



**Installation Guide**

# **Netsurion Open XDR 9.4**

**Publication Date**

September 22, 2023

## Abstract

This guide facilitates the procedures to install and configure Netsurion Open XDR 9.4 and helps to verify the expected functionality of all its components.

Netsurion Open XDR is a reliable, policy-driven SIEM solution that further monitors and manages critical events generated by Windows Operating System, Solaris BSM, Unix (SYSLOG), SYSLOG-NG and SNMP devices. Netsurion Open XDR is an Enterprise-Grade solution for managing IT security, log management, and auditing user activity that provides real-time alerts, secure warehousing, and flexible reporting.

**Note:**

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

## Audience

This guide is for Netsurion Open XDR users and Network/ System administrators responsible for installing and configuring Netsurion Open XDR 9.4.

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>System Requirements</b>	<b>5</b>
2.1	Hardware Requirements	5
2.2	Software Requirements	6
<b>3</b>	<b>Installing Netsurion Open XDR</b>	<b>7</b>
3.1	Pre-installing Instructions for Local Account and Active Directory Authentication	7
3.2	Installing the Netsurion Open XDR Manager	8
3.3	Pre-install Checklist for the Netsurion Open XDR Manager	8
3.3.1	IIS Settings	9
3.3.2	User Permission on SQL Server	9
3.4	Installing the Netsurion Open XDR Manager - Custom	10
3.4.1	Netsurion Open XDR Preinstall Check	12
3.4.2	The Netsurion Open XDR 9.4 Setup Wizard	23
3.4.3	Configuring Netsurion Open XDR 9.4	34
3.5	Installing the Netsurion Open XDR Manager – Standard or Collection Point Evaluation Version	35
<b>4</b>	<b>Deploying the Netsurion Open XDR Windows Sensor</b>	<b>37</b>
4.1	Pre-install Instructions for Windows Sensor	37
4.2	Pre-install checklist for Windows Sensor	38
4.3	Different methods to install the Netsurion Open XDR Sensors	38
4.4	Deploying the Netsurion Open XDR Windows Sensor via System Manager for Sensor Based Systems (full featured)	39
4.5	Configuring the Netsurion Open XDR Windows Sensors	47
4.6	Configuring Sensor-less collection via System Manager (limited features)	48
4.7	Deploying the Netsurion Open XDR Windows Sensor - Microsoft Windows 10 and above	54
4.7.1	Prerequisites for Windows Sensor – Microsoft Windows 10 and above	54
4.7.2	Installing / Uninstalling Microsoft Windows 10 and above Sensor	55
<b>5</b>	<b>Sensor Deployment</b>	<b>55</b>
<b>6</b>	<b>Securing Netsurion Open XDR</b>	<b>55</b>
<b>7</b>	<b>Uninstalling the Netsurion Open XDR Windows Sensor</b>	<b>55</b>
7.1	Uninstalling via Control Panel	55
7.2	Uninstalling via System Manager	56
<b>8</b>	<b>Uninstalling Netsurion Open XDR</b>	<b>59</b>

<b>9</b>	<b>Ports in Netsurion Open XDR.....</b>	<b>60</b>
<b>10</b>	<b>URL or Domain Accessed by Netsurion Open XDR.....</b>	<b>61</b>
<b>11</b>	<b>Troubleshooting .....</b>	<b>62</b>
11.1	Known Issues while installing Netsurion Open XDR 9.4 .....	62
11.2	Frequently Asked Questions.....	63

# 1 Introduction

Today, the concern for security has rapidly increased among leading-edge entities and requires technology-driven, tenable solutions to work in a secure environment. Netsurion Open XDR, our Managed Threat Protection platform, efficiently conducts vulnerabilities, prevents malware attacks, detects skeptical behavior, and promptly acknowledges suspicious anomalies. This installation guide helps you to install our product effortlessly.

To familiarize with the various product features, follow our web site, [Threat Protection Platform](#) in the brochure of this package.

# 2 System Requirements

For optimal performance, the following are the hardware and software requirements to host **Netsurion Open XDR**.

**Note**

Ensure the update of the latest service packs of all Microsoft Windows.

## 2.1 Hardware Requirements

The **minimum hardware configuration** required to install and smoothly run Netsurion Open XDR.

**IMPORTANT**

Netsurion Open XDR 9.4 installation is supported on 64-bit Operating System only.

<b>CPU</b>		2.80 GHz and above, 8 Core or equivalent
<b>RAM</b>		16GB
<b>HDD</b>	<b>SSD</b>	200 GB for application and search cache
	<b>Non - SSD</b>	100 GB for storing archives (varies as per data retention needs)

**Note**

Recommended to have two Partitions in Disk 1 (SSD); Partition 1 for Operating System and Partition 2 for Netsurion Open XDR and search cache. The Archives are stored in a NON-SSD disk (for example, Disk 2).

## 2.2 Software Requirements

### ❖ The Netsurion Open XDR console

Microsoft Windows Platforms	64-bit
Server 2022	Supported
Server 2019	Supported

SQL server	64-bit
SQL Server 2019	Supported

#### Console Components

- Microsoft .NET Framework 4.8 and above.
- Elastic Search 7.10.2.
- Update of the latest service packs of all Microsoft Windows.

### ❖ The Netsurion Open XDR sensor

Microsoft Windows Platforms	32-bit	64-bit
Server 2022	Not Applicable	Supported
Server 2019	Not Applicable	Supported
Server 2016	Not Applicable	Supported
Server 2012 R2	Not Applicable	Supported
Windows 11	Not Applicable	Supported
Windows 10	Supported	Supported

#### Sensor Components

- Microsoft .NET Framework 3.5 and above.

#### Note:

Versions other than those listed above are not supported.

## ❖ Web Browsers:

- Microsoft Edge Browser latest.
- Firefox Browser latest.
- Google Chrome latest.

### Note:

Installing **Elasticsearch 7.10.2** will automatically install the compatible OpenJDK version 15.0.1. **TLS-1.2** should be enabled for Netsurion Open XDR 9.4 Installation and all other protocols must be disabled.

### Note:

Recommended not to install Netsurion Open XDR on a Domain Controller and to run the Netsurion Open XDR console on a dedicated Microsoft Windows Server.

## 3 Installing Netsurion Open XDR

### 3.1 Pre-installing Instructions for Local Account and Active Directory Authentication

Netsurion Open XDR users will be authenticated locally or against the Microsoft Windows Active Directory. You can also configure the same via Netsurion Open XDR pre-installer and this entire process is automated.

### Note:

To configure via Pre-Installer, refer to [Procedure to Install the Netsurion Open XDR Manager](#) and to configure manually, refer to [How To Create Local Account And Active Directory Authentication](#) guide to create Local User or Active Directory User and Group Accounts.

### IMPORTANT

Recommended users to refer the [Install and Customize IIS Web Server v9x guide](#) prior installing Netsurion Open XDR 9.4.

### 3.2 Installing the Netsurion Open XDR Manager

Run Netsurion Open XDR 9.4 installation package. During the installation, the application prompts to provide the path of the digital certificate. The certificate is validated against the latest CRL. Installation proceeds only if the certificate is found to be valid.

**Note:**

The installation procedure is identical for all Operating System(s).

### 3.3 Pre-install Checklist for the Netsurion Open XDR Manager

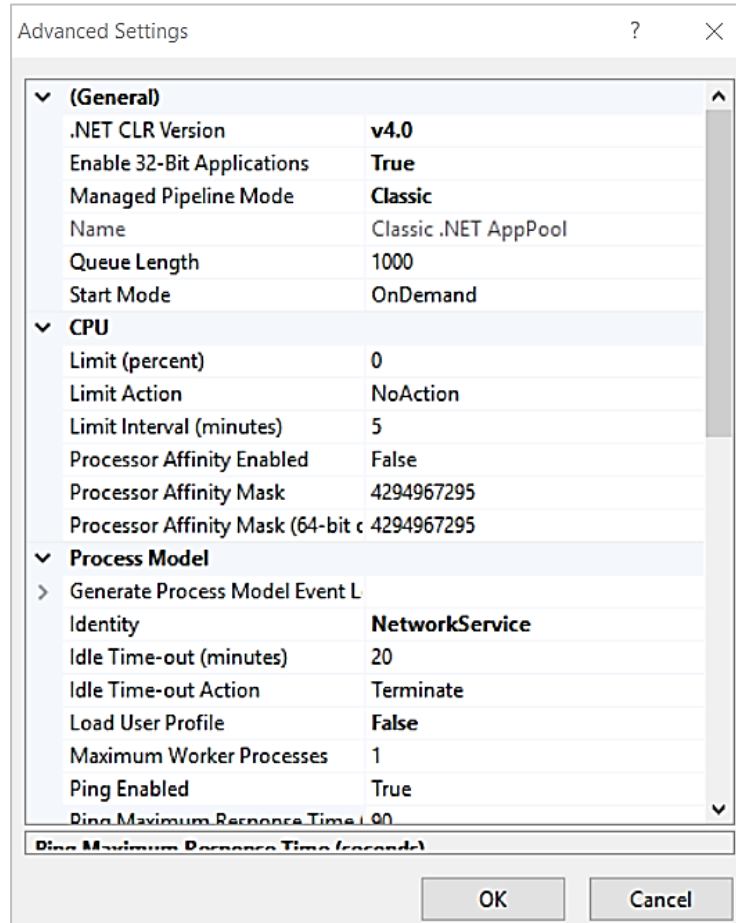
The pre-install checklist describes the specific settings, permissions, and privileges that are required for installing the Netsurion Open XDR Manager. Read the checklist before installing the application to avoid installation failure.

<b>ENSURE</b>	The update of the latest service packs of all Microsoft Windows.
	User is a member of the 'Local Administrators' group
	MSI package installation is allowed
	User has 'Logon As Service' rights
	User has 'Logon As Batch job' rights
	Network Discovery is enabled
	<b>System cryptography:</b> Use of FIPS 140 compliant cryptographic algorithms, with encryption, and hashing and signing algorithms disabled.
<b>VERIFY IF</b>	The user has permission on 'Application install directory' (Folders and sub folders).
	The user has created the service permission on the target system (SCM- Service Control Manager).
	The user has Read/Write permission on the Microsoft Windows registry.



### 3.3.1 IIS Settings

For the Microsoft Windows Operating System, ensure to configure the IIS Settings details in the Application Pools as follows.



**Note:**

For details to configure the above settings, refer to [Install and Customize IIS Web Server Guide](#).

### 3.3.2 User Permission on SQL Server

Users installing Netsurion Open XDR must have sysadmin privilege on the respective SQL Server 2019.

- In the SQL Server 2019, verify that the sysadmin privilege has been granted to **NT AUTHORITY\SYSTEM**.
- If the SQL Server 2019 is used by the customer, then the SQL service in the service control manager must be changed from **'NT Service\MSSQL\$SQLEXPRESS'** to **'Network Service'**.

### 3.4 Installing the Netsurion Open XDR Manager - Custom

Perform the following procedure to install Netsurion Open XDR. If you are launching Netsurion Open XDR for the first time, then run the executable program and proceed.

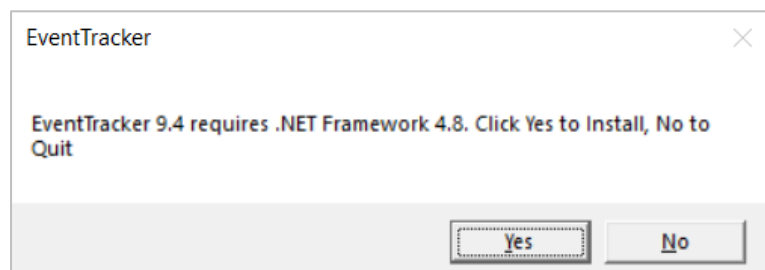
**Note:**

If the previous version of the Netsurion Open XDR is already installed, refer the [Upgrade Guide](#) for detailed instructions.

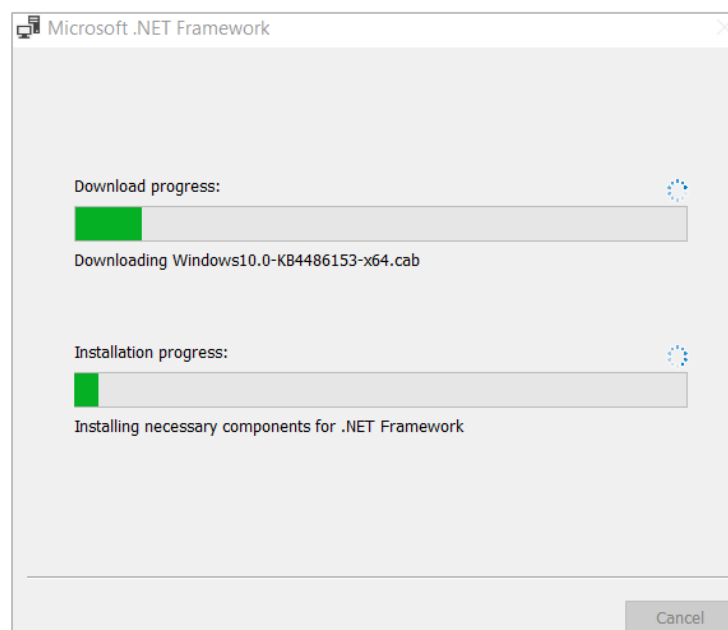
1. Run the Netsurion Open XDR 9.4 set-up file via **Run as Administrator**.
2. Netsurion Open XDR prompts to install the .NET Framework 4.8 to proceed with the installation. Click **Yes** to install.

**Note:**

The .NET 4.8 is enabled by default for Microsoft Windows 2019/2022. If it is not available, Netsurion Open XDR verifies and installs in the Pre-install check window.

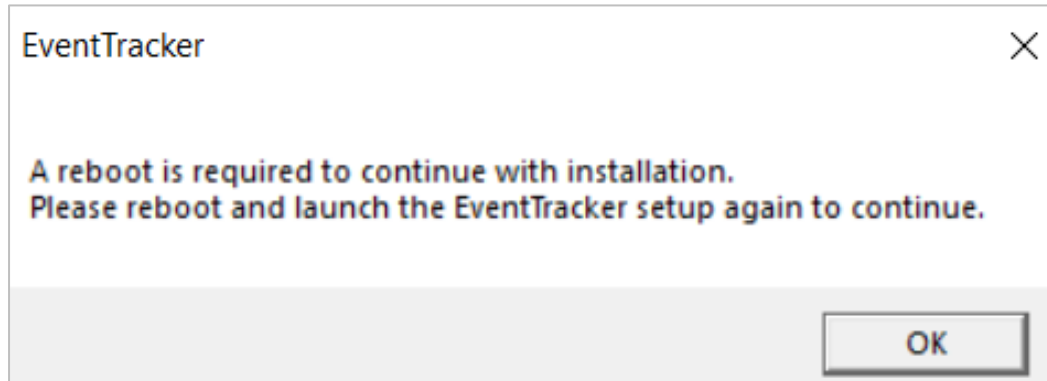


The following is the sample representation of the Microsoft .Net Framework Download and Installation progress details.

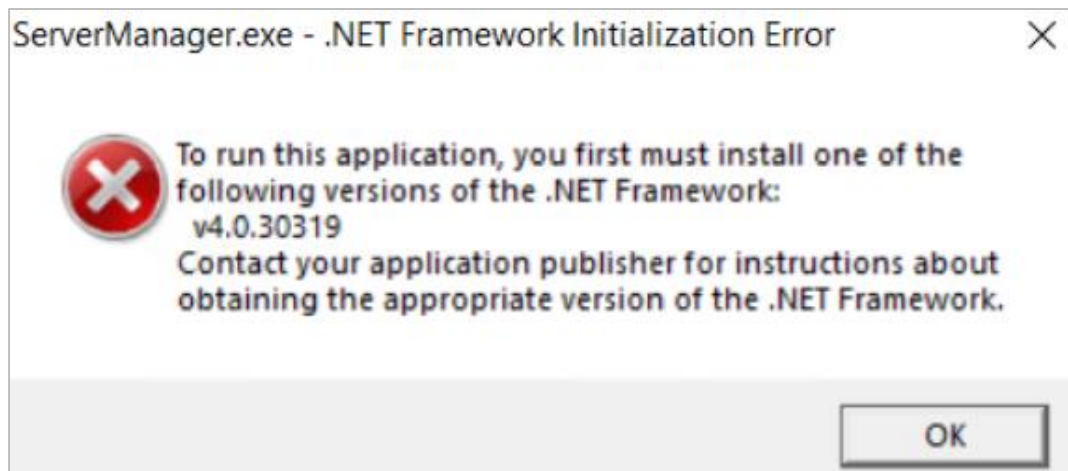


After the .net framework 4.8 installation is complete, Netsurion Open XDR pops-up a message window stating, **A reboot is required to continue with installation.**

3. Click **OK** to reboot and re-run Netsurion Open XDR setup.



4. After the reboot, it is required to re-run Netsurion Open XDR 9.4 set-up file via **Run as Administrator**. The following pop-up window appears, if the system does not contain the latest Windows updates.

