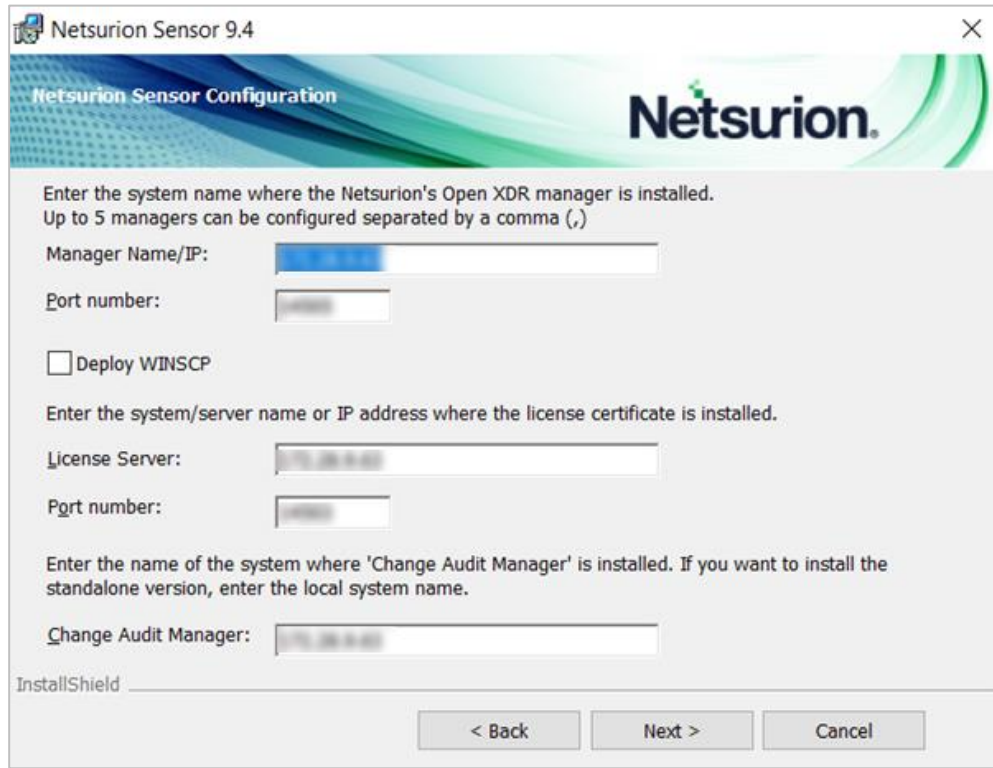
Select ***'This feature, and all sub features, will be installed on local hard drive'*** option to install the sensor as well as its sub features. (OR),

Select the ***'This feature will not be available'*** option if you do not wish to install the sensor.

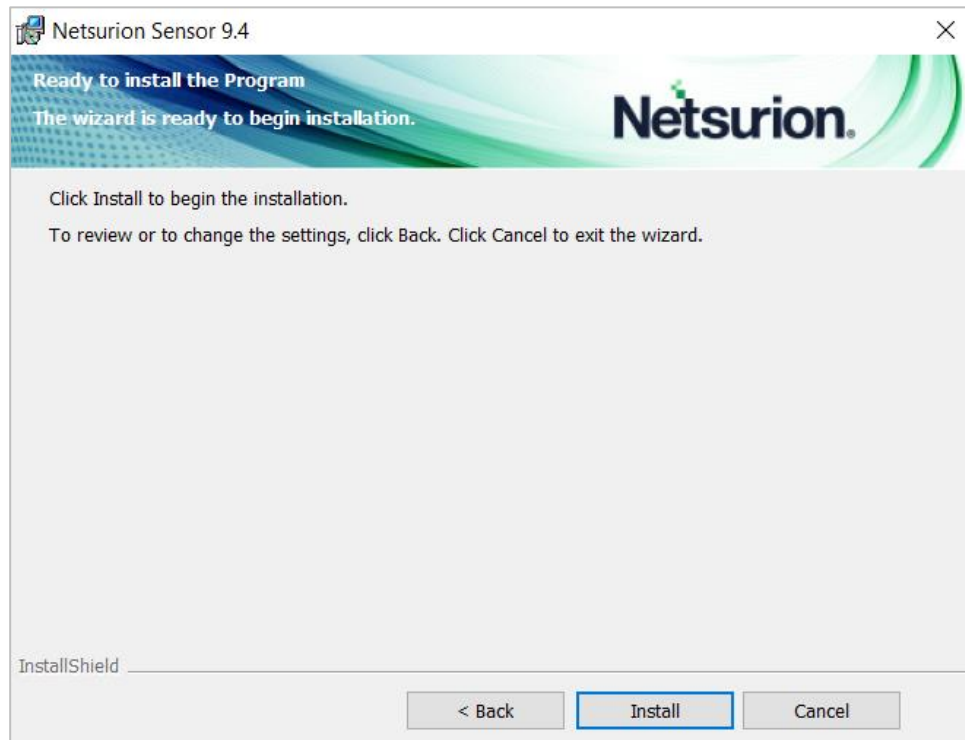
11. Then, click the **Change** button to change the installation path of the sensor and then click **Next >** to proceed.



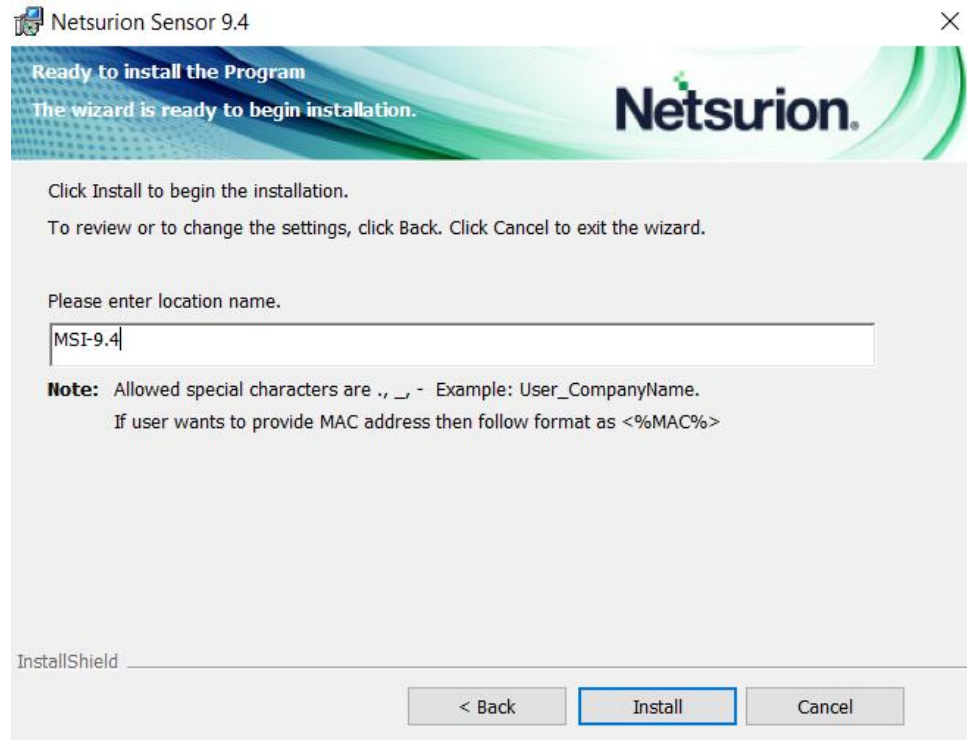
- In **Netsurion Sensor Configuration**, all the details will be fetched from the command line. Click **Next >** to proceed.



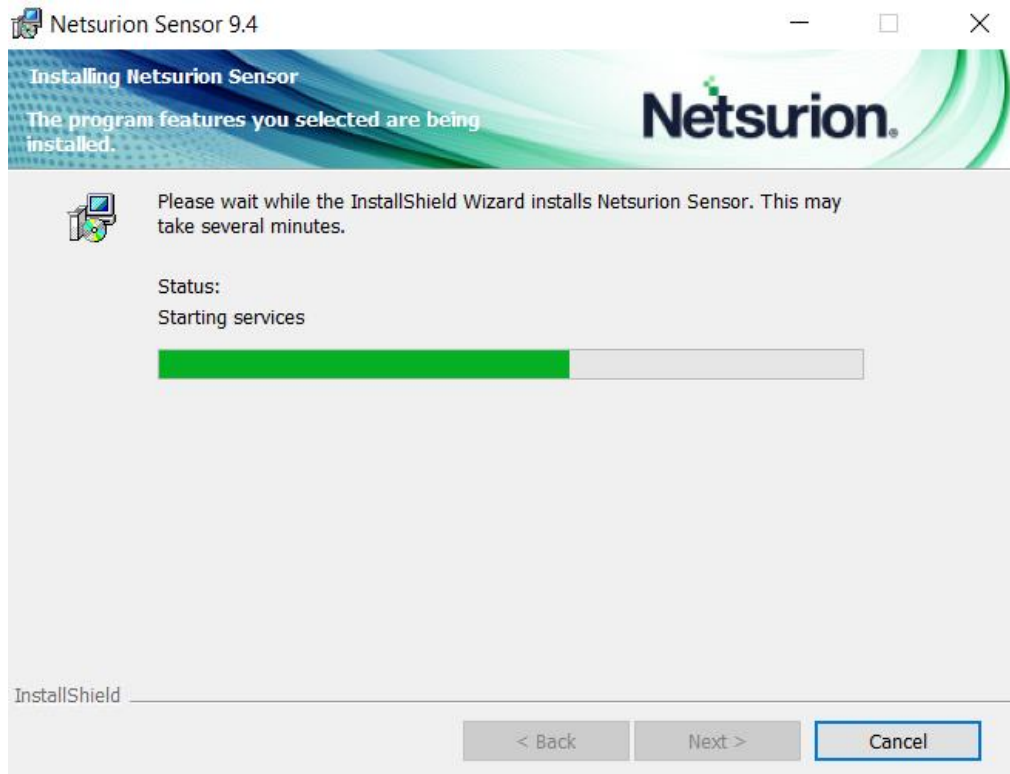
- The following **Ready to Install the Program** wizard appears if the **Command Line** contains the parameter for **IS_SUFFIX=0**. Click **Install**.



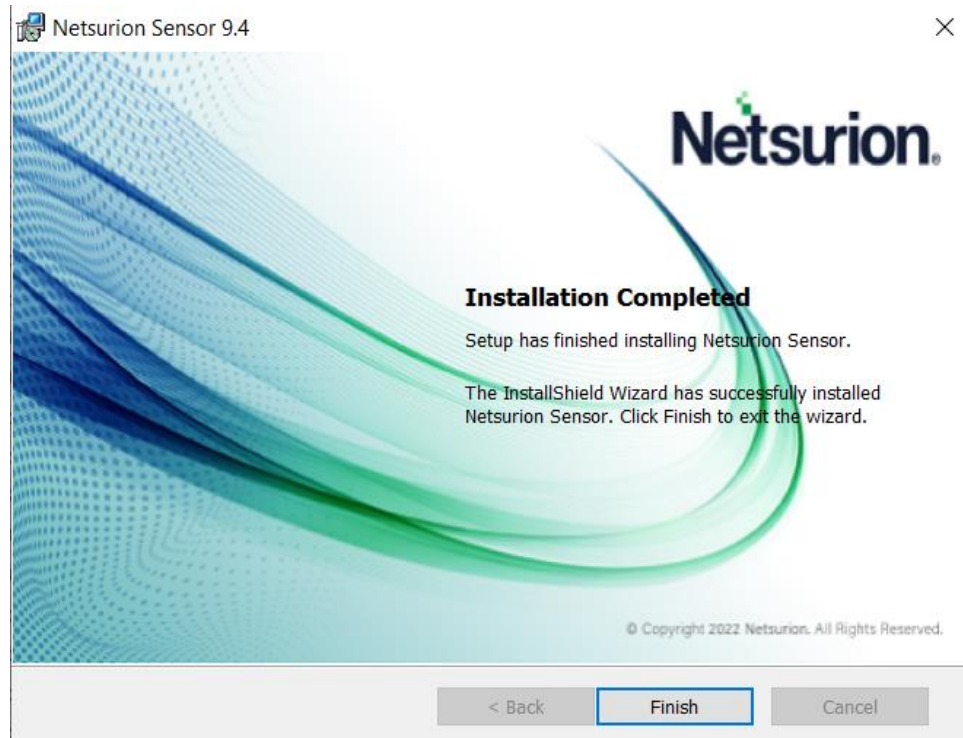
The following **Ready to Install the Program** wizard appears if the **Command Line** contains the parameter for **IS_SUFFIX=1** and the location name displayed in the field is determined by the value specified for the parameter **SUFFIX**.



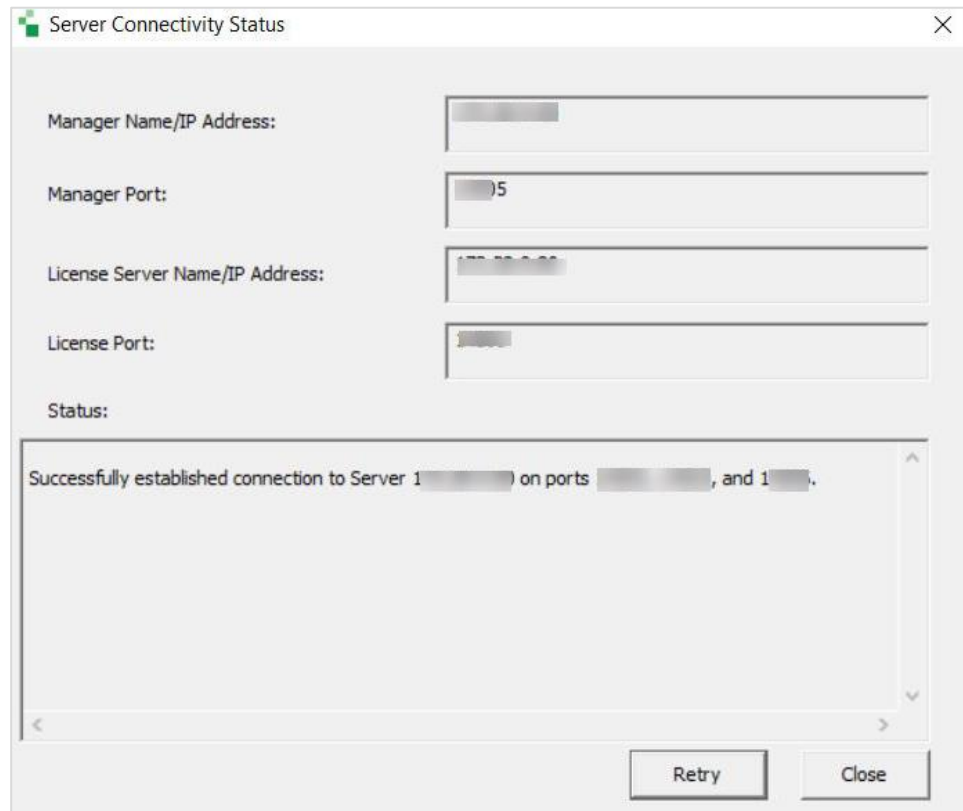
It may take a few minutes for the installation to process.



