How - To Guide

Deploy and Configure the Netsurion Open XDR Windows and Change Audit Sensor

Publication Date:

January 27, 2023

Abstract

The Netsurion Open XDR sensor deployment processes are described in detail in this manual for version 9.3 and above. Netsurion's Open XDR sensor can be deployed using methods like 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

The Netsurion Open XDR platform users or system administrators wish to deploy the Netusiorn Open XDR sensor and Change Audit sensor.

Product Terminology

The following terms are used throughout this guide:

- The term "Netsurion's Open XDR platform" or "the Netsurion Open XDR platform" or "the Open XDR platform" refers to EventTracker.

Table of Contents

1 Overview

The Netsurion Open XDR sensor is the front-line security component on the Netsurion Open XDR platform which provides detailed visibility into your network. The Open XDR sensor facilitates to understand 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 network, collects information about your assets and IT environment.

The Netsurion Open XDR Endpoint Security sensor (EES) is an advanced endpoint security platform, which is powered by Deep Instinct. It protects against zero-day threats, APT (Advanced Persistent Threat), ransomware, and fileless attacks against all endpoints.

1.1 Benefits/Advantages of the Netsurion Open XDR sensor

Netsurion's Open XDR sensor delivers the following essential capabilities:

- Log collection.
- Scans for authenticated asset.
- 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 and installed/uninstalled software.
- Software install/uninstall.
- Finds services start/stop.
- Sends events with guaranteed delivery (TCP).
- Monitor file and registry changes on the system.
- Monitor/ terminate suspicious activity.
- Provides immediate visibility into the attacks against your systems.
- The capability of syslog relay.

1.2 Prerequisite

Before deploying the Netsurion Open XDR sensor, it is essential to set up a few things as detailed below,

- Ensure that the Open XDR platform Scheduler service of the Open XDR Manager is running during the installation process.

> **Note:**
>
> This is necessary for the installer to connect to the Open XDR Manager to retrieve the license information, which is handled by the Open XDR Scheduler service. If this scheduler service is not running during the installation, then you will not be able to use the Open XDR features that you select.

- All target systems must have access to the Network Share where the Open XDR sensor MSI files are stored.
- Domain systems must have at least the **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** or from **Start** > **All Programs**.
- The .NET Framework 3.5 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.
- Recommended to install the Open XDR sensor and Change Audit sensor either by command line, System Manager or by group policy.
- Must restart the target system(s) after configuring the software deployment policy to complete the installation.

> **Note:**
>
> The new snapshots required for Change Audit will be taken at 2AM.

> **Note:**
>
> If you uninstall the latest MSI package v 9.3 and above via System Manager, both the features, that is the Open XDR sensor and Change Audit will be uninstalled. If you uninstall any one of the feature, then the entire MSI package will be uninstalled (where all components of the MSI package will become similar to the Manager sensor components).

> **Note:**
>
> Installing Windows Sensor and then installing Change Audit Sensor or vice-versa will result in an error.

1.3 Supported Operating Systems

Windows Platforms	32 bit	64 bit
Windows Server 2022	Not Applicable	Supported
Windows Server 2019	Not Applicable	Supported
Windows Server 2016	Supported	Supported
Server 2012 R2	Not Applicable	Supported
Server 2012	Not Applicable	Supported
Server 2008 R2	Supported	Supported
Windows 7	Supported	Supported
Windows 8, 8.1	Supported	Supported
Windows 10	Supported	Supported
Windows 11	Not Applicable	Supported

1.4 Resource Requirement

<table>
<tr><th colspan="3">Minimum Configuration</th><th colspan="3">Resource Utilization
(in a typical environment)</th></tr>
<tr><th rowspan="2">CORE</th><th rowspan="2">RAM</th><th rowspan="2">DISK</th><th colspan="2">CPU</th><th rowspan="2">MEMORY</th></tr>
<tr><th>AVG</th><th>MAX</th></tr>
<tr><td>4</td><td>8 GB</td><td>200 MB</td><td>1-2 %</td><td>10 %</td><td>50 MB</td></tr>
</table>

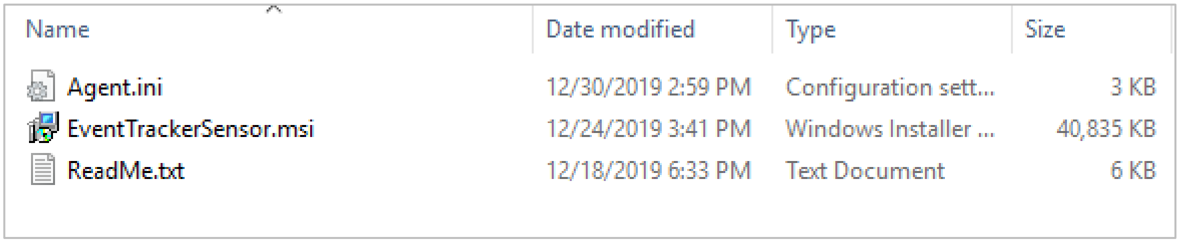
2 Preparing the Netsurion Open XDR sensor MSI Installer Package for Deployment

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

For the Netsurion Open XDR v9.3 and above,

1. Download the MSI package (V9.3 is considered in this example in AgentMSI_93.zip) from the location provided by the Netsurion Open XDR platform support team.

2. Extract the **AgentMSI_93.zip** file to the AgentMSI_93\ folder.



Name	Date modified	Type	Size
Agent.ini	12/30/2019 2:59 PM	Configuration sett...	3 KB
EventTrackerSensor.msi	12/24/2019 3:41 PM	Windows Installer ...	40,835 KB
ReadMe.txt	12/18/2019 6:33 PM	Text Document	6 KB

3 Deploying through Command Prompt

Run the executable MSI Installer with the administrative privilege.

3.1 Parameters used for GUI and Silent Installation

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.
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 etaconfig.ini. **3** - Enterprise Configuration file in TCP mode. **4** - Enterprise anomalous audit configuration file in TCP mode. **5** - FIM only 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

Argument	Description
IR	Remedial Actions **1** - Predefined scripts will be placed in the EventTracker\Agent\Script folder.
LS	License Server
LP	License Port
DW	Deploy WinSCAP 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.
IS_SUFFIX	Enable Suffix **2** - enable (Location Name window will not appear) (any configuration) **1** - enable (GUI will contain control to take input as suffix) **0** - disable (no extra GUI control)
SUFFIX	Suffix string
SUPPORT_CONTACTS	Support Details
PIP	Protection IP If the user provides PIP, the FQDN or the Hostname needs to be added here. When The FQDN or the Hostname is provided, the “protect_flag” is enabled and provided IP will appear in “protect_ip” field.
PKG_UID	Package UID

Argument	Description
Agent.ini	Agent.ini **0** - Command prompt installation (It won't consider Agent.ini details) **1** - Considers Agent.ini filled details

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
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 etaconfig.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

Parameters	Default Value
DW	0
MIN_GUI	0
AGENTINI	0
PKG_UID	NIL

Note:

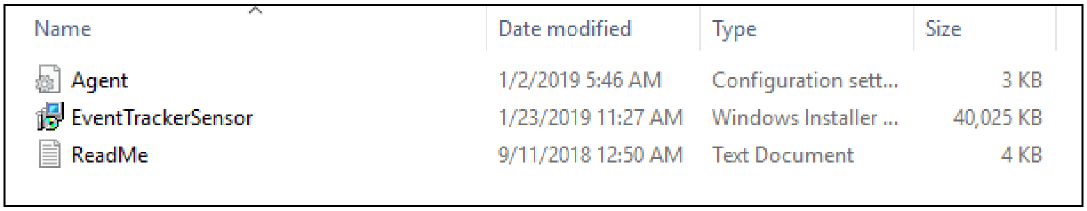
If the user wants MAC address as Suffix, then the **SUFFIX** =”<%MAC%>”.

Note:

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

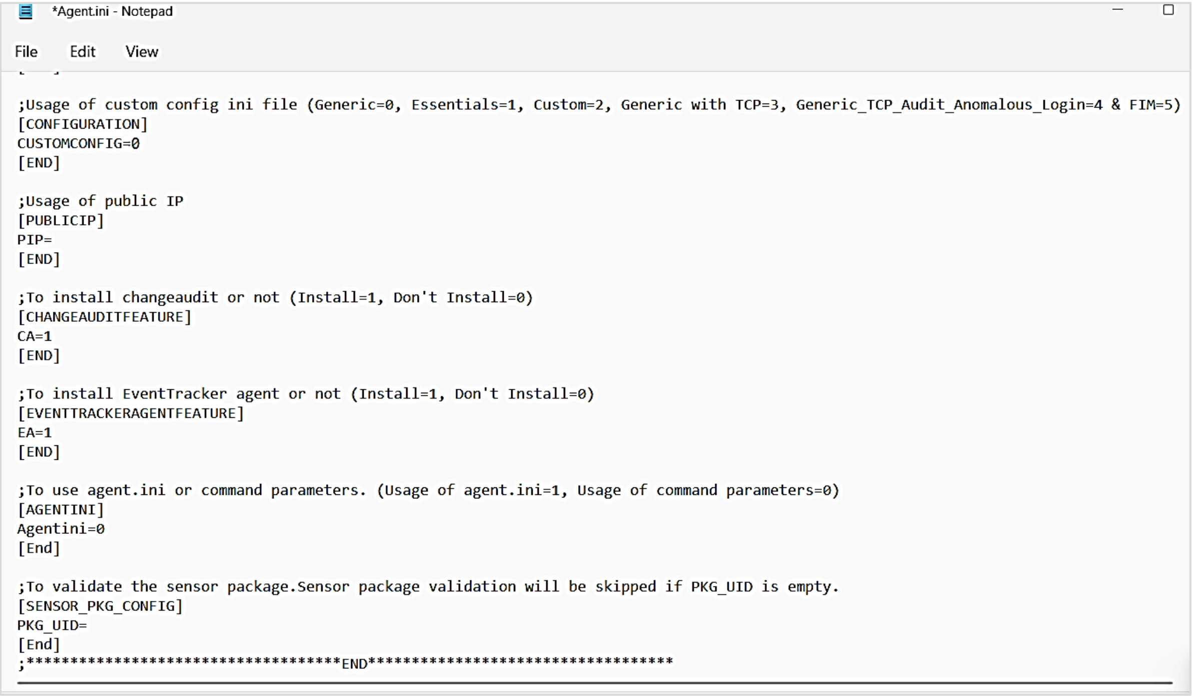
3.2 MSI Installation via GUI without Agent.ini

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



Name	Date modified	Type	Size
Agent	1/2/2019 5:46 AM	Configuration sett...	3 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 KB

2. Edit the **Agent.ini** file and change the value for **Agent.ini=0**.



```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2, Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4 & FIM=5)
[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=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 Parameters used for GUI and Silent Installation 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 changes, save the **Agent.ini** file.

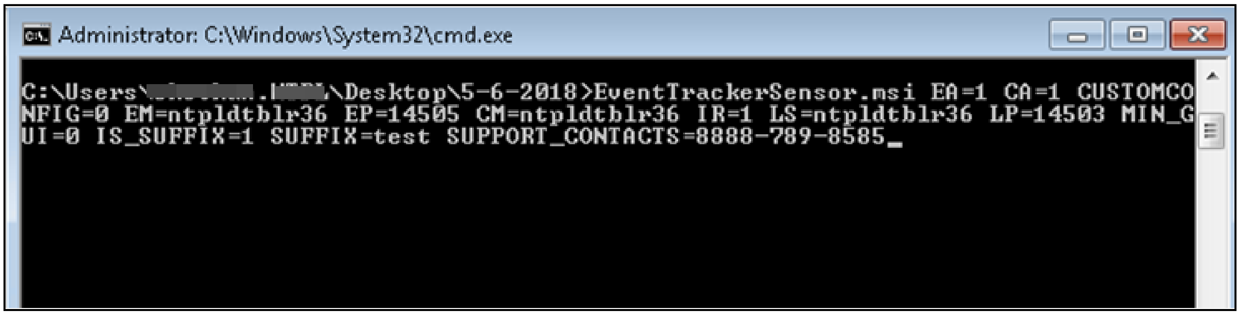
4. Then, launch the Command prompt as "**Run as Administrator**".

5. Change the directory to **AgentMSI_93**.

6. Provide the following command with the required CUSTOMCONFIG value

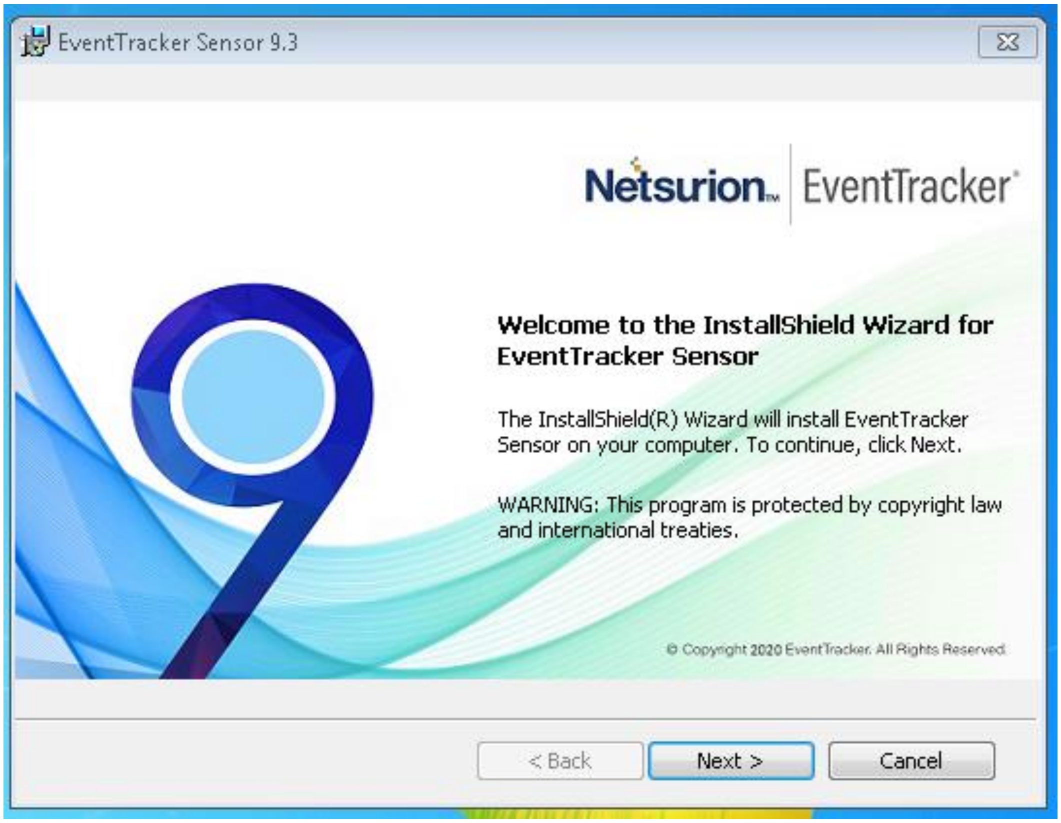
```
EventTrackerSensor.msi EA=1 CA=1 CUSTOMCONFIG=0(or 3/4/5) EM=Enterprise
Manager name EP=Manager port number CM=Change Audit Manager name IR=1
LS=License server name LP=License port number MIN_GUI=0 IS_SUFFIX=1
SUFFIX=Suffix name SUPPORT_CONTACTS=Contact details
```

7. Press the **Enter** key after providing the command and the **Netsurion's Open XDR InstallShield Wizard** interface will appear.