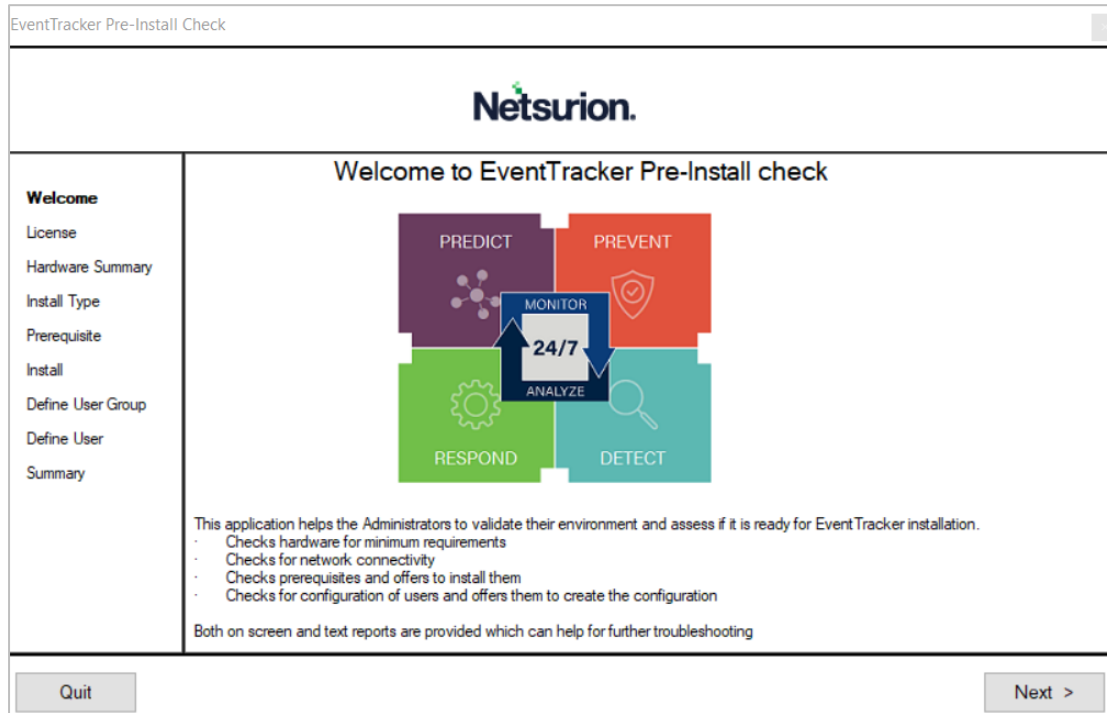


The Installation process involves the following procedures,

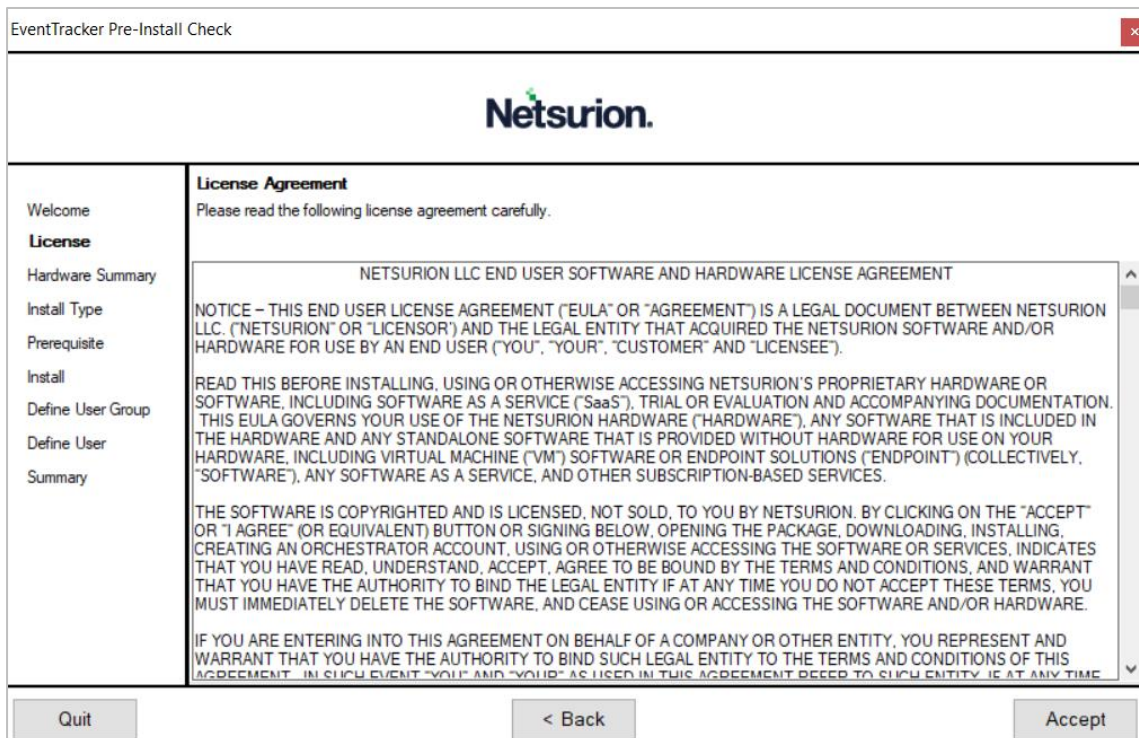
- ❖ [Preinstallation checks](#)
- ❖ [Netsurion Open XDR 9.4 Setup Program](#)
- ❖ [Configuring Netsurion Open XDR 9.4](#)

### 3.4.1 Netsurion Open XDR Preinstall Check

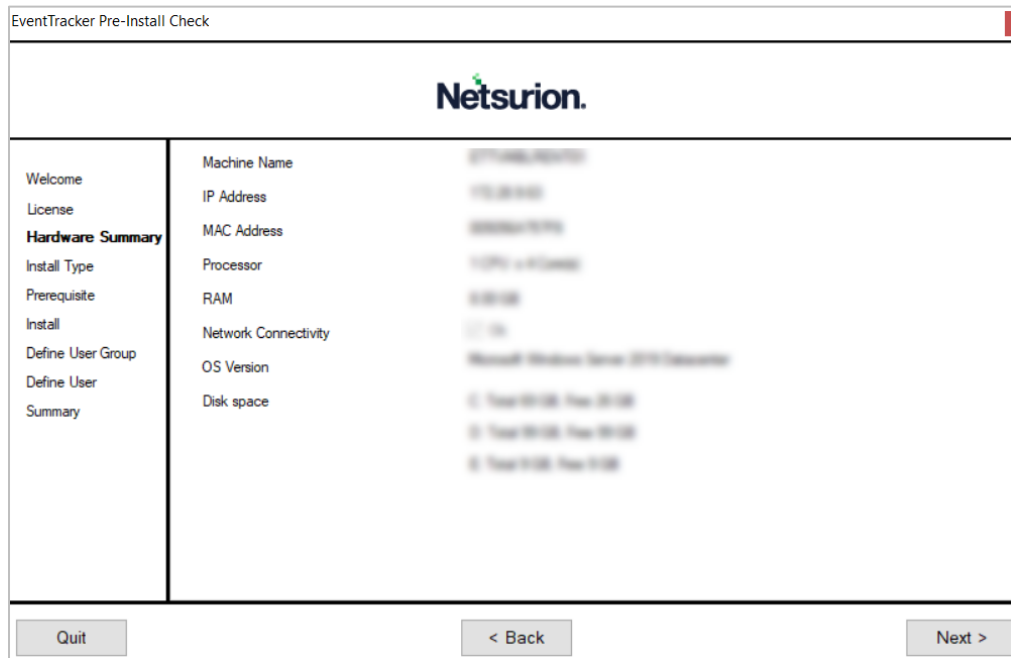
1. The Netsurion Open XDR console launches the Pre-Install Check window. Click **Next** to continue with the process.



2. In the **License** section, (read the agreement,) click **Accept** to acknowledge and proceed with the process.



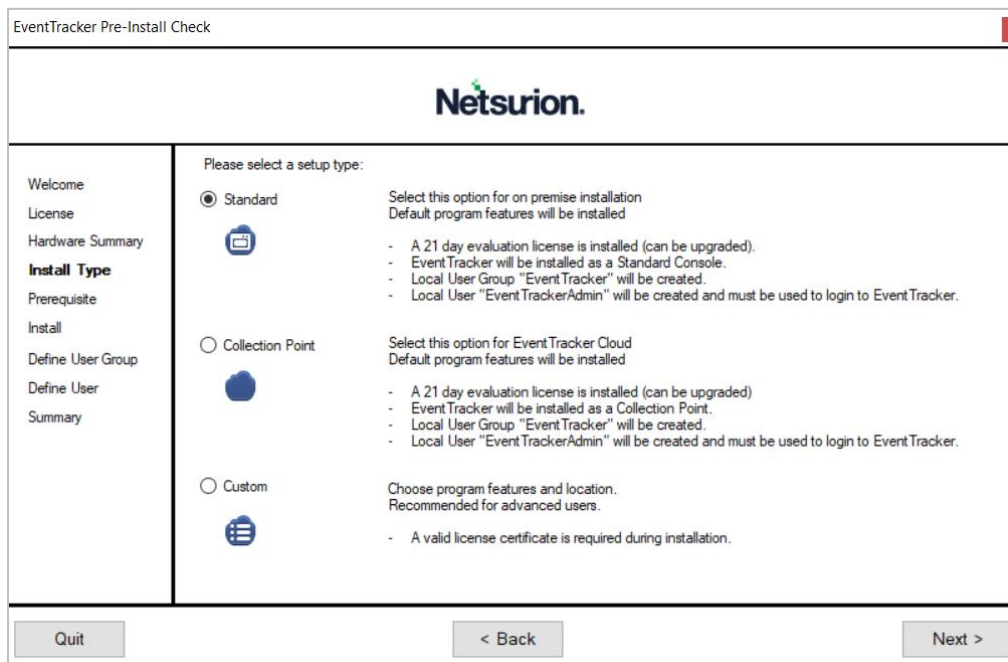
- In the **Hardware Summary** section, it may take a few seconds to fetch the hardware details and a processing icon appears during the data collection process. Click **Next** to proceed.



- In the **Install Type** section, choose the appropriate installation setup type from the listed options, **Standard** or **Collection Point** or **Custom**, and then click **Next**.

**Note:**

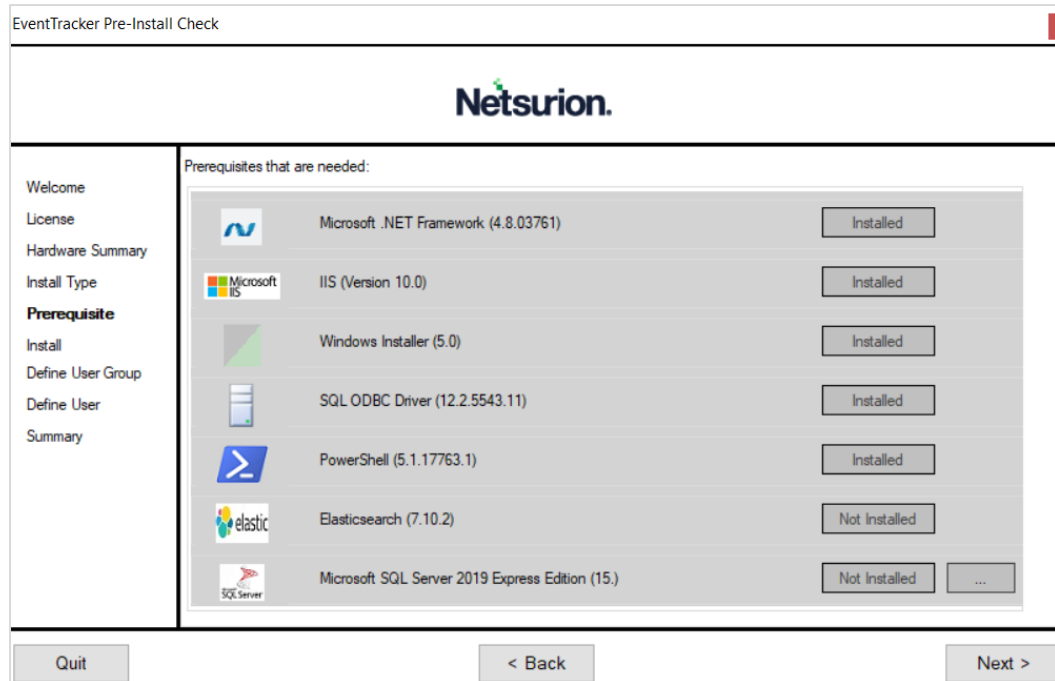
By default, the **Standard** option is selected and you may select the required option.




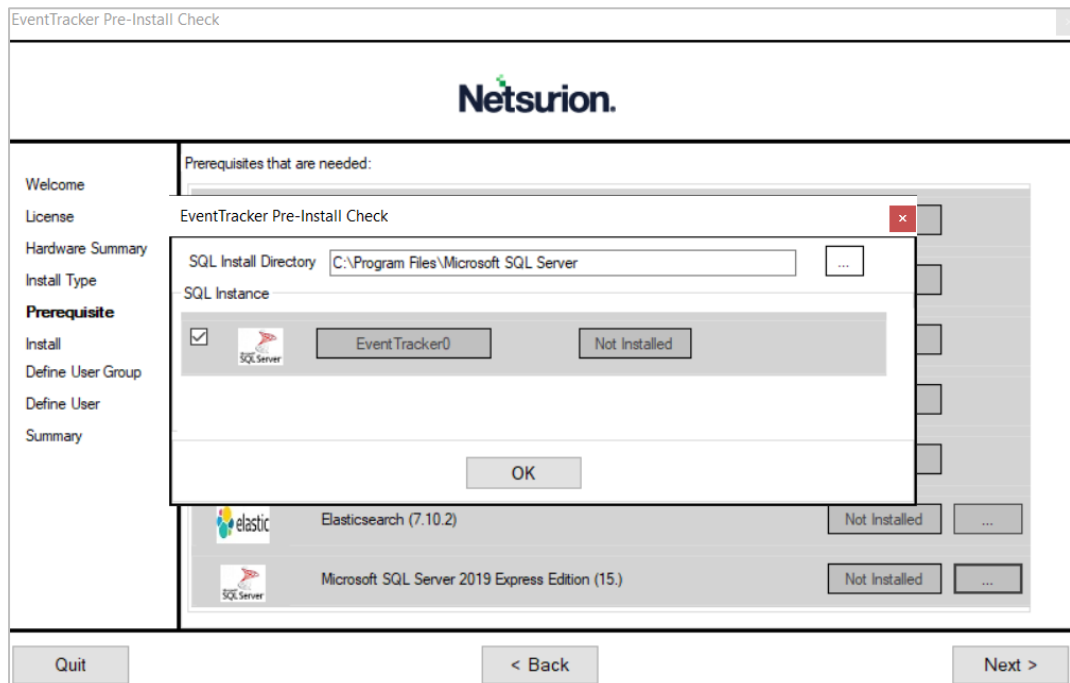
- In the **Prerequisite** section, click **Next** to proceed with the installation of the softwares that are not installed.

**Note:**

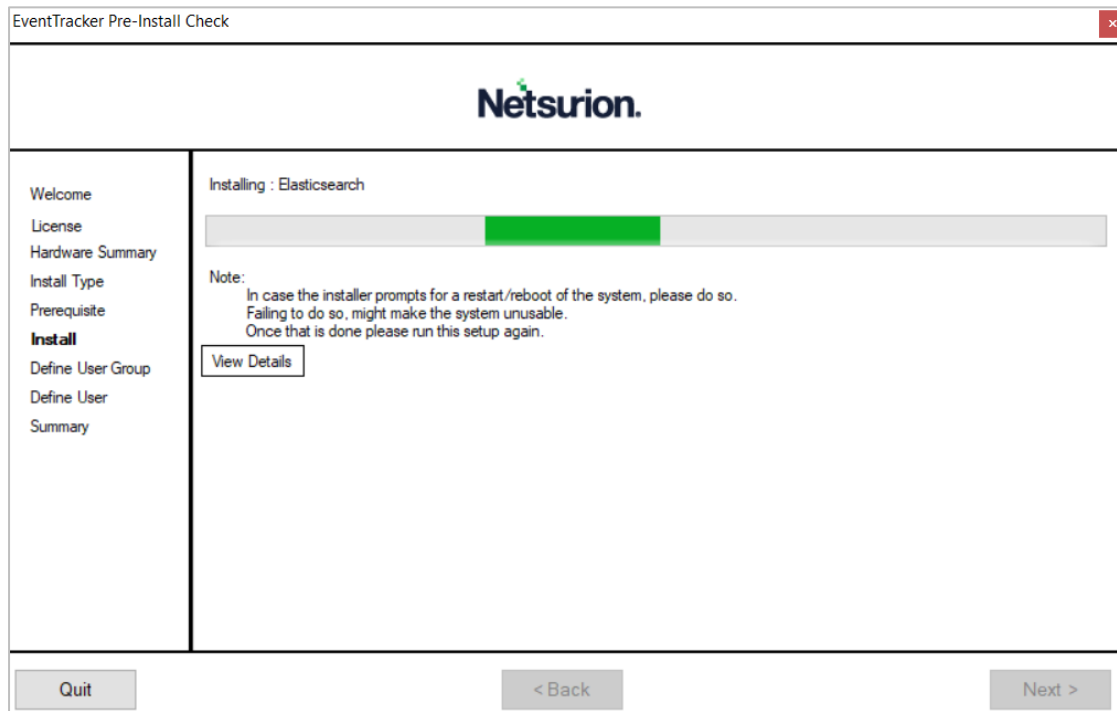
The **Prerequisite** section lists all of the required softwares, as well as their status (Installed or Not Installed) adjacent to it.