14. After the installation is complete, click **Finish**.



15. The **Server Connectivity Status** window will be displayed providing the connectivity status. Click **Close**.



Procedure to install with etaconfig.ini file.

1. Extract the **MSI Package** which contains the following files as shown in the below image.

Name	Date modified	Type	Size
Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

2. Then, place the necessary **etaconfig.ini** file within the MSI package as shown in the below image.

Name	Date modified	Type	Size
Agent	3/2023 7:00 AM	Configuration setti...	3 KB
etaconfig	/2023 1:00 AM	Configuration setti...	83 KB
EventTrackerSensor	/2023 9:28 PM	Windows Installer ...	46,387 KB
ReadMe	0/2023 5:28 AM	Text Document	6 KB

Note:

In this installation type, the user must keep the required **etaconfig.ini** file in the extracted MSI package path.

3. Open the **Agent.ini** file and ensure the value for **Agentini=0**.

```

*Agent - Notepad
File Edit Format View Help
CUSTOMCONFIG=2
[END]

;Usage of public IP
[PUBLICICIP]
PIP=
[END]

;To install changeaudit or not (Install=1, Don't Install=0)
[CHANGEAUDITFEATURE]
CA=1
[END]

;To install EventTracker agent or not (Install=1, Don't Install=0)
[EVENTTRACKERAGENTFEATURE]
EA=1
[END]

;To use agent.ini or command parameters. (Usage of agent.ini=1, Usage of command parameters=0)
[AGENTINI]
Agentini=0
[End]

;To validate the sensor package.Sensor package validation will be skipped if PKG_UID is empty.
[SENSOR_PKG_CONFIG]
PKG_UID=
[End]
;*****END*****

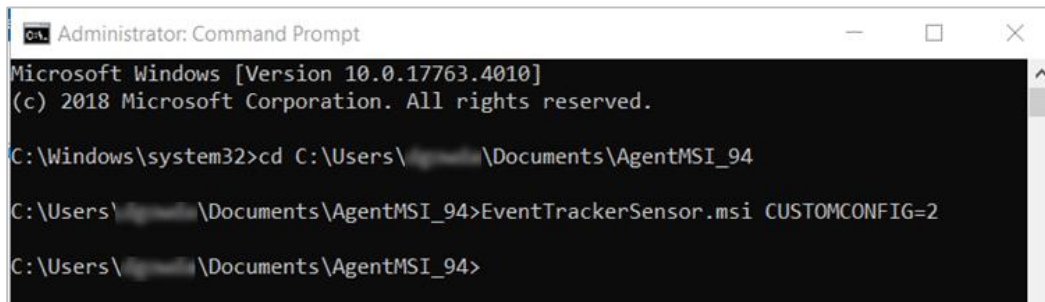
```

Note:

All the necessary parameter details will be fetched from the **etaconfig.ini** file and it is not required to run any parameters from the command line except for **“EventTrackersensor.msi CUSTOMCONFIG=2”**.

To install the sensor with etacfg.ini file,

1. Launch Command prompt as “Run as Administrator”.
2. Change directory to **AgentMSI_94**.
3. Run the command - **EventTrackersensor.msi CUSTOMCONFIG=2** to launch the **InstallShield Wizard**.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.4010]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\ [redacted] \Documents\AgentMSI_94

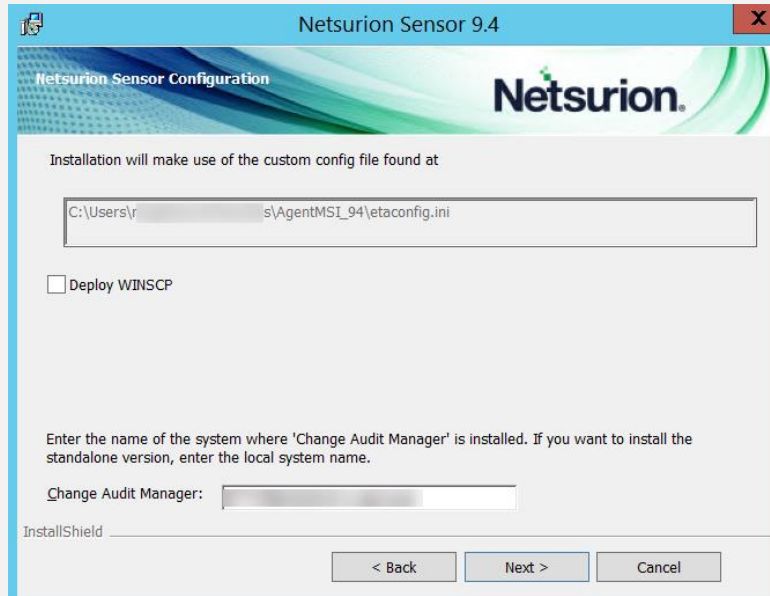
C:\Users\ [redacted] \Documents\AgentMSI_94>EventTrackerSensor.msi CUSTOMCONFIG=2

C:\Users\ [redacted] \Documents\AgentMSI_94>
  
```

Refer the GUI Installation procedure from [Step 8](#) to [Step 14](#) to proceed with the installation.

Note:

In the **InstallShield** utility > **Netsurion Sensor Configuration** window ensure the etacfg.ini path and the Change Audit Manager details and click **Next** to proceed with the installation.



6.3 MSI Installation via Silent mode without Agent.ini

1. Launch the Command prompt as “Run as Administrator”.
2. Change the directory to AgentMSI_94.
3. Use any of the following commands based on the requirement.

Mandatory Parameters

Parameter	Default Value
EM	Mandatory Parameter

Default values

Parameter	Default Value
EA	1
CA	1
CUSTOMCONFIG	0
INSTALLPATH	Custom installation path
EP	14505
CM	default value EM name
IR	1(Remedial Action scripts are deployed in the Agent directory) For etacfg.ini (Remedial action is disabled)
LS	default value EM name
LP	14503
IS_SUFFIX	0
SUFFIX	exists if IS_SUFFIX=1 , please provide the suffix name

- Provide the following command with the required CUSTOMCONFIG value.

When CUSTOMCONFIG = 0 (or 3/4),

```
EventTrackersensor.msi EA=1 CA=1 CUSTOMCONFIG=0(or 3/4) EM=Enterprise
Manager name EP=Manager port number CM=Change Audit Manager name IR=1
LS=License server name LP=License port number DW=Deploy WinSCP
IS_SUFFIX=1 SUFFIX=Suffix name SUPPORT_CONTACTS=Contact details
```



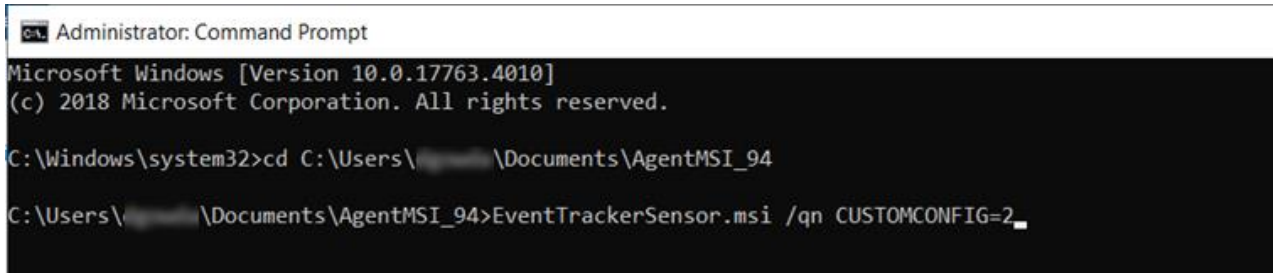
```
Administrator: Command Prompt
C:\Windows\system32>cd C:\Users\...s\AgentMSI_94
C:\Users\...s\AgentMSI_94>etacfg.ini EventTrackerSensor.msi EA=1 CA=1
CUSTOMCONFIG=0 EM=... EP=14505 CM=... IR=1 LS=... LP=
14503 IS_SUFFIX=1 SUFFIX=MSI-9.4
```

When CUSTOMCONFIG = 2,

```
EventTrackersensor.msi /qn CUSTOMCONFIG=2 //Customer Existing etacfg.ini .
```

Note:

In this installation type, keep the required etacfg.ini file in the path where the MSI package is extracted.






Note:

All the necessary parameter details will be fetched from the **etacfg.ini** file and it is not required to run any parameters from the command line except for “**EventTrackersensor.msi/qn CUSTOMCONFIG=2**”.

7 Deploying through Agent.ini File

7.1 MSI Installation via GUI Mode

1. Extract the **MSI Package** which has the following files as shown in the below image.

Name	Date modified	Type	Size
 Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
 EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
 ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

2. Go to the **Agent.ini** file and update the value for **Agentini=1**.

Note:

Update the following mandatory fields in the **Agent.ini** file.

EM, EP, CM (if the user is installing Change Audit), LS, LP, CUSTOMCONFIG, CA, EA and AGENTINI.

For example,

```

;*****Copyright 2022 Netsurion LLC. All Rights Reserved.*****
;This configuration file will be used to deploy EventTracker/ Change Audit agents
;The location where you wish to place the files. If this section is left blank, the files will be placed in the default location
;i.e. Program Files Folder depending on the OS, for 32 bit it will be "<C:\Program Files>", for 64 bit it will be "<C:\Program Files (x86)>".
;If user wants to specify the install path on 64 bit OS, do not provide the path as "<C:\Program Files>".
[INSTALL_PATH]
INSTALLDIR=
[END]

;Specify the EventTracker manager name. Agent will send events to the
;manager specified here. Up to 5 EventTracker managers can be configured
;separated by a comma(,)
[ENTERPRISE_MANAGER]
EM=
[END]

;Specify the port number on which you wish to send events to EventTracker manager.
[ENTERPRISE_PORT]
EP=14585
[END]

;Specify the change Audit manager name.
[CHANGEAUDIT_MANAGER]
CM=
[END]

;Remedial Actions are scripts or EXEs that can be launched at either the Agent or Manager side,
;in response to events. If this option is enabled, predefined scripts will be placed in the
;EventTracker\Agent\Script folder.
[REMEDIAL_ACTIONS]
IR=1
[END]

;License Server name
[LICENSE_SERVER]
LS=
[END]

;License Server port
[LICENSE_SERVER_PORT]
LP=
[END]

;Deploy WINSCP components
[DEPLOY_WINSXP]
DW=
[END]

;Create startmenu shortcut,For 1 means shortcut enable and 0 means disable.
[SHORTCUT]
SC=1
[END]

;Setup wizard with minimal GUI,For 1 means Minimal Gui enable and 0 means Full GUI wizard.
[MINIMAL_GUI]
MIN_GUI=0
[END]

;Ask for suffix is enable or not, For 1 means enable(GUI will contain control to take input as suffix) and 0 disable (no extra GUI control).
[ENABLE_SUFFIX]
IS_SUFFIX=1
[END]

;System suffix name
[SUFFIX_STRING]
SUFFIX =Windows_11
[END]

;Contact Details
[Contact_Details]
Message = Test
[END]

;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2, Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]

;Usage of public IP
[PUBLICIP]
PIP=
[END]

;To install changeaudit or not (Install=1, Don't Install=0)
[CHANGEAUDITFEATURE]
CA=1
[END]

;To install EventTracker agent or not (Install=1, Don't Install=0)
[EVENTTRACKERAGENTFEATURE]
EA=1
[END]

;To use agent.ini or command parameters. (Usage of agent.ini=1, Usage of command parameters=0)
[AGENTINI]
Agentini=1
[End]

;To validate the sensor package.Sensor package validation will be skipped if PKG_UID is empty.
[SENSOR_PKG_CONFIG]
PKG_UID=
[End]
;*****END*****

```

Note:

Refer the parameter abbreviation specified in the [GUI and Silent Installation Parameters](#) section for more details.

If the user wants to install only the Open XDR sensor, then the CA should be equal to 0 and vice versa.

Types of sensor installation using GUI Mode in Agent.ini

```
CUSTOMCONFIG=0 (or 3/4) EM = (Manager name) - Enterprise etacconfig.ini
```

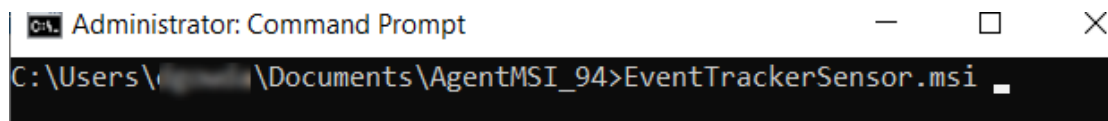
1. Here, fill the **Agent.ini** file with the mandatory fields as illustrated in the [sample image](#), and change the value for CUSTOMCONFIG=0

Example of the modified Agent.ini field.

```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2,
Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]
```

2. Specify the other required parameters in the **Agent.ini** file, as per requirement and save the **Agent.ini** file.
3. Launch the Command Prompt via **Run as Administrator** and change the directory to **AgentMSI_94**.
4. In the **Command Prompt**, execute the following command to launch Netsurion Open XDR sensor InstallShield Wizard.

Command: EventTrackersensor.msi.



Note:

Refer the GUI Installation procedure from [Step 8](#) to [Step 14](#).

CUSTOMCONFIG=2 - Customer Existing etacnfig.ini.

Make sure the custom **etacnfig.ini** is placed in the extracted MSI package as illustrated in the below image.

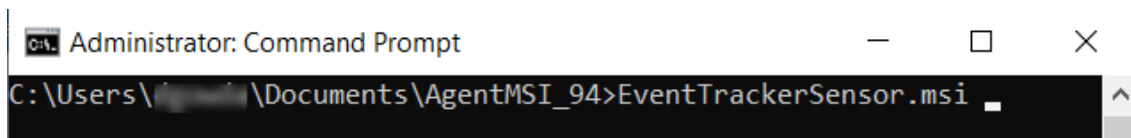
Name	Date modified	Type	Size
Agent	2/13/2023 7:00 AM	Configuration setti...	3 KB
etacnfig	3/7/2023 1:00 AM	Configuration setti...	83 KB
EventTrackerSensor	3/6/2023 9:28 PM	Windows Installer ...	46,387 KB
ReadMe	2/20/2023 5:28 AM	Text Document	6 KB

1. Here, in the **Agent.ini** file, fill only the mandatory fields (that is, EA=1, CA=1, Agent.ini=1) and change the CUSTOMCONFIG=2.