```
C:\Users\[redacted].[redacted]\Desktop\5-6-2018>EventTrackerSensor.msi EA=1 CA=1 CUSTOMCO
NFIG=0 EM=ntpldtblr36 EP=14505 CM=ntpldtblr36 IR=1 LS=ntpldtblr36 LP=14503 MIN_G
UI=0 IS_SUFFIX=1 SUFFIX=test SUPPORT_CONTACTS=8888-789-8585_
```

8. Click **Next >** to proceed with the GUI installation.



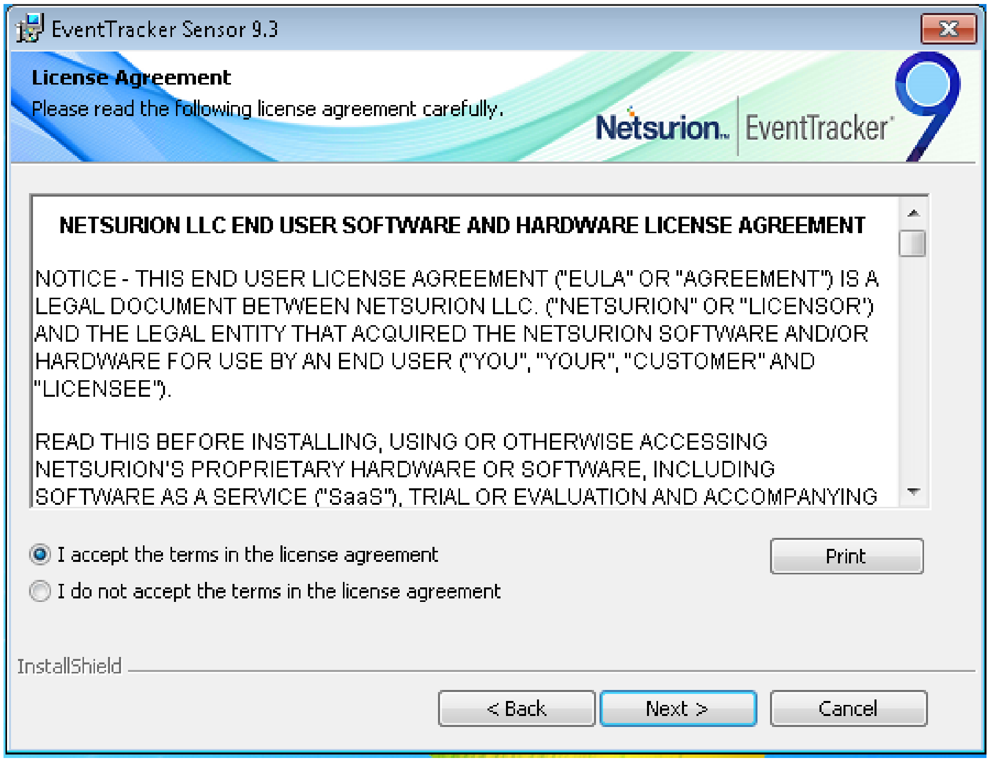
Welcome to the InstallShield Wizard for EventTracker Sensor

The InstallShield(R) Wizard will install EventTracker Sensor on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

© Copyright 2020 EventTracker. All Rights Reserved.

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



EventTracker Sensor 9.3

License Agreement

Please read the following license agreement carefully.

NETSURION LLC END USER SOFTWARE AND HARDWARE LICENSE AGREEMENT

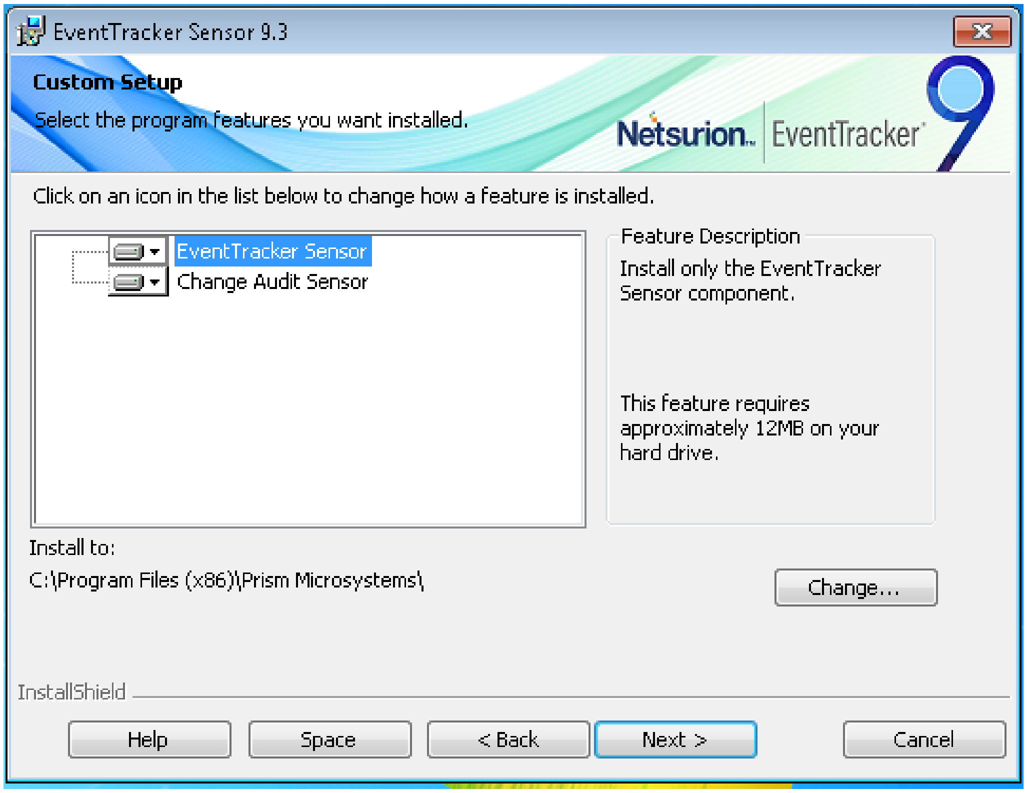
NOTICE - THIS END USER LICENSE AGREEMENT ("EULA" OR "AGREEMENT") IS A LEGAL DOCUMENT BETWEEN NETSURION LLC. ("NETSURION" OR "LICENSOR") AND THE LEGAL ENTITY THAT ACQUIRED THE NETSURION SOFTWARE AND/OR HARDWARE FOR USE BY AN END USER ("YOU", "YOUR", "CUSTOMER" AND "LICENSEE").

READ THIS BEFORE INSTALLING, USING OR OTHERWISE ACCESSING NETSURION'S PROPRIETARY HARDWARE OR SOFTWARE, INCLUDING SOFTWARE AS A SERVICE ("SaaS"), TRIAL OR EVALUATION AND ACCOMPANYING

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

10. In **Custom Setup**, select EventTracker sensor and Change Audit sensor based on the requirement.



EventTracker Sensor 9.3

Custom Setup

Select the program features you want installed.

Click on an icon in the list below to change how a feature is installed.

- EventTracker Sensor
- Change Audit Sensor

Feature Description

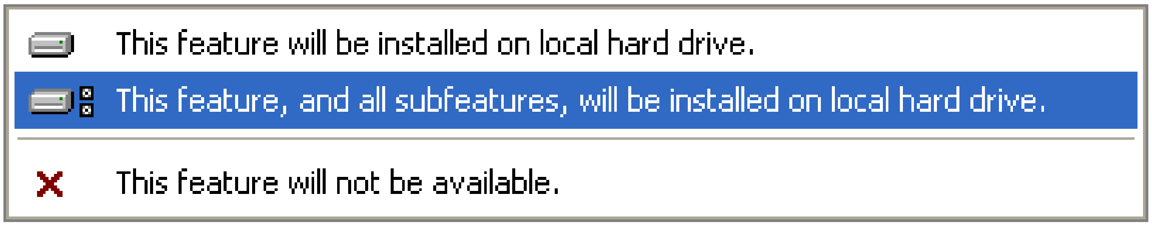
Install only the EventTracker Sensor component.

This feature requires approximately 12MB on your hard drive.

Install to:

C:\Program Files (x86)\Prism Microsystems\

- 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.

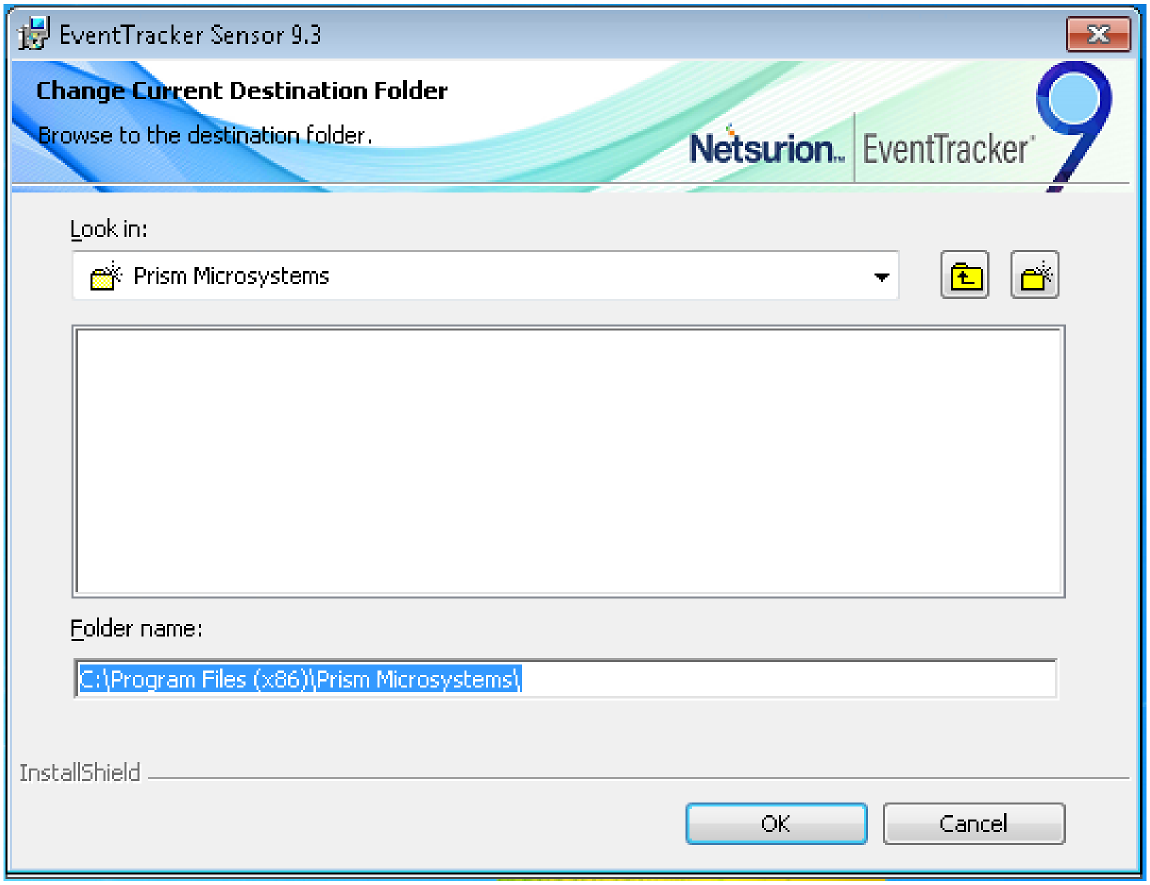
Note:

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.



EventTracker Sensor 9.3

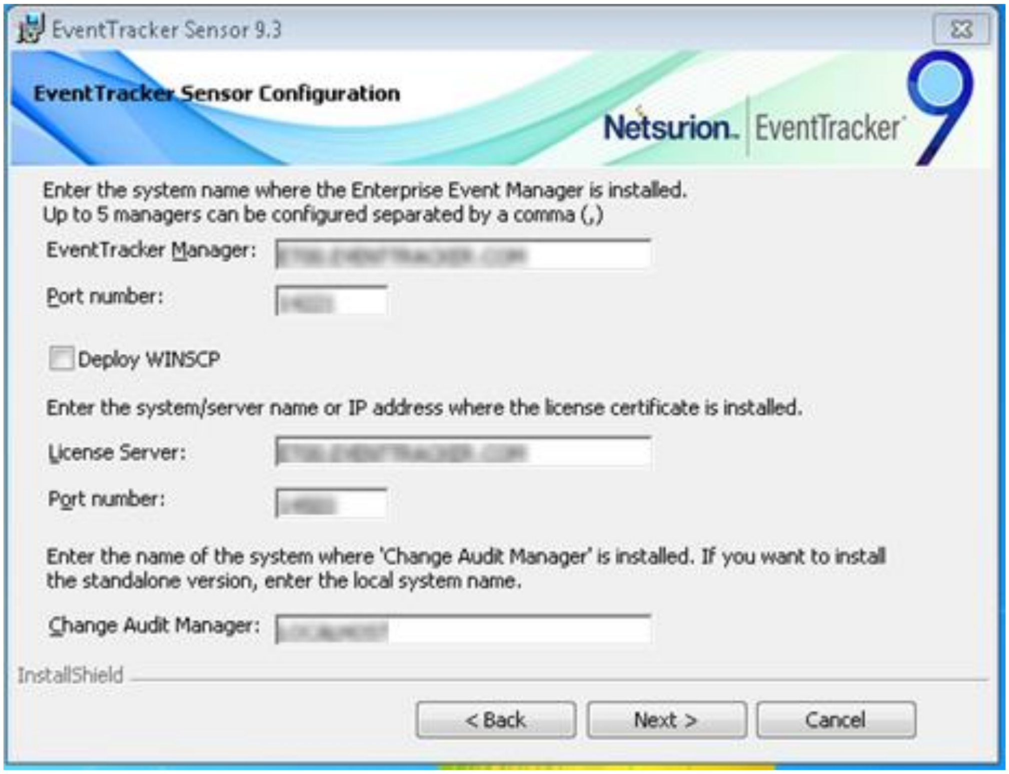
Change Current Destination Folder

Browse to the destination folder.

Look in: Prism Microsystems

Folder name: C:\Program Files (x86)\Prism Microsystems\

12. In **sensor Configuration**, the details for all the fields will be fetched from the command line, click **Next >** to proceed.



EventTracker Sensor 9.3

EventTracker Sensor Configuration

Enter the system name where the Enterprise Event Manager is installed.
Up to 5 managers can be configured separated by a comma (,)

EventTracker Manager: [redacted]

Port number: [redacted]

□ Deploy WINSCP

Enter the system/server name or IP address where the license certificate is installed.

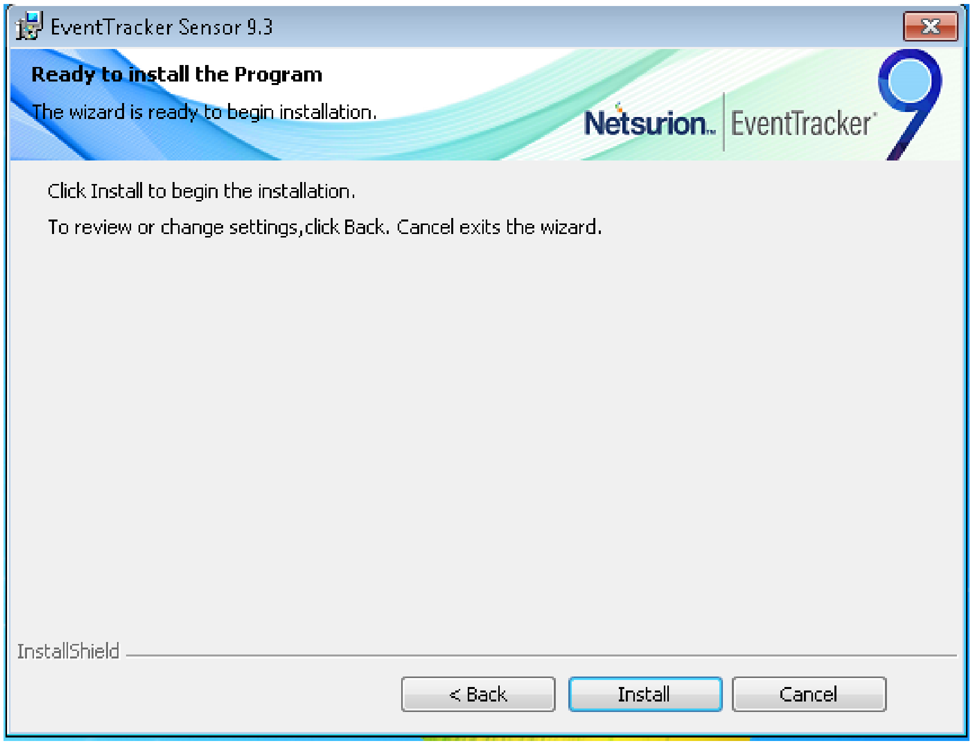
License Server: [redacted]

Port number: [redacted]

Enter the name of the system where 'Change Audit Manager' is installed. If you want to install the standalone version, enter the local system name.

Change Audit Manager: [redacted]

13. In **Ready to Install the Program**, the location details will be fetched from the command line, click **Install**.



EventTracker Sensor 9.3

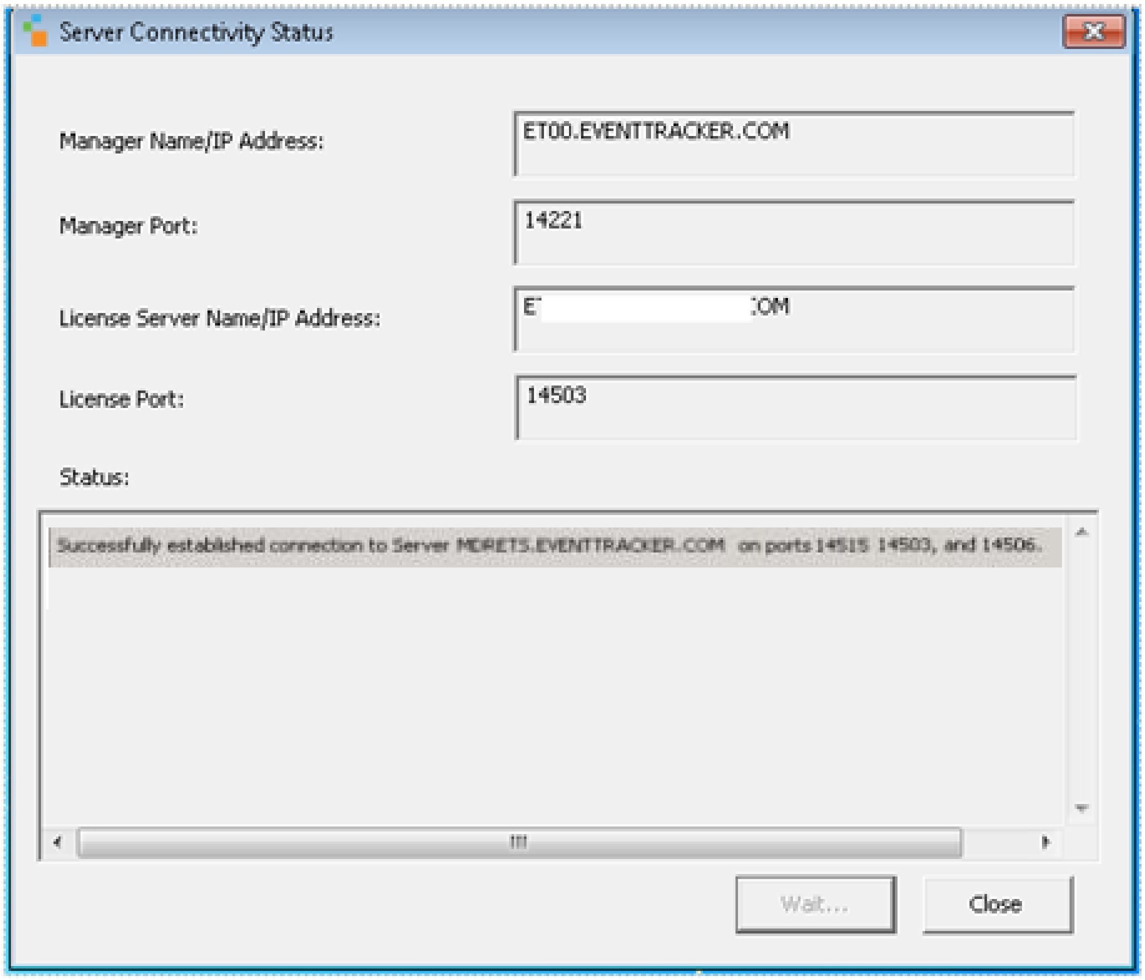
Ready to install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

To review or change settings,click Back. Cancel exits the wizard.

14. Once the installation is successful, the **Server Connectivity Status** window will be displayed providing the connectivity status.



Manager Name/IP Address: ET00.EVENTTRACKER.COM

Manager Port: 14221

License Server Name/IP Address: E :OM

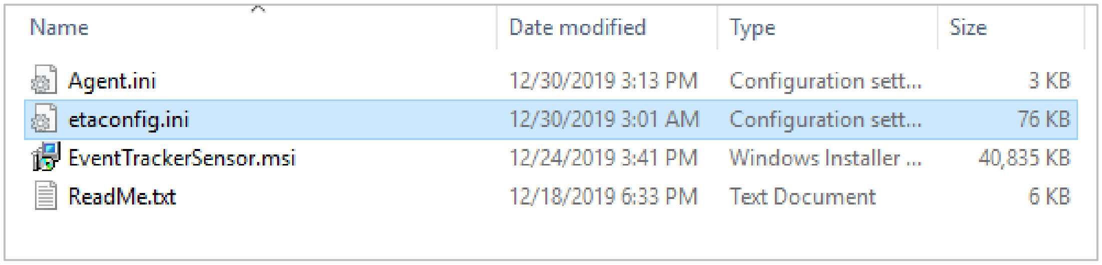
License Port: 14503

Status:

Successfully established connection to Server MDRETS.EVENTTRACKER.COM on ports 14515 14503, and 14506.

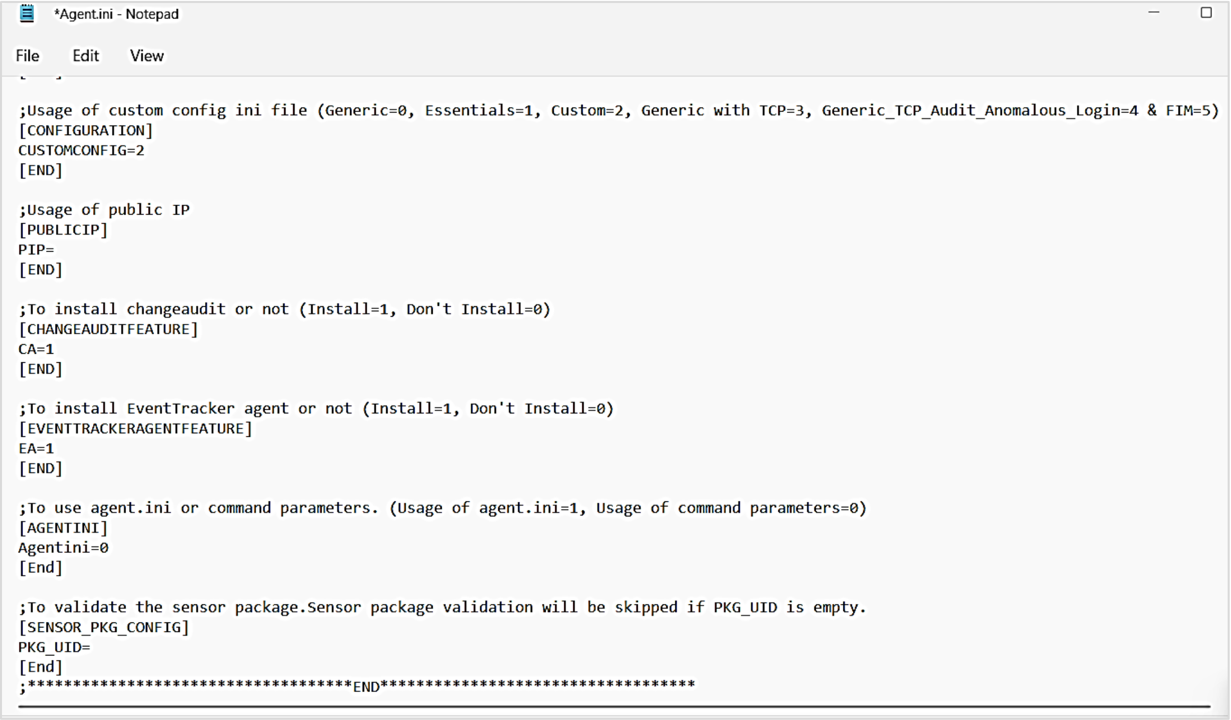
Procedure to install with etaconfig.ini file

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



Name	Date modified	Type	Size
Agent.ini	12/30/2019 3:13 PM	Configuration sett...	3 KB
etaconfig.ini	12/30/2019 3:01 AM	Configuration sett...	76 KB
EventTrackerSensor.msi	12/24/2019 3:41 PM	Windows Installer ...	40,835 KB
ReadMe.txt	12/18/2019 6:33 PM	Text Document	6 KB

2. Edit the **Agent.ini** file and change the value of Agent.ini=0.