- If the SQL Server is running with multiple instances, click the **Browse**  button to select the appropriate instance.

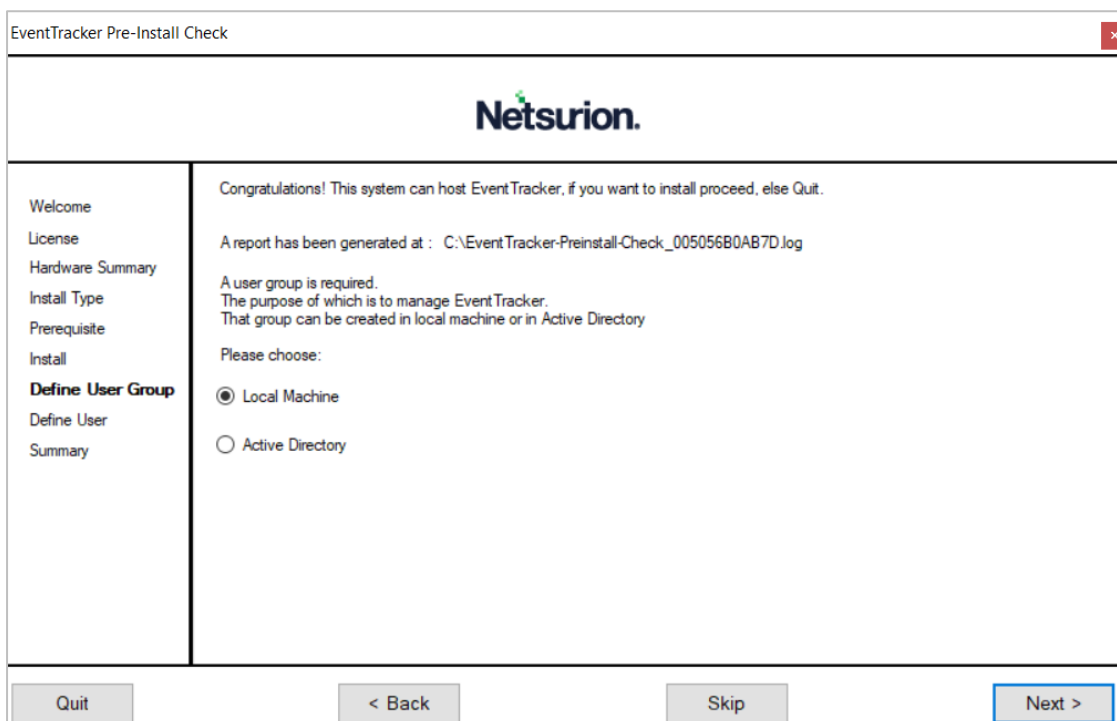


6. In the **Install** section,click **Next** to proceed with the installation of the requisite softwares.



7. In the **Define User Group** section, choose the required option to create a user group in local machine or in Active Directory, and then click **Next**.

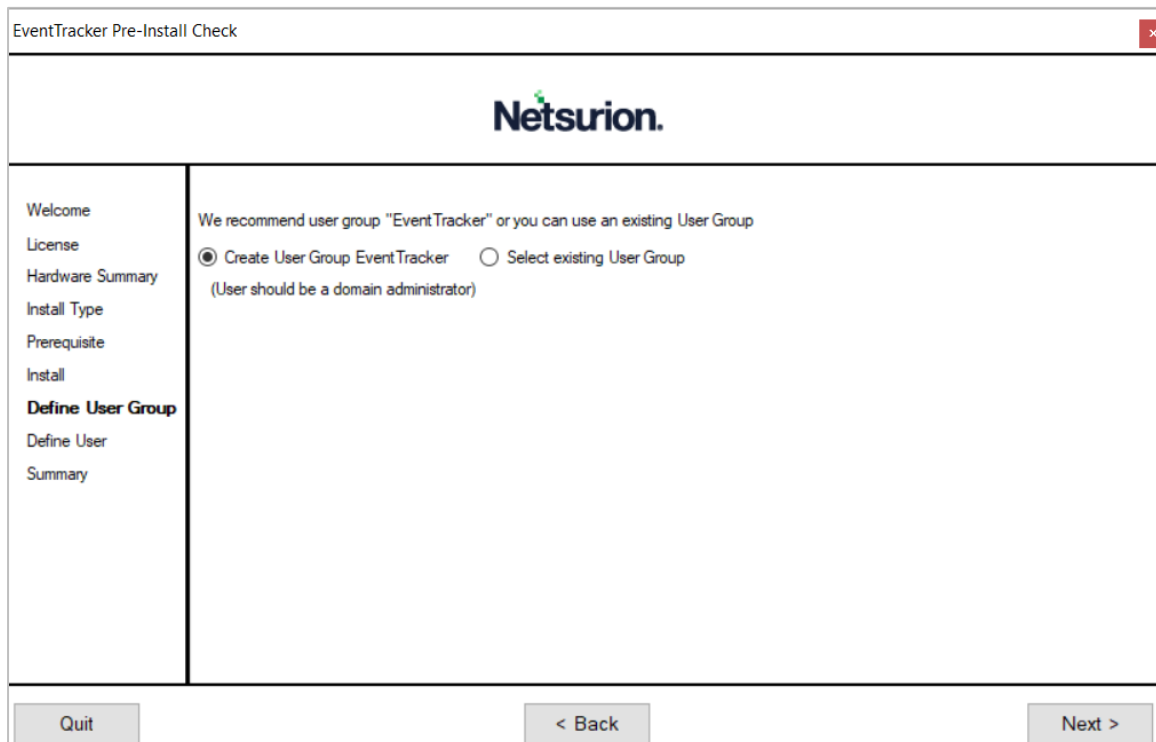
- [Creating a user group in Local Machine](#)
- [Creating a user group in Active Directory](#)



**Note:**

While creating a group and/or user, the user should be part of the administrator’s group in the local machine. The user should have “Logon as Batch’ and “Logon as Service’ rights granted.

- a. If choosing the **Local Machine** option, click **Next** and in the **You have selected to use local machine** window, choose either the [Create User Group EventTracker](#) or [Select existing User Group](#) option, and then click **Next**.



**Note:**

When creating a group, suggested to use the group name as **EventTracker**, though Netsurion Open XDR works with any group name. In case this group name does not exist then it is necessary choose the **Create User Group EventTracker** option else choose the **Select Existing** Group option.



- If choosing the **Create User Group EventTracker** option, then click **Next** and specify a unique name in **Group Name** field, and then click **Next**.

EventTracker Pre-Install Check

**Netsurion.**

Welcome

License

Hardware Summary

Install Type

Prerequisite

Install

**Define User Group**

Define User

Summary

Members of this User Group can access EventTracker

Group Name

- Otherwise, if choosing the **Select existing User Group** option, then select the required group name from the available list, and click **Next**.

EventTracker Pre-Install Check

**Netsurion.**

Welcome

License

Hardware Summary

Install Type

Prerequisite

Install

**Define User Group**

Define User

Summary

We recommend user group "Event Tracker" or you can use an existing User Group

Create User Group EventTracker
  Select existing User Group

(User should be a domain administrator)

Access Control Assistance Operators

Administrators

Backup Operators

Certificate Service DCOM Access

Cryptographic Operators

Device Owners

Distributed COM Users

Event Log Readers

Event Tracker

Guests

Hyper-V Administrators

IIS\_IUSRS

Network Configuration Operators

Performance Log Users

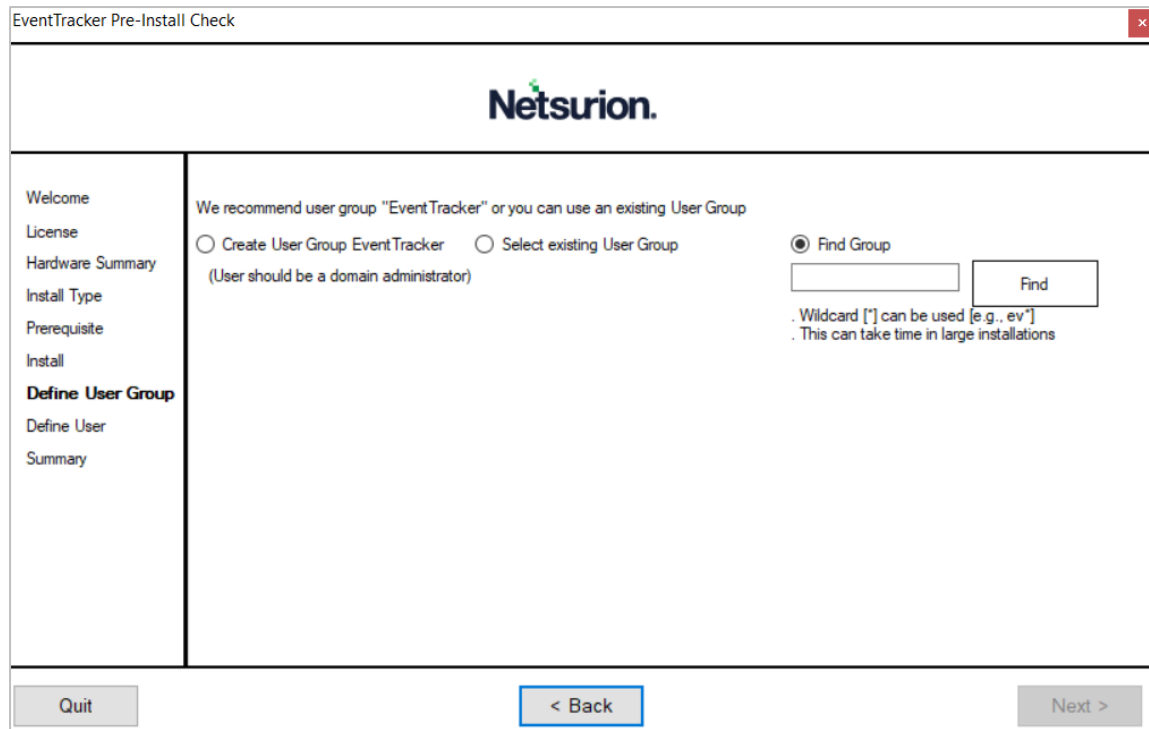
Performance Monitor Users

Power Users

- b. Alternatively, if choosing the **Active Directory** option, then click **Next** and in the **You have selected Active Directory domain** window, choose either [Create User Group EventTracker](#) or [Select existing User Group](#) option, and then click **Next**.

**Note:**

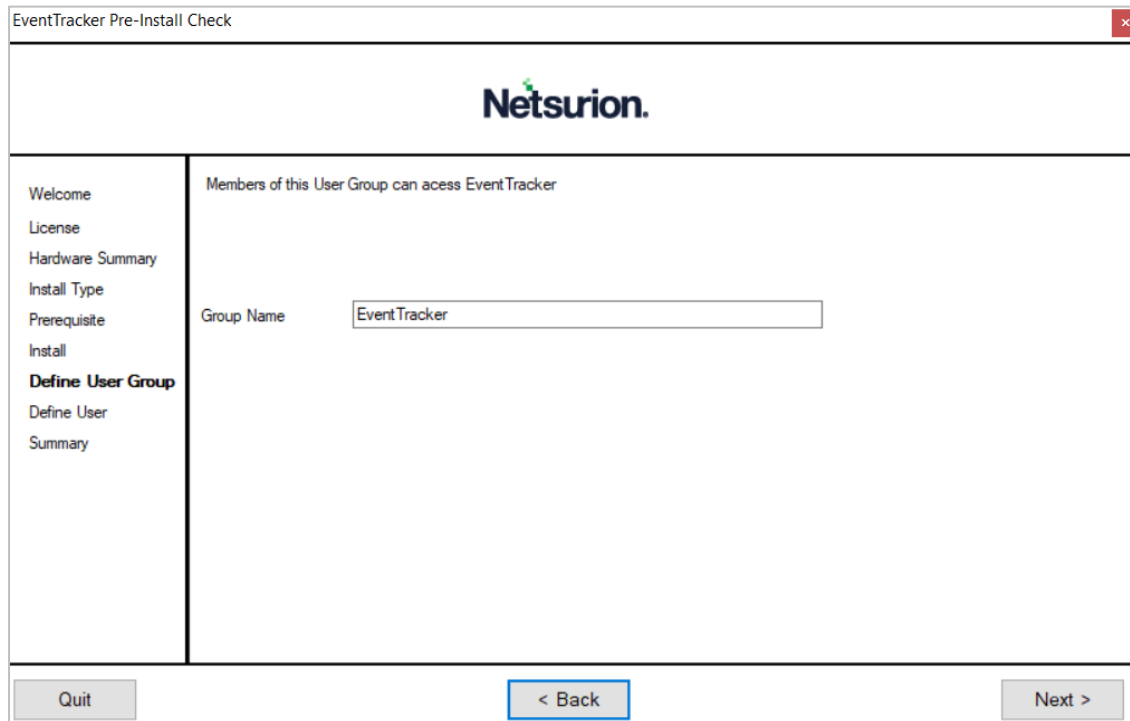
The administrator should have sufficient privileges on the active directory to create a user group.



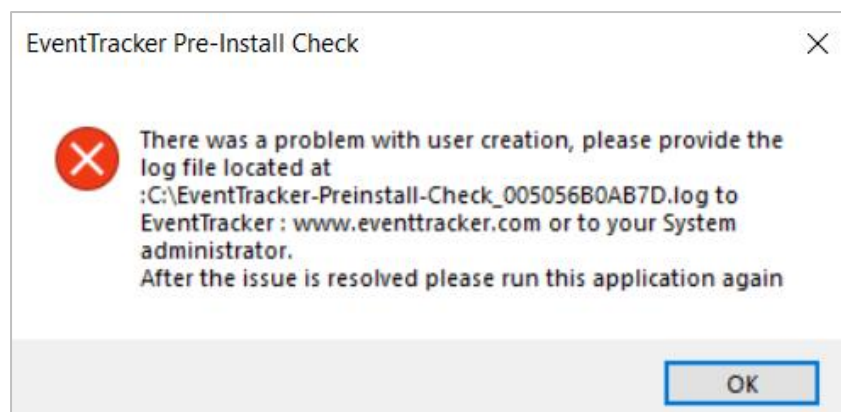
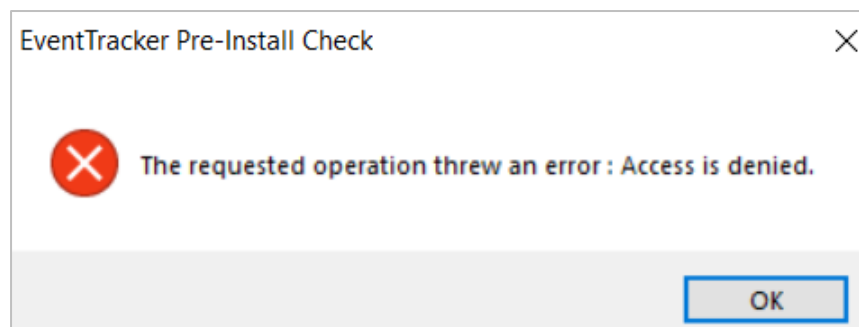
**Note:**

When creating a group, suggested to use the group name as **EventTracker**, though Netsurion Open XDR works with any group name. In case this group name does not exist then it is necessary to choose the **Create User Group EventTracker** option else choose the **Select Existing Group** option.

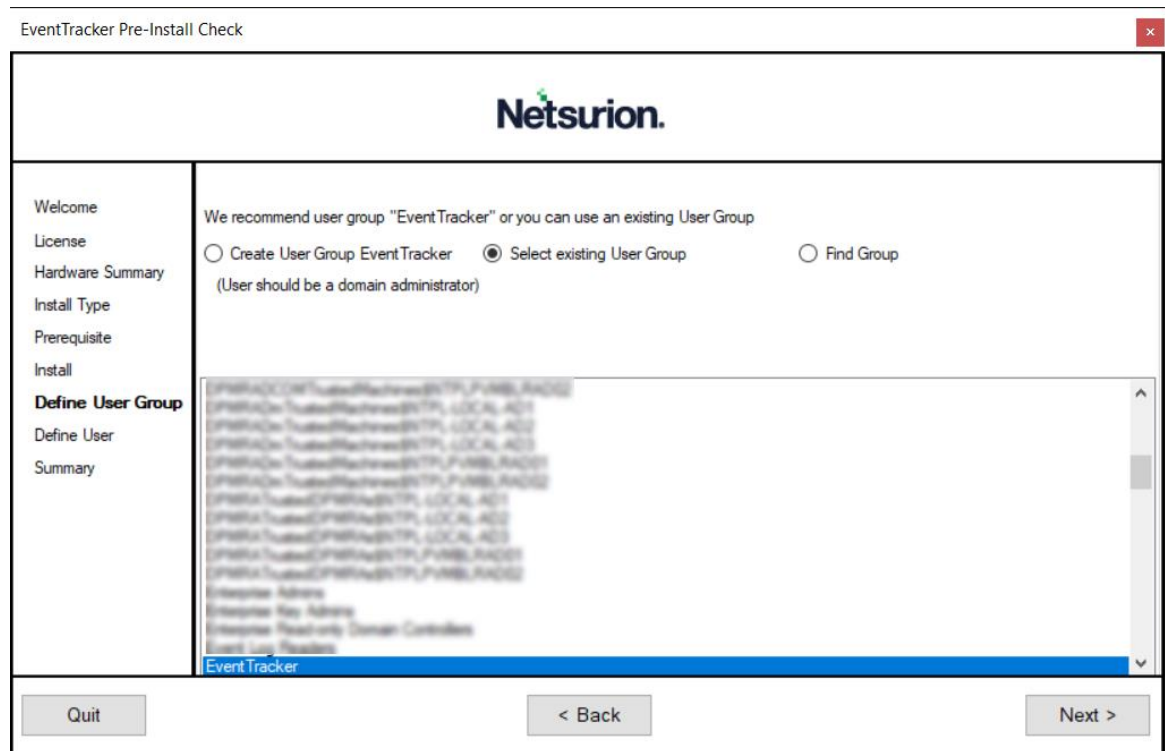
- If choosing the **Create User Group EventTracker** option, then click **Next** and specify a unique name in **Group Name** field, and then click **Next**.