```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2,
Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]
```

2. Save the **Agent.ini** file.
3. Launch the Command Prompt via “**Run as Administrator**” and change the directory to **AgentMSI_94**.
4. In the **Command Prompt**, execute the following command.

Command: EventTrackersensor.msi.






This command will launch Netsurion Open XDR sensor InstallShield Wizard.

Note:

Refer the GUI Installation procedure from [Step 8](#) to [Step 14](#).

7.2 MSI Installation via Silent Mode

1. Extract the MSI Package which has the following files as shown in the below image.

Name	Date modified	Type	Size
 Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
 EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
 ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

2. Go to the **Agent.ini** file and update the value for **Agentini=1**.

Note:

Update the following mandatory fields in the **Agent.ini** file:

EM, EP, CM (if the user is installing Change Audit), LS, LP, CUSTOMCONFIG, CA, EA and AGENTINI. Refer the [sample image](#) for more details.

Note:

Refer the parameter abbreviation specified in the [GUI and Silent Installation Parameters](#) section for more details.

If you require to install only Netsurion Open XDR sensor, then the value for CA should be equal to 0 and vice versa.

Types of sensor installation using Silent Mode in Agent.ini

```
CUSTOMCONFIG=0 (or 3/4) EM = (Manager name) - Enterprise etacconfig.ini
```

1. Here, fill the **Agent.ini** file with the mandatory fields as shown in the [sample image](#), and change the **CUSTOMCONFIG=0(or 3/4)**

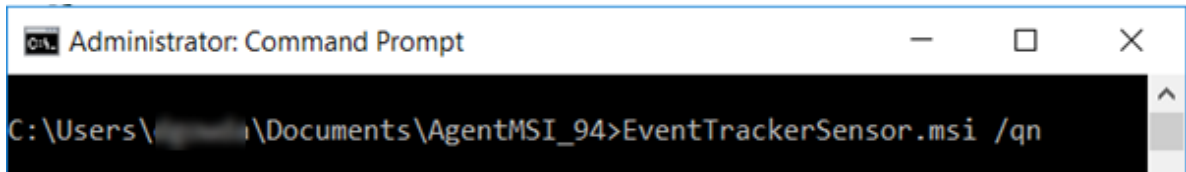
Example of the modified Agent.ini field:

```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2,
Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]
```

2. Specify the other required parameters in the **Agent.ini** file as per requirement and save the **Agent.ini** file.

3. Launch the Command Prompt via **Run as Administrator** and change the directory to **AgentMSI_94**.
4. In the **Command Prompt**, execute the following command.

```
Command: EventTrackersensor.msi /qn
```



The sensor will take some time to get installed. To verify, go to the Install Directory and check the folder structure.

```
CUSTOMCONFIG=2 - Customer Existing etacnfig.ini
```

Make sure the **etacnfig.ini** file is kept in the extracted MSI package as shown below:

Name	Date modified	Type	Size
Agent	2/13/2023 7:00 AM	Configuration setti...	3 KB
etacnfig	3/7/2023 1:00 AM	Configuration setti...	83 KB
EventTrackerSensor	3/6/2023 9:28 PM	Windows Installer ...	46,387 KB
ReadMe	2/20/2023 5:28 AM	Text Document	6 KB

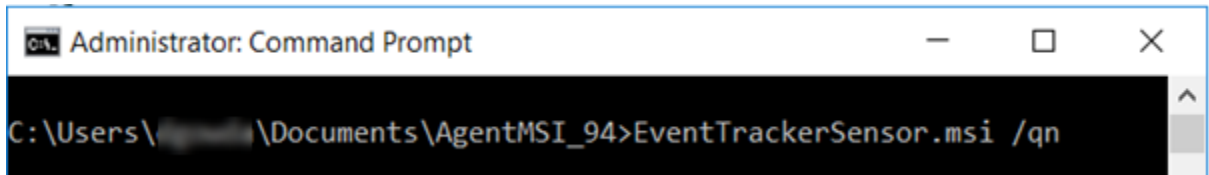
1. Fill in the **Agent.ini** file only with the mandatory fields that is, (EA=1, CA=1, Agent.ini=1) and change the CUSTOMCONFIG=2.

```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2,
Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]
```

2. Save the Agent.ini file.
3. Launch the Command Prompt via **“Run as Administrator”** and change the directory to **AgentMSI_94**.

- In the **Command Prompt**, execute the following command.