```
;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2, Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4 & FIM=5)
[CONFIGURATION]
CUSTOMCONFIG=2
[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=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:

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

Note:

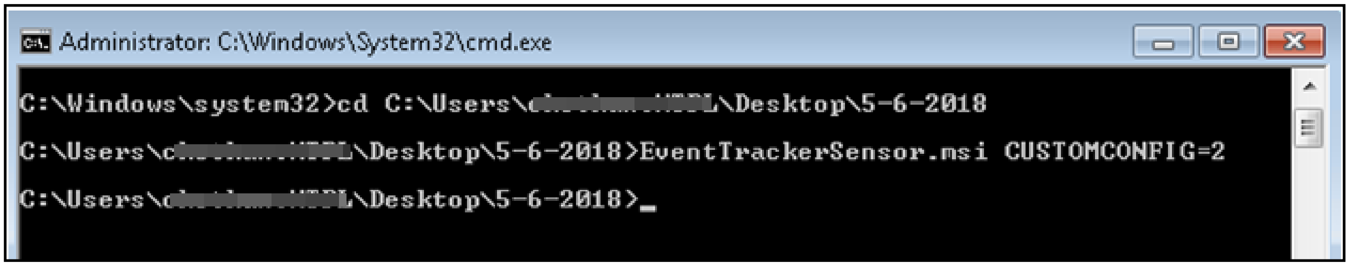
The attributes need to be filled in the **etaconfig.ini** file for **CUSTOMCONFIG=2**.When the user is using the customized etaconfig.ini file, they should not run any parameters in the command line except “**EventTrackersensor.msi CUSTOMCONFIG=2**”.

To install the sensor with customized etaconfig.ini file,

1. Launch Command prompt as “**Run as Administrator**”.

2. Change directory to **AgentMSI_93**.

3. Enter the command: **`EventTrackersensor.msi CUSTOMCONFIG=2`**



```
C:\Windows\system32>cd C:\Users\[redacted]\Desktop\5-6-2018
C:\Users\[redacted]\Desktop\5-6-2018>EventTrackerSensor.msi CUSTOMCONFIG=2
C:\Users\[redacted]\Desktop\5-6-2018>_
```

It will launch the **InstallShield Wizard**.

Note:

Refer the GUI Installation procedure from Step 8 to Step 14.

3.3 MSI Installation via Silent mode without Agent.ini

1. Launch the Command prompt as “**Run as Administrator**”.
2. Change the directory to AgentMSI_93.
3. Use any of the following commands based on the requirement.

Mandatory Parameters

Parameter	Default Value
EM	Mandatory Parameter

Default values

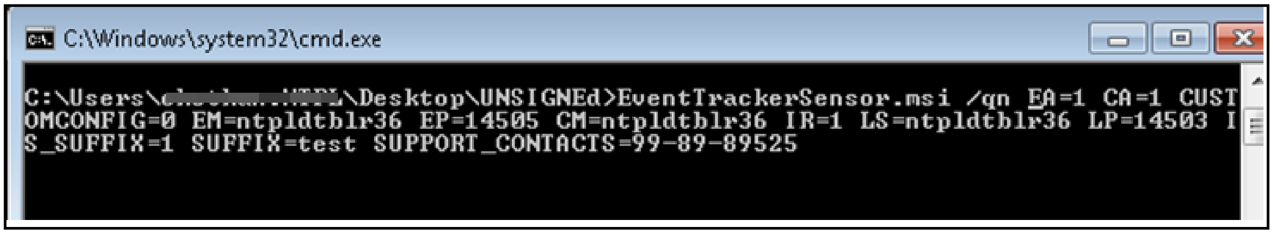
Parameter	Default Value
EA	1
CA	1
CUSTOMCONFIG	0

Parameter	Default Value
INSTALLPATH	Custom installation path
EP	14505
CM	default value EM name
IR	1(Remedial Action scripts are deployed in the Agent directory) For etaconfig.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**

4. Provide the following command with the required CUSTOMCONFIG value.

   When CUSTOMCONFIG = 0 (or 3/4/5),

```
EventTrackersensor.msi EA=1 CA=1 CUSTOMCONFIG=0(or 3/4/5)
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 WinScap IS_SUFFIX=1 SUFFIX=Suffix name
SUPPORT_CONTACTS=Contact details
```



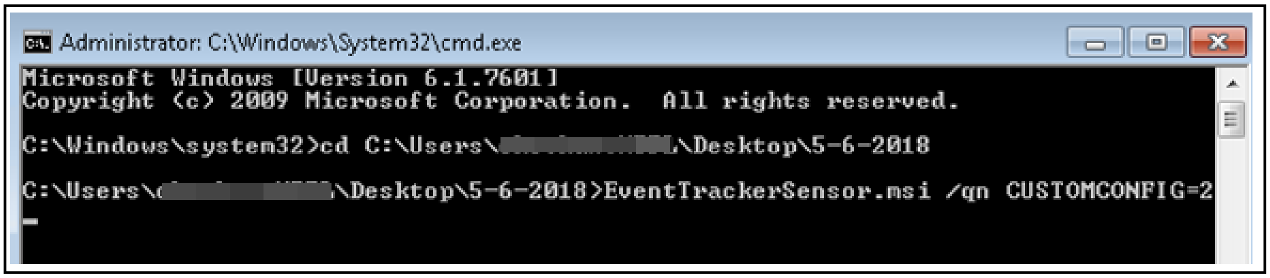
```
C:\Users\[redacted]\Desktop\UNSIGNEd>EventTrackerSensor.msi /qn EA=1 CA=1 CUST
OMCONFIG=0 EM=ntpldtblr36 EP=14505 CM=ntpldtblr36 IR=1 LS=ntpldtblr36 LP=14503 I
S_SUFFIX=1 SUFFIX=test SUPPORT_CONTACTS=99-89-89525
```

When CUSTOMCONFIG = 2,

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

Note:

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



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:\Users\[redacted]\Desktop\5-6-2018

C:\Users\[redacted]\Desktop\5-6-2018>EventTrackerSensor.msi /qn CUSTOMCONFIG=2
_
```

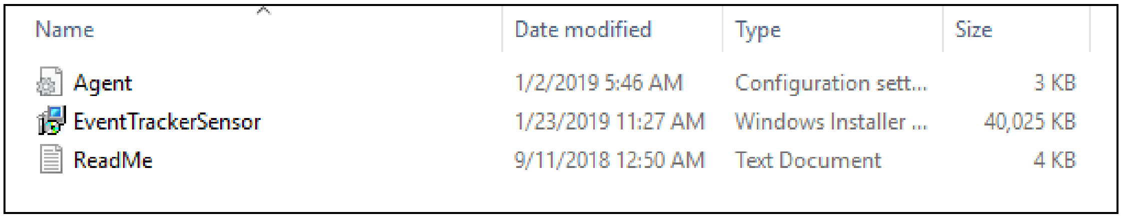
Note:

The attributes need to be filled in the etaconfig.ini for **CUSTOMCONFIG=2**.When the user is using the customized etaconfig.ini file, they should not run any parameters in the command line except “EventTrackersensor.msi /qn CUSTOMCONFIG=2”.

4 Deploying through Agent.ini file

4.1 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	1/2/2019 5:46 AM	Configuration sett...	3 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 KB

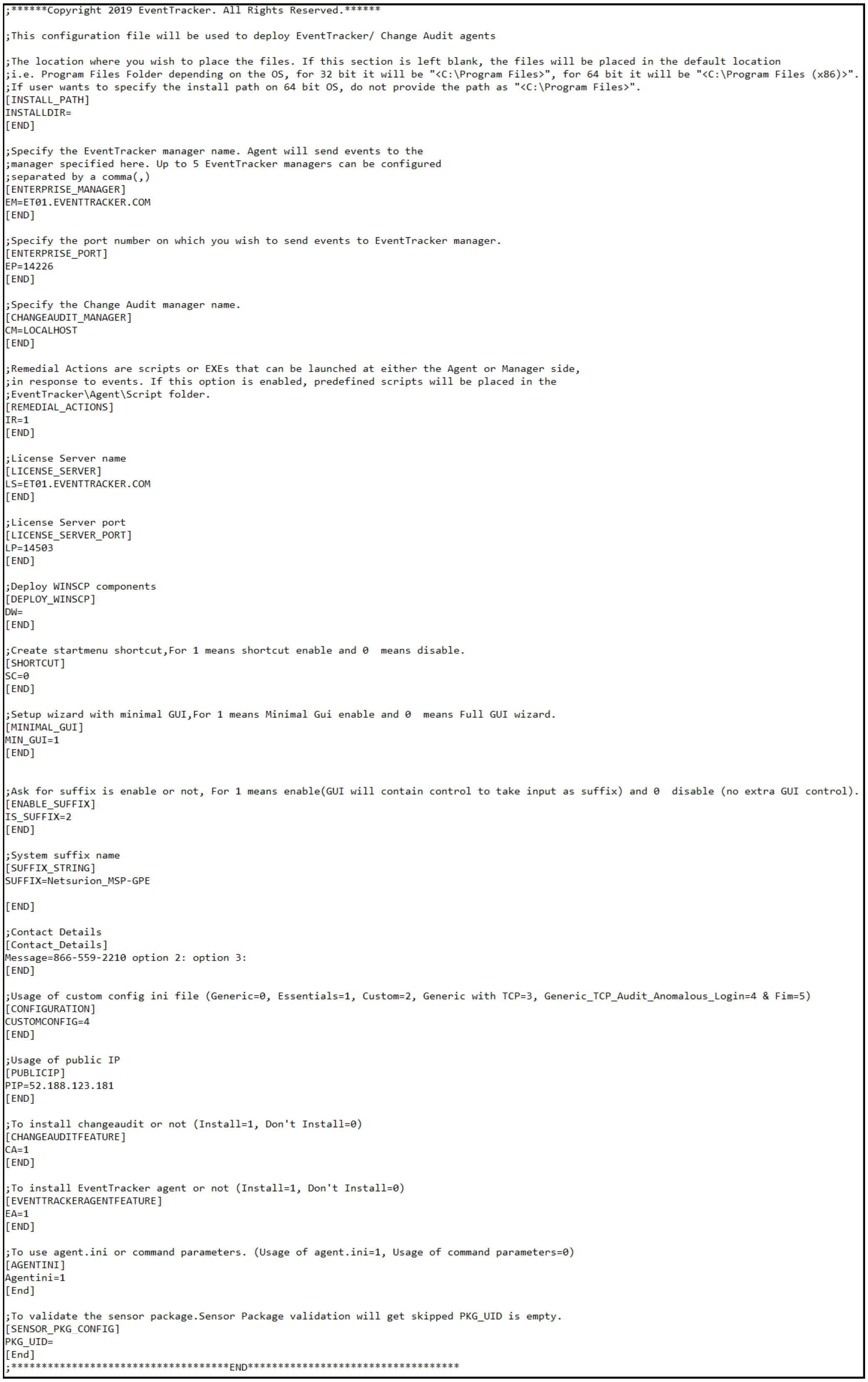
2. Edit the **Agent.ini** file and change the value for **Agent.ini=1**.

Note:

The mandatory fields to fill 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 2019 EventTracker. 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=ET01.EVENTTRACKER.COM
[END]

;Specify the port number on which you wish to send events to EventTracker manager.
[ENTERPRISE_PORT]
EP=14226
[END]

;Specify the Change Audit manager name.
[CHANGEAUDIT_MANAGER]
CM=LOCALHOST
[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=ET01.EVENTTRACKER.COM
[END]

;License Server port
[LICENSE_SERVER_PORT]
LP=14503
[END]

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

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

;Setup wizard with minimal GUI,For 1 means Minimal Gui enable and 0  means Full GUI wizard.
[MINIMAL_GUI]
MIN_GUI=1
[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=2
[END]

;System suffix name
[SUFFIX_STRING]
SUFFIX=Netsurion_MSP-GPE

[END]

;Contact Details
[Contact_Details]
Message=866-559-2210 option 2: option 3:
[END]

;Usage of custom config ini file (Generic=0, Essentials=1, Custom=2, Generic with TCP=3, Generic_TCP_Audit_Anomalous_Login=4 & Fim=5)
[CONFIGURATION]
CUSTOMCONFIG=4
[END]

;Usage of public IP
[PUBLICIP]
PIP=52.188.123.181
[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 get skipped PKG_UID is empty.
[SENSOR_PKG_CONFIG]
PKG_UID=
[End]
;************************************END***********************************
```

Note:

Refer the parameter abbreviation specified in the Parameters used for GUI and Silent Installation section for more details.

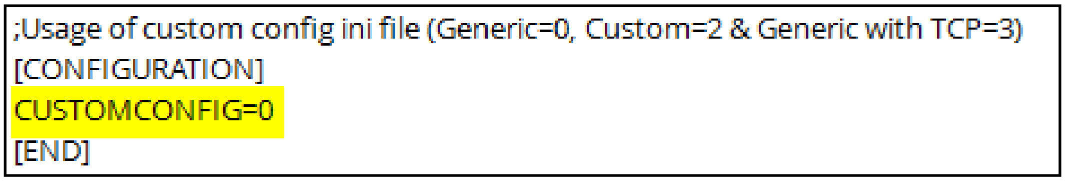
If the user wants to install only the Open XDR sensor, then the CA should be equal to 0 and vice-versa.