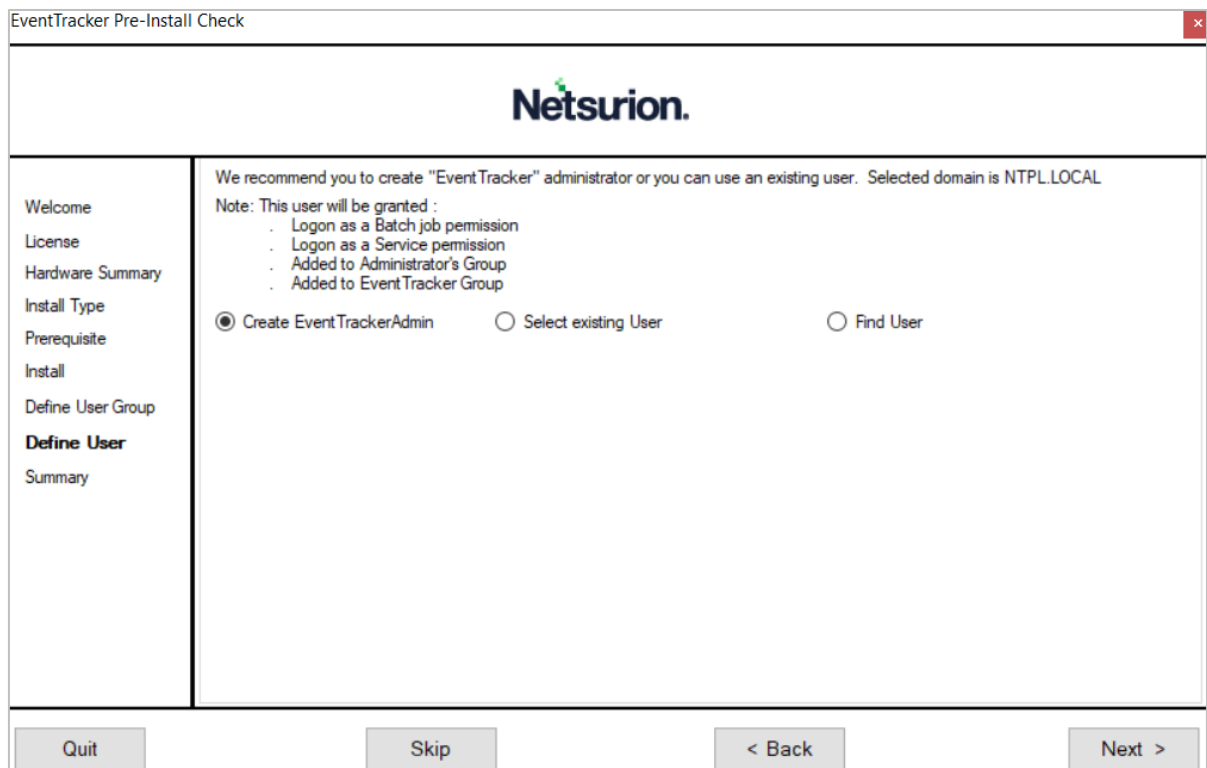
Contact the administrator if an error message occurs stating **Access Denied** as shown in the below image. This error occurs in the case if you do not have sufficient permissions to create a user group in the Active Directory.



- If choosing the **Select existing User Group** option, then select the required group name from the available list, and then click **Next**.

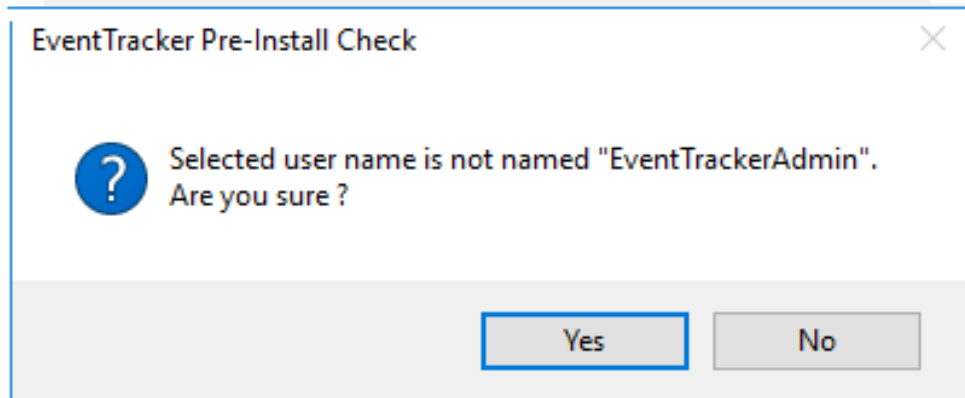


8. In the **Define User Group** section, choose either [Create EventTrackerAdmin](#) or [Select existing User](#) or [Find User](#) to find the user.



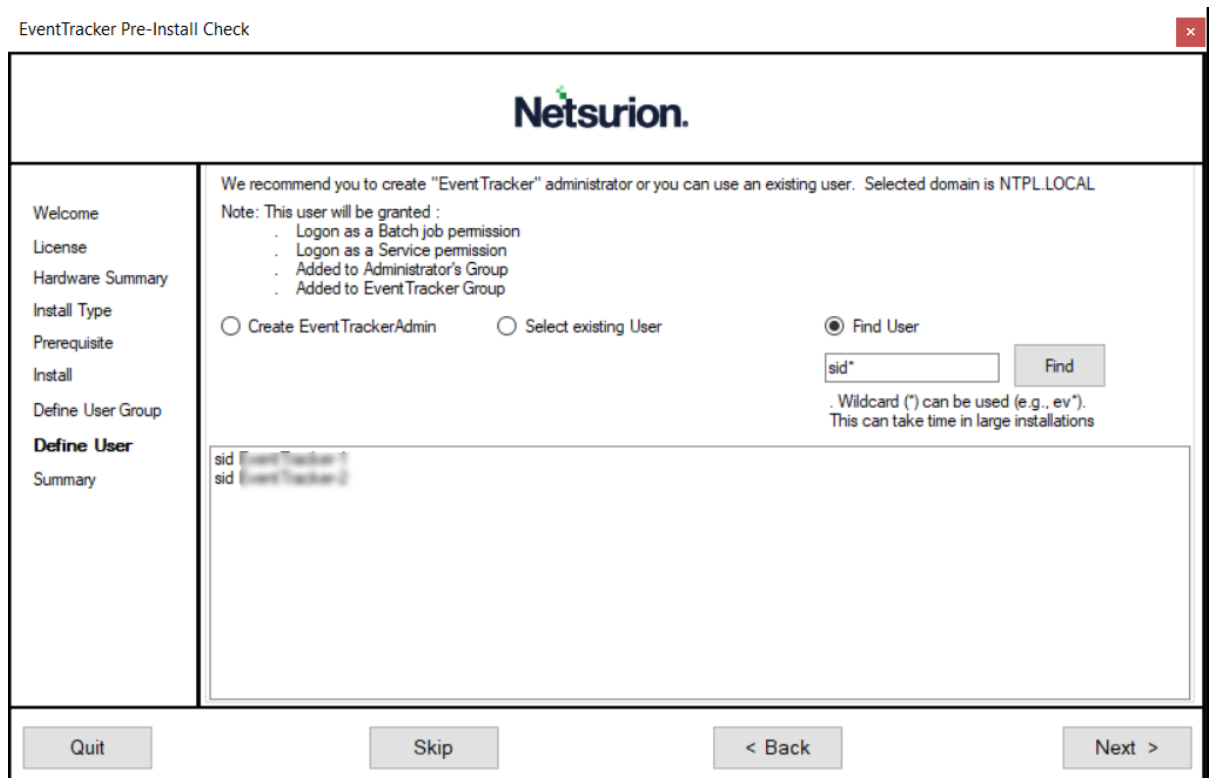


- The following message pops-up if the selected user name is not a EventTracker Administrator. Click **Yes** to proceed.



- If choosing the **Find User** option, then in the **text** field, provide the appropriate user name, and then click **Find**.

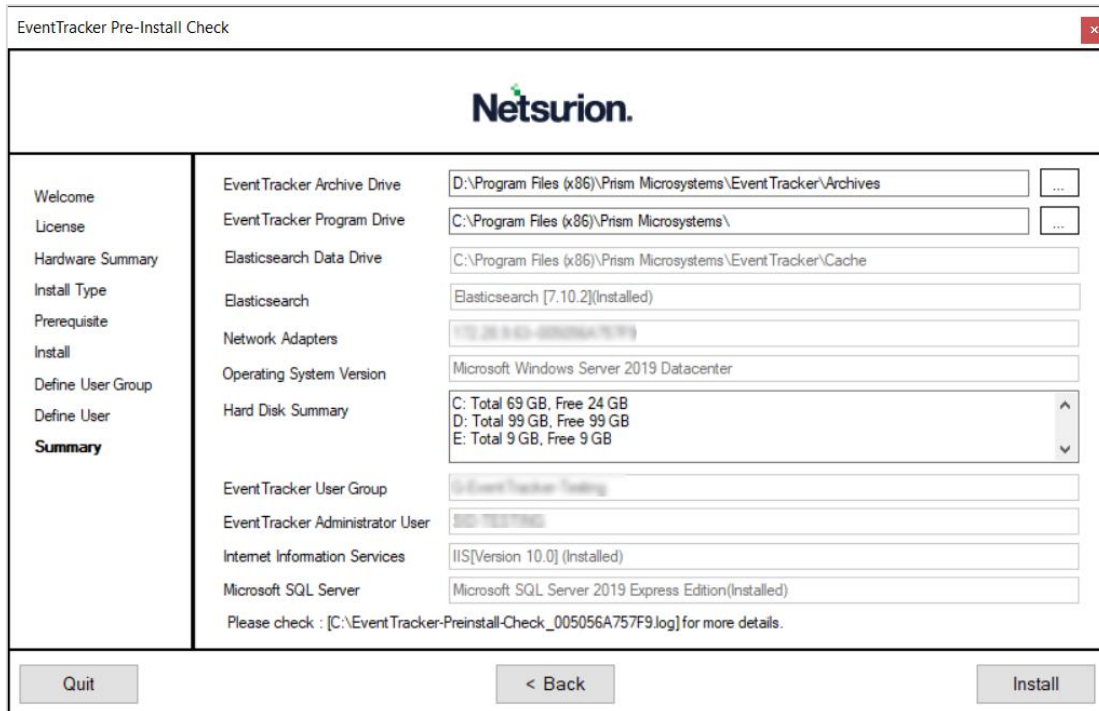
**Note:**  
A wildcard can also be entered.



- In the **Summary** section, verify all the details and click **Install** to proceed with the Installation process.

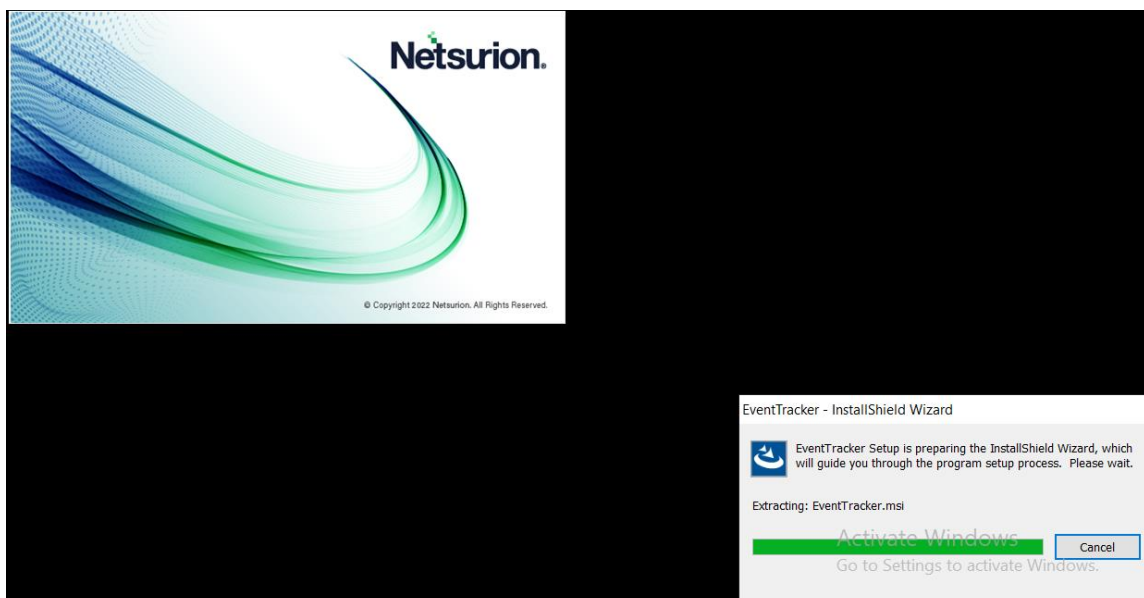
**Note:**

If required click the **Browse** button to modify the **EventTracker Archive Drive** or the **Program Drive** location.

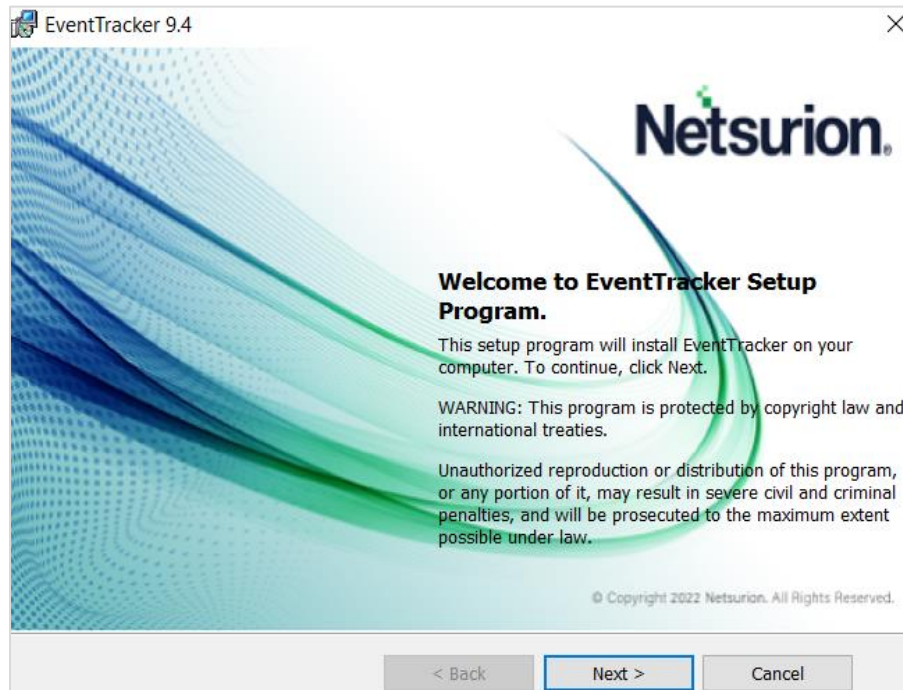


### 3.4.2 The Netsurion Open XDR 9.4 Setup Wizard

When Installing, Netsurion Open XDR displays the **EventTracker - InstallShield Wizard**.



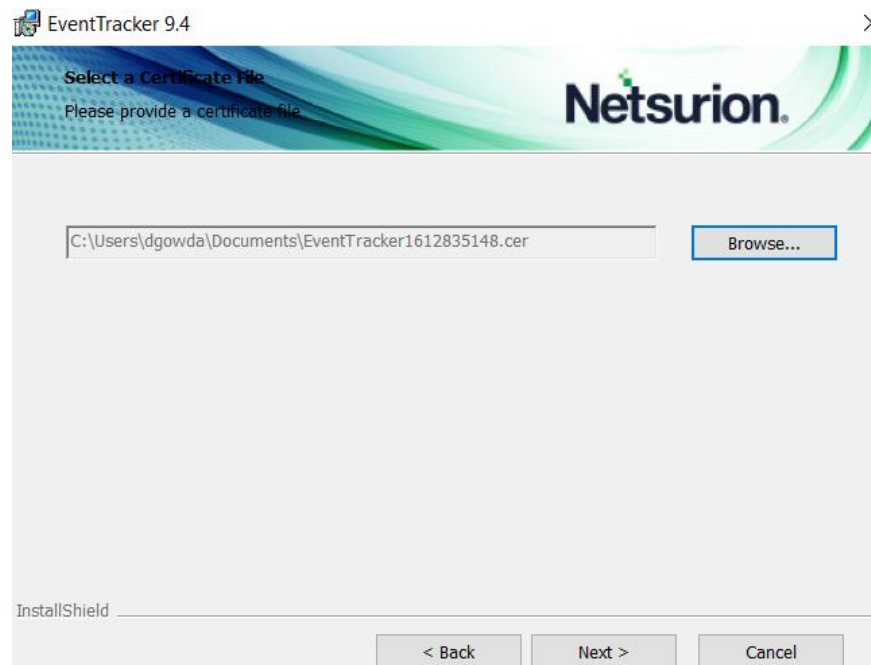
1. In EventTracker - InstallShield **Welcome** window, click **Next** to proceed with Netsurion Open XDR setup process.