```
Command: EventTrackersensor.msi /qn
```



The sensor will take some time to get installed. To verify, go to the Install Directory and check the folder structure.

8 Deploying via Group Policy

8.1 Preparing Agent.ini File with Configuration Settings

Modify **Agent.ini** and change **EM** (ENTERPRISE_MANAGER), **CM** (Change Audit manager), **INSTALLDIR** (the Open XDR sensor install directory for custom path), **EP** (ENTERPRISE_PORT), **LS** (License server name/ FQDN or the Hostname where the digital certificate is installed), **LP** (License server port number), **CUSTOMCONFIG** (Generic=0, Custom=2 and Generic with TCP=3), **CA** (CHANGEAUDITFEATURE), **EA** (EVENTTRACKERAGENTFEATURE), **Agentini** (AGENTINI) value appropriately. The other fields can also be changed as per requirement.

Configuration Settings	Sample Configuration
[INSTALL_PATH]	[INSTALL_PATH]
INSTALLDIR=<Installation directory if agent need to be installed in other than default path>	INSTALLDIR=
[END]	[END]
[ENTERPRISE_MANAGER]	[ENTERPRISE_MANAGER]
EM=<EventTracker Manager Hostname or FQDN>	EM=Win2k3x64
[END]	[END]
[ENTERPRISE_PORT]	[ENTERPRISE_PORT]
EP=<EventTracker Enterprise Port number>	EP=14505
[END]	[END]
[CHANGEAUDIT_MANAGER]	[CHANGEAUDIT_MANAGER]
CM=<Change Audit Manager Hostname or FQDN>	CM=Win2k3x64
	[END]
	[REMEDIAL_ACTIONS]

Configuration Settings	Sample Configuration
<pre>[END] [REMEDIAL_ACTIONS] IR=1 [END] [LICENSE_SERVER] LS=<The server name/ FQDN or the Hostname where the digital certificate is installed> [END] [LICENSE_SERVER_PORT] LP=<License server port number> [END] Deploy WINSXP components [DEPLOY_WINSXP] DW= '1' or '0' [END] Create startmenu shortcut [SHORTCUT] SC= '1' or '0' [END] Setup wizard with minimal GUI [MINIMAL_GUI] MIN_GUI='1' or '0' [END] Ask for suffix is enable or not [ENABLE_SUFFIX] IS_SUFFIX=0 [END] System suffix name [SUFFIX_STRING]</pre>	<pre>IR=1 [END] [LICENSE_SERVER] LS=Win2k3x64 [END] [LICENSE_SERVER_PORT] LP=14503 [END] Deploy WINSXP components [DEPLOY_WINSXP] DW=1 [END] Create startmenu shortcut [SHORTCUT] SC=1 [END] Setup wizard with minimal GUI [MINIMAL_GUI] MIN_GUI=1 [END] Ask for suffix is enable or not [ENABLE_SUFFIX] IS_SUFFIX=1 [END] System suffix name [SUFFIX_STRING] SUFFIX = EventTracker [END] Contact Details</pre>

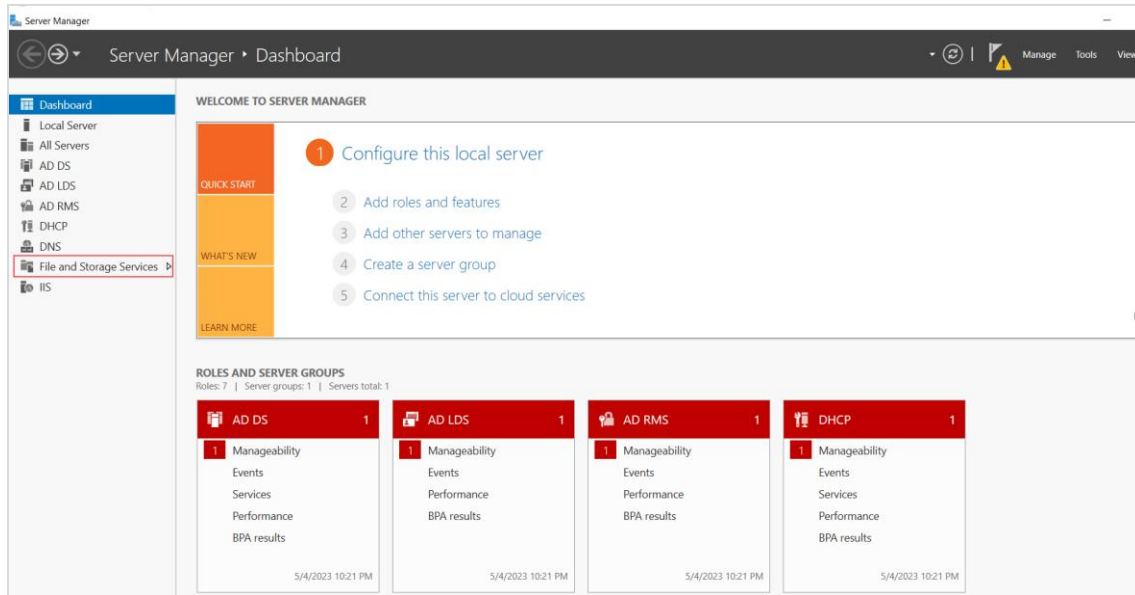
Configuration Settings	Sample Configuration
<pre> SUFFIX = [END] Contact Details [Contact_Details] Message = [END] Usage of custom config ini file (Generic=0, Custom=2 and Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4) [CONFIGURATION] CUSTOMCONFIG=0/2/3/4 [END] Usage of public IP [PROTECT IP] PIP=<Protect IP> [END] To install Change Audit or not (Install=1, Don't Install=0) [CHANGEAUDITFEATURE] CA=0/1 [END] To install EventTracker Agent or not (Install=1, Don't Install=0) [EVENTTRACKERAGENTFEATURE] EA=0/1 [END] To use Agent.ini or command parameters. (Usage of Agent.ini=1, Usage of command parameters=0) [AGENTINI] Agentini=0/1 </pre>	<pre> [Contact_Details] Message = 999-888-777 [END] Usage of custom config ini file (Generic=0, Custom=2 and Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4) [CONFIGURATION] CUSTOMCONFIG=0 [END] Usage of public IP [PROTECT IP] PIP=193.XXX.X.5X5 [END] To install Change Audit or not (Install=1, Don't Install=0) [CHANGEAUDITFEATURE] CA=1 [END] To install EventTracker Agent or not (Install=1, Don't Install=0) [EVENTTRACKERAGENTFEATURE] EA=1 [END] To use Agent.ini or command parameters. (Usage of Agent.ini=1, Usage of command parameters=0) [AGENTINI] Agentini=1 [End] </pre>