Types of sensor installation using GUI Mode in Agent.ini

```
CUSTOMCONFIG=0(or 3/4/5) EM = (Manager name) - Enterprise etaconfig.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.



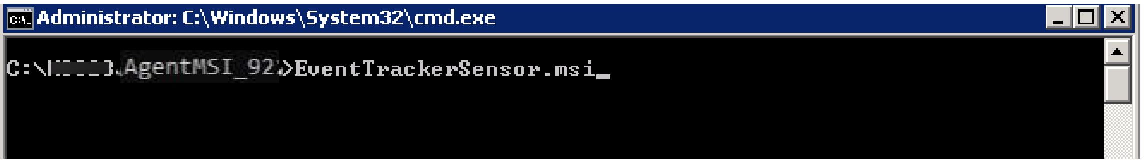
```
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]
```

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

3. Open the Command Prompt as **Run as Administrator** and change the directory to **AgentMSI_93**.

4. In the **Command Prompt**, type the following command and press the **Enter** key.

   Command: `EventTrackersensor.msi.`



```
C:\[redacted]\AgentMSI_92>EventTrackerSensor.msi_
```

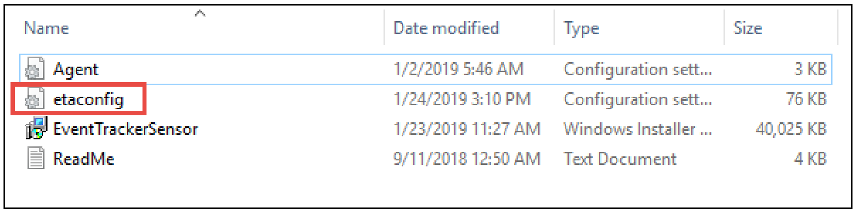
This command will open the Netsurion Open XDR sensor InstallShield Wizard.

Note:

Refer the GUI Installation procedure from Step 8 to Step 14.

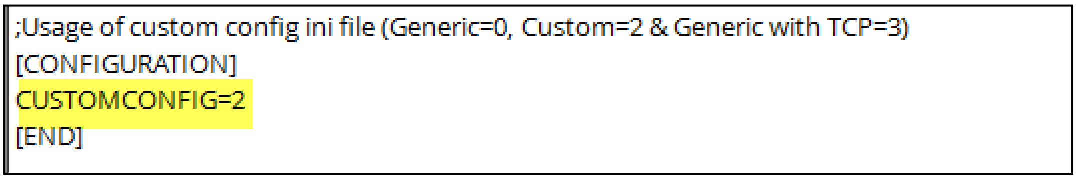
```
CUSTOMCONFIG=2 - Customer Existing etaconfig.ini.
```

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



Name	Date modified	Type	Size
Agent	1/2/2019 5:46 AM	Configuration sett...	3 KB
etaconfig	1/24/2019 3:10 PM	Configuration sett...	76 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 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.



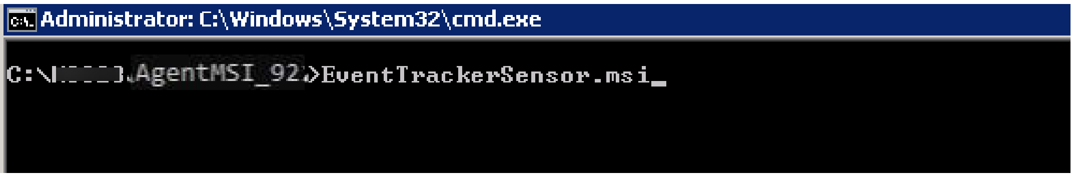
```
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]
```

2. Save the **Agent.ini** file.

3. Open the Command Prompt as "**Run as Administrator**" and change directory to **AgentMSI_93**.

4. In the **Command Prompt**, type the following command and press the **Enter** key.

Command : `EventTrackersensor.msi.`



```
C:\[redacted]AgentMSI_92>EventTrackerSensor.msi_
```

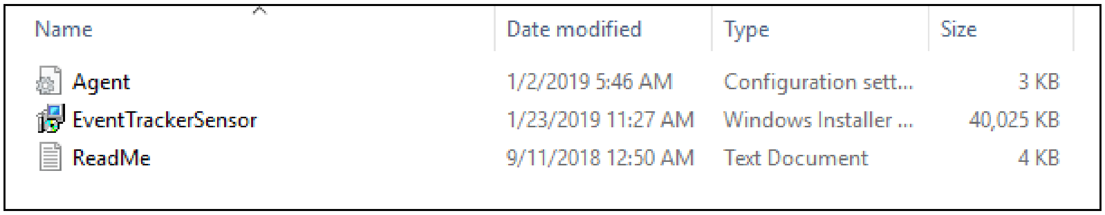
This command will open the Netsurion Open XDR sensor InstallShield Wizard.

Note:

Refer the GUI Installation procedure from Step 8 to Step 14.

4.2 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	1/2/2019 5:46 AM	Configuration sett...	3 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 KB

2. Edit the **Agent.ini** file and change the value for **Agent.ini=1**.

Note:

The mandatory fields to fill 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 Parameters used for GUI and Silent Installation section for more details.

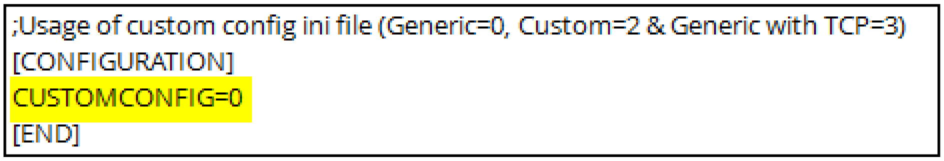
If the user wants to install only the Netsurion’s Open XDR sensor, then the CA should be equal to 0 and vice-versa.

Types of sensor installation using Silent Mode in Agent.ini

```
CUSTOMCONFIG=0(or 3/4/5) EM = (Manager name) - Enterprise etaconfig.ini
```

1. Here, fill the **Agent.ini** file with the mandatory fields as shown in the sample image, and change the **CUSTOMCONFIG=0(or 3/4/5)**

   Example of the modified Agent.ini field:



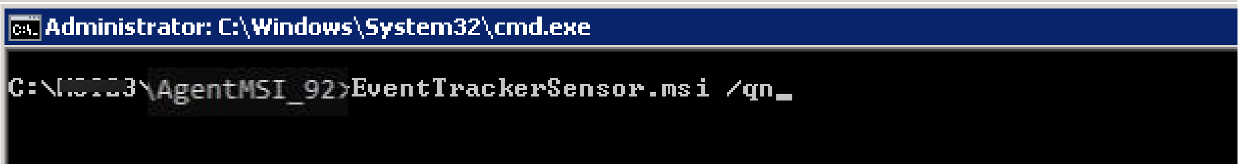
```
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=0
[END]
```

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

3. Open the Command Prompt as **Run as Administrator** and change the directory to **AgentMSI_93.**

4. In the **Command Prompt**, type the following command and press the **Enter** key.

Command : `EventTrackersensor.msi /qn`

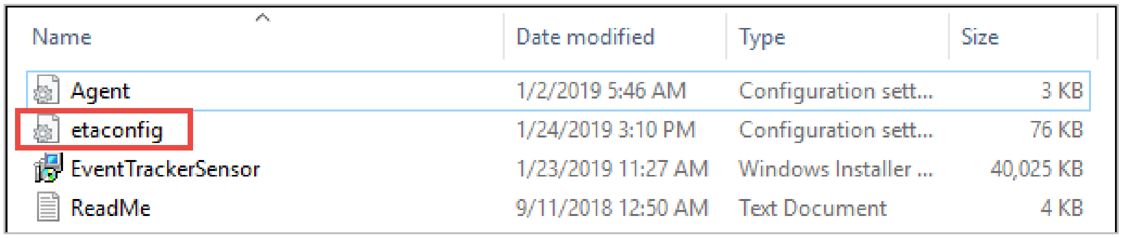


```
Administrator: C:\Windows\System32\cmd.exe
C:\[redacted]3\AgentMSI_92>EventTrackerSensor.msi /qn_
```

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

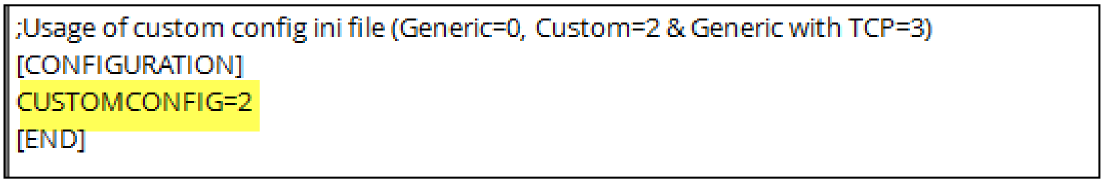
```
CUSTOMCONFIG=2 - Customer Existing etaconfig.ini
```

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



Name	Date modified	Type	Size
Agent	1/2/2019 5:46 AM	Configuration sett...	3 KB
etaconfig	1/24/2019 3:10 PM	Configuration sett...	76 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 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



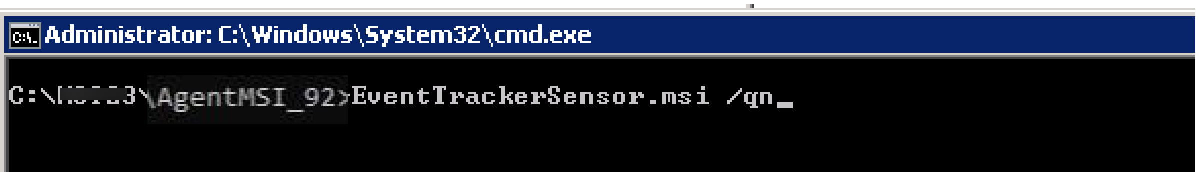
```
;Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3)
[CONFIGURATION]
CUSTOMCONFIG=2
[END]
```

2. Save the Agent.ini file.

3. Open the Command Prompt as "**Run as Administrator**" and change the directory to **AgentMSI_93**.

4. In the **Command Prompt**, type the following command and press the **Enter** key.

Command : `EventTrackersensor.msi /qn`