2. In **Select a Certificate File** window, click **Browse** and locate the appropriate certificate file (the file with **.cer** extension), and then click **Next**.

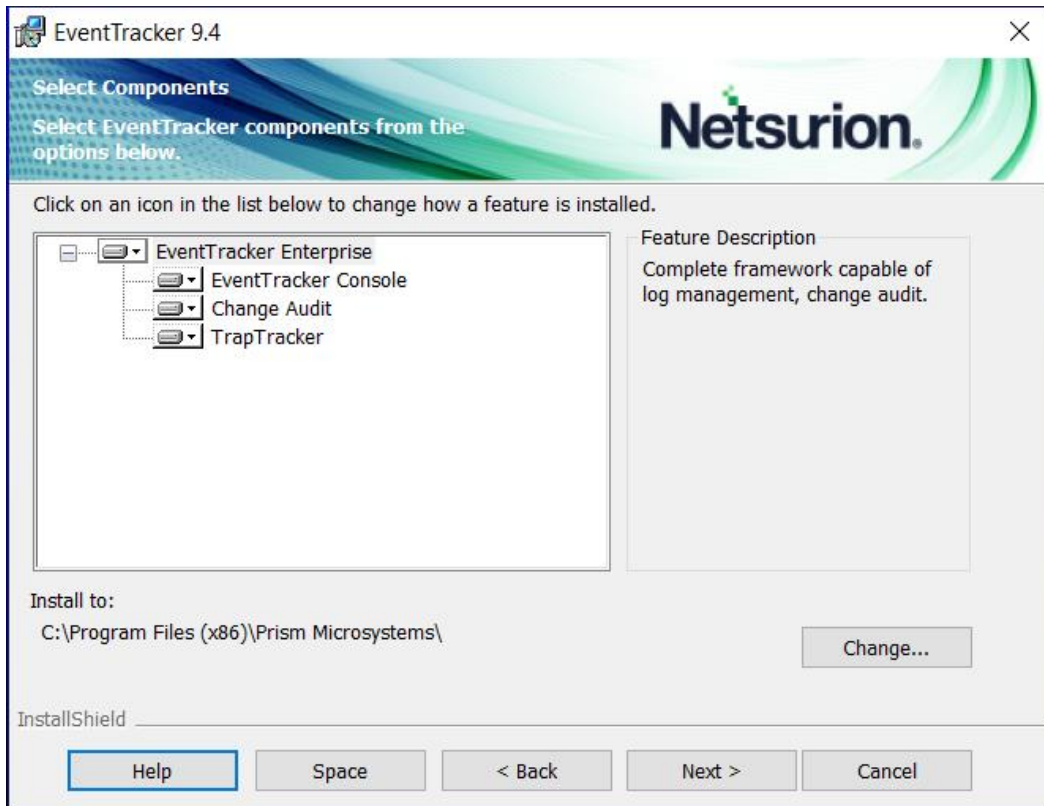
**Note:**

If the user has selected **Custom** option in EventTracker Pre Install Check, then the installer prompts to add the certificate file.

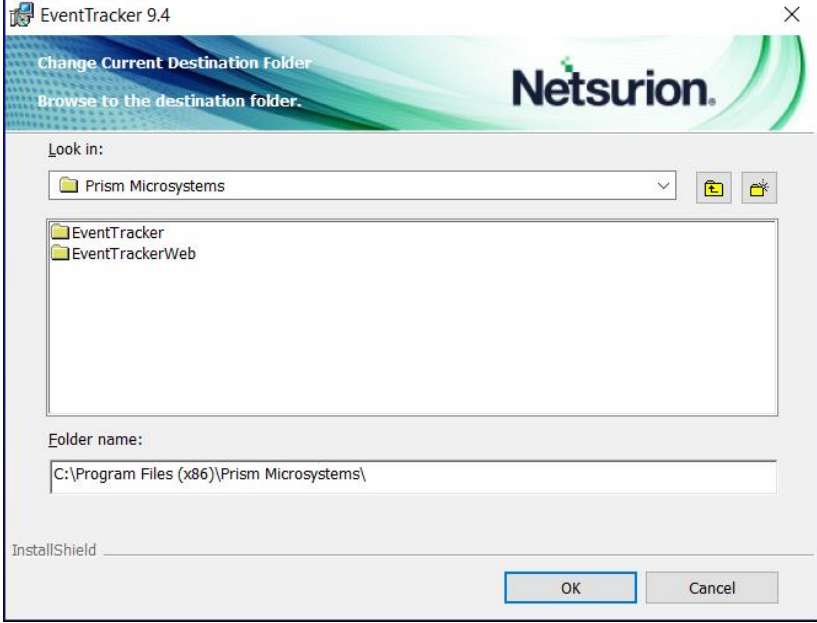
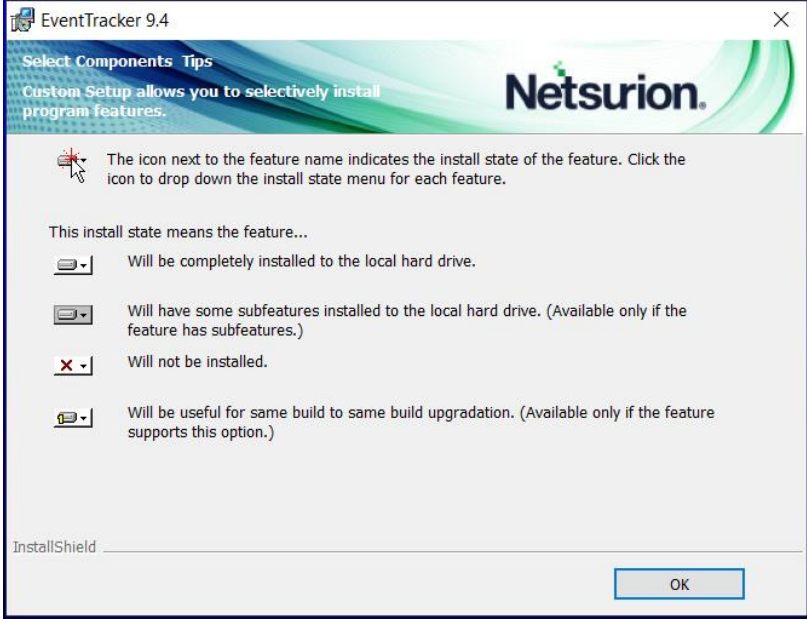




3. In **Select Components** window, select the required component details and click **Next**.

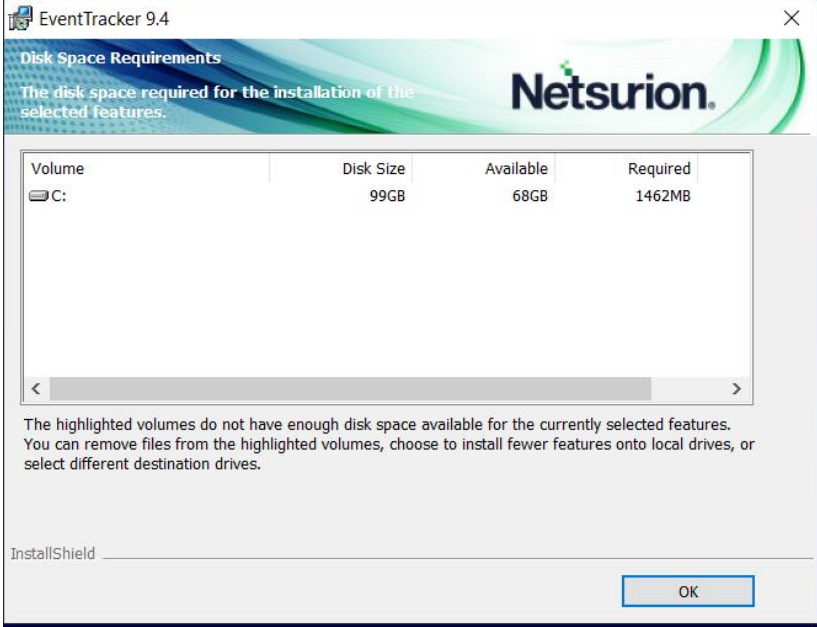


Components	Description
EventTracker Console	Select this component to install the manager console on the target computer.
Change Audit	Optional component. Installing this component enables you to monitor and manage change over the enterprise. The sensor component will also be installed along with the Manager Console. You can also deploy the sensor to the monitored computers using System Manager after installing the Manager Console.
Trap Tracker	Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.

Click	To
<p style="text-align: center;"><b>Change...</b></p>	<p>Select a different destination folder to install the setup.</p> 
<p style="text-align: center;"><b>Help</b></p>	<p>View Select Component conventions.</p> 

Check the disk space available on the target computer.

Space



The disk space required for the installation of the selected features.

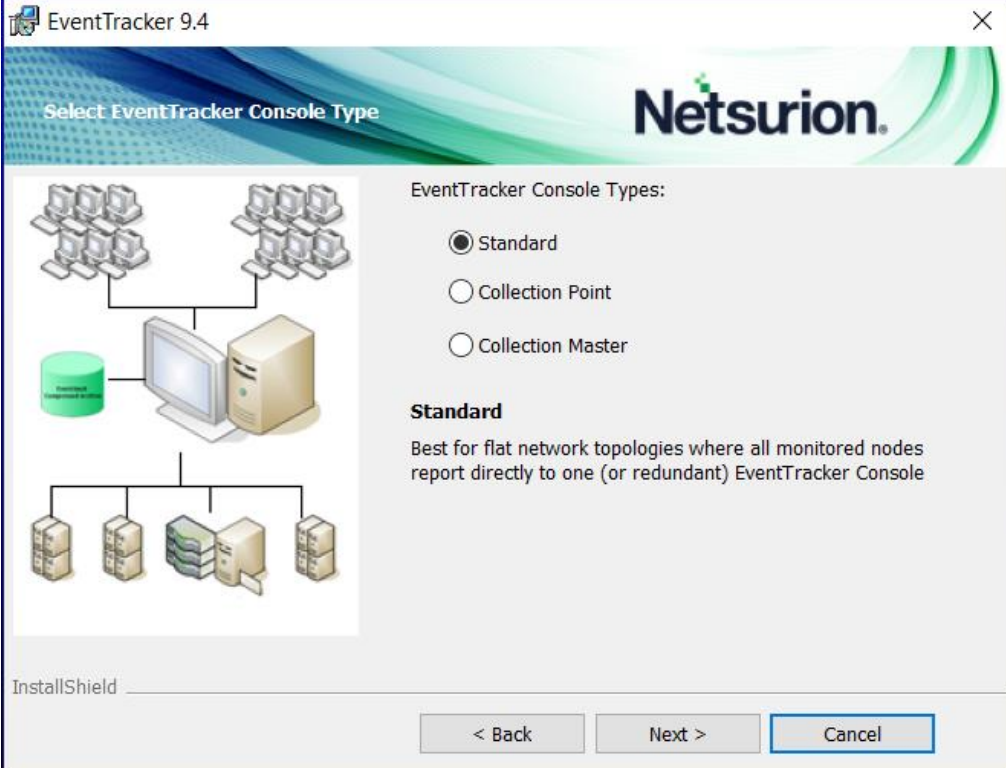
Volume	Disk Size	Available	Required
C:	99GB	68GB	1462MB

The highlighted volumes do not have enough disk space available for the currently selected features. You can remove files from the highlighted volumes, choose to install fewer features onto local drives, or select different destination drives.

InstallShield

OK

4. In **Select EventTracker Console Type** window, choose the appropriate **Console Type** and click **Next** to proceed.
  - a. **Standard Console** option is suitable for flat network topologies, where all the monitored nodes report directly to one (or redundant) Netsurion Open XDR console.



The dialog box shows three console types: Standard (selected), Collection Point, and Collection Master. The Standard option is described as being best for flat network topologies where all monitored nodes report directly to one (or redundant) EventTracker Console.

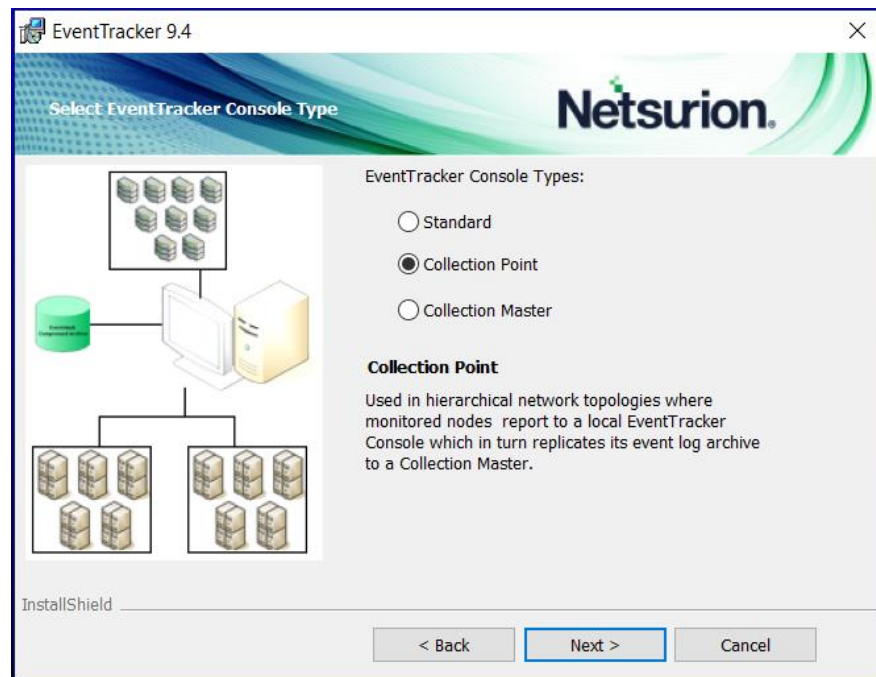
EventTracker Console Types:

- Standard
- Collection Point
- Collection Master

**Standard**  
Best for flat network topologies where all monitored nodes report directly to one (or redundant) EventTracker Console

InstallShield

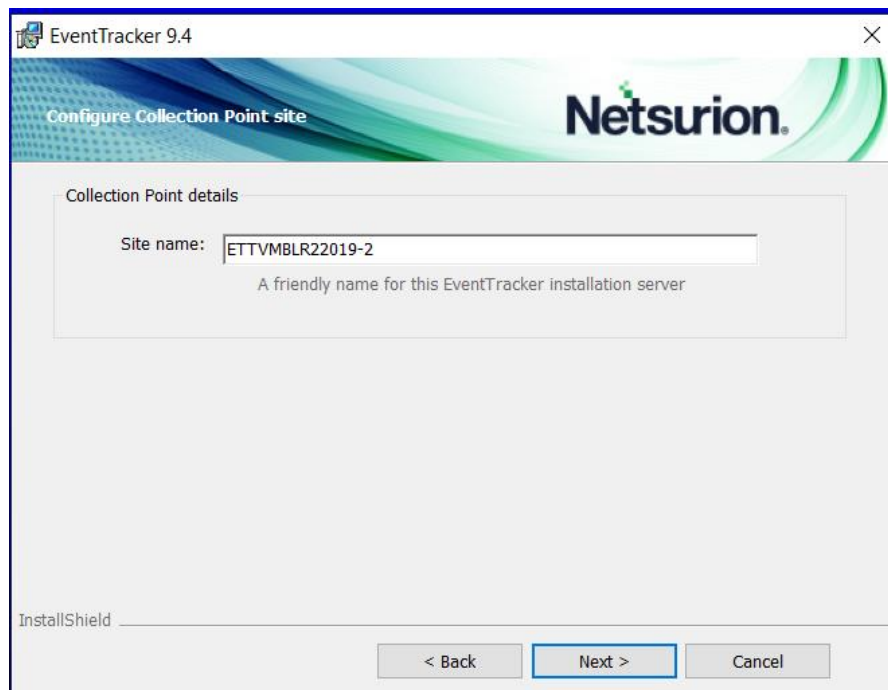
- b. **Collection Point** is applicable for hierarchical network topologies, where the monitored nodes report to a local Netsurion Open XDR console which in turn replicates its event log archive to a Collection Master.



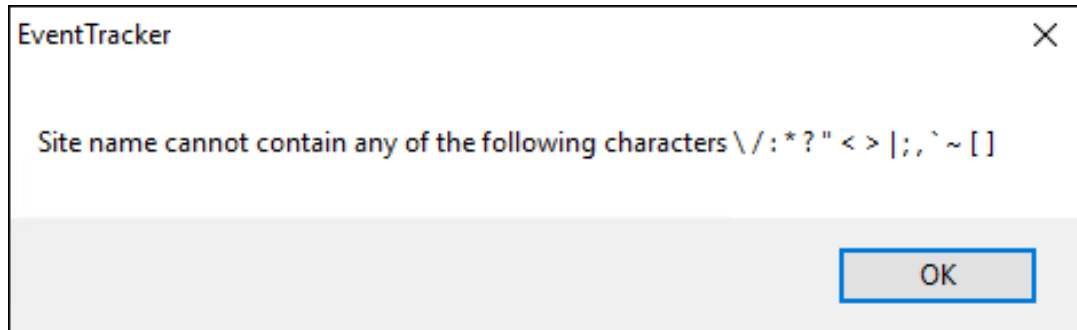
- If choosing the **Collection Point** option, then click **Next** and in the **Configure Collection Point site** window, specify the **Site name**, and then click **Next**.