Configuration Settings	Sample Configuration
[End]	

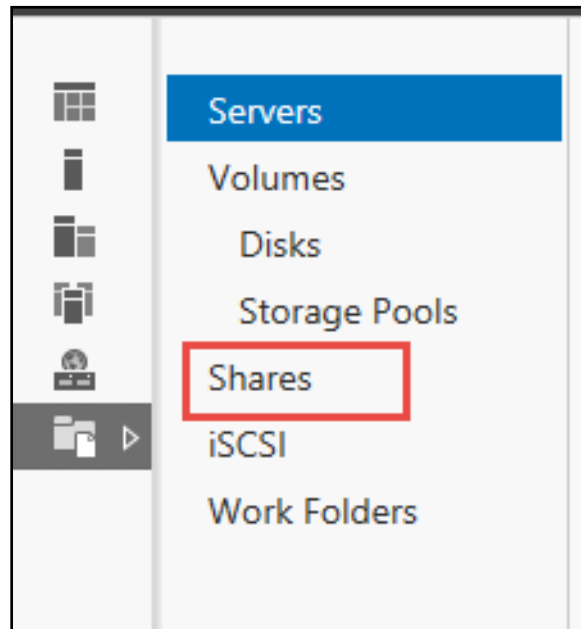
Create a network share on the server and allow **Domain Computers** to have at least **READ** access permission.

8.2 Creating a Network Share

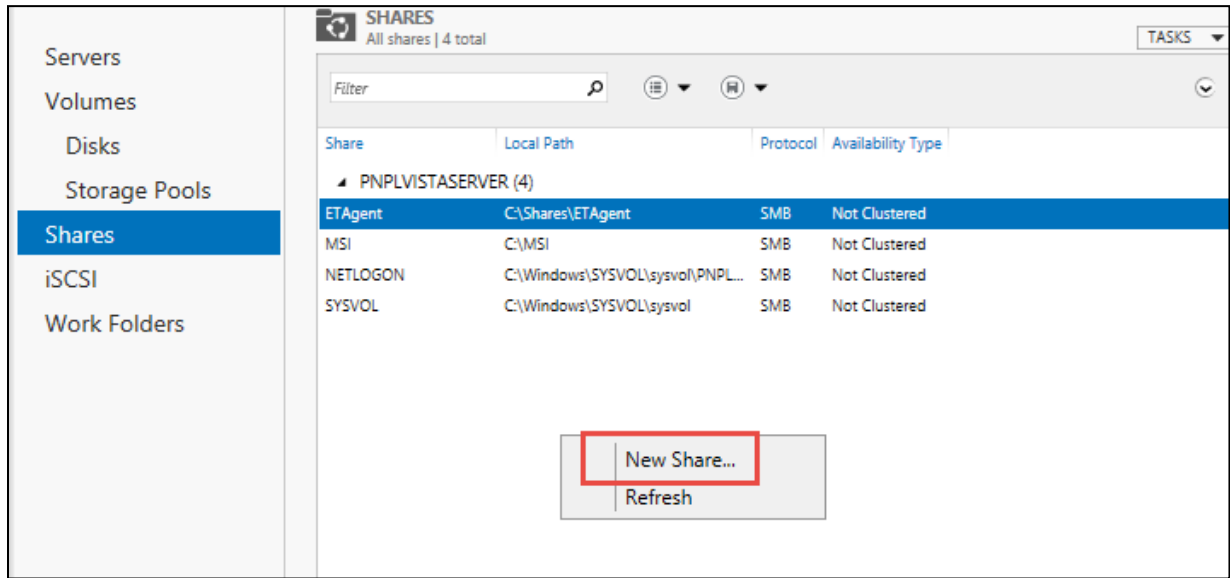
1. Go to the **Server Manager** and click **File and Storage Services**.



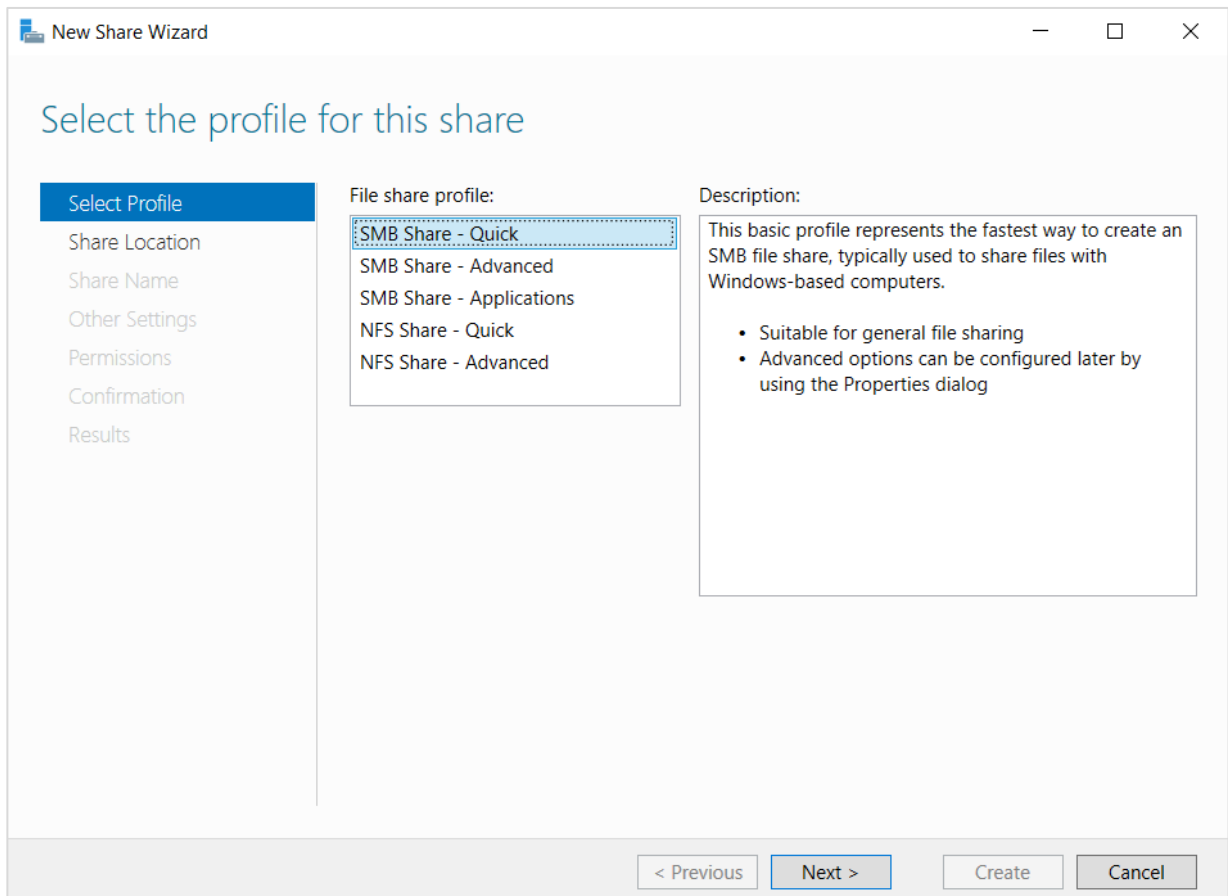
2. Here, in the right pane, click **Shares**.



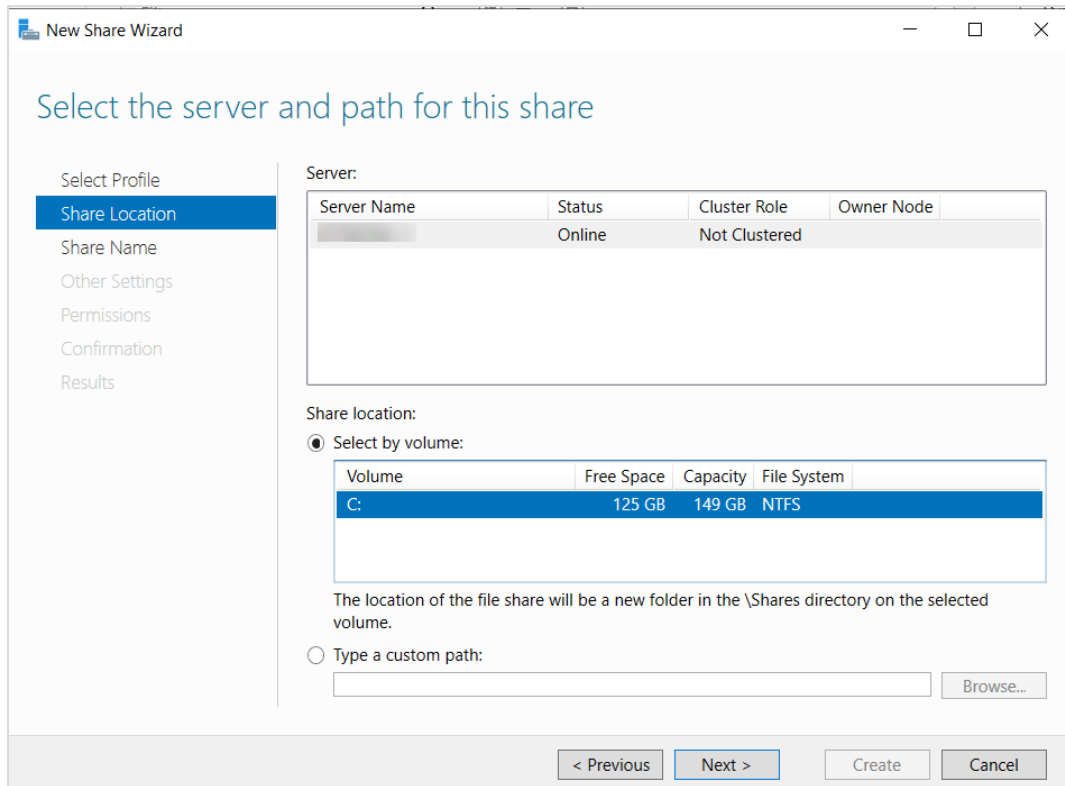
- From the **Shares** interface, right-click on the screen and click **New Share**.



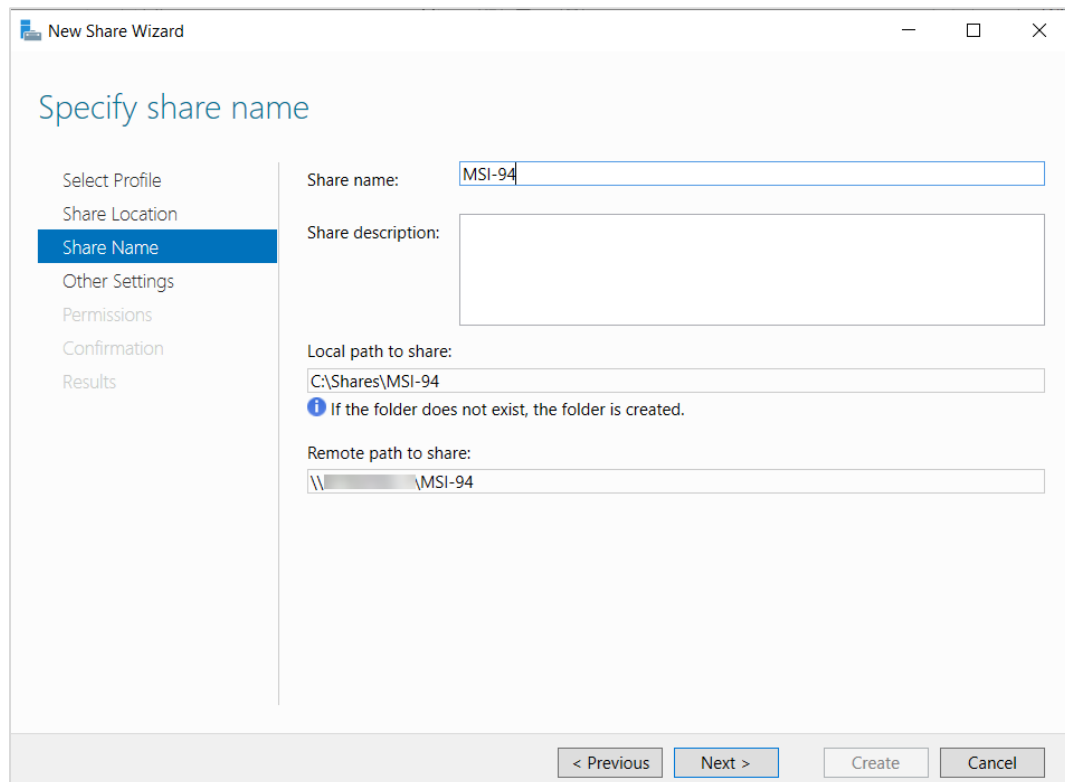
- In the **New Share Wizard**, go to **Select Profile** and select the appropriate **File share profile**, and then click **Next**.



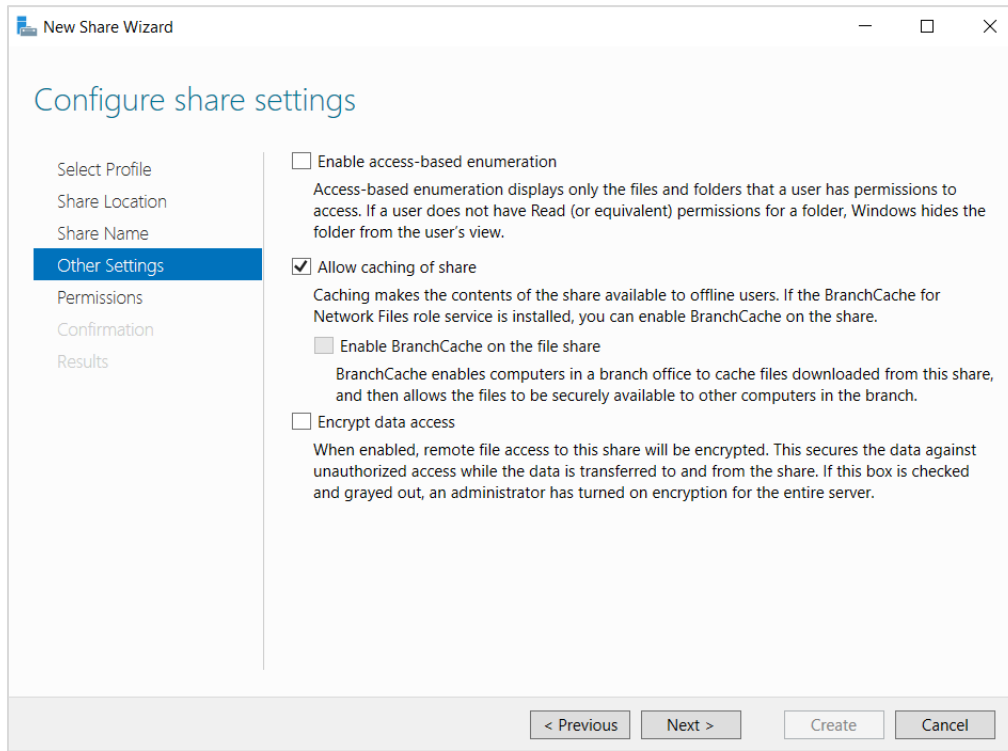
- In the **Share Location** section, select the appropriate file share location and click **Next**.



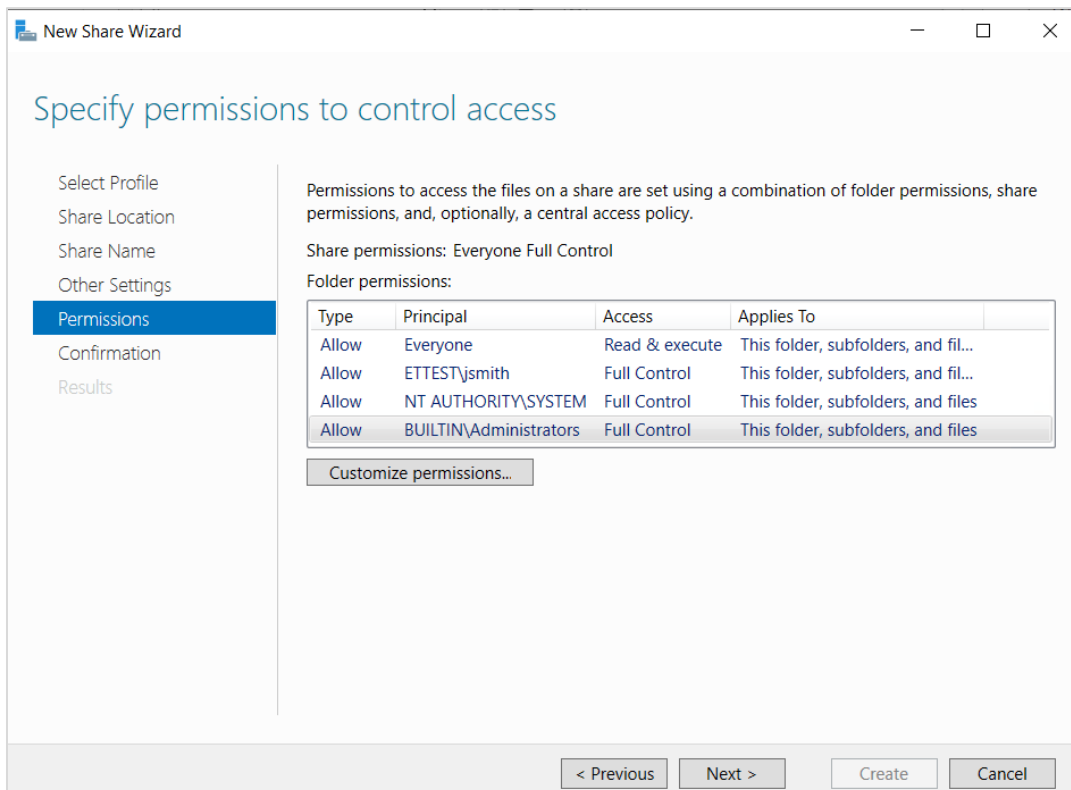
- Type in the Share folder Name to be shared and click **Next**.



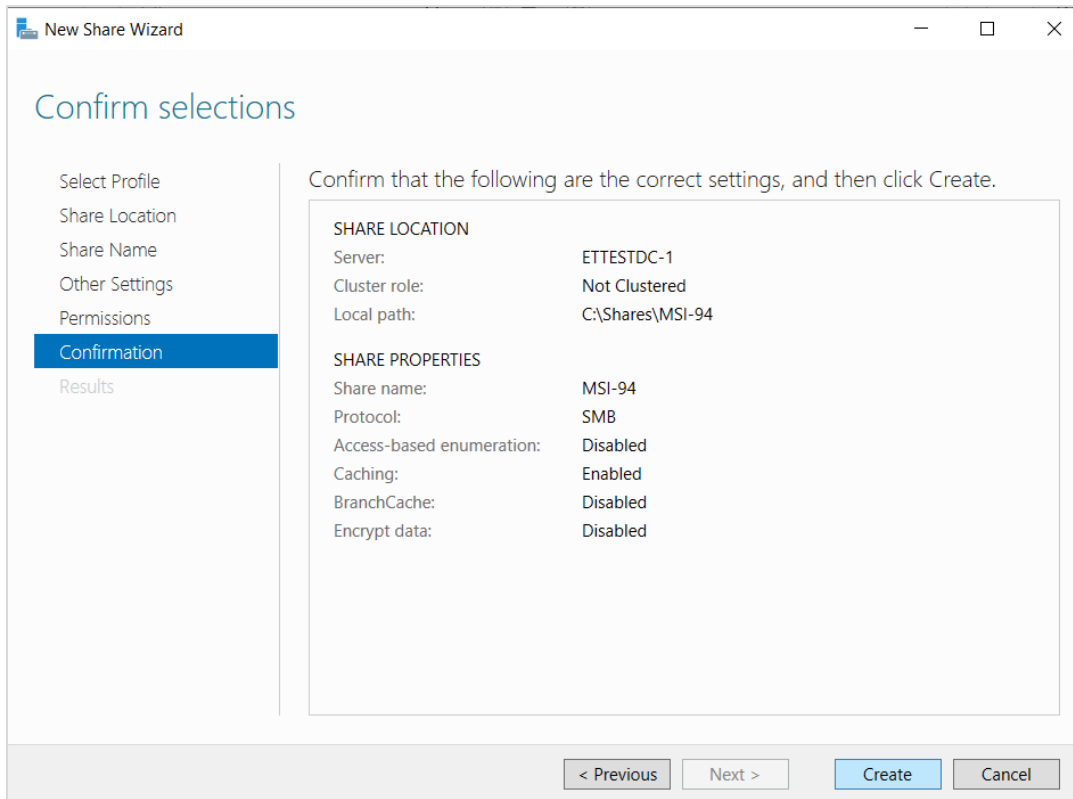
7. In **Other Settings**, keep the default selection and click **Next** to proceed.



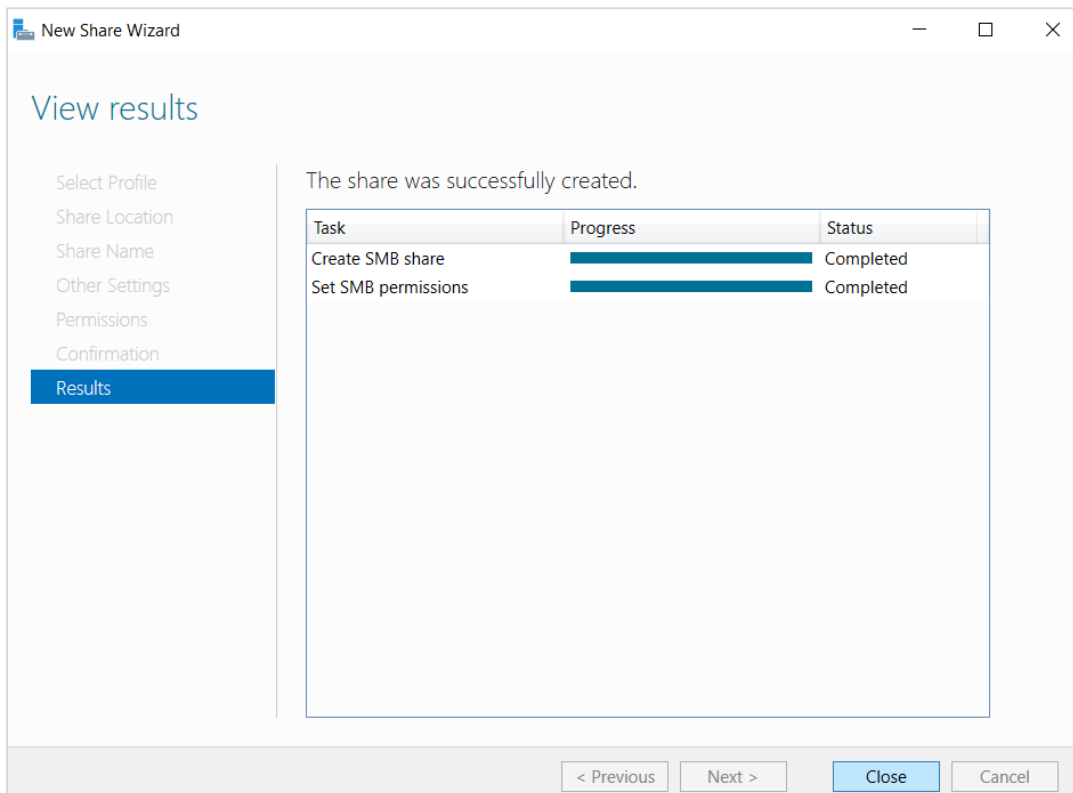
8. In **Permissions**, the following access should be allowed for successful installation. Click **Next** to proceed.



9. In Confirm selections, verify the details, and click **Create**.






10. Once the creation is complete, click **Close**.



11. Copy the **AgentMSI_94** folder to the created Network Share folder.

The Network Share folder should have the below files.

Name	Date modified	Type	Size
 Agent.ini	4/5/2023 4:42 PM	Configuration setti...	3 KB
 EventTrackerSensor.msi	4/5/2023 12:39 PM	Windows Installer ...	43,846 KB
 ReadMe.txt	4/5/2023 12:39 PM	Text Document	6 KB

Parameters in Agent.ini file

Argument	Description
INSTALLDIR -	<p>If this parameter is left blank, the files will be installed in the default location that is, %ProgramFiles%\Prism Microsystems. Else specify the path where you require to install the files.</p> <p>Note: All the parameters will be read from the "Agent.ini" file when the installer is running silently.</p>
EM -	<p>Specify the Enterprise Manager name. The sensor will send events to the Manager specified here.</p> <p>Note: Enterprise Manager is same as Open XDR Manager.</p> <p>Note: If you require to install Netsurion Open XDR sensor, then Enterprise Manager (EM) name is mandatory.</p>
EP -	<p>Specify the appropriate port number to send events from Netsurion Open XDR sensor to Enterprise Manager.</p>
CM -	<p>Specify the Change Audit Manager name.</p> <p>Note: If you require to install Change Audit sensor, then Change Audit Manager Name (CM) is mandatory.</p>

Argument	Description
<p>IR -</p>	<p>If 1, then remedial actions will be installed, and if 0, then remedial actions will not be installed.</p> <p>Note: Remedial Actions are scripts or EXEs that can be launched at either the sensor or Manager side in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder.</p>
<p>LS -</p>	<p>It is the system name/ FQDN/ HOSTNAME where the digital certificate is installed. If this parameter is left blank, the value will be read from EM (that is, License server name will be the same as Enterprise Manager).</p>
<p>LP -</p>	<p>If this parameter is left blank, the default port value (that is, 14503) will be taken by the installer.</p>