```
C:\[redacted]3\AgentMSI_92>EventTrackerSensor.msi /qn
```

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

5 Deploying through Group Policy

5.1 Preparing the 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 & 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] INSTALLDIR=<Installation directory if agent need to be installed in other than default path> [END] [ENTERPRISE_MANAGER] EM=<Netsurion’s Open XDR Manager Hostname or FQDN> [END] [ENTERPRISE_PORT] EP=<Netsurion’s Open XDR Enterprise Port number> [END] [CHANGEAUDIT_MANAGER] CM=<Change Audit Manager Hostname or	[INSTALL_PATH] INSTALLDIR= [END] [ENTERPRISE_MANAGER] EM=Win2k3x64 [END] [ENTERPRISE_PORT] EP=14505 [END] [CHANGEAUDIT_MANAGER] CM=Win2k3x64 [END] [REMEDIAL_ACTIONS]

Configuration Settings	Sample Configuration
FQDN> [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 WINSCP components [DEPLOY_WINSCP] 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	IR=1 [END] [LICENSE_SERVER] LS=Win2k3x64 [END] [LICENSE_SERVER_PORT] LP=14503 [END] Deploy WINSCP components [DEPLOY_WINSCP] 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

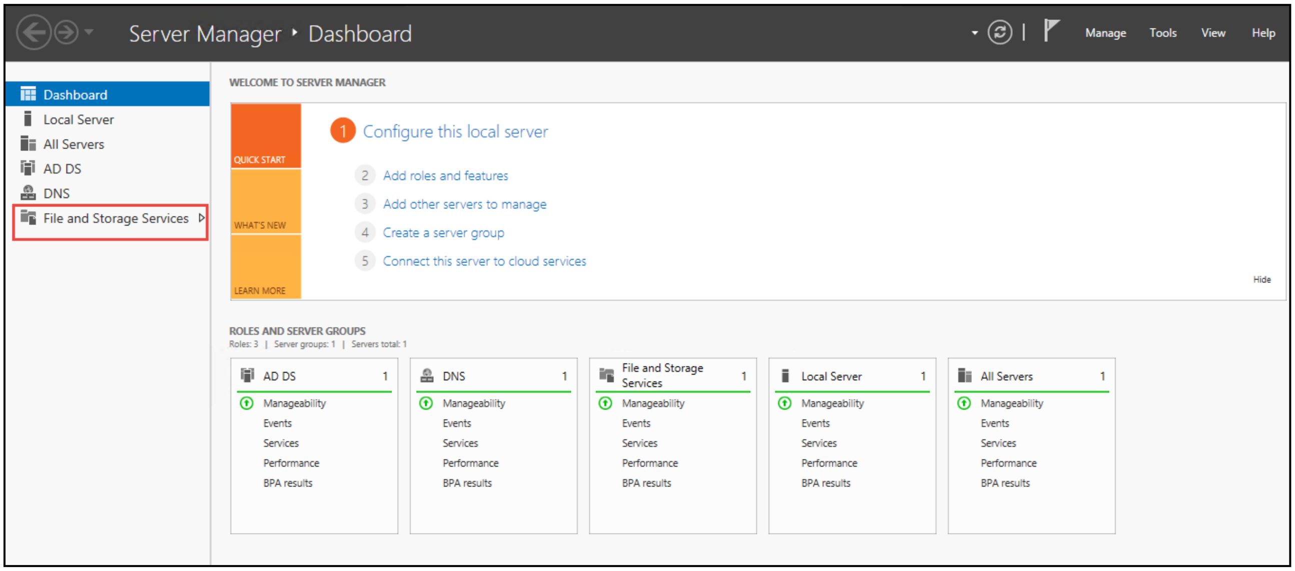
Configuration Settings	Sample Configuration
[SUFFIX_STRING] SUFFIX = [END] Contact Details [Contact_Details] Message = [END] Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3) [CONFIGURATION] CUSTOMCONFIG=0/2/3 [END] Usage of public IP [PROTECT IP] PIP=<Protect IP> [END] To install changeaudit or not (Install=1, Don't Install=0) [CHANGEAUDITFEATURE] CA=0/1 [END] To install Netsurion’s Open XDR sensor 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	[Contact_Details] Message = 999-888-777 [END] Usage of custom config ini file (Generic=0, Custom=2 & Generic with TCP=3) [CONFIGURATION] CUSTOMCONFIG=0 [END] Usage of public IP [PROTECT IP] PIP=193.XXX.X.5X5 [END] To install changeaudit or not (Install=1, Don't Install=0) [CHANGEAUDITFEATURE] CA=1 [END] To install Netsurion’s Open XDR sensor 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]

Configuration Settings	Sample Configuration
[End]	

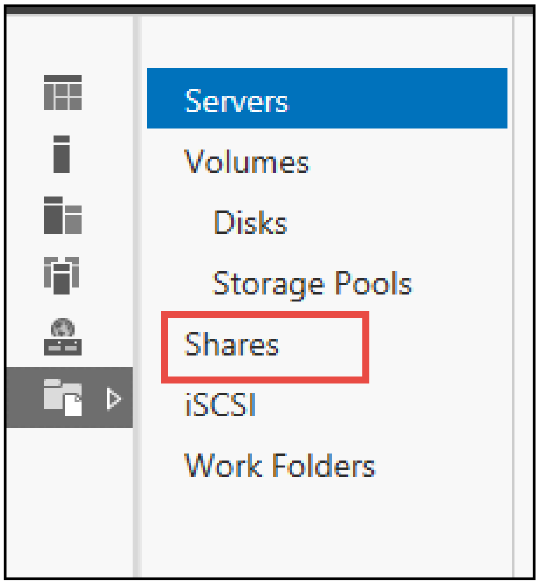
Create a network share on the server and allow **Domain Computers** to have at least **READ** access permission.

5.2 Creating a network share

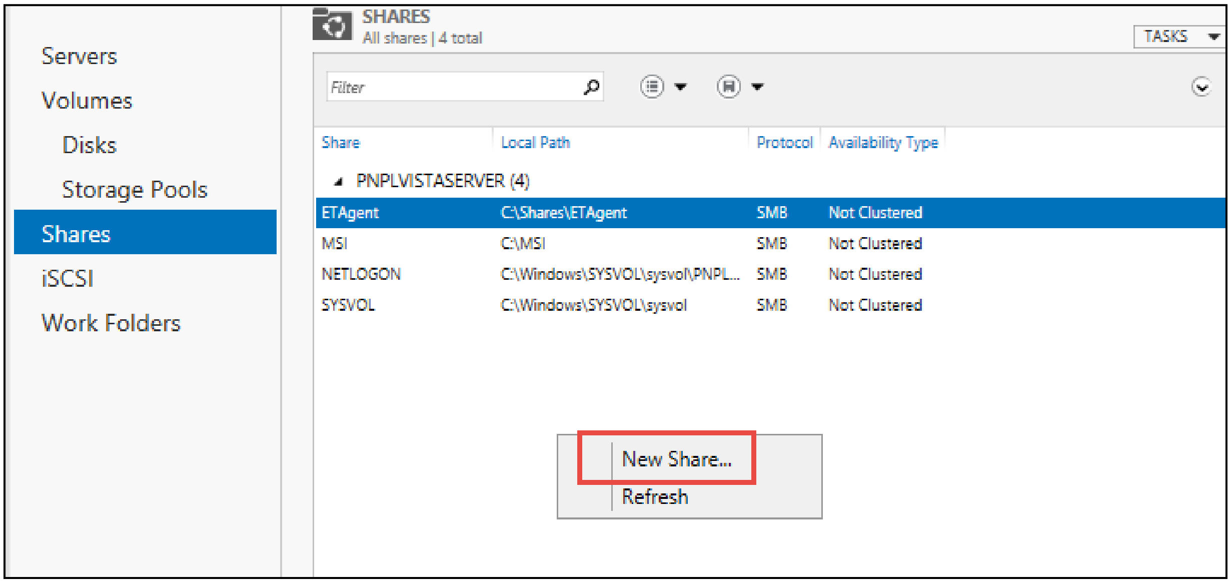
1. Go to the **Server Manager** and click **File and Storage Services.**



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



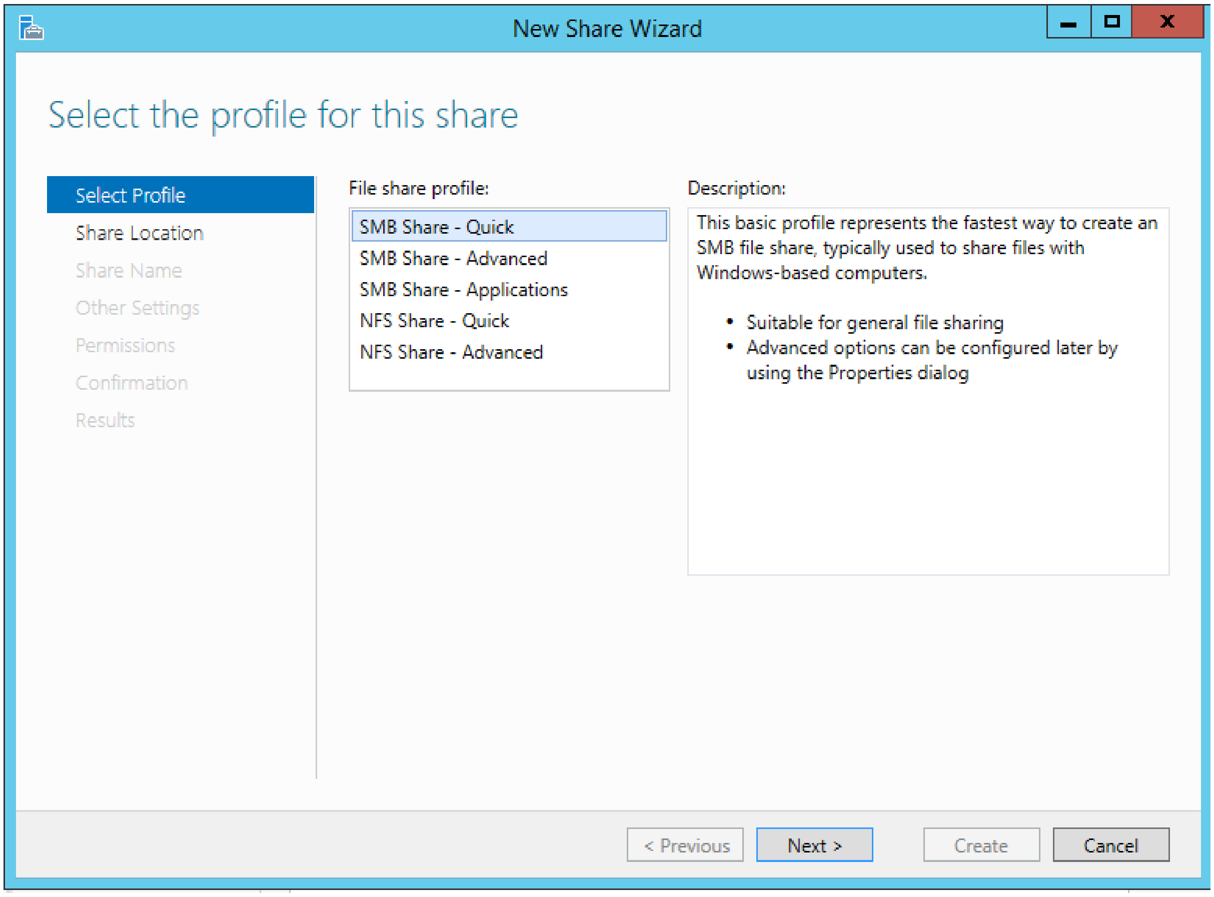
3. From the **Shares** interface, right-click on the screen and click **New Share**.



◢ PNPLVISTASERVER (4)

Share	Local Path	Protocol	Availability Type
ETAgent	C:\Shares\ETAgent	SMB	Not Clustered
MSI	C:\MSI	SMB	Not Clustered
NETLOGON	C:\Windows\SYSVOL\sysvol\PNPL...	SMB	Not Clustered
SYSVOL	C:\Windows\SYSVOL\sysvol	SMB	Not Clustered

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



File share profile:

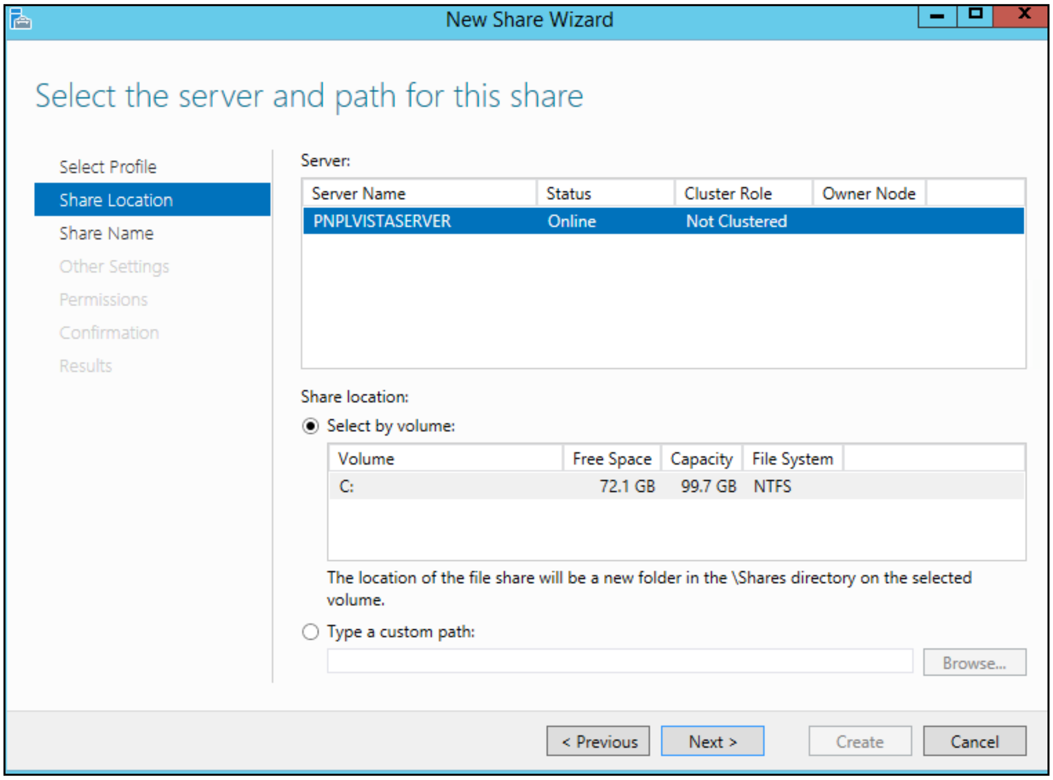
- SMB Share - Quick
- SMB Share - Advanced
- SMB Share - Applications
- NFS Share - Quick
- NFS Share - Advanced

Description:

This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog

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



Select the server and path for this share

Server:

Server Name	Status	Cluster Role	Owner Node
PNPLVISTASERVER	Online	Not Clustered	

Share location:

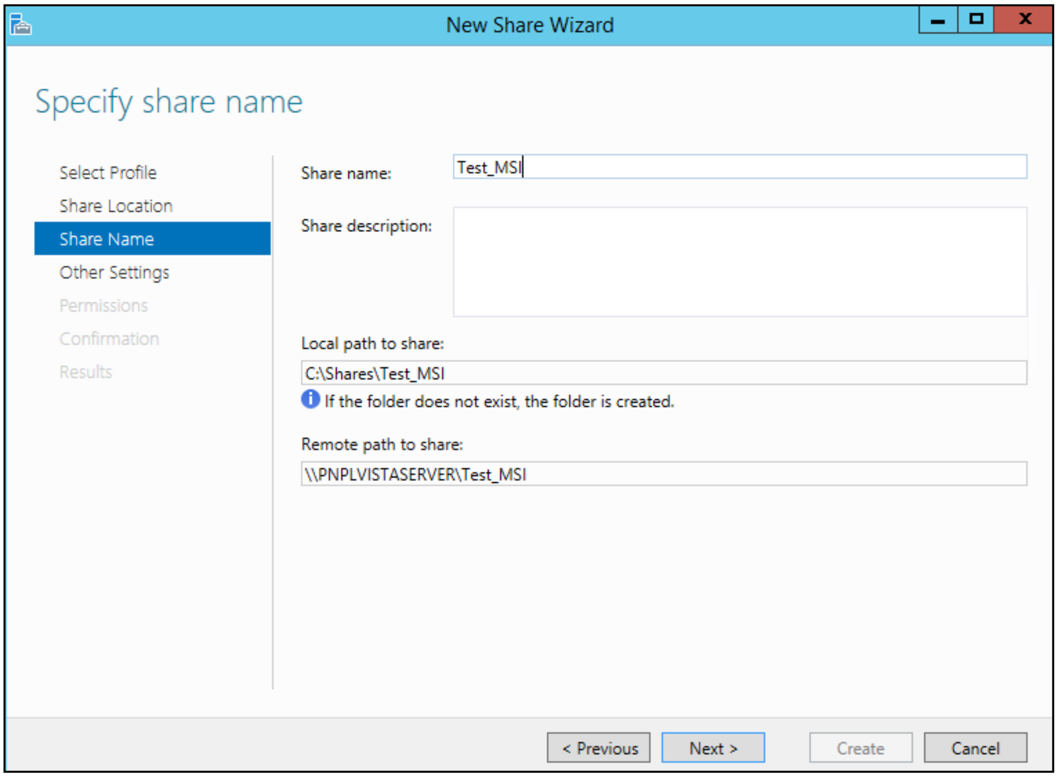
● Select by volume:

Volume	Free Space	Capacity	File System
C:	72.1 GB	99.7 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

○ Type a custom path:

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



Specify share name

Share name: Test_MSI

Share description:

Local path to share:

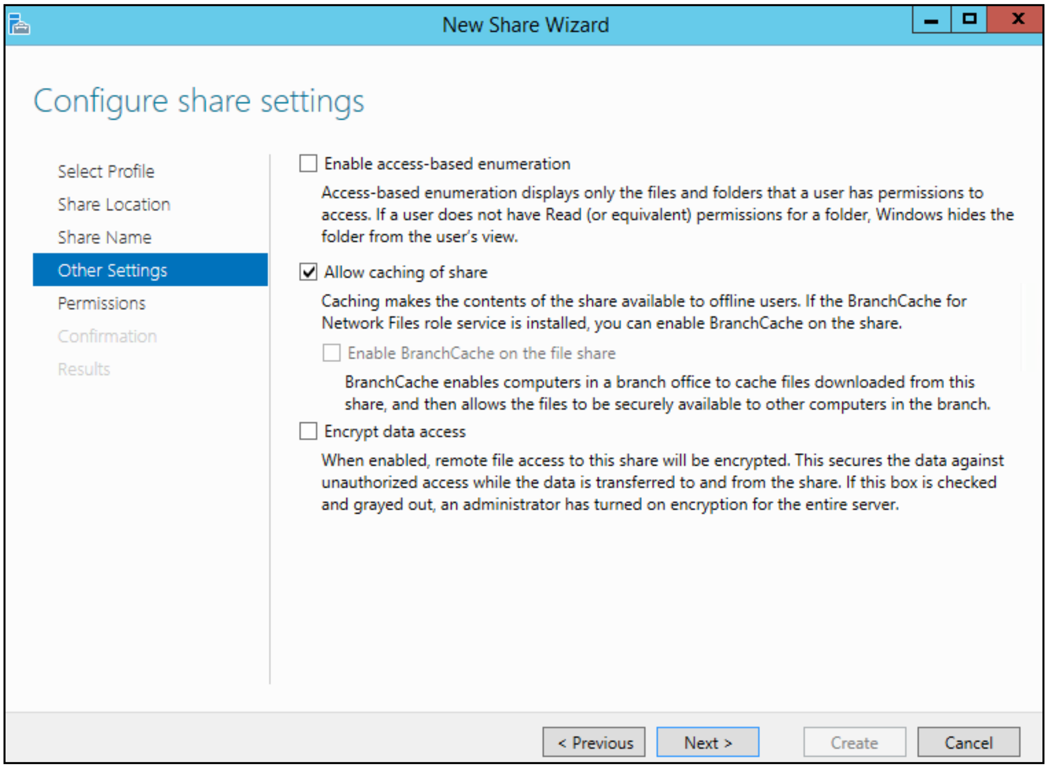
C:\Shares\Test_MSI

If the folder does not exist, the folder is created.

Remote path to share:

\\PNPLVISTASERVER\Test_MSI

7. Keep the default selection and click **Next** to proceed.



Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☑ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

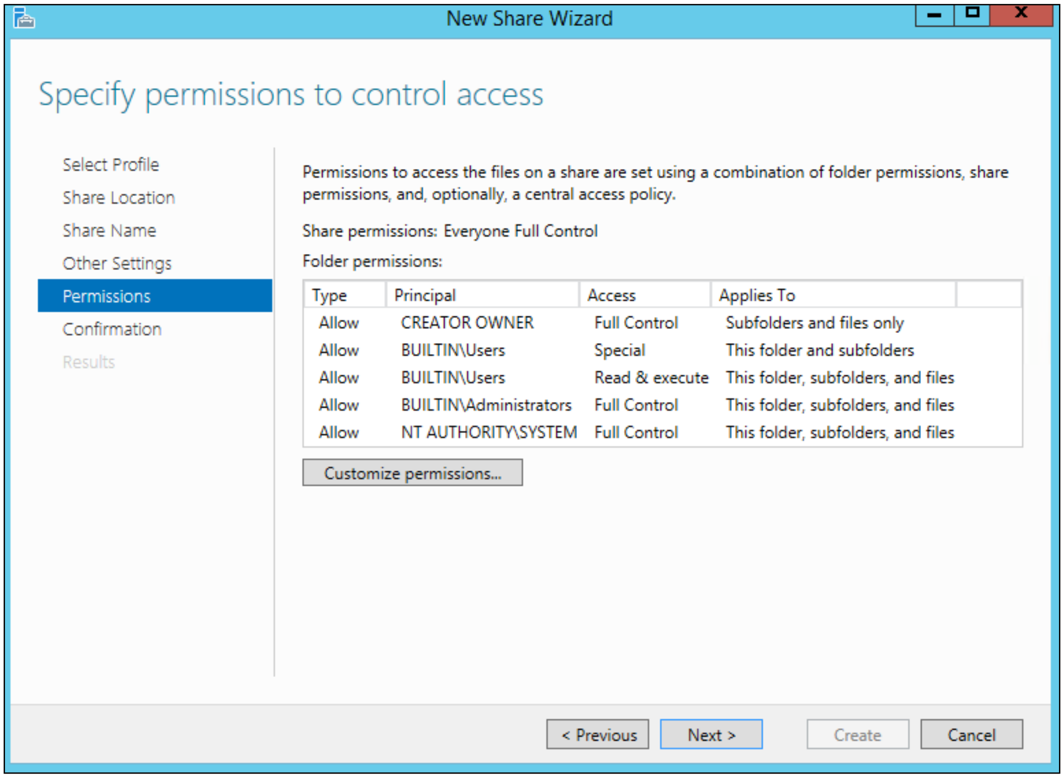
□ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

□ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

8. The following access should be allowed for successful installation. Click **Next**.



Specify permissions to control access

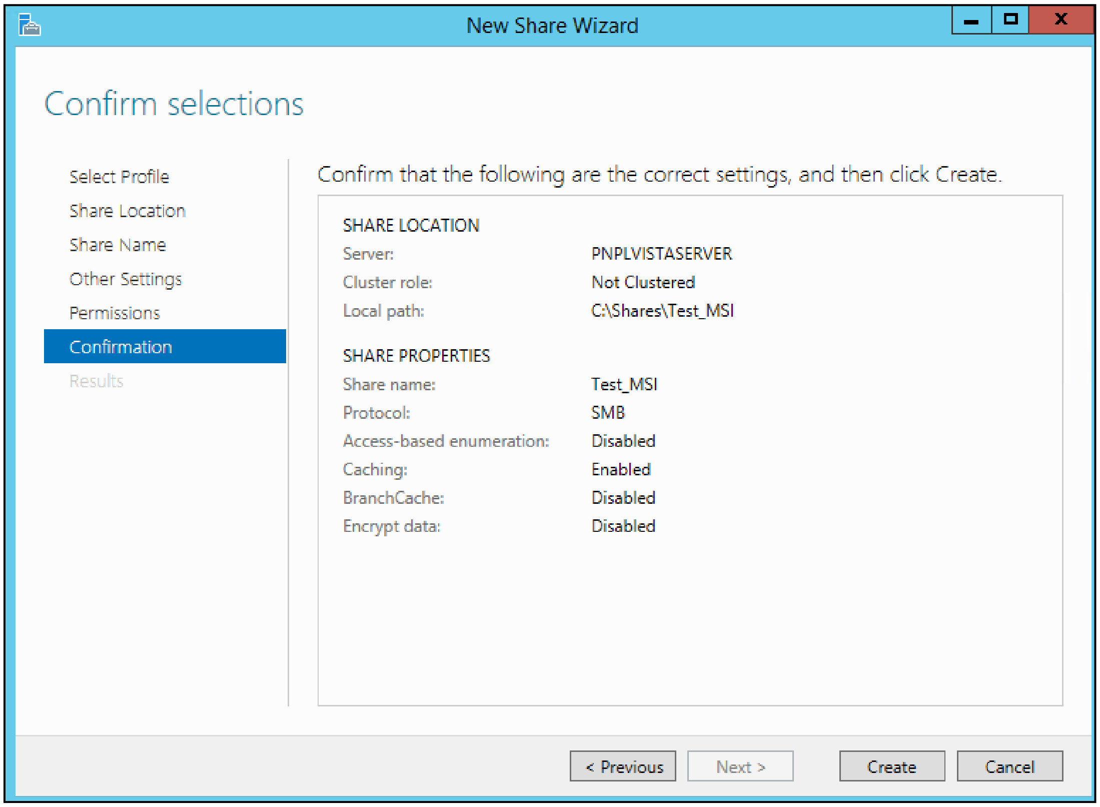
Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files

9. Verify to confirm the details and click **Create**.



Confirm selections

Confirm that the following are the correct settings, and then click Create.

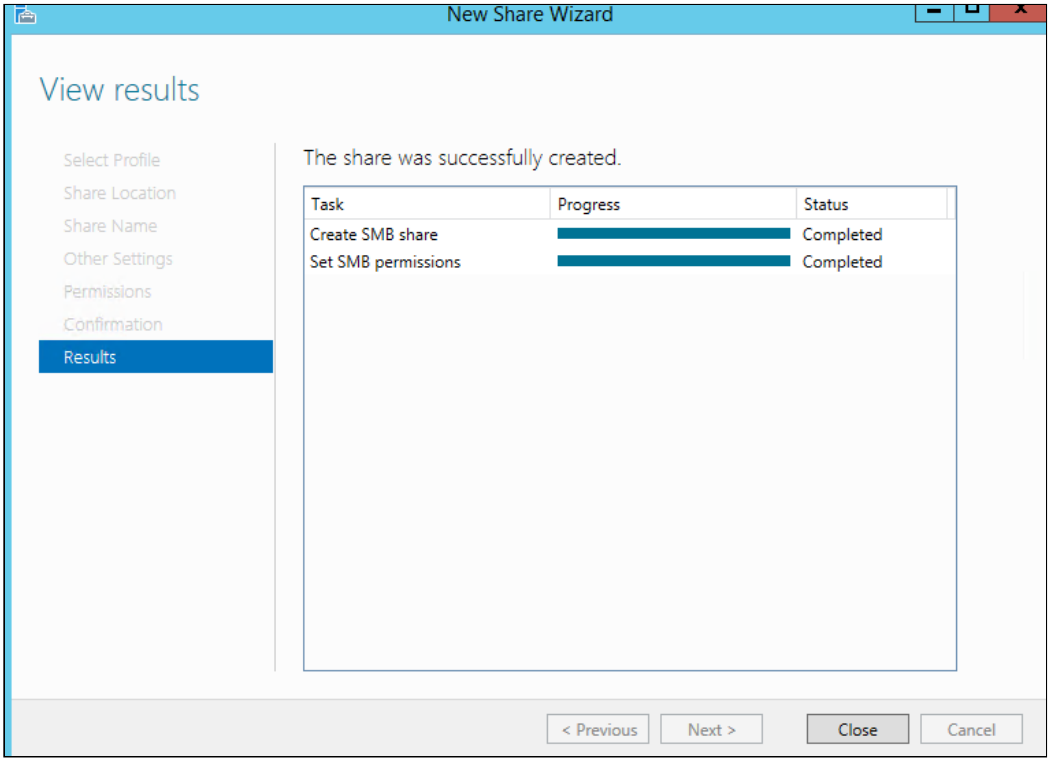
SHARE LOCATION

Server:	PNPLVISTASERVER
Cluster role:	Not Clustered
Local path:	C:\Shares\Test_MSI

SHARE PROPERTIES

Share name:	Test_MSI
Protocol:	SMB
Access-based enumeration:	Disabled
Caching:	Enabled
BranchCache:	Disabled
Encrypt data:	Disabled

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



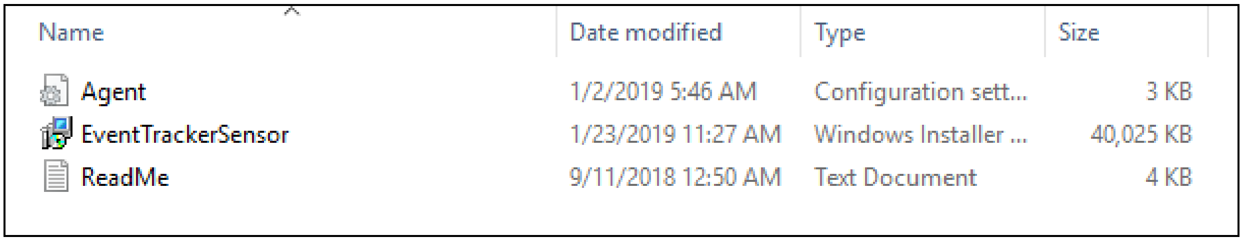
View results

The share was successfully created.

Task	Progress	Status
Create SMB share		Completed
Set SMB permissions		Completed

11. Copy the **AgentMSI_93** folder to the created network share folder.

Network share folder should have the below files.



Name	Date modified	Type	Size
Agent	1/2/2019 5:46 AM	Configuration sett...	3 KB
EventTrackerSensor	1/23/2019 11:27 AM	Windows Installer ...	40,025 KB
ReadMe	9/11/2018 12:50 AM	Text Document	4 KB

5.2.1 Parameters used in Agent.ini

Argument	Description
INSTALLDIR -	If this parameter is left blank, the files will be installed in the default location that is, %ProgramFiles%\Prism Microsystems. Else you can specify the path where you wish to install the files. **Note:** All the parameters will be read from the "Agent.ini" configuration settings file, when the installer is running silently.
EM -	Specify the Netsurion's Open XDR manager name. sensor will send events to the manager specified here. **Note:** It is mandatory to specify the Enterprise Manager name. **Note:** If user wish to install Netsurion's Open XDR sensor, then Enterprise Manager Name (EM) is mandatory.
EP -	Specify the port number on which you wish to send events to Netsurion's Open XDR manager.
CM -	Specify the Change Audit manager name. **Note:** If user wish to install **Change Audit sensor,** then Change Audit Manager Name (CM) is mandatory.

Argument	Description
IR -	If 1, then remedial actions are installed, and if 0, then remedial actions are not installed. **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.
LS -	The system name/ FQDN OR THE 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).
LP -	If this parameter is left blank, the default port (that is, 14503) will be assumed by the installer.
DW -	Deploy WINSCP components. If the value is empty, then WINSCP components will not be installed. If the value is '1', then WINSCP components will be installed.
SC -	Shortcut will not be created in startmenu if the value is '0' or empty. If the value is '1', then shortcut will be created in startmenu.
MIN_GUI -	Setup wizard with minimal GUI, if the value is '1'**.** If the value is '0', it means full GUI wizard. **Note:** The checkbox setting in GUI that is, "Deploy WINSCP components" will populate as per Agent.ini configuration.