**Note:**

The following special characters \ / : \* ? " < > | ; , ' ~ [ ] are not applicable while specifying the site or the group name

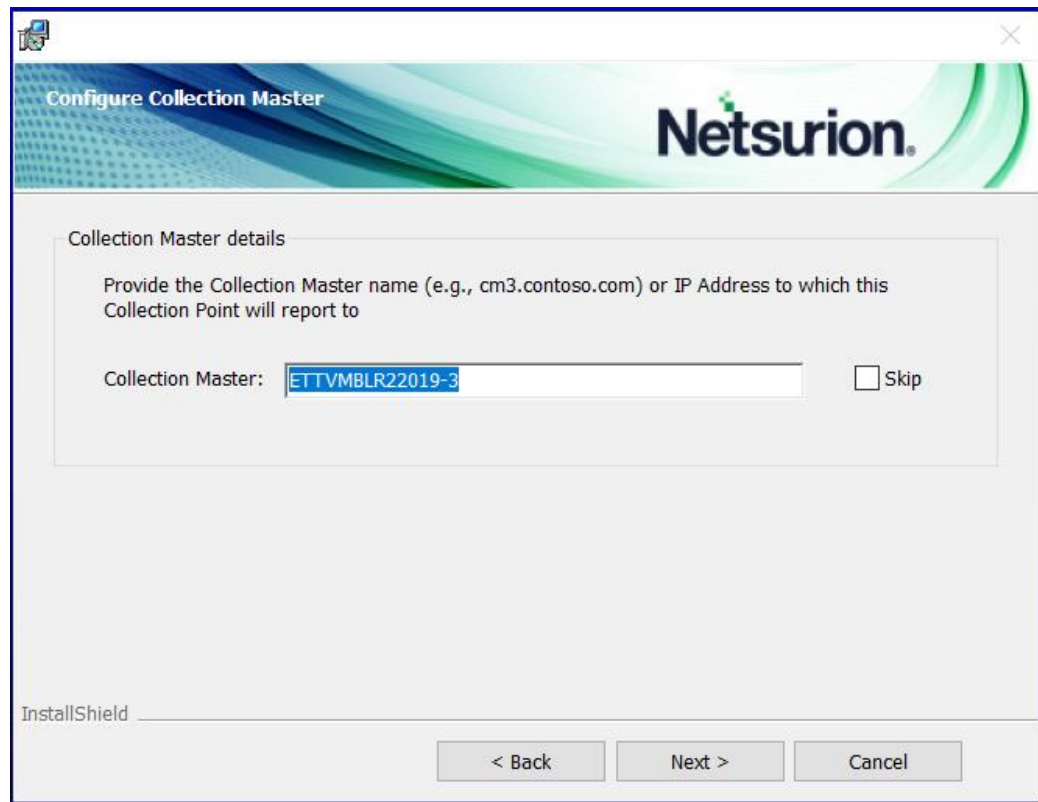


The Wizard pops up the following message if the site or group name includes inapplicable special characters.



The setup wizard navigates to the Configure Collection Master window for Collection Point – Collection Master setup.

- Here, provide either the Collection Master details or select the **Skip** check box, and then click **Next**.

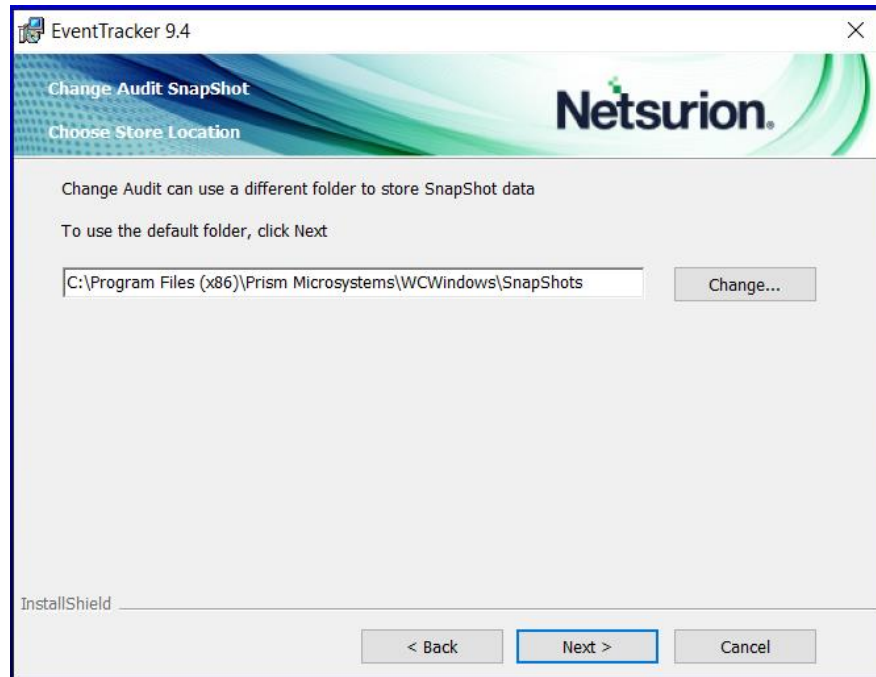


- c. **Collection Master** is applicable for hierarchical network topologies where collection points replicate their event log archives to a Collection Master.
  - If choosing the **Collection Master** option, then click **Next**.



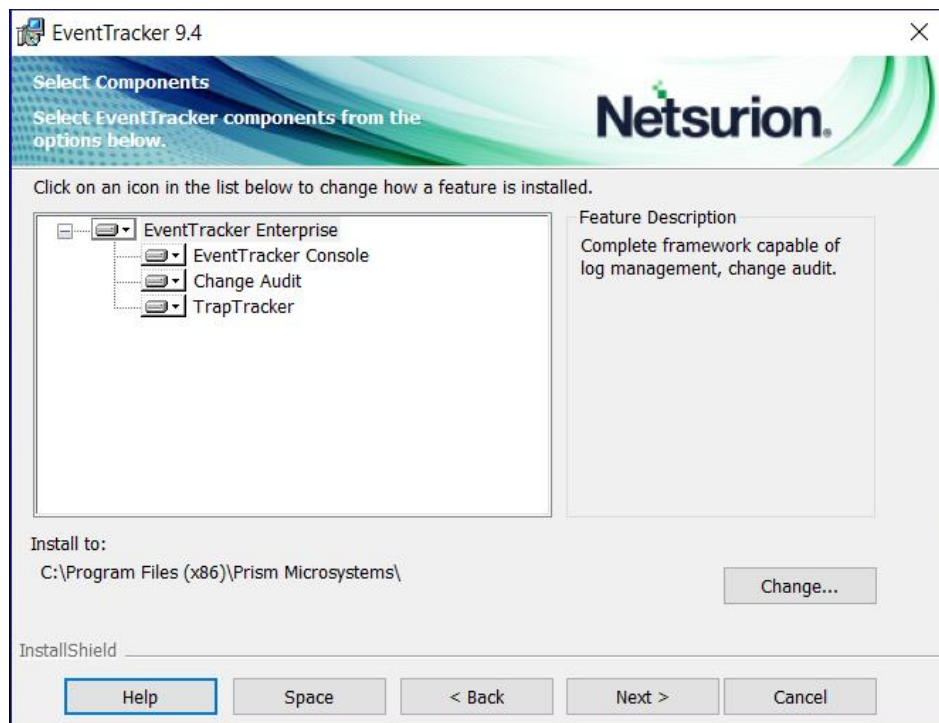
In the **Select Components** window, if the **Change Audit** component is also selected, then the InstallShield Wizard navigates to the **Change Audit SnapShot** window.

- In the **Change Audit SnapShot** window, keep either the default folder location or click **Change** to browse the required store location, and then click **Next**.

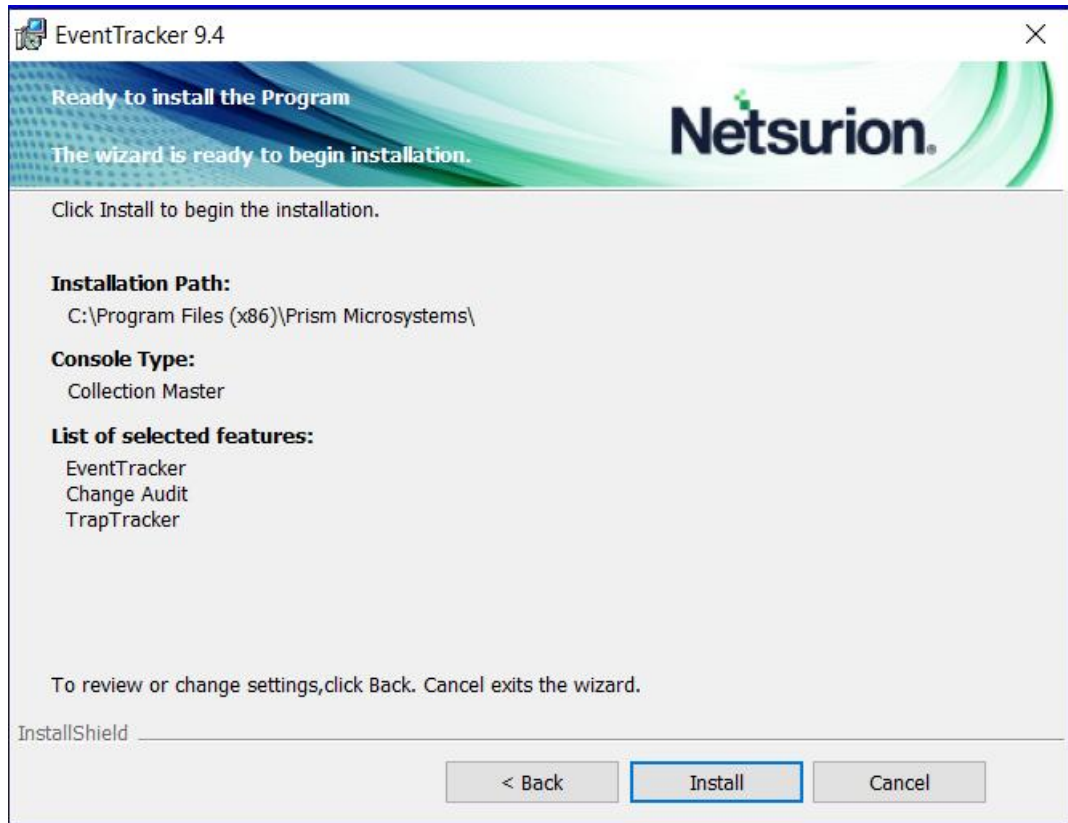


**Note:**

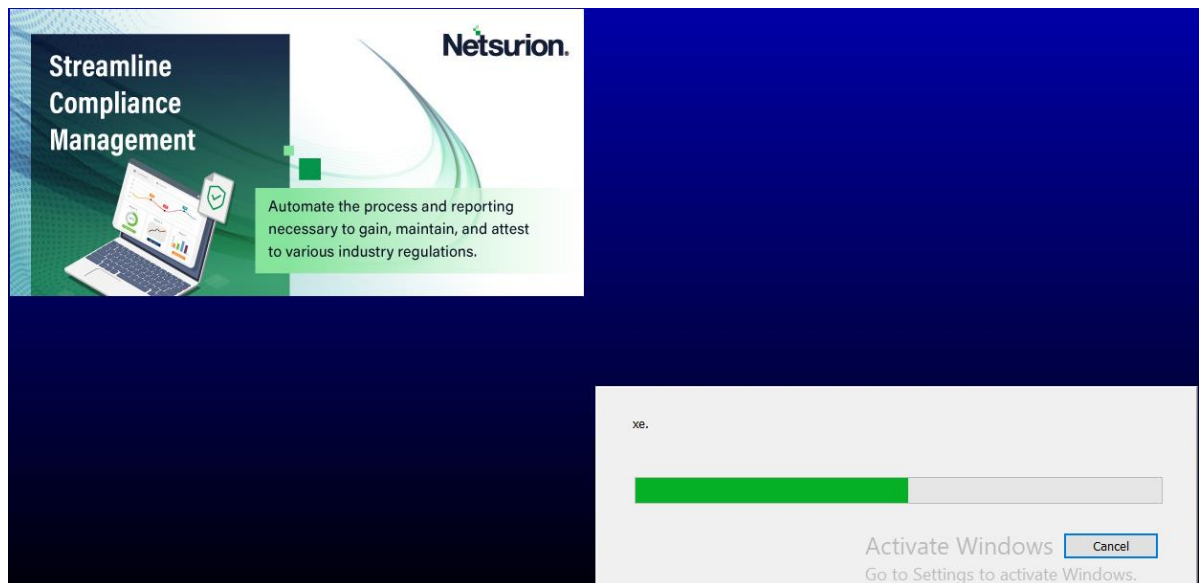
The Change Audit snapshot store location can be changed only during fresh install and if snapshots are not retained during uninstall. In case of an upgrade, if the change audit snapshots are retained during product un-installation, then the snapshot store location path cannot be changed.



- The **Ready to Install the Program** screen provides the summary of the details, the installation path, console type, and the selected features. Verify and click **Install** to install the selected components.

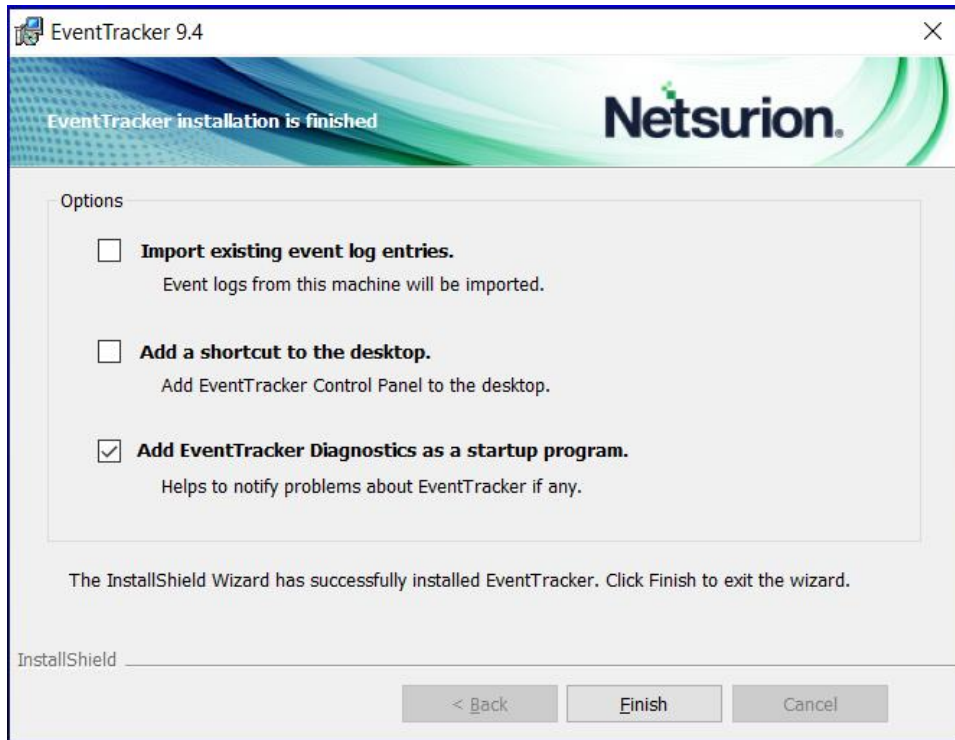


InstallShield Wizard installs the selected components.



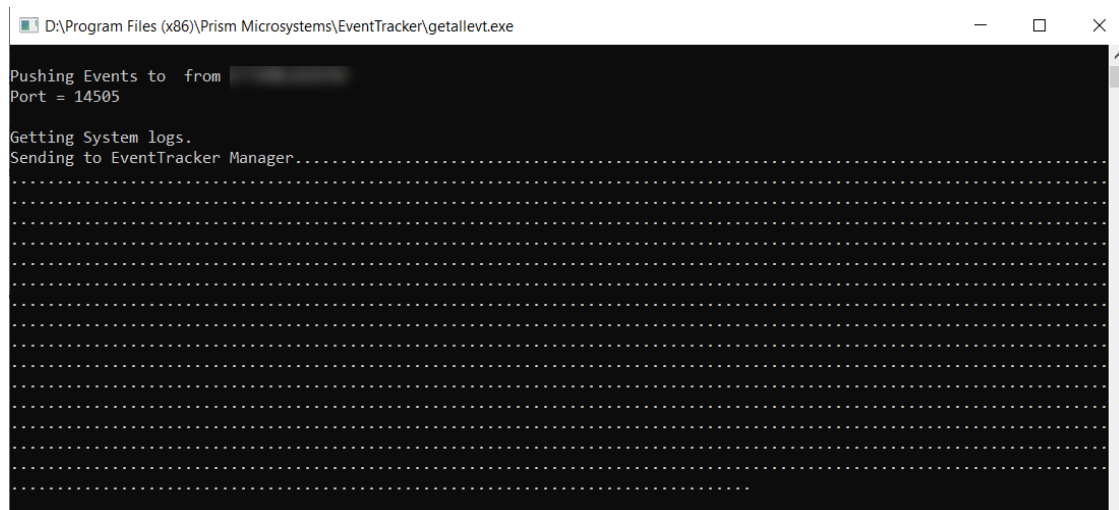


7. In the **Installation is finished** window, select the required option details and click **Finish** to conclude the installation process.