<p>DW -</p>	<p>It is used for deploying the WINS CP components. If the value is empty, then WINS CP components will not be installed. If the value is '1', then WINS CP components will be installed.</p>
<p>SC -</p>	<p>Shortcuts will not be created in startmenu if the value is '0' or left blank. If the value is '1', then shortcut will be created in startmenu.</p>
<p>MIN_GUI -</p>	<p>If the value is '1', then it sets the wizard with minimal GUI. If the value is '0', it sets the full GUI wizard.</p> <p>Note: Though the wizard is set with minimal GUI mode, the location details will be displayed when IS_SUFFIX is enabled with appropriate SUFFIX name.</p>
<p>IS SUFFIX -</p>	<p>If the value is "0" then IS SUFFIX will be disabled and if the value is "1" it will be enabled.</p>
<p>SUFFIX -</p>	<p>Enter the system suffix name in this field.</p> <p>Note: In silent/GPO installation, the installation will be aborted if the suffix (IS SUFFIX) is in enable state and the suffix value is left blank in the Agent.ini file.</p>
<p>MESSAGE -</p>	<p>Customized Contact details.</p>

Argument	Description
CUSTOMCONFIG -	Usage of the custom configurations in the Agent.ini file. <ul style="list-style-type: none"> ▪ EventTrackersensor.msi CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etacnfig.ini in UDP mode. ▪ EventTrackersensor.msi CUSTOMCONFIG=3 EM = (Manager name) - Enterprise etacnfig.ini in TCP mode. ▪ EventTrackersensor.msi CUSTOMCONFIG=2 - Customer Existing etacnfig.ini ▪ EventTrackersensor.msi CUSTOMCONFIG=4 EM= (Manager name) Generic TCP Audit Anomalous Login.
PIP -	Usage of Protect IP.
CA -	To install Change Audit.
EA -	To install EventTracker sensor.
AGENTINI -	To use Agent.ini or command parameters (Agentini=1 uses the Agent.ini file, Agentini=0 uses the command parameters). <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>Note:</p> <p>For deploying Netsurion Open XDR sensors via GPO, the value for the parameter Agentini=1.</p> </div>

Note:

Microsoft XML Core Services (MSXML) is installed along with the MSI sensor Installer setup for 32-bit and 64-bit machines respectively.

Note:

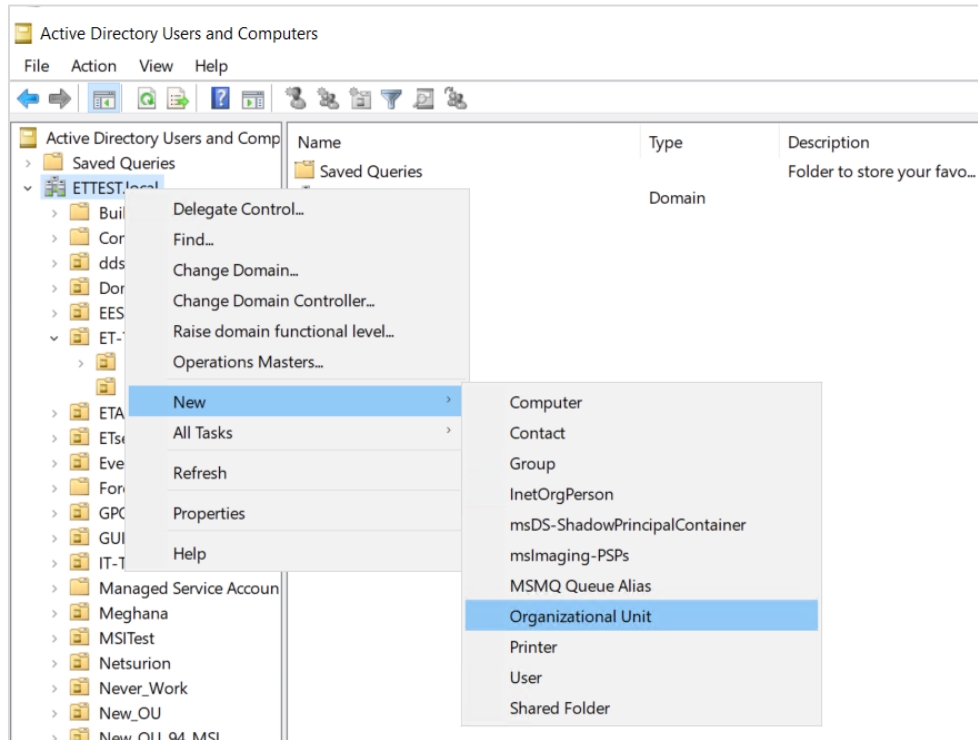
The Microsoft Visual C++ 2008 Redistributable Package (x86) is installed along with the MSI sensor Installer setup.

Note:

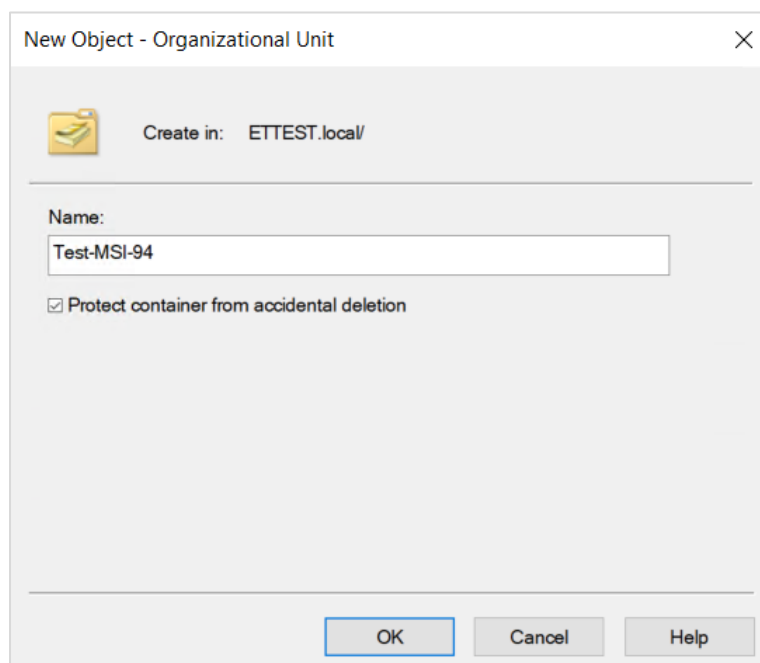
Before deploying the sensor, make sure that the sensor system(s) and domain controller are synchronized.

8.3 Assigning Systems to New Organization Unit

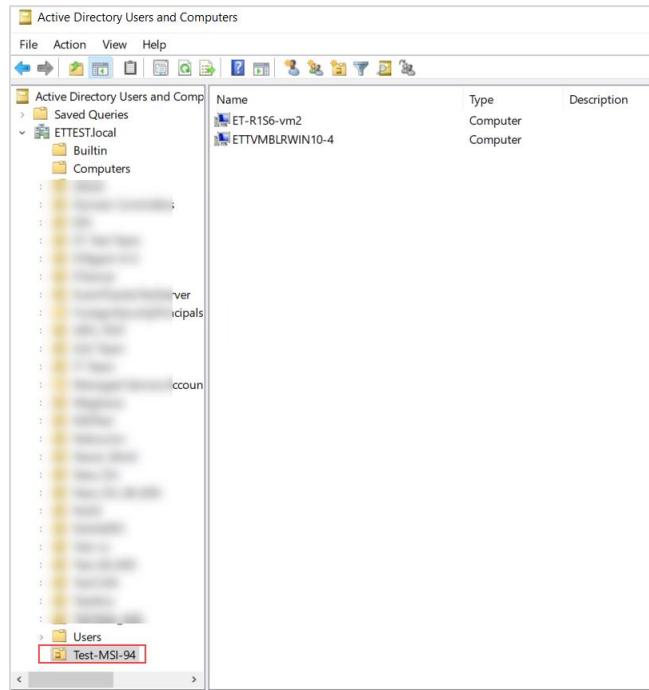
1. In the **Active Directory domain** machine, click **Windows + R** and type **“dsa.msc”**.
2. Then, right-click the group name and click **New > Organizational Unit**.



3. In the **Name Object** window, specify the required name and click **OK**.

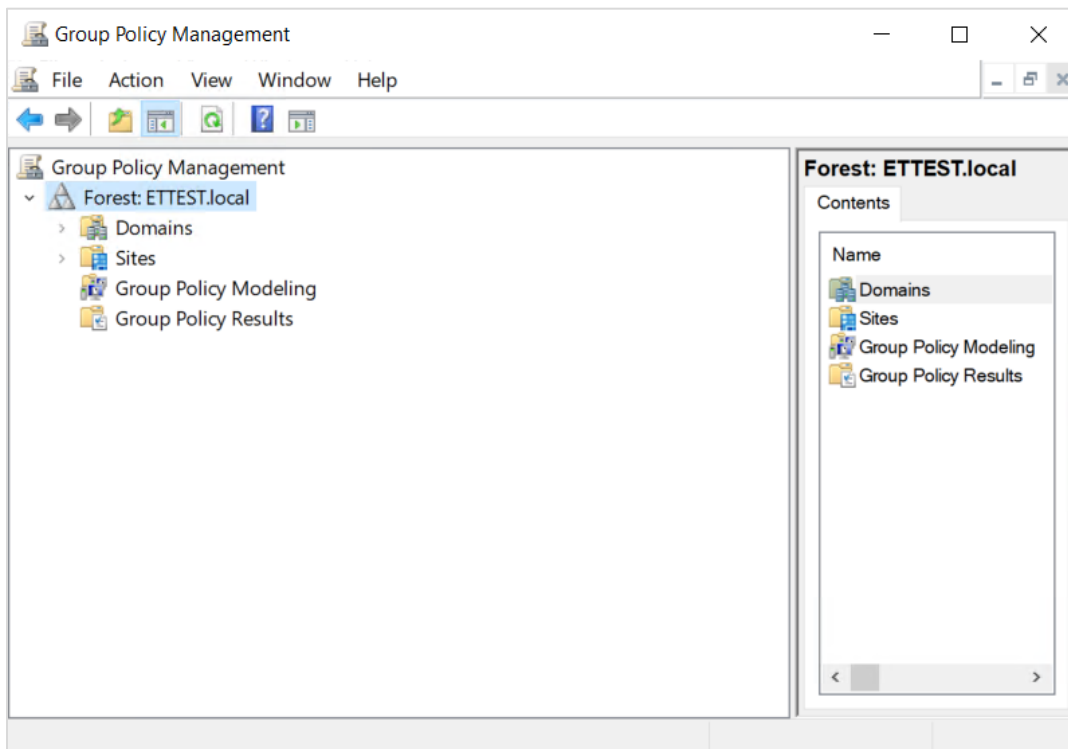


- Once the Organizational Unit (OU) is created, move the systems to this newly created OU Group.



8.4 Launching Group Policy Management Console

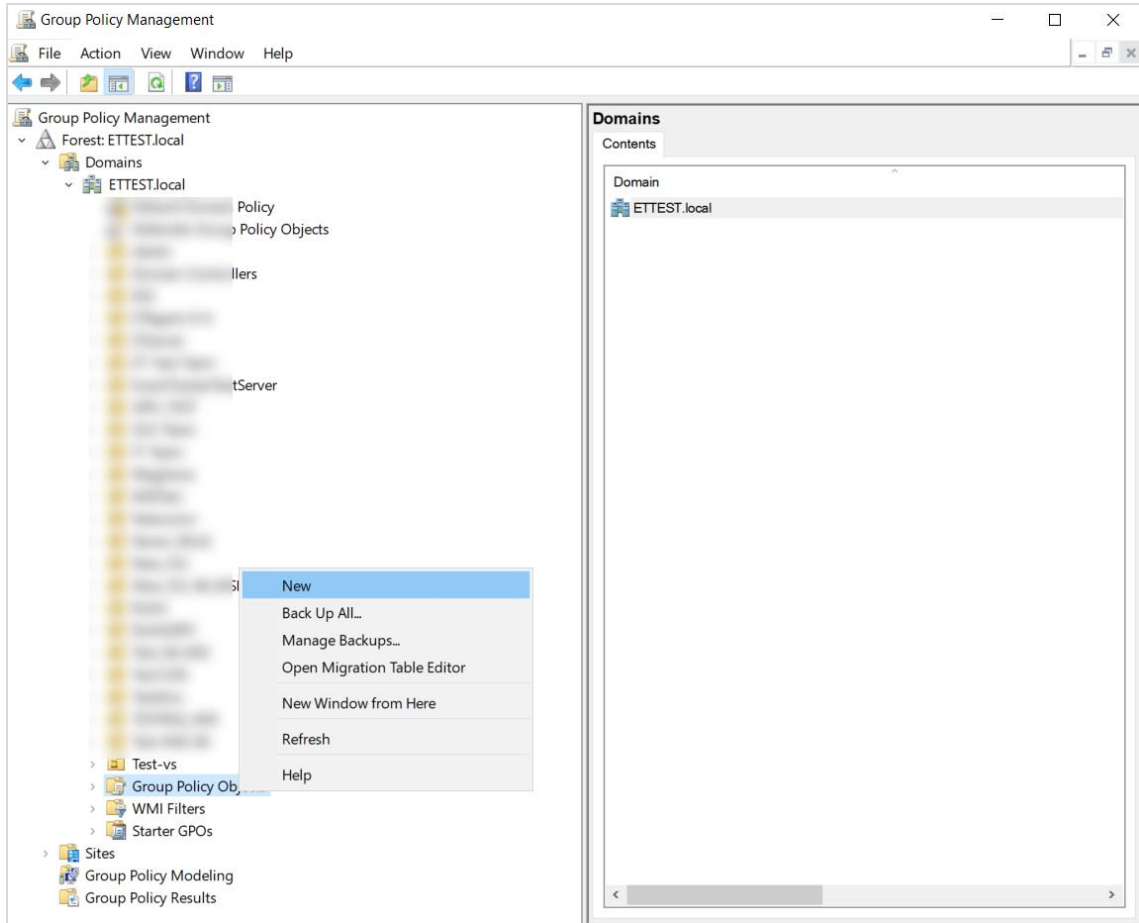
- Go to the Windows Search bar, and search and launch the **Group Policy Management** via **Run as Administrator**.



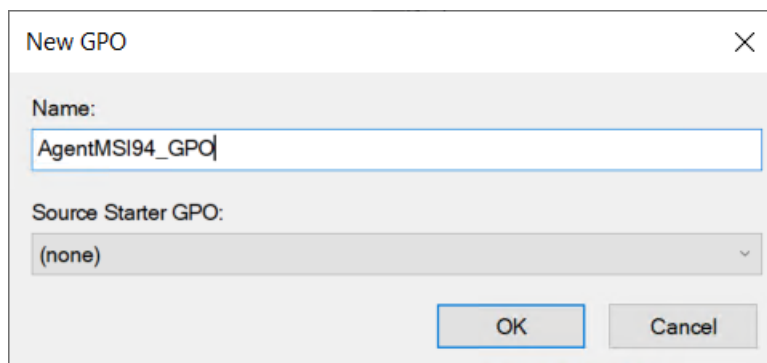
8.5 Creating Group Policy Object in Active Directory for Software Deployment

Perform the following procedure to create the new 'Group Policy Object' using the 'Group Policy Management'.

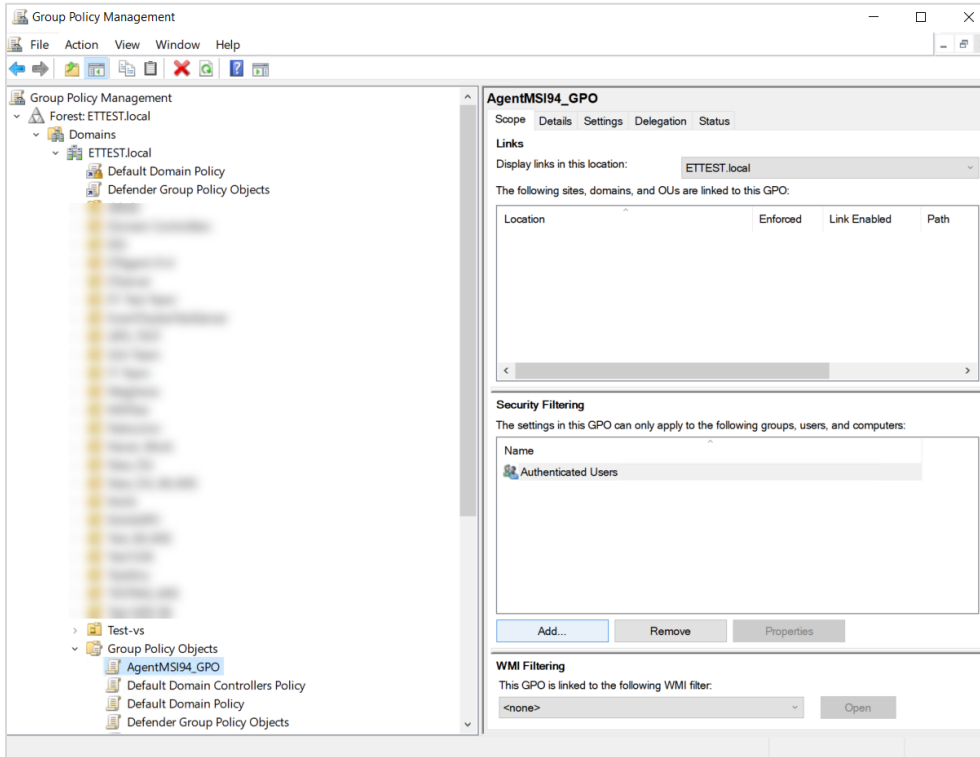
1. In the **Group Policy Management** pane, expand the Domains group, and then expand domain system group.
2. Right-click Group Policy Objects, and then click **New**.