IS SUFFIX -	Will ask for Suffix enabled or not. If the value is "0" it will be disabled and if the value is "1" it will be enabled
SUFFIX -	Enter the system suffix name in this field. **Note:** For silent/GPO installation- the installation will be aborted if the suffix/location name is in enable state in Agent.ini and its value is empty.
MESSAGE -	Customized Contact details.

Argument	Description
CUSTOMCONFIG -	Usage of the custom config in the .ini file. ▪ EventTrackersensor.msi CUSTOMCONFIG=0 EM = (Manager name) - Enterprise etaconfig.ini in UDP mode. ▪ EventTrackersensor.msi CUSTOMCONFIG=3 EM = (Manager name) - Enterprise etaconfig.ini in TCP mode. ▪ EventTrackersensor.msi CUSTOMCONFIG=2 - Customer Existing etaconfig.ini
PIP -	Usage of Protect IP.
CA -	To install Change Audit.
EA -	To install Netsurion's Open XDR sensor.
AGENTINI -	To use Agent.ini or command parameters (Usage of Agent.ini=1, Usage of command parameters=0).

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) which installs runtime components of Visual C++ Libraries required to run applications developed with Visual C++ is also installed along with the MSI sensor Installer setup.

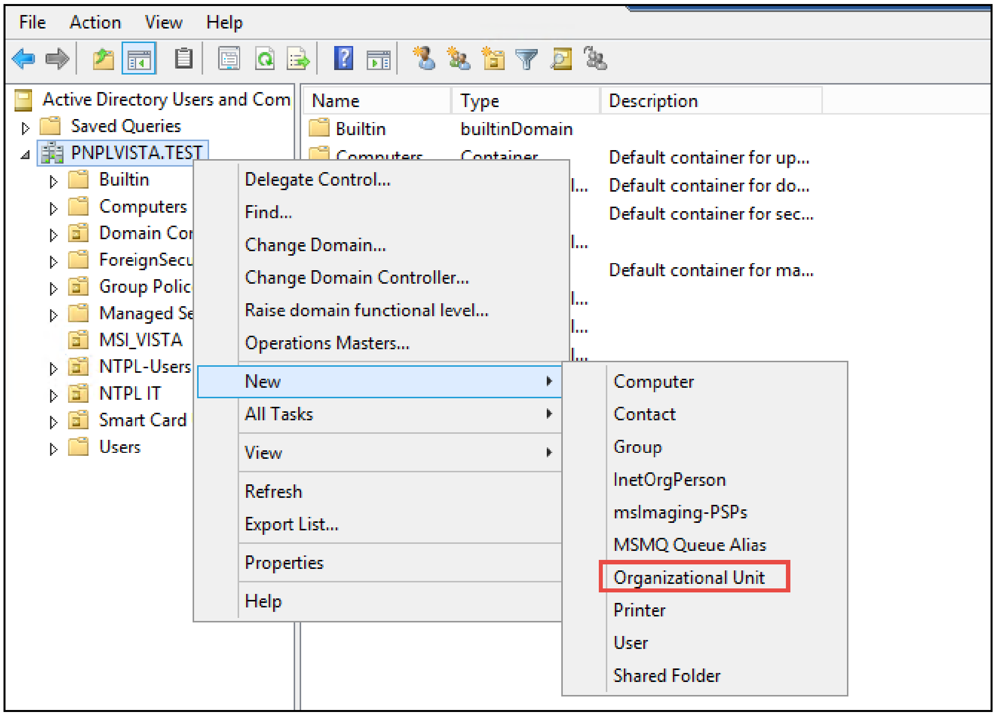
Note:

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

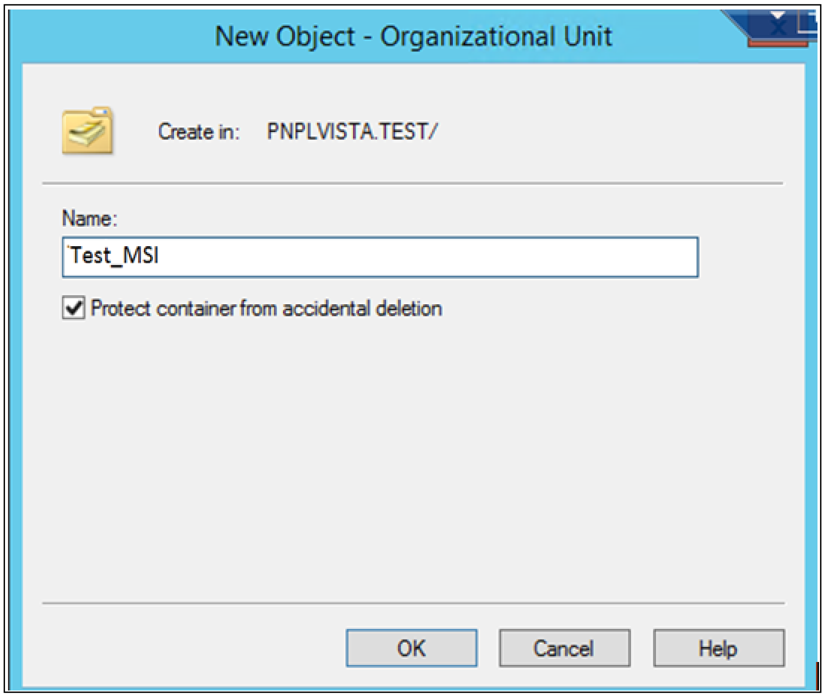
5.3 Assigning Systems to New Organization Unit

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** > **Name** field, specify the appropriate name and click **OK**.

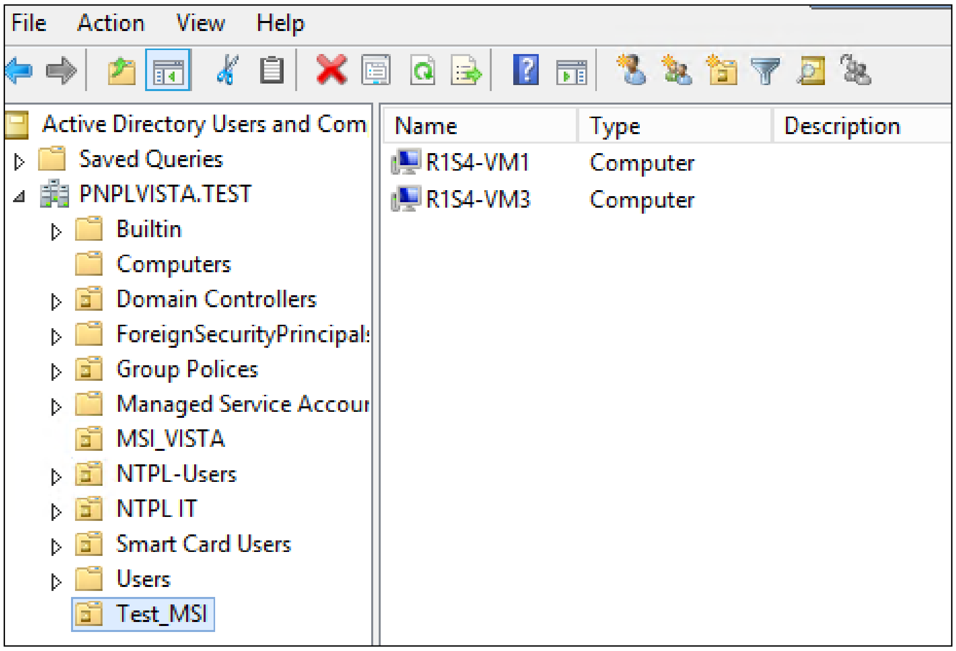


Create in: PNPLVISTA.TEST/

Name: Test_MSI

☑ Protect container from accidental deletion

4. Once the group is created, move the systems to this newly created OU Group.

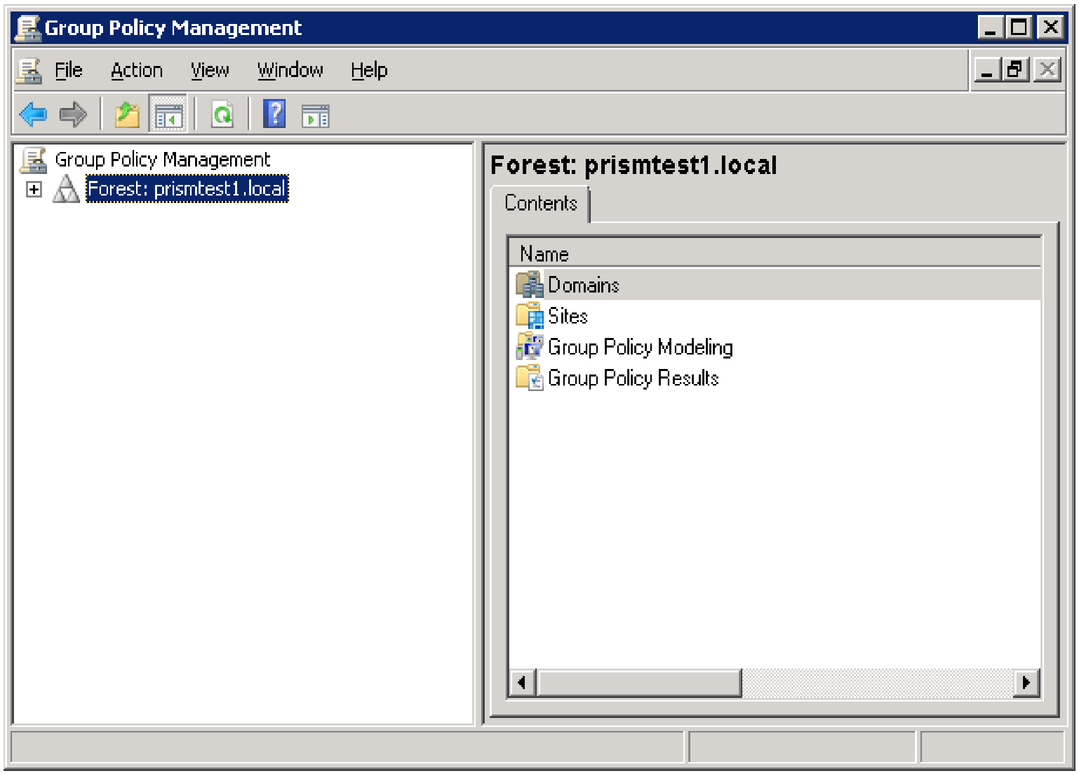


Name	Type	Description
R1S4-VM1	Computer	
R1S4-VM3	Computer	

5.4 Launching the Group Policy Management Console

1. Go to **Start** > **Settings** > **Control Panel**.

2. Click **Administrative** tools and launch the **Group Policy Management**.

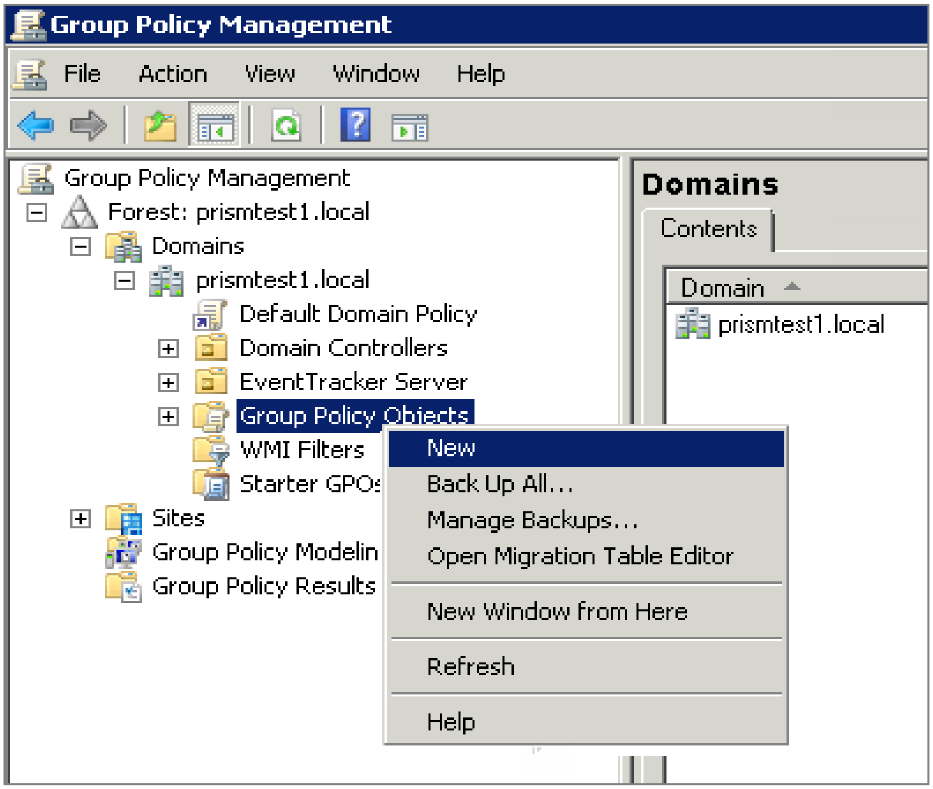


5.5 Creating the Group Policy Object in Active Directory for Software Deployment

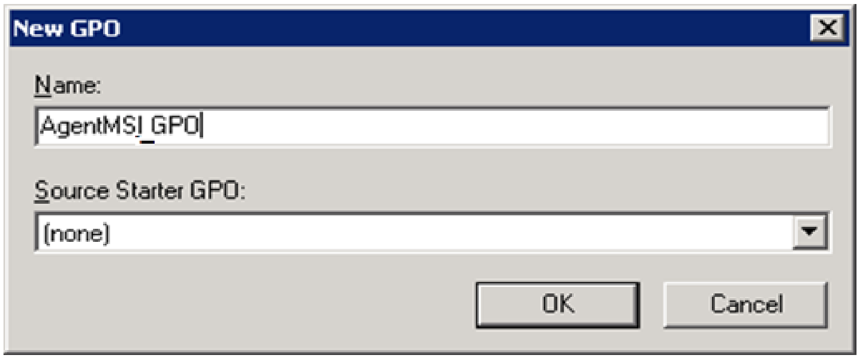
Follow the steps given below to create the new 'Group Policy Object' using the 'Group Policy Management' Snap-in,

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**.



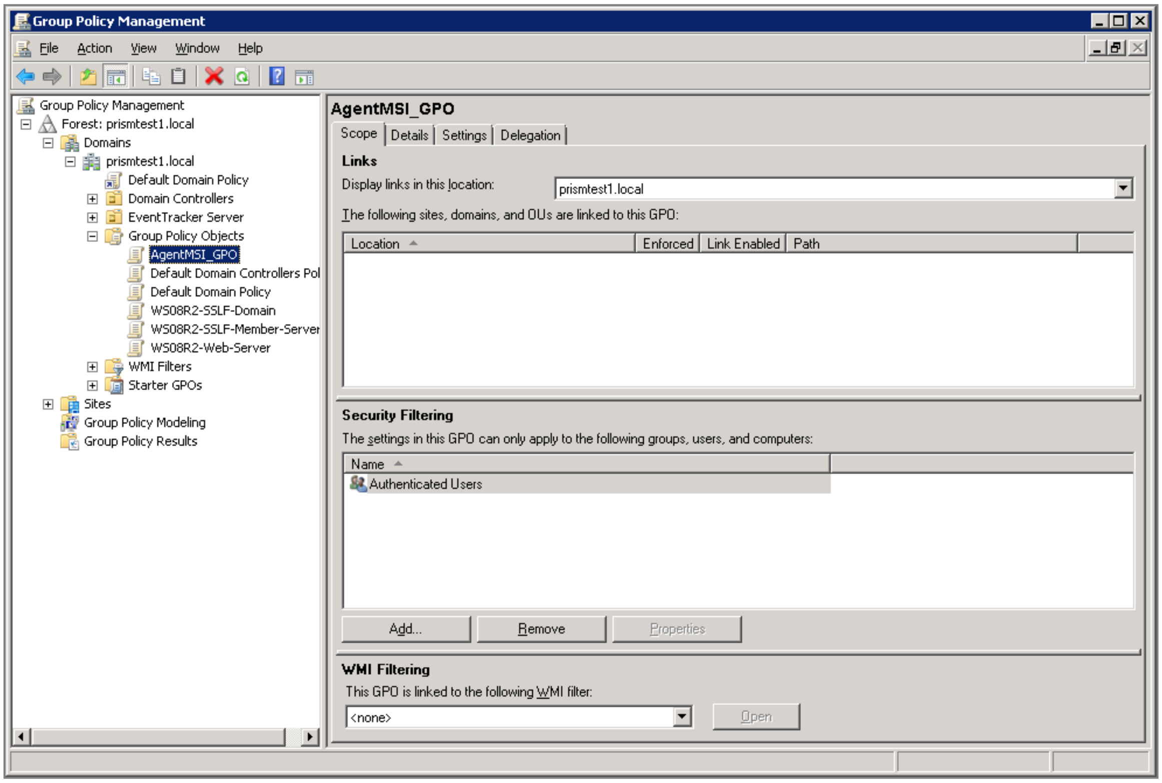
3. Enter a name for this new GPO (Ex. AgentMSI_GPO) and then click **OK**.



Name: AgentMSI_GPO

Source Starter GPO: (none)

4. Click the name of the newly created GPO. For example, ‘AgentMSI_GPO’.



Display links in this location: prismtest1.local

The following sites, domains, and OUs are linked to this GPO:

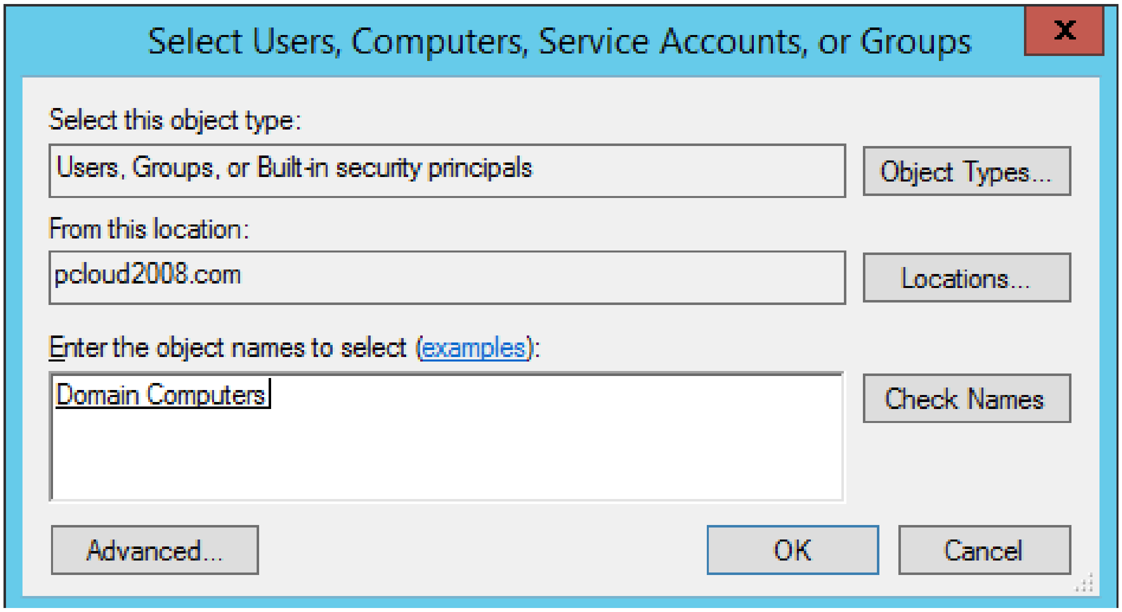
The settings in this GPO can only apply to the following groups, users, and computers:

Authenticated Users

This GPO is linked to the following WMI filter: <none>

5. In the **Security Filtering** pane, click the **Add** button to apply GPO settings to the domain computers group (or ensure the authenticated user’s group is listed).

6. 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**.



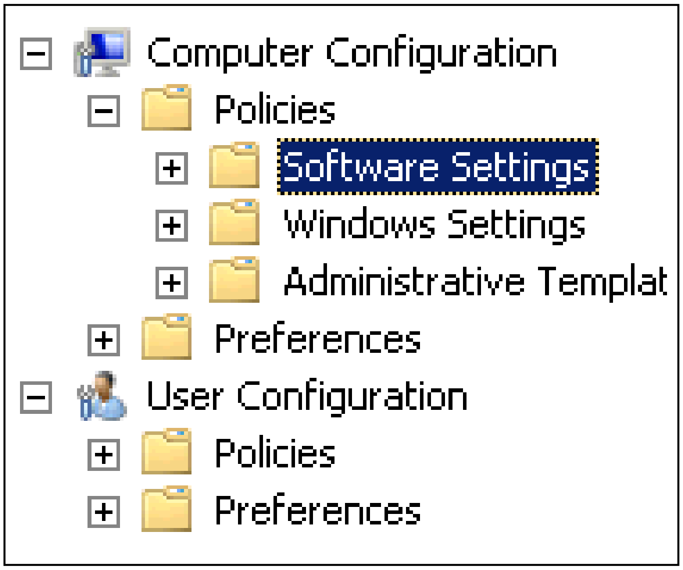
Select this object type: Users, Groups, or Built-in security principals

From this location: pcloud2008.com

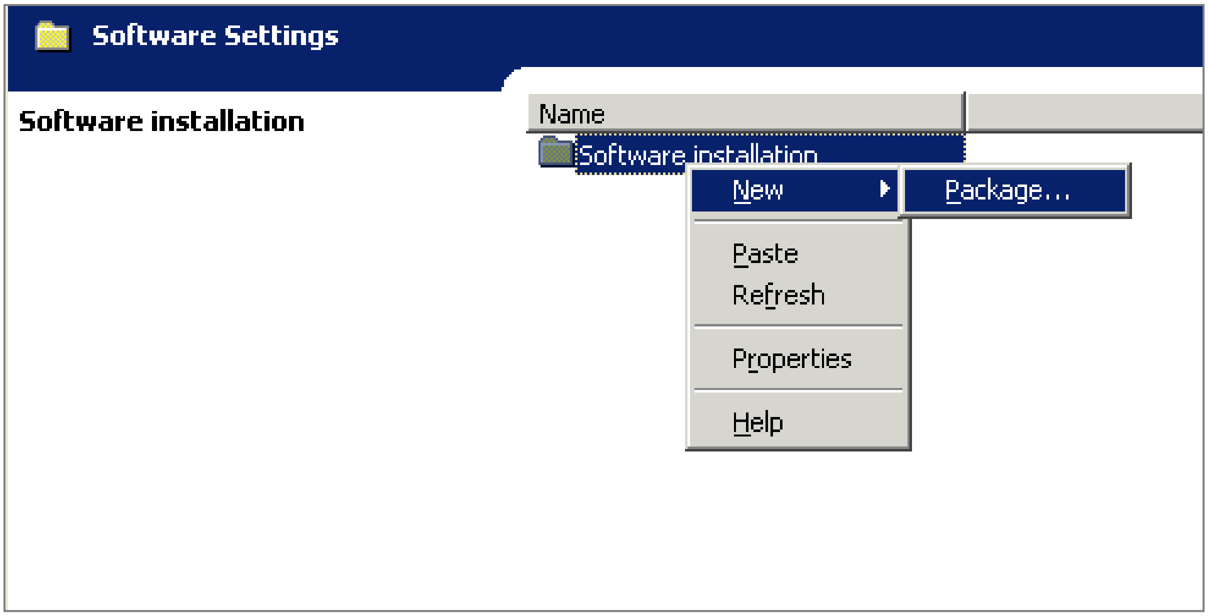
Enter the object names to select (examples): Domain Computers

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

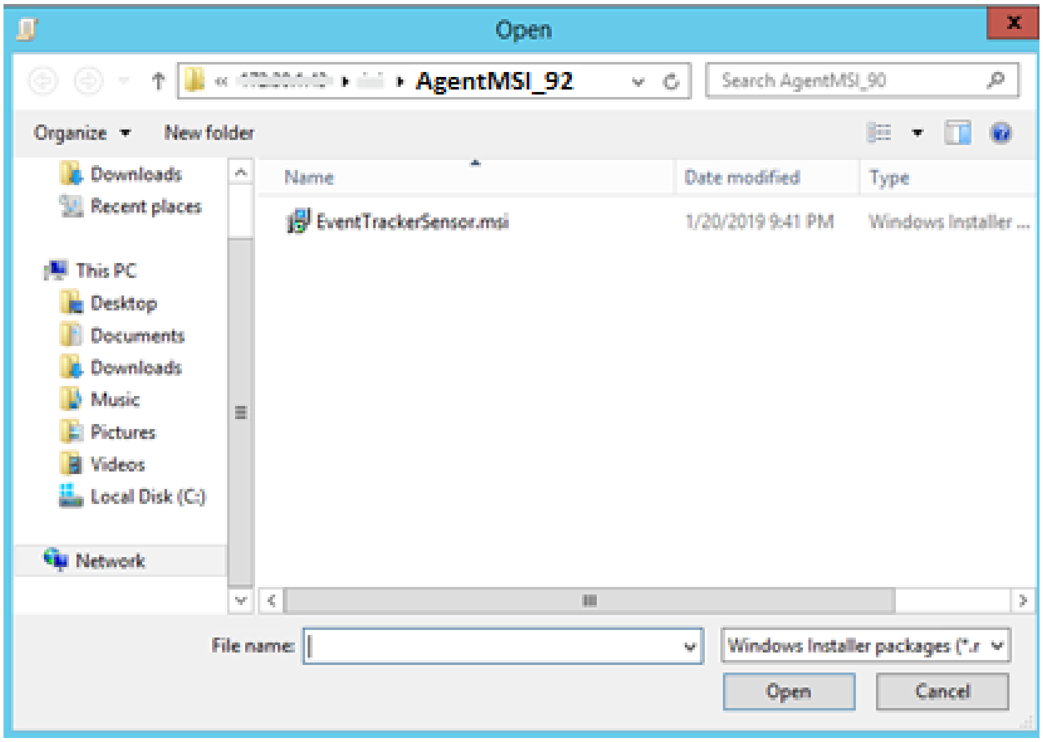
8. In the **Group Policy Object Editor** window, expand the **Computer Configuration**, and open Software Settings.



9. 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_93\).



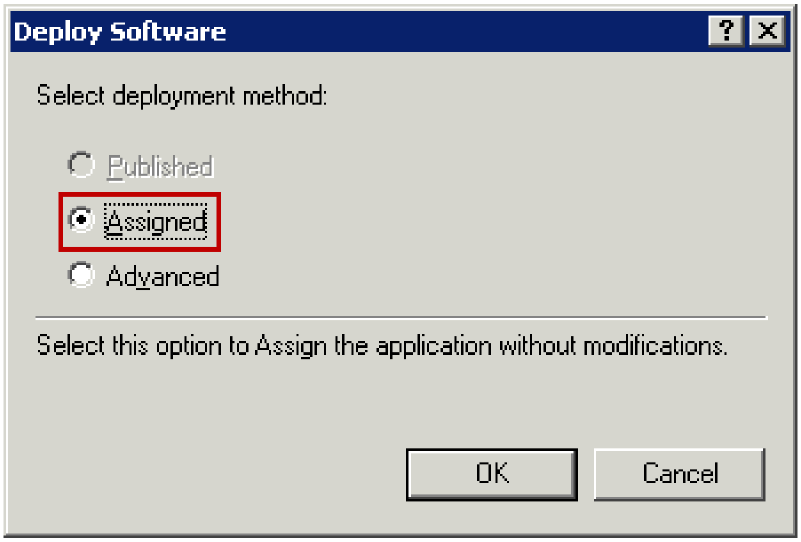
Name	Date modified	Type
EventTrackerSensor.msi	1/20/2019 9:41 PM	Windows Installer ...

File name:

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

Netsurion's Open XDR displays 'Deploy Software' dialog box.

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



Select deployment method:

○ Published

● Assigned

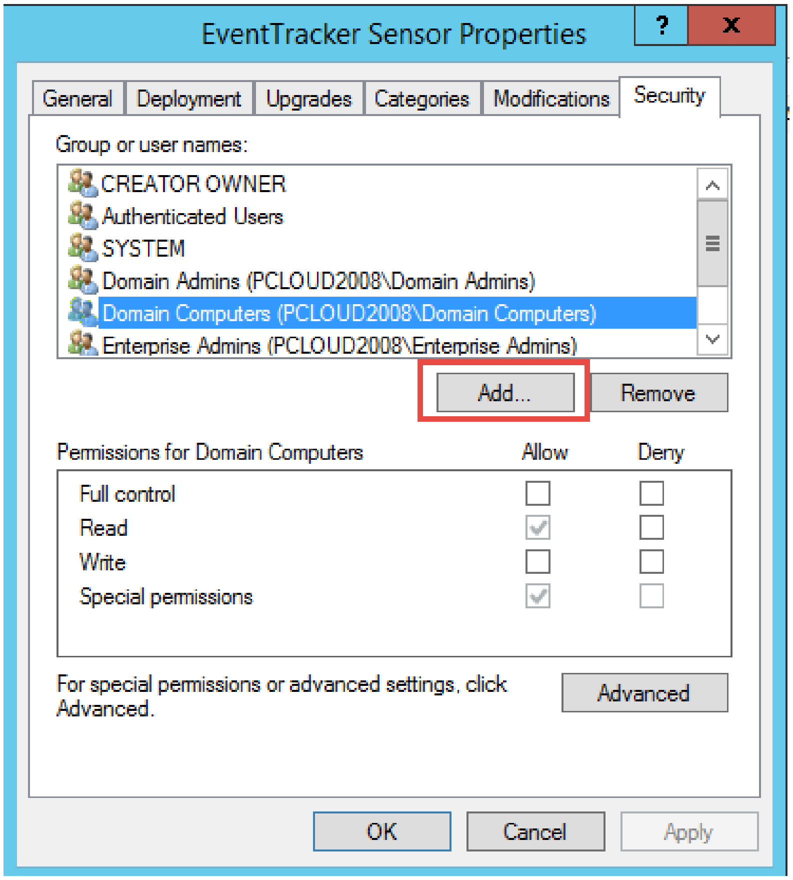
○ Advanced

Select this option to Assign the application without modifications.

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

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

14. Go to the **Security** tab and click the Add to add Domain Computers to provide security permissions.



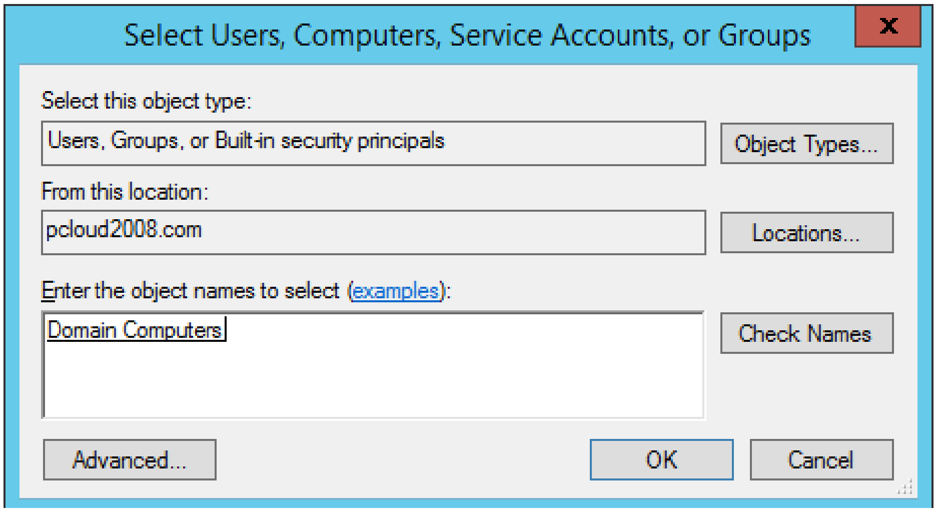
Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- Domain Admins (PCLOUD2008\Domain Admins)
- Domain Computers (PCLOUD2008\Domain Computers)
- Enterprise Admins (PCLOUD2008\Enterprise Admins)

Permissions for Domain Computers	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Special permissions	☑	□

For special permissions or advanced settings, click Advanced.

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



Select this object type:

Users, Groups, or Built-in security principals

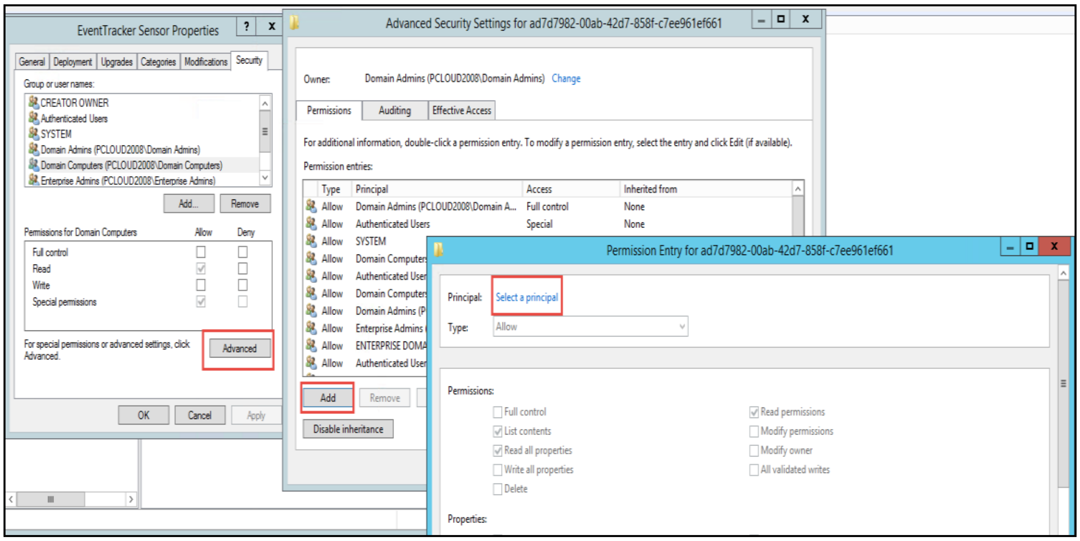
From this location:

pcloud2008.com

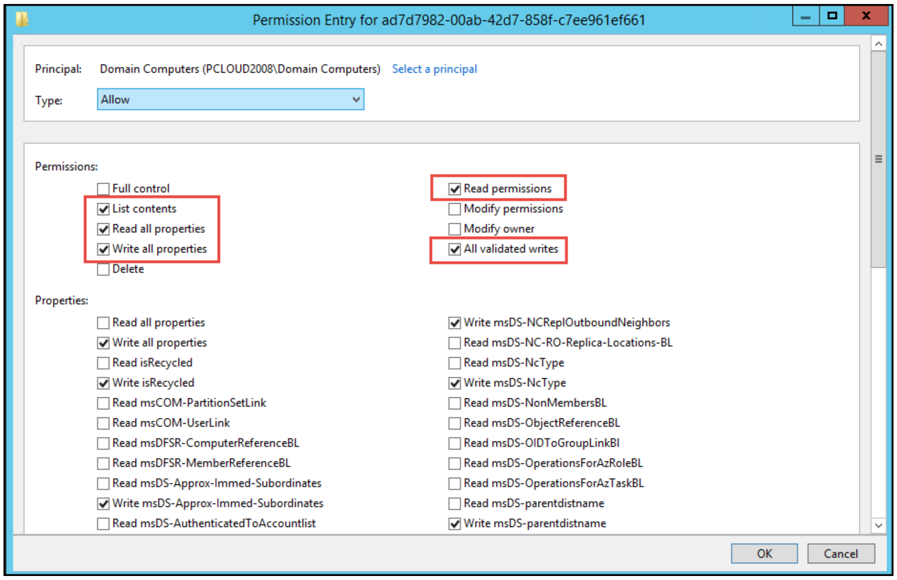
Enter the object names to select (examples):

Domain Computers

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



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



Principal: Domain Computers (PCLOUD2008\Domain Computers)

Type: Allow

Permissions:

☐ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☐ Delete
☑ Read permissions
☐ Modify permissions
☐ Modify owner
☑ All validated writes

Properties:

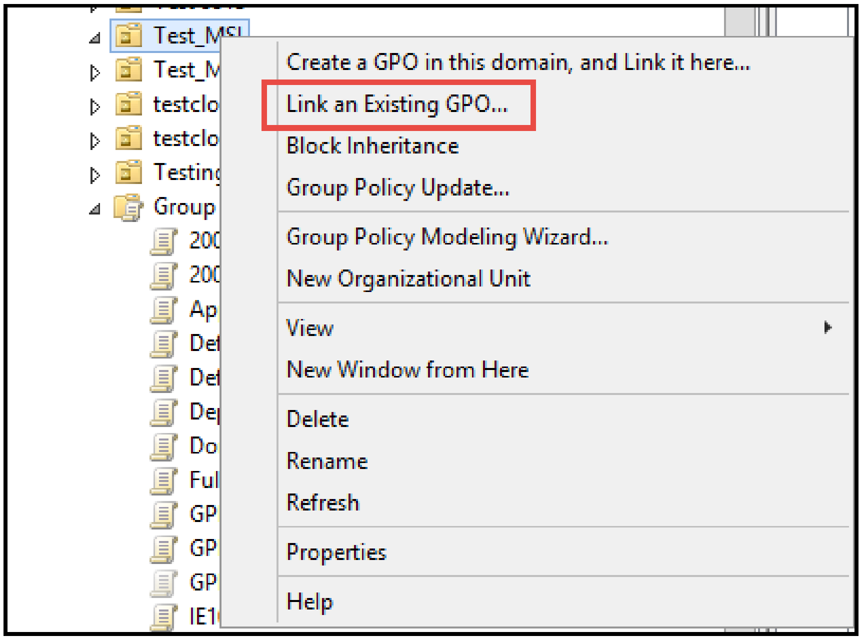
☐ Read all properties
☑ Write all properties
☐ Read isRecycled
☑ Write isRecycled
☐ Read msCOM-PartitionSetLink
☐ Read msCOM-UserLink
☐ Read msDFSR-ComputerReferenceBL
☐ Read msDFSR-MemberReferenceBL
☐ Read msDS-Approx-Immed-Subordinates
☑ Write msDS-Approx-Immed-Subordinates
☐ Read msDS-AuthenticatedToAccountlist
☑ Write msDS-NCReplOutboundNeighbors
☐ Read msDS-NC-RO-Replica-Locations-BL
☐ Read msDS-NcType
☑ Write msDS-NcType
☐ Read msDS-NonMembersBL
☐ Read msDS-ObjectReferenceBL
☐ Read msDS-OIDToGroupLinkBl
☐ Read msDS-OperationsForAzRoleBL
☐ Read msDS-OperationsForAzTaskBL
☐ Read msDS-parentdistname
☑ Write msDS-parentdistname

Note:

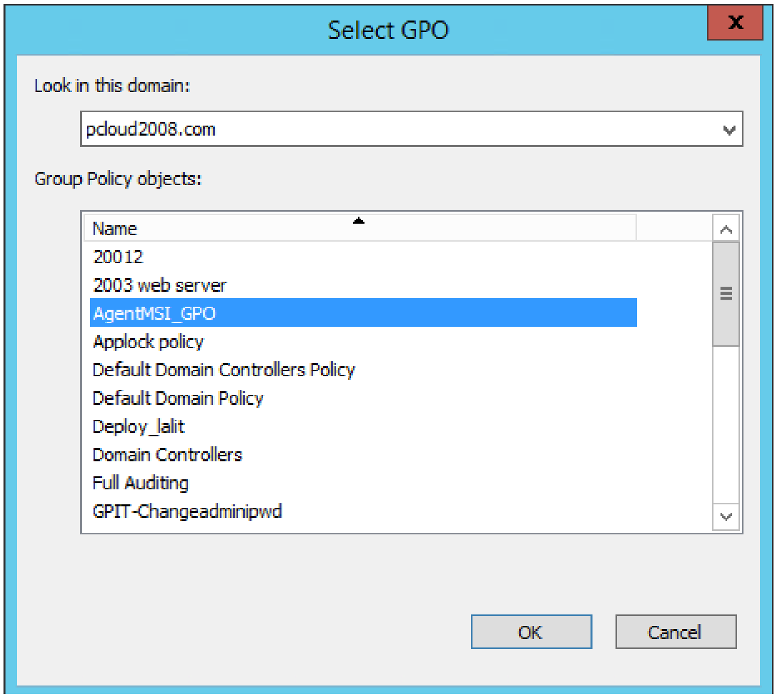
Ensure Domain Computers has the Read and Write rights.

18. In the **Netsurion's Open XDR sensor Properties** window, click **OK**.

19. In **Group Policy Management** pane, right-click the new organizational unit created earlier (Refer Assigning Systems to New Organization Unit section) and click **Link Existing GPO** from the drop-down menu.



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



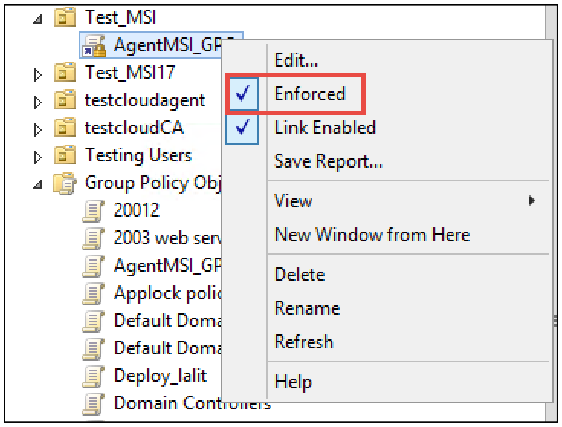
Look in this domain:

pcloud2008.com

Group Policy objects:

Name
20012
2003 web server
AgentMSI_GPO
Applock policy
Default Domain Controllers Policy
Default Domain Policy
Deploy_lalit
Domain Controllers
Full Auditing
GPIT-Changeadminipwd

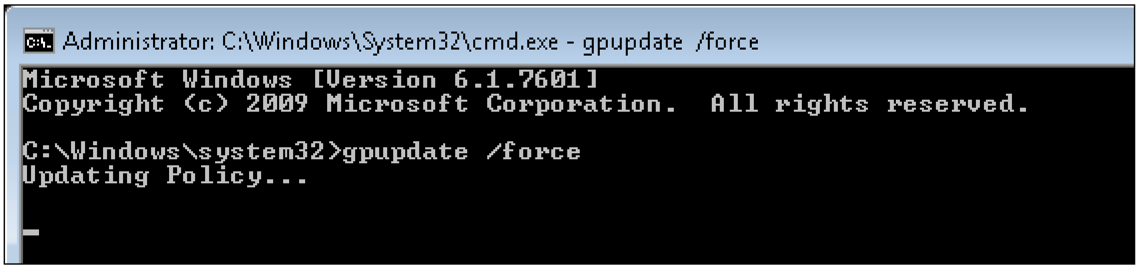
21. Navigate to Linked GPO, right-click and enable **Enforced**.



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

22. Now the user can go to Target machine and update the Group policy by using the following command in command prompt.

Command: `gpupdate /force`