- a. Select the **Import existing event log entries** option if you require to import the Netsurion Open XDR event logs.

The progress of importing the logs will be displayed through the command prompt window.



- b. Select the **Add a shortcut to the desktop** option to add the shortcuts to the Netsurion Open XDR application on the desktop.
- c. The **Add EventTracker diagnostics as a startup program** option is selected by default to notify the Netsurion Open XDR issues (if any).

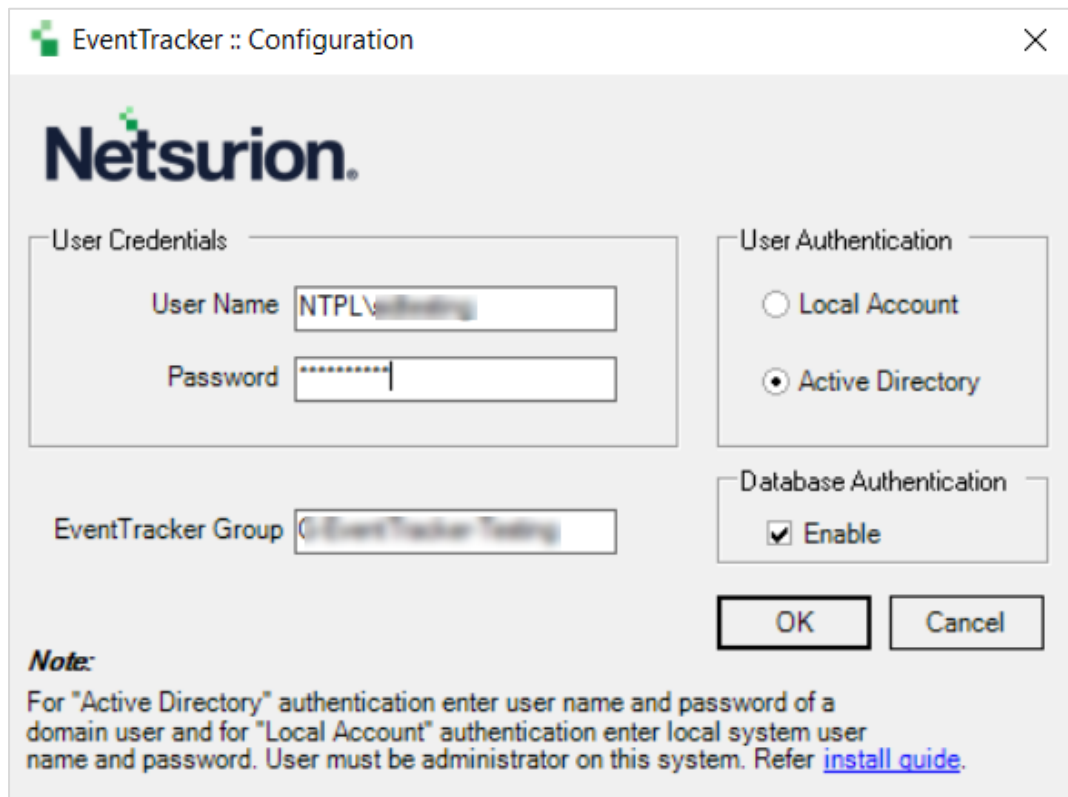
### 3.4.3 Configuring Netsurion Open XDR 9.4

After the InstallShield Wizard is complete, it navigates to the **EventTracker :: Configuration**.

1. In the **EventTracker :: Configuration** interface, specify the User Credentials, User Authentication and EventTracker Group, and then click OK to login.

**Note:**

Though the username/authentication provided in the EventTracker Preinstall Check reflects in this interface, the user still has the option to override it.



**Note:**

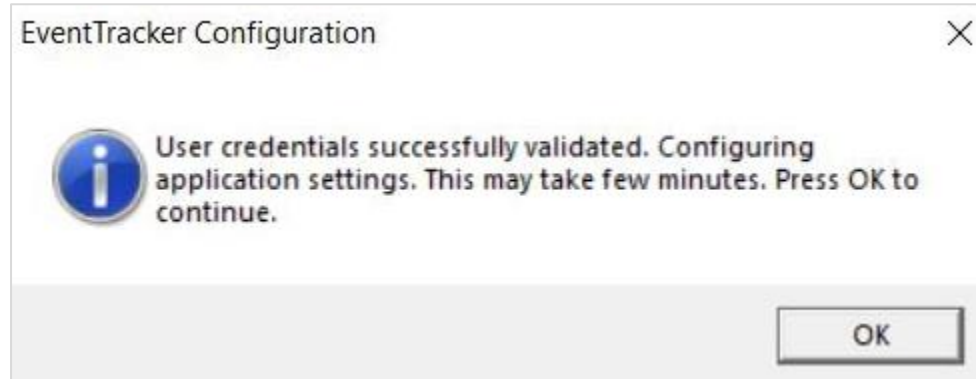
The Netsurion Open XDR services run under this account. By default, this user is assigned the 'EventTracker Administrator' role and can log in to Netsurion Open XDR.

<b>User Credentials</b>		Specify the valid user credentials in the User Name and Password fields.
<b>User Authentication</b>	<b>Local Account</b>	Authentication will be done locally on the computer where Netsurion Open XDR is installed
	<b>Active Directory</b>	Authentication will be done in the Active Directory.

**EventTracker Group**

Specify the EventTracker group name

- The following **EventTracker Configuration** message box pops-up after successfully validating the user credentials. Click **OK**.

**Note:**

If the password is changed for the above-configured user, it is mandatory to re-run the **EventTracker :: Configuration** with the updated password.

**Note:**

You can also access **EventTracker :: Configuration** via **Start > All Programs > Prism Microsystems > EventTracker > EventTracker Configuration**.

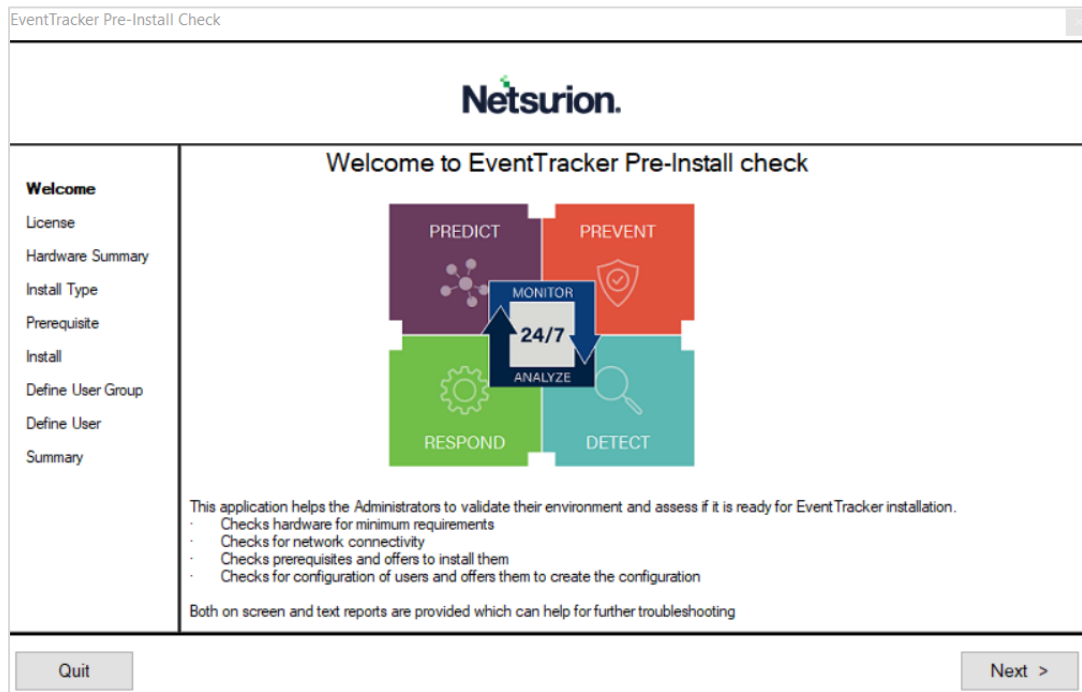
## 3.5 Installing the Netsurion Open XDR Manager – Standard or Collection Point Evaluation Version

If Standard or Collection Point is selected, then,

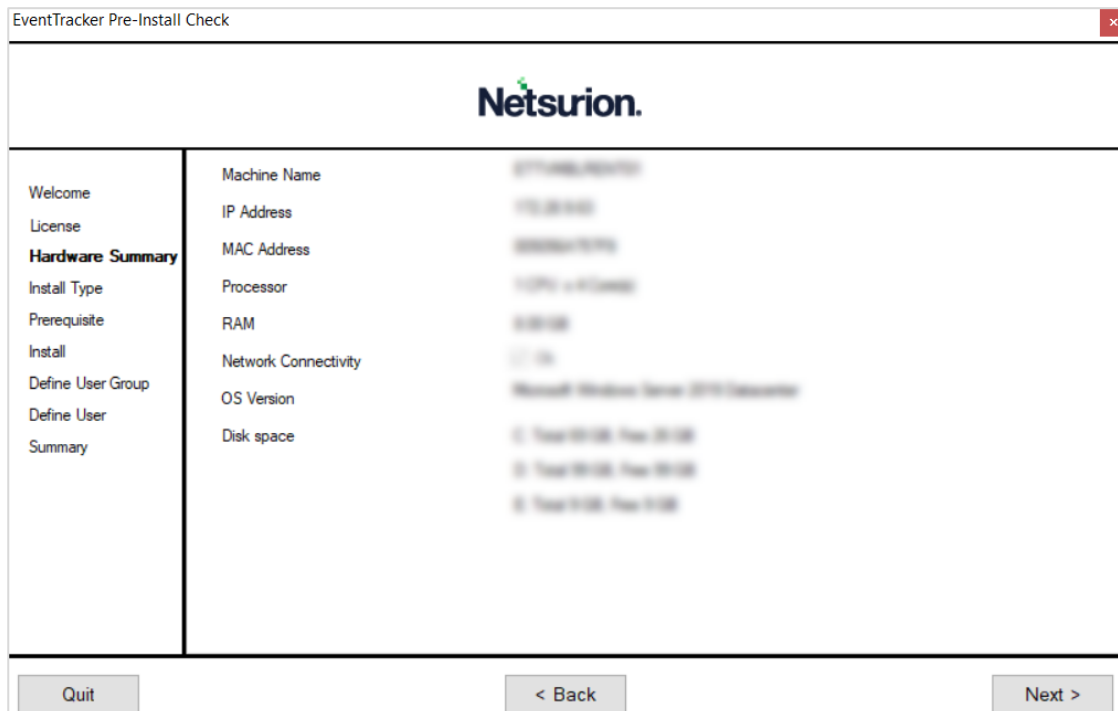
- The archive path is the drive with the maximum free space.
- Local machine authentication is used.
- Group created as 'EventTracker'.
- Username is 'EventTrackerAdmin'.
- This user is local machine admin.
- This user is given 'Logon as batch user' rights, and 'Logon as Service' rights.
- Only express versions of IIS and SQL can be used.

To install Netsurion Open XDR 21-day trial for Standard or Collection Point.

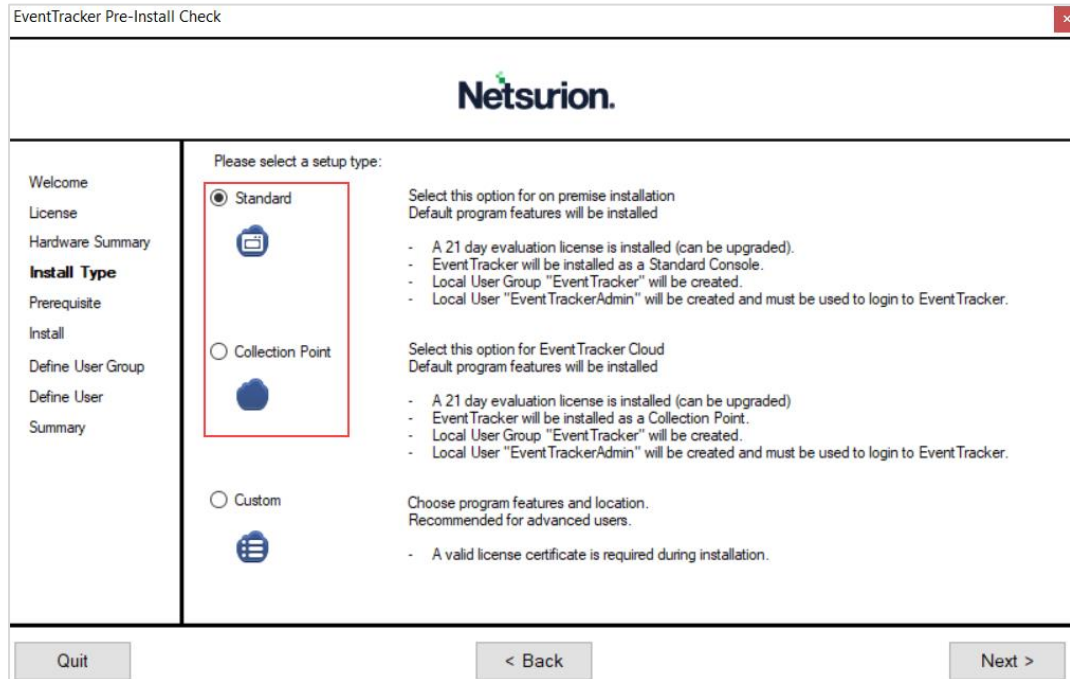
1. Run the Netsurion Open XDR 9.4 installation package via **Run as Administrator**.
2. Netsurion Open XDR launches the **Pre-Install Check** window. Click **Next** to continue with the process.



3. In the **Hardware Summary** section, it may take a few seconds to fetch the hardware details and a processing icon appears during the data collection process. Click **Next** to proceed.



- In the **Install Type** section, choose either the **Standard** or **Collection Point** option, and then click **Next**.



To proceed with the further installation, refer to the [ETLM-Install Guide](#).

**Note:**

After logging in to Netsurion Open XDR, some of the components will not be available as this is a trial version.

In Collection Point installation, components like Trap Tracker, Reports are omitted.

## 4 Deploying the Netsurion Open XDR Windows Sensor

### 4.1 Pre-install Instructions for Windows Sensor

- You must have **Local Admin** privileges on the remote systems where you want to remotely install the **Sensors**.
- You can also install **Sensors** with **Local Admin** privileges.
- Ensure that the systems you are selecting to monitor are accessible through the network, have disks that are shared for the **Admin**, and have disk space up to 90MB that can be used by the **Sensor**.
- If the remote system is accessed through a **VPN** with slow line speed, the installation may take time and it is recommended that you schedule your activities accordingly.
- To monitor a system that supports syslog messages (for example, Unix, Linux, and Cisco, etc.) configure that specific system to forward the syslog messages to the Netsurion Open XDR Manager.

## 4.2 Pre-install checklist for Windows Sensor

The following settings, permissions, and privileges are necessary when deploying the Netsurion Open XDR sensor to ensure safe and smooth sensor installation.

<b>ENSURE</b>	User is a member of the 'Local Administrators' group
	MSI package installation is allowed
	User has 'Logon As Service' rights
	Network Discovery is enabled
	File sharing is allowed
	Access this computer from the network
<b>VERIFY</b>	The user has permission on 'Application install directory' (Folders and sub folders).
	The user must create service permission on the target system(SCM- service control manager)
	The user has Read/Write permission on the Microsoft windows registry.
	The user has permission to Admin share(C\$) of Target systems and C\$ should be accessible from the Netsurion Open XDR Manager.

## 4.3 Different methods to install the Netsurion Open XDR Sensors

There are two methods to deploy the Netsurion Open XDR Sensors,

- Using the **System Manager** which is as part of Netsurion Open XDR. From this **System Manager**, the Netsurion Open XDR Sensors can be deployed to all systems.
- Using the **Manual Sensor** Installation package for all systems.

**Note:**

If the Auto agent update is enabled on the console, all the reporting sensors are automatically upgraded to latest version.

## 4.4 Deploying the Netsurion Open XDR Windows Sensor via System Manager for Sensor Based Systems (full featured)

The installation procedure is identical for all the supported Microsoft Windows Operating Systems.

1. Log in to Netsurion Open XDR with the appropriate user credentials.
2. In Netsurion Open XDR, hover over the **Admin** and click **Systems**.

This interface displays the list of systems that are members of all the trusted domains including the operating system type, asset value, port number, and managed system status through which the Sensor communicates with the Netsurion Open XDR Receiver.

### Note:

Make sure **Auto Discover** is in ON state to view the list of systems. If it is not in ON state then the interface displays only the Netsurion Open XDR Manager details.