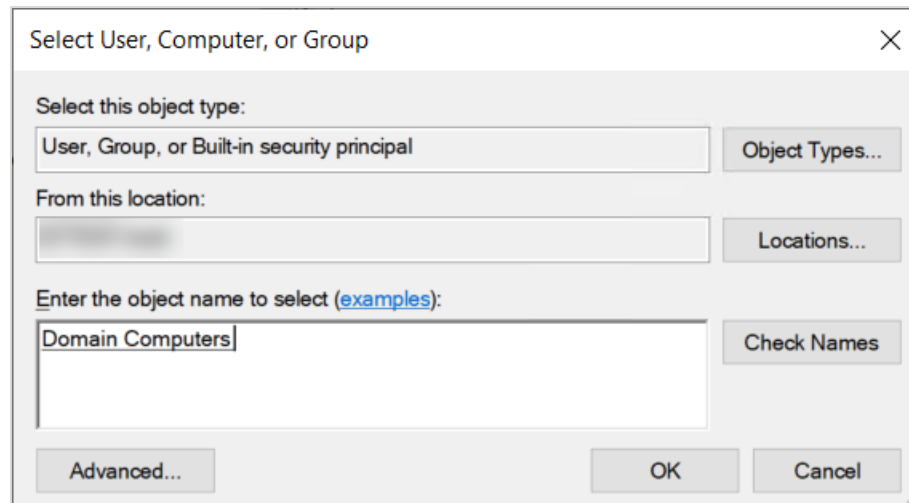
3. Enter a name for this new GPO (for example, AgentMSI94_GPO) and then click **OK**.



- Click the name of the newly created GPO. For example, 'AgentMSI94_GPO'.

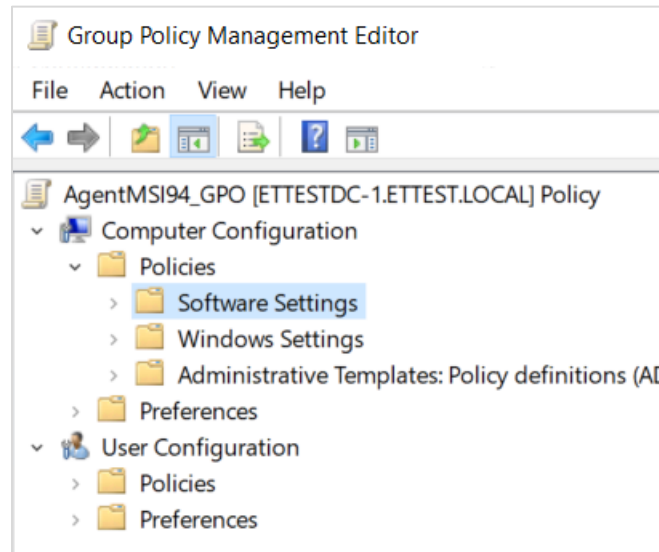


- Then, go to the **Security Filtering** pane located on the right, and click the **Add** button to apply GPO settings to the domain computers group (or ensure the authenticated user's group is listed).
- In the **Enter the object name to select** field, type the object name or a part of the object name and click the **Check Names** button to select the object name, and then click **OK**.

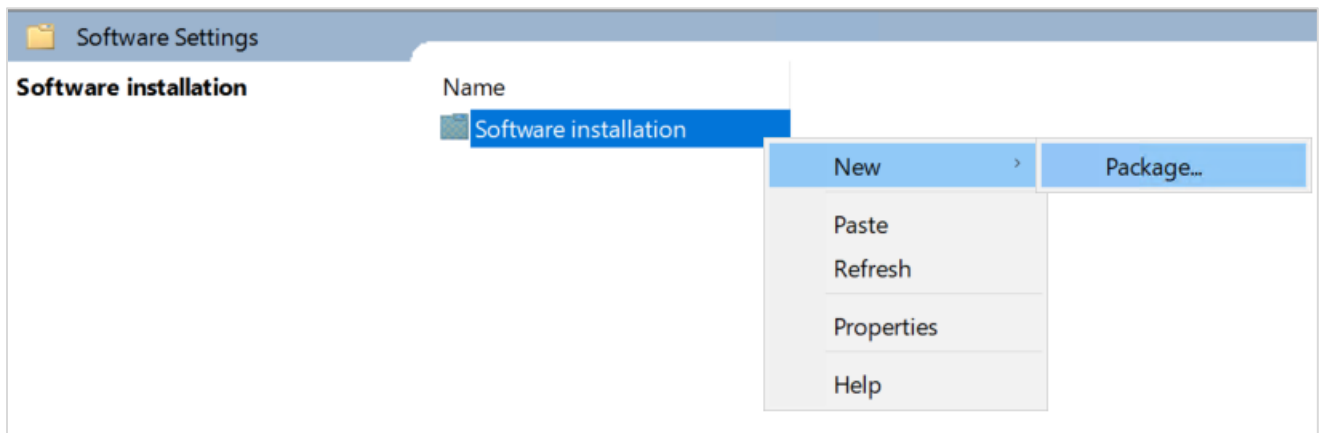


- Right-click the newly created GPO, and then click **Edit**.

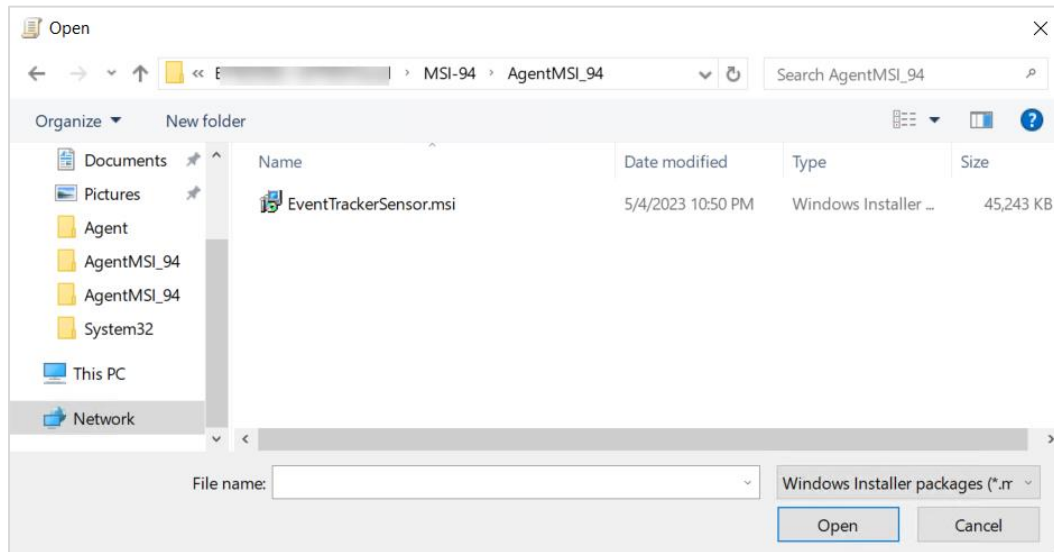
- In the **Group Policy Object Editor** window, expand the **Computer Configuration**, and open Software Settings.



- Right-click **Software Installation** and select **New > Package** from the drop-down menu.



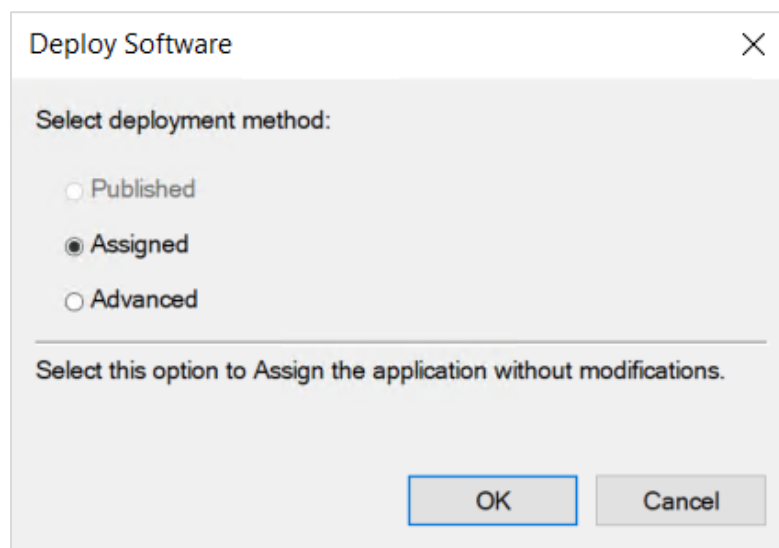
10. In the **Open** window, browse for the server share UNC path where the MSI installer file is located (\\XXXXX\AgentMSI_94\).



11. Select the MSI installer file **EventTrackerAgent.msi**, and then click **Open**.

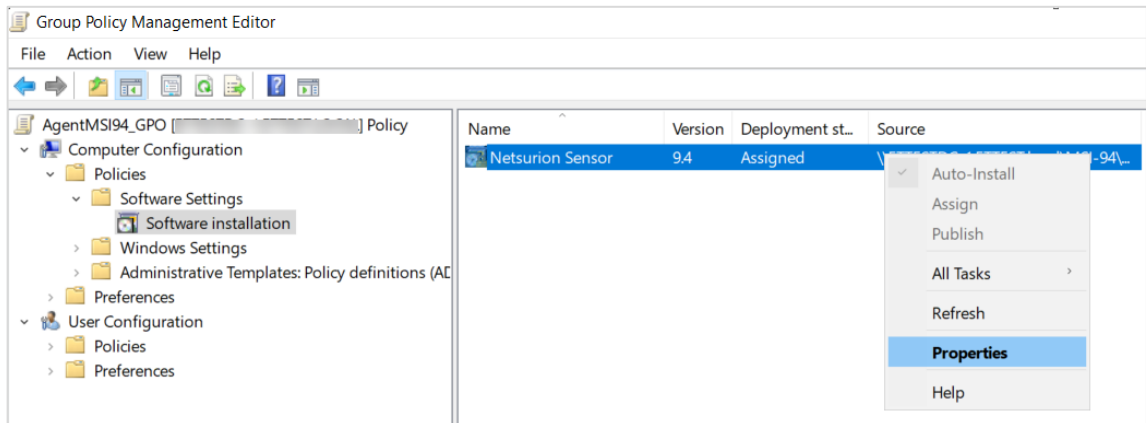
Netsurion Open XDR displays the **Deploy Software** dialog box.

12. Choose **Assigned** and click **OK**.

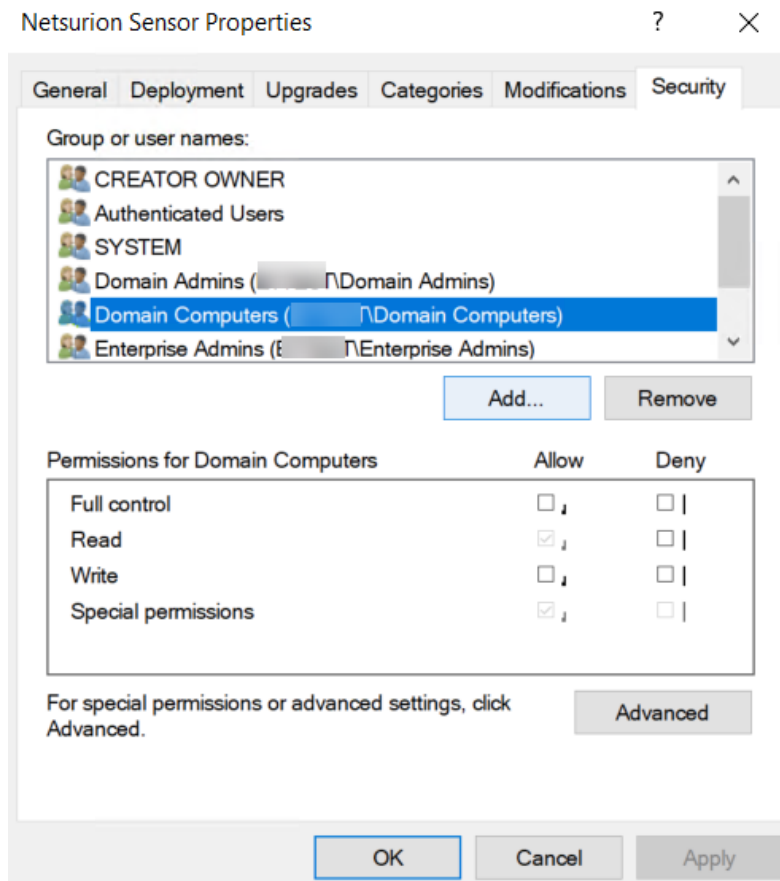


Now the **Package Object** is created and assigned.

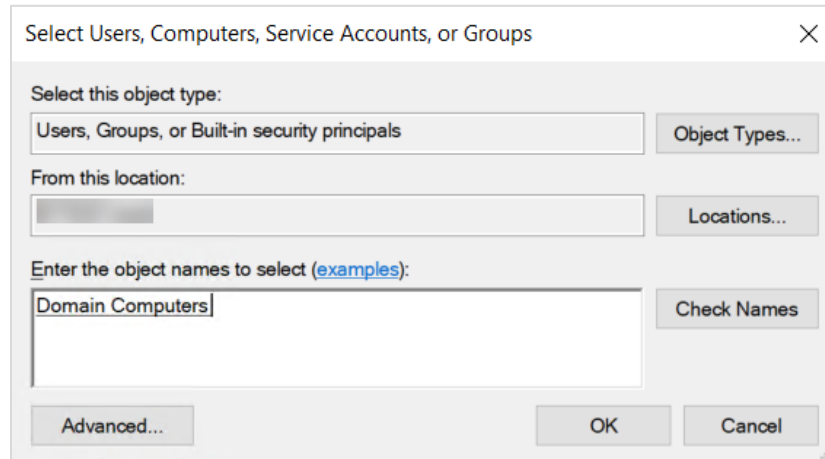
13. Right-click the **Package Object**, and then select **Properties**.



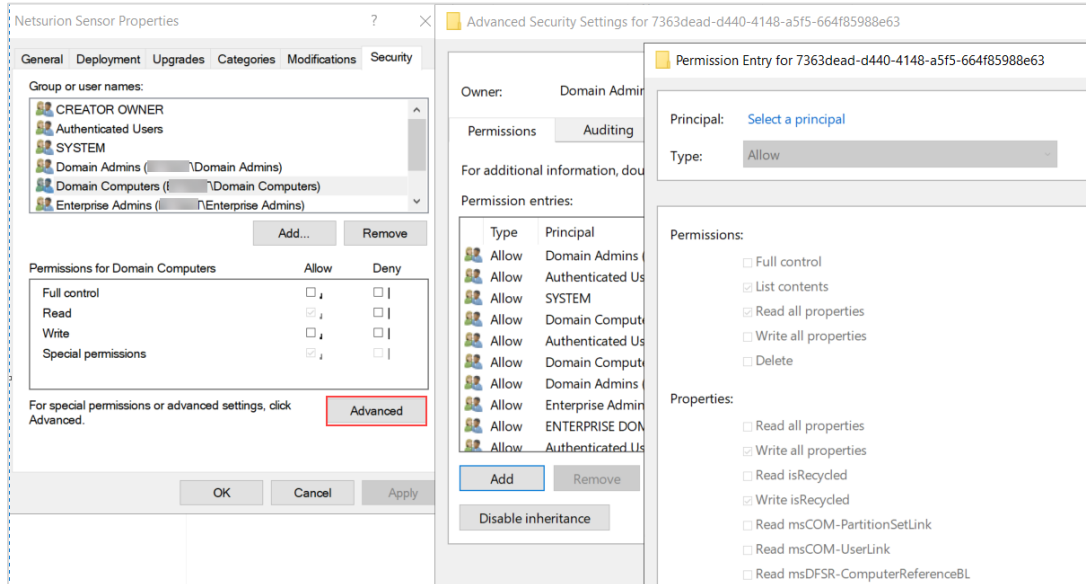
14. In the **Netsurion Sensor Properties** window, go to the **Security** tab and click **Add** to add Domain Computers to provide security permissions.



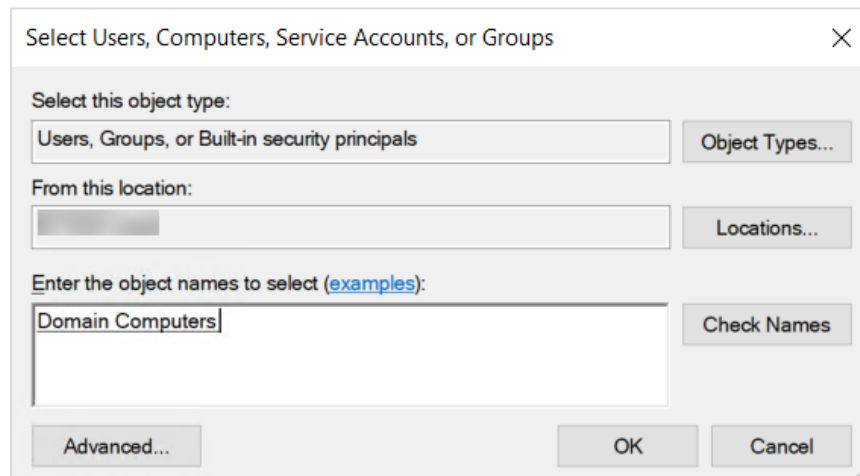
15. Enter the object names “Domain Computers” and click **OK**.



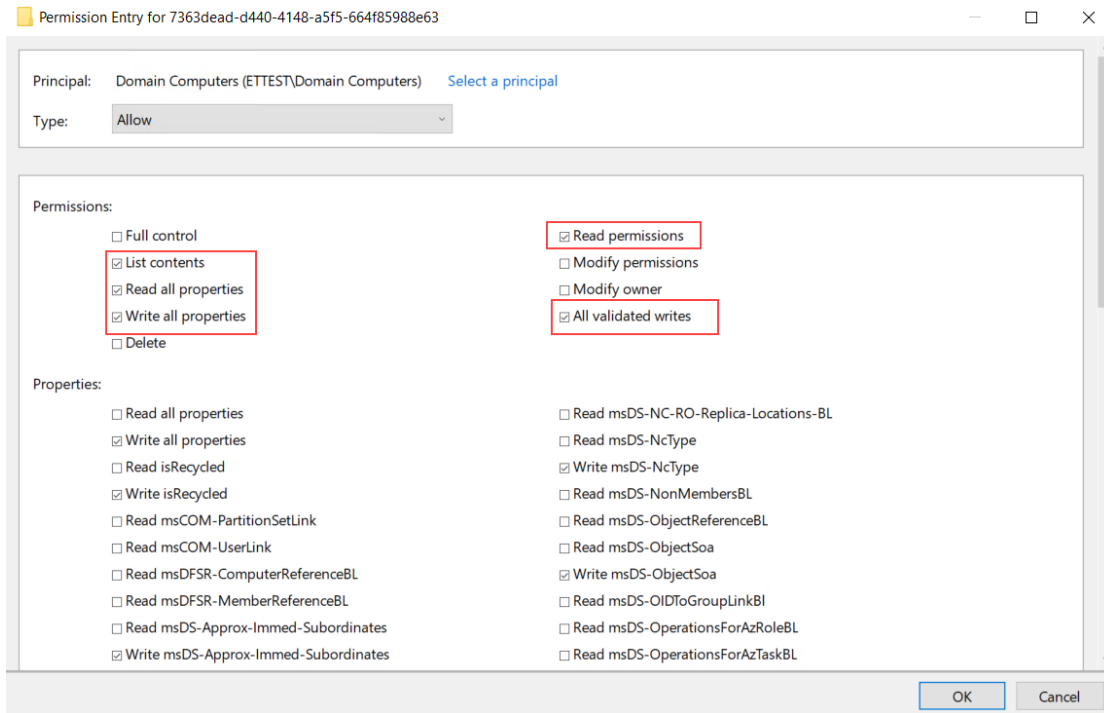
16. Next, select the **Advanced** button, click **Add** and then go to **Select Principal**.



17. Enter the object names “Domain Computers” and click **OK**.



18. Here, select the following **List Contents** (highlighted in the below image), and click **OK**.



Note:
Ensure Domain Computers has the Read and Write permissions.

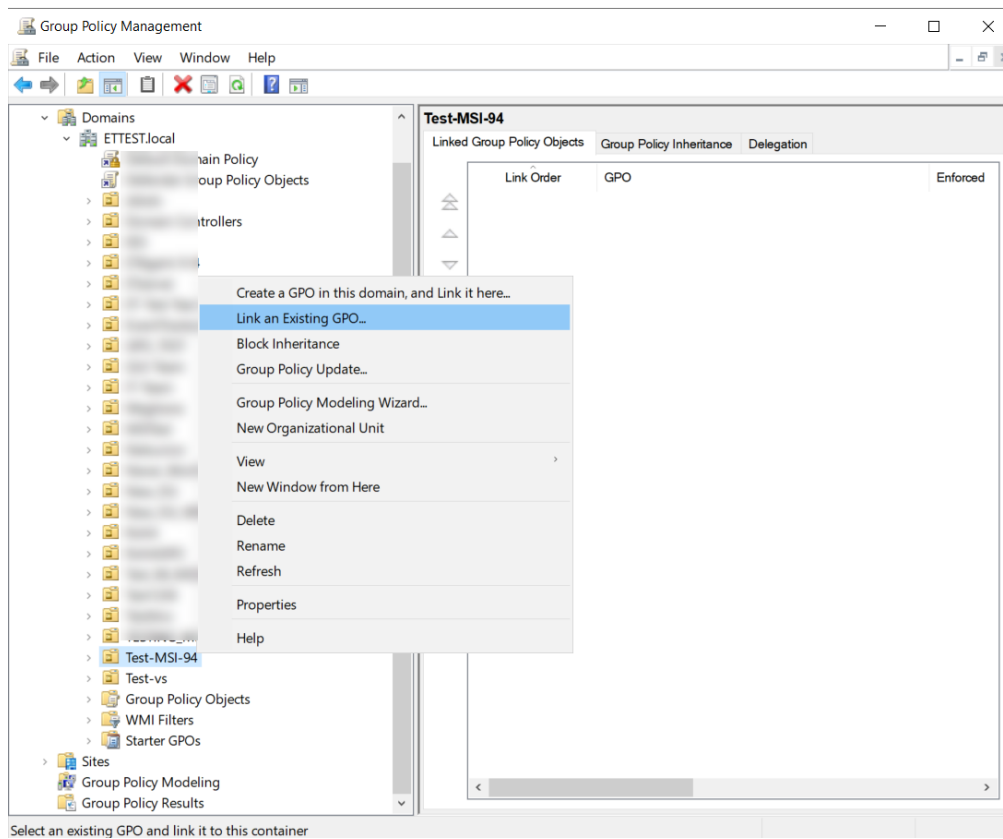
19. Next, in Advanced Security Settings, click **Apply** and **OK**.

20. In the **Netsurion sensor Properties** window, click **OK**.

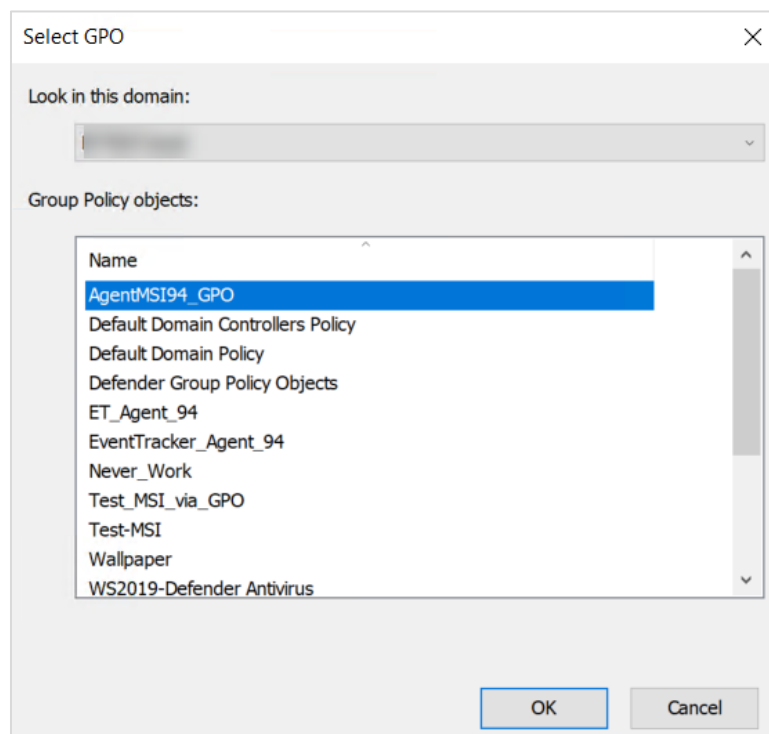
21. In the **Group Policy Management** pane, right-click the new organizational unit created earlier.

Note:
Refer to the [Assigning Systems to New Organization Unit](#) section to create an Organizational Unit.

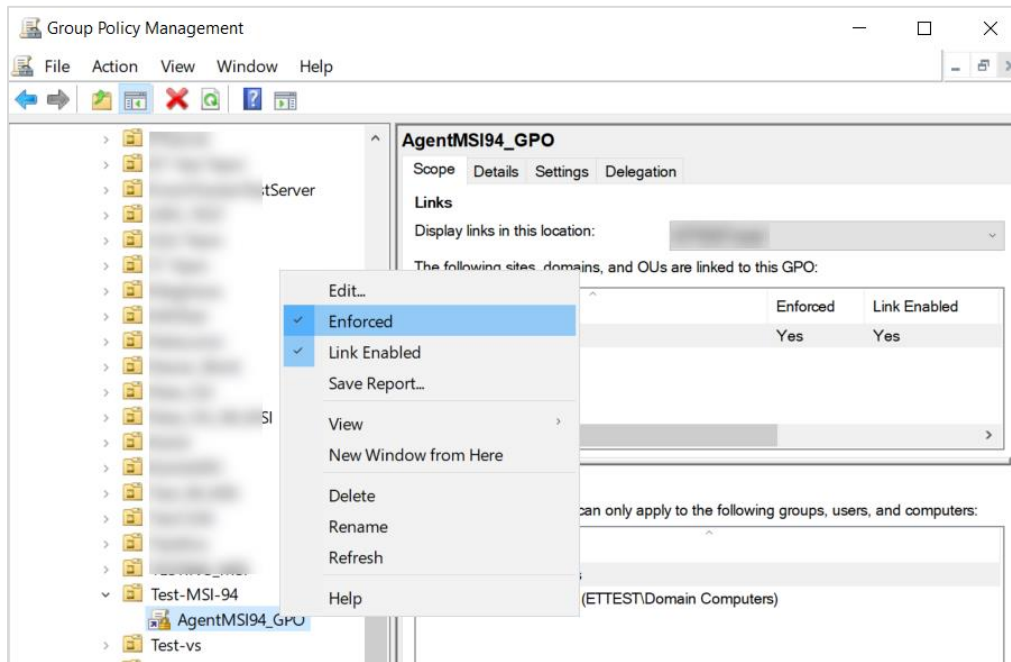
22. Then, click **Link an Existing GPO** from the drop-down menu.



23. In the **Select GPO** window, select the created GPO and click **OK**.



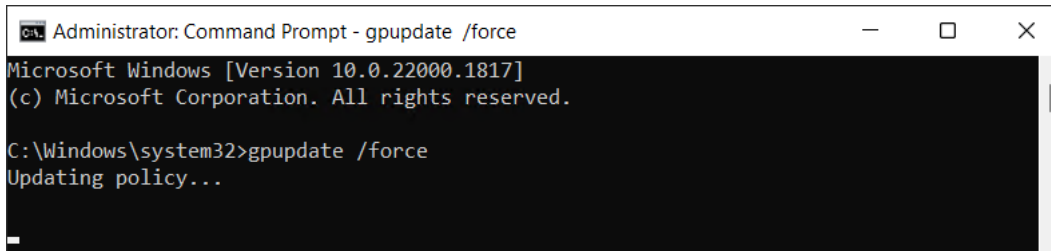
24. Navigate to Linked GPO, right-click and enable **Enforced**.



The **MSI package** is now defined and is ready for deployment.

25. Now, go to Target machine and update the Group policy by executing the following command in the command prompt.

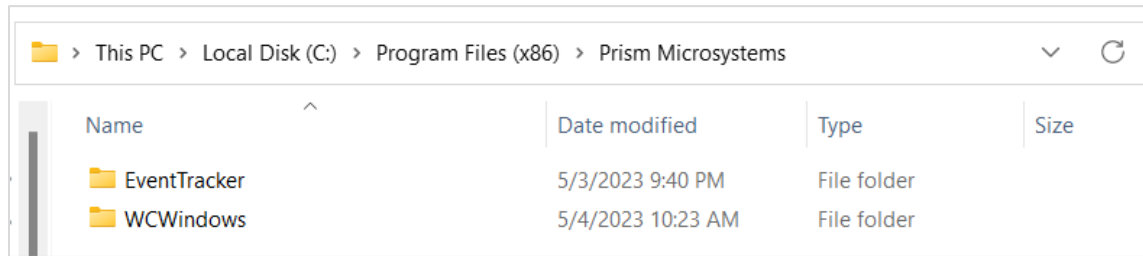
```
Command: gpupdate /force
```



Note:
Netsurion Open XDR and Change Audit sensors will be installed once the target machine is restarted.

Note:
If Agent.ini and etacnfig.ini files are present in same folder, and the CUSTOMCONFIG=2 in the Agent.ini file, then the configurations will be deployed from etacnfig.ini file.

After the GPO is updated, verify the folder structure in the target machine as shown below:



8.6 Verifying Installation

Events will be sent to the reporting Manager systems upon successful deployment of Netsurion Open XDR/Change Audit sensors. The name of the deployed sensor along with its version will appear on the System Manager screen. On the reporting Manager systems, the following events will be generated in the System Event Log.

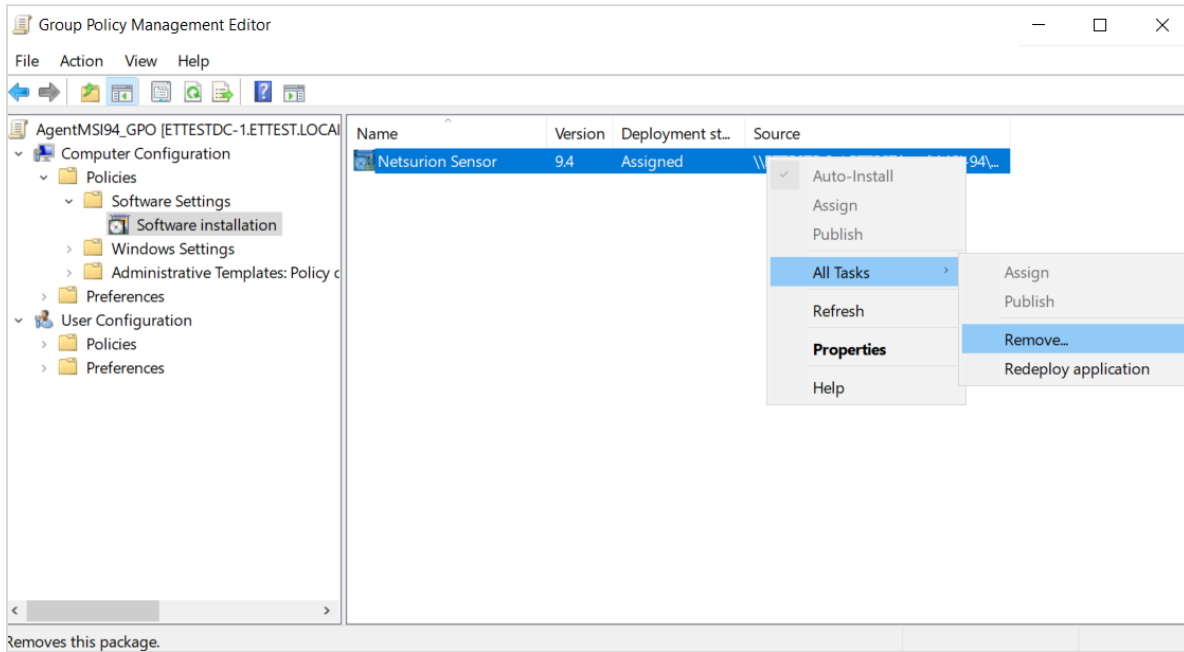
On Windows Operating Systems

The following are the sample Event ID and Description for Successful sensor deployment.

Log Name	Application
Source	MSIInstaller
Event ID	1040
Task Category	None
Level	Information
Keywords	Classic
User	SYSTEM
Computer	Test-10-HC.pcloud2008.com
Description	Beginning a Windows Installer transaction: {c4bb317c-adce-4feb-9875-7339dd4781e4}. Client Process Id: 1224

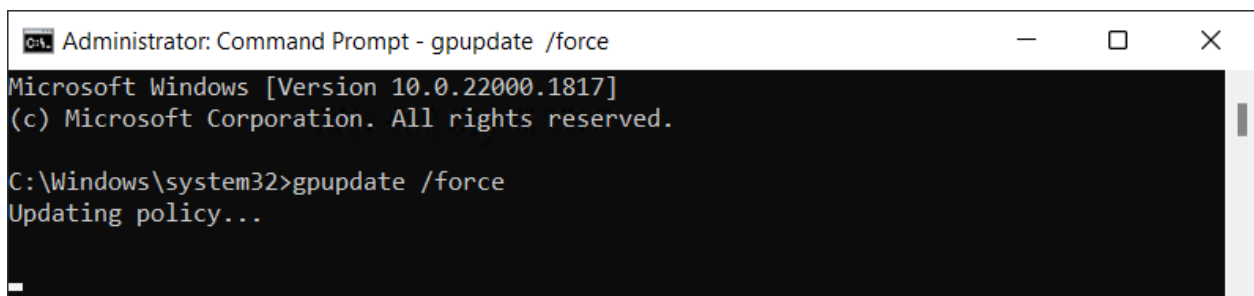
8.7 Uninstalling Netsurion Open XDR Sensor via GPO

1. Edit the linked Group Policy Object (that is, AgentMSI_94) and navigate to **Policies > Software Settings > Software Installation** and then select **MSI**.
2. Then, right-click **MSI** and click **All Tasks > Remove** to remove the assigned MSI package.



3. Then, go to the target machine and update the Group policy by executing the following command in the Command prompt to successfully uninstall the sensor package.

Command: `gpupdate /force`

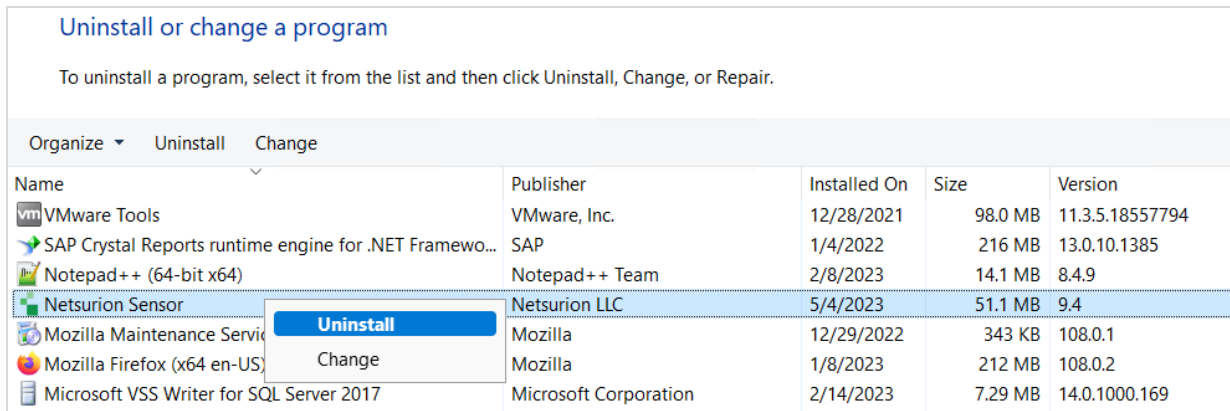


8.8 Limitation for Group Policy Installation

- Retaining the sensor configuration details does not work via Group policy.
- **Upgrade agent** function is not supported via Group policy.
- Modification features are not supported via Group policy.
- Command line or Silent installation does not support the retain, upgrade, and modify functions.
- While uninstalling, both Netsurion Open XDR and Change Audit sensor will be uninstalled.
- If both the Open XDR sensor and Change Audit sensor are installed via group policy, then it is not possible to configure group policy to uninstall either Open XDR sensor or Change Audit sensor individually. The uninstallation removes both the Open XDR sensor and Change Audit sensor.
- Once the Open XDR sensors are installed via group policy, you will not be able to uninstall the sensors from Netsurion Open XDR System Manager module.
- The shortcut value in Agent.ini must be kept as "SC=1" in case the user wants to uninstall sensor from individual systems.
- In case the user wants to uninstall sensor from all the systems via GPO, then the shortcut value "SC=0" in Agent.ini need not be changed.

9 Uninstallation of Netsurion Sensor via Control Panel

1. Go to **Control Panel > Program & Features**.
2. Right-click **Netsurion Sensor** and click **Uninstall**.



3. After the un-installation is complete, verify whether the sensor files in registry, the installation path and the services are removed.
4. Event id **3209** is sent to the Open XDR Manager.

Sample Description

event_description: Detected software Netsurion Open XDR sensor has been uninstalled from this system.

Name: Netsurion Open XDR sensor

Agent Type: Netsurion Open XDR sensor and Change Audit

Agent Version: 9.4

User Name: NTPL\ Karen

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the [form](#) to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

<https://www.netsurion.com/support>