```
Administrator: C:\Windows\System32\cmd.exe - gpupdate /force
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>gpupdate /force
Updating Policy...

_
```

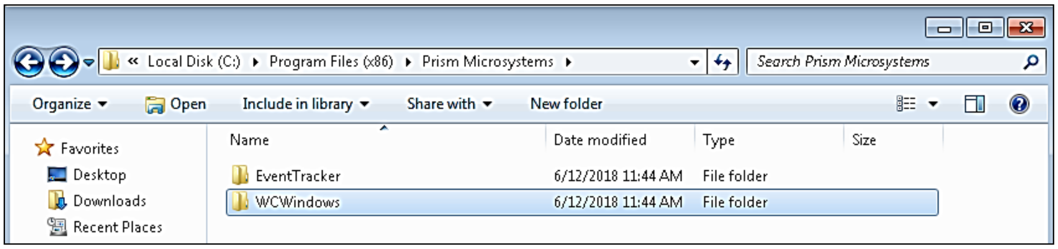
Note:

Netsurion's Open XDR platform and Change Audit sensors will be installed once the target machines are restarted.

Note:

If Agent.ini and etaconfig.ini files are present in same folder, and the CUSTOMCONFIG=2 in the Agent.ini file, then configuration will be deployed from etaconfig.ini file.

Once the gpo is updated, you can verify the folder structure in the target machine as shown below:



Name	Date modified	Type	Size
EventTracker	6/12/2018 11:44 AM	File folder	
WCWindows	6/12/2018 11:44 AM	File folder	

5.6 Verify Installation

Events will be sent to the target systems (that is, "Manager" systems) upon successful deployment of Netsurion/ Change Audit sensors. The name of the deployed sensor along with their version number will appear in the System manager screen. On the target systems, the following events will be generated in System Event Log.

On Windows Operating Systems

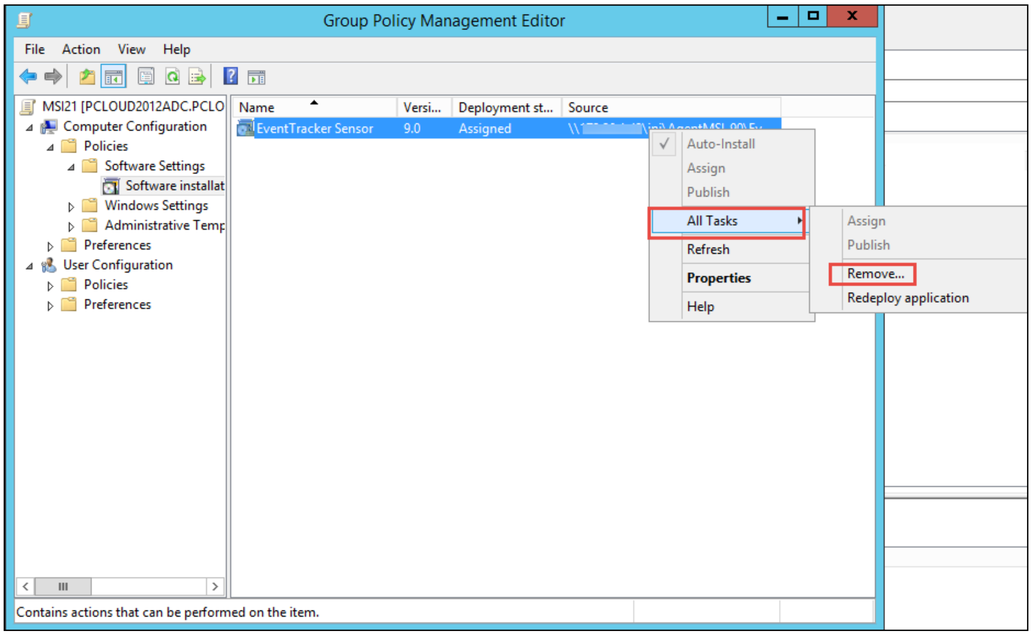
On Successful sensor Deployment the following are the sample Event ID and Description.

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

5.7 Uninstalling Netsurion's Open XDR sensor via GPO

1. Edit the linked Group Policy Object (that is, AgentMSI_93) and navigate to **Policies** > **Software Settings** > **Software Installation** and then select **msi**.

2. Then, right-click **msi** and click **All Tasks** > **Remove**.

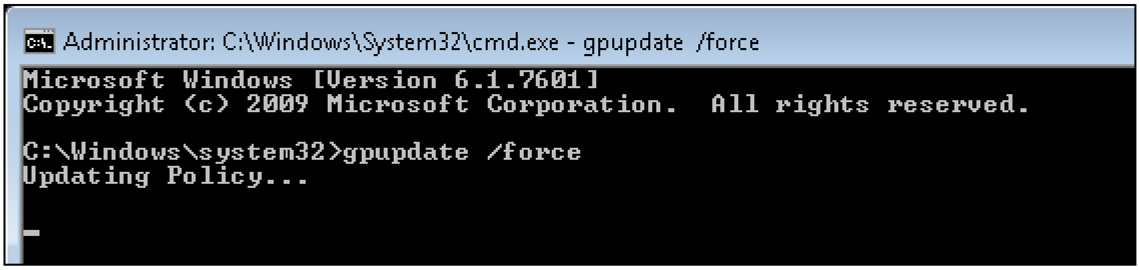


Name	Versi...	Deployment st...	Source
EventTracker Sensor	9.0	Assigned	\\[redacted]\ini\AgentMSI_90\Ev...

Contains actions that can be performed on the item.

Now, the user can go to the target machine and update the Group policy by specifying the following command in the Command prompt and it gets successfully uninstalled.

Command: `gpupdate /force`



Administrator: C:\Windows\System32\cmd.exe - gpupdate /force

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>gpupdate /force
Updating Policy...

_
```