The screenshot shows the 'Systems' interface in Netsurion. At the top, there are four summary cards: 'Non Reporting Systems' (2), 'Request Status' (0), 'Managed vs Unmanaged' (8), and 'EventTracker Sensor Version' (3). Below these is a 'Groups' sidebar on the left. The main area is titled 'Systems' and has a navigation bar with 'Request Status', 'Non Reporting Systems', 'Search Computers', 'System Report', 'Auto Discover' (highlighted in red), and 'Source type'. Below the navigation bar, there is a search field and a table of systems. The table has columns for 'Computer', 'Type', 'Port', 'EventTracker version', 'Change audit version', and 'Asset value'. The table contains several rows of system data.

Computer	Type	Port	EventTracker version	Change audit version	Asset value
CT-HIN-DL	2008 R2	14	---	---	Undefined
NTTRIEB-B-DOCUMENTATION	Win 7	14	9.0 - Build 10	---	Low
BY-MI-M	2016	14	9.2 - Build 8	9.2 - Build 8	Serious
BY-MI-MXLA	2016	14	---	---	Serious
SA-CV-CVOLA	Unknown	14	---	---	Undefined
SA-PO-SOLA	Unknown	14	---	---	Undefined
NI-CV-CVOLA	2008 R2	14	---	---	Undefined

3. In the **Systems** interface, select the required group or system to install the sensor.

### Note:

Refer [Installing Sensors for a Group](#) section to install the sensors for a group or the [Installing Sensor for a System](#) section to install the sensor for a system, and then proceed with the next step.

- **Installing Sensors for a Group**
  - a. In the **Systems** interface, from the **All Groups** pane, click the required domain or the group name, and then click the gear icon and select **Install agent/Start poll** from the drop-down list.

The screenshot shows the 'Systems' management page. A context menu is open over a table of systems, with 'Install agent/Start poll' highlighted. The table below shows system details:

Type	Port	EventTracker version	Change audit version	Asset value
Unknown	50	9.1 - Build 19	--	Undefined
2008 R2	59	--	--	Undefined
Win 7	50	9.0 - Build 18	--	Low
DOCUMENTATION	2016	50	9.2 - Build 8	Serious
2016	50	--	--	Serious
Unknown	50	--	--	Undefined
Unknown	50	--	--	Undefined
2008 R2	.50	--	--	Undefined

b. In the **Install agent/Start poll** window, the following three options are available,

The dialog box 'Install agent/Start poll' contains the following options:

- All systems in the selected group
- Take systems from text file
- Specific systems in the selected group

Agent Type  EventTracker  Change Audit

Buttons: Cancel, Back, Next, Advanced, Install

c. Choose the appropriate option and select the required **Agent Type** to upgrade the sensors.


Options	Description
<b>All systems in the selected group</b>	<ul style="list-style-type: none"> <li>Click this option to upgrade all the sensors available in the selected group.</li> </ul>

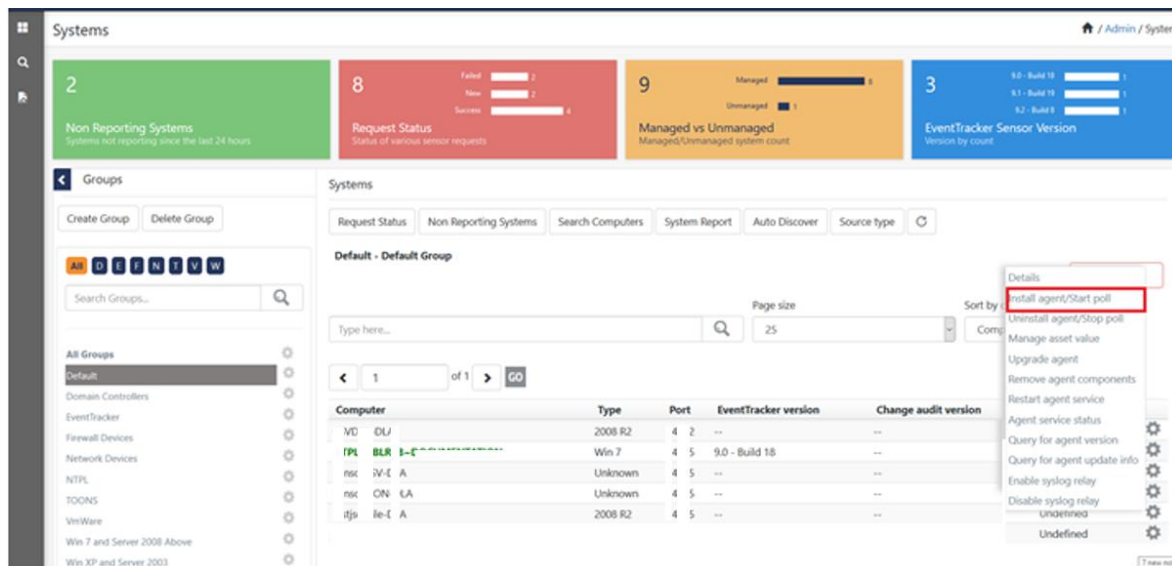


Options	Description
<b>Take systems from the text file</b>	<ul style="list-style-type: none"> <li>Browse for the text file holding sensor system names for which you require to upgrade. The text file should contain one system name per line.</li> <li>If you desire to select this option, then create the text file to select the sensor system names.</li> </ul>
<b>Agent Type</b>	Select the appropriate sensor type to upgrade. <ul style="list-style-type: none"> <li>EventTracker</li> <li>Change Audit</li> </ul>
<b>Specific systems in the selected group</b>	Out of all the sensor systems available in the group, select a specific sensor system(s) to upgrade.

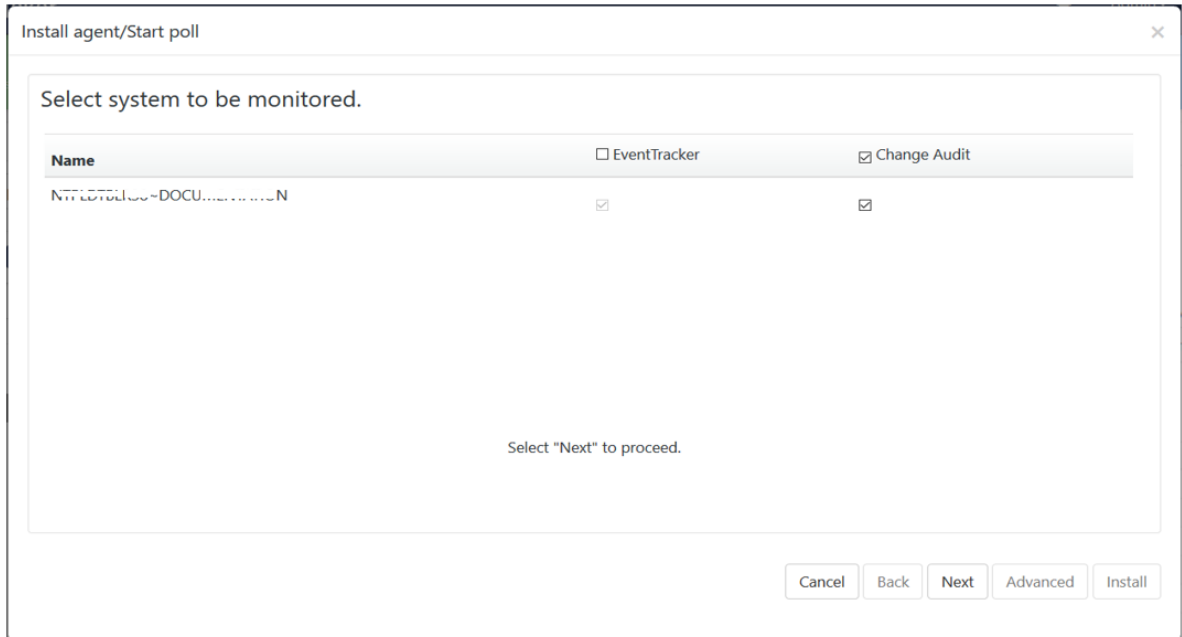
d. After selecting the appropriate details click **Next** to proceed.

• **Installing Sensor for a System**

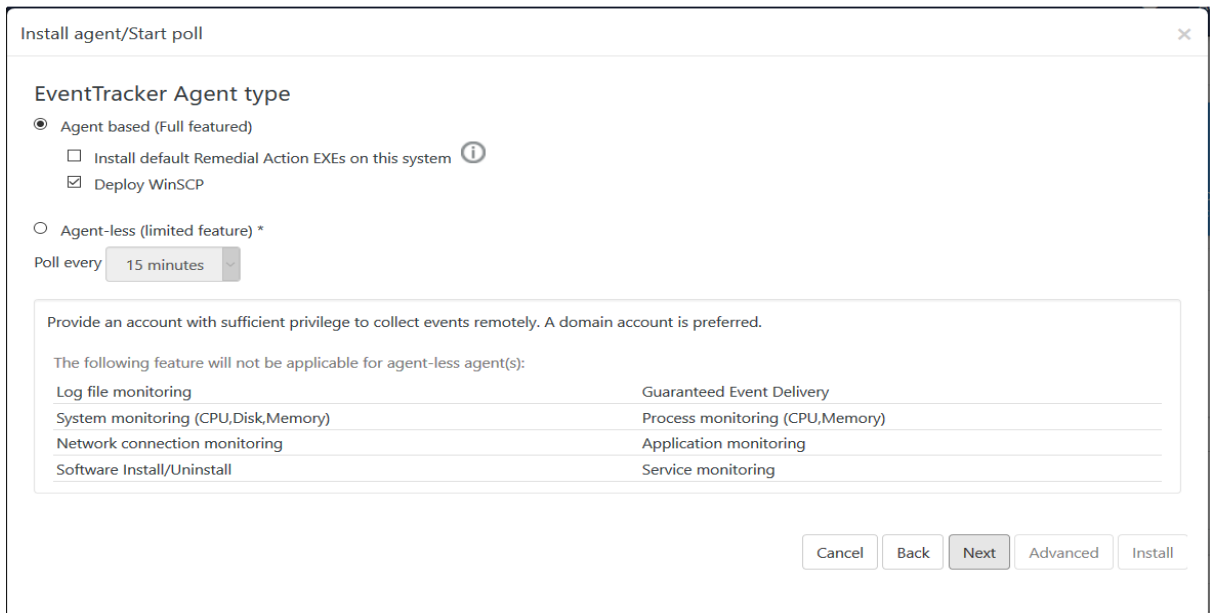
- a. In the **Systems** interface, from the **Computer** list, click the gear  icon (located corresponding to the remote system's name) for which you require to install the sensor, and then click **Install agent/Start poll** from the drop-down list.



- b. In the **Install Agent/Start poll** window, select the required sensor type (EventTracker or Change Audit) check box, and then click **Next**.



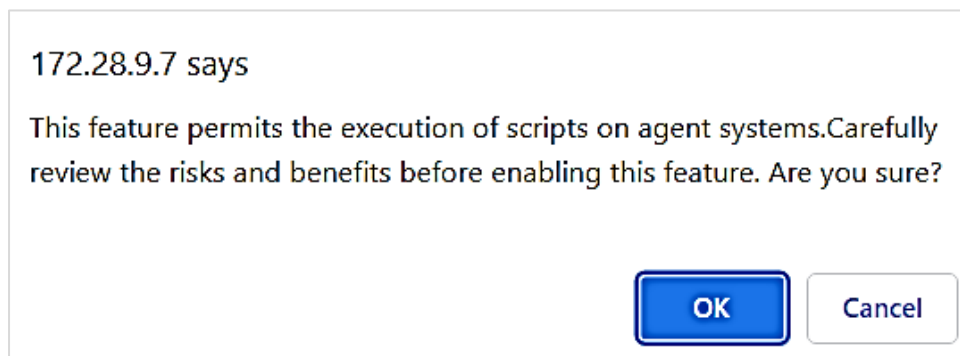
- c. Next, choose the required **EventTracker Agent Type** that is, either the **Agent based (Full Featured)** option or the **Agent-less (limited feature)\*** option.



Agent based (Full featured)	
Install default Remedial Action EXEs on this system	<p><b>Remedial Actions</b> are scripts or executable files that can be launched at either the sensor or the manager side, in response to events.</p> <p>If this option is enabled, predefined scripts are placed in the <code>EventTracker\Agent\Script</code> folder at the manager side. These may be installed at the Sensor side also, during deployment via the <b>System</b> manager.</p>
Deploy WinSCP	Provides an option to install WinSCP components to remote machines while deploying Sensor(s).
Agentless (limited feature)	
Poll Every	By default, the frequency is set to 15 min to receive events from the remote Sensor system. You can change the poll frequency as per the requirement.

If the **EventTracker Agent type** is selected as '**Agent based (Full Featured)**', then remedial actions EXEs can be installed on the system.

- d. Select the **Install default Remedial Action EXEs on this system** check box if you require to install remedial action scripts.
- e. The following message window pops-up to confirm to enable this feature. Review and either click **OK** to proceed or click **Cancel** if you do not require to install the remedial action EXEs, and then click **Next**.



**Note:**

'Install default Remedial Action EXEs on this system' option is available for 'Agent based (Full featured)' installation.

The **Install agent/Start poll** interface displays the default client installation path on the remote computer.

- Specify the required location details in the **Installation path** field to install the Sensor in a different drive apart from the default one.
- Select the **Create 'Program Menu' shortcuts** check box to create shortcuts.
- Specify the valid **Account** name and **Password** and click **Next**.

The Sensor is installed on the selected machine with the default 'etaconfig.ini' configuration.

f. To set a more specific configuration, click **Advanced**.

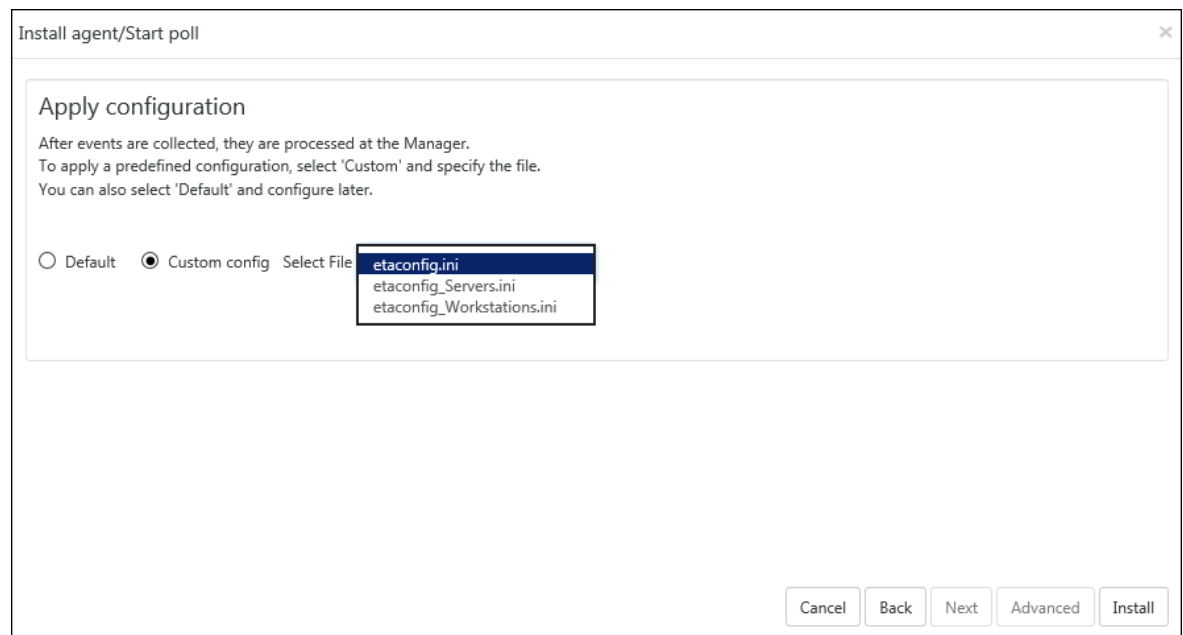
- g. Choose the **Custom config** option to select a custom configuration file.

**Note:**

The **Default** option is selected by default to apply the manager side ‘Sensor configuration’ settings (etaconfig.ini).

The custom configuration will provide the templates you created in Sensor configuration along with two more predefined templates.

etaconfig_Servers.ini	This predefined template contains the ideal server configurations which can be applied to the selected sensor system.
etaconfig_Workstations.ini	This predefined template contains the ideal workstation configurations which can be applied to the selected sensor system. This option disables the ‘Offline event sending’ option.

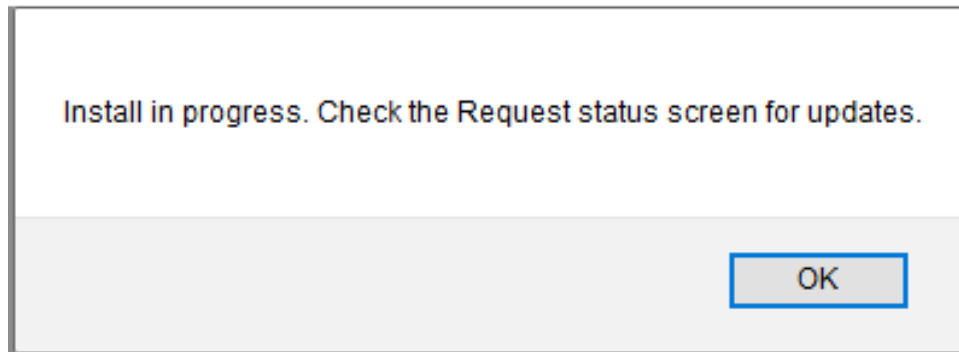


**Note:**