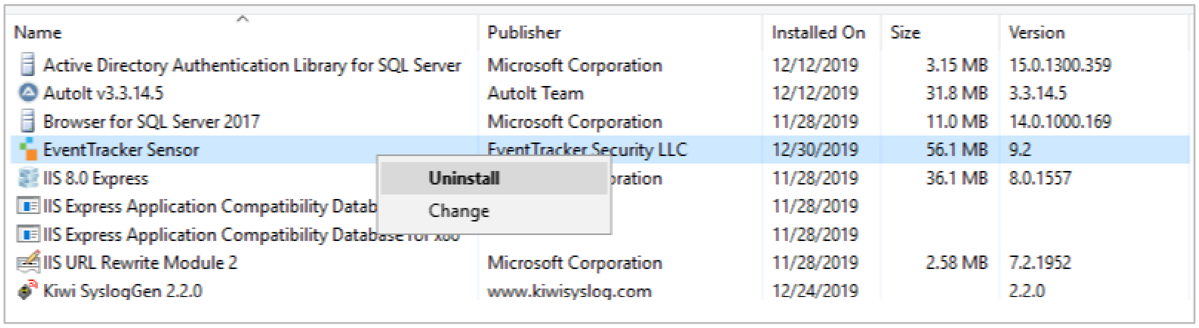
5.8 Limitation for Group Policy Installation

- Retain configuration does not work via Group policy.
- Upgrade sensors is not supported via Group policy.
- Modification features are not supported via Group policy.
- Command line or Silent installation does not support retain, upgrade, and modify functions.
- 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 the Netsurion's Open XDR sensor manager.
- While uninstalling, both Netsurion's Open XDR and Change Audit sensor will be uninstalled.
- GPO: shortcut value in Agent.ini must be kept as "One" in case the user wants to uninstall sensor from individual systems.
- GPO: In case the user wants to uninstall sensor from all the systems using GPO uninstall option, then the shortcut value in Agent.ini need not be changed.

6 Uninstallation of the Netsurion sensor via Control Panel

1. Go to **Control Panel** > **Program & Features**.

2. Right-click **Netsurion's Open XDR sensor** and click **Uninstall**.



Name	Publisher	Installed On	Size	Version
Active Directory Authentication Library for SQL Server	Microsoft Corporation	12/12/2019	3.15 MB	15.0.1300.359
AutoIt v3.3.14.5	AutoIt Team	12/12/2019	31.8 MB	3.3.14.5
Browser for SQL Server 2017	Microsoft Corporation	11/28/2019	11.0 MB	14.0.1000.169
EventTracker Sensor	EventTracker Security LLC	12/30/2019	56.1 MB	9.2
IIS 8.0 Express	ration	11/28/2019	36.1 MB	8.0.1557
IIS Express Application Compatibility Datab		11/28/2019		
IIS Express Application Compatibility Database for x86		11/28/2019		
IIS URL Rewrite Module 2	Microsoft Corporation	11/28/2019	2.58 MB	7.2.1952
Kiwi SyslogGen 2.2.0	www.kiwisyslog.com	12/24/2019		2.2.0

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 EventTracker sensor has been uninstalled from this system.

`Name`: EventTracker sensor

`Agent Type`: EventTracker sensor and Change Audit

`Agent Version:` 9.3

`User Name`: NTPL\ Karen

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that 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 and Response (MDR) and a Top 25 Global MSSP. Learn more at netsurion.com.

Contact Us

Corporate Headquarters

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

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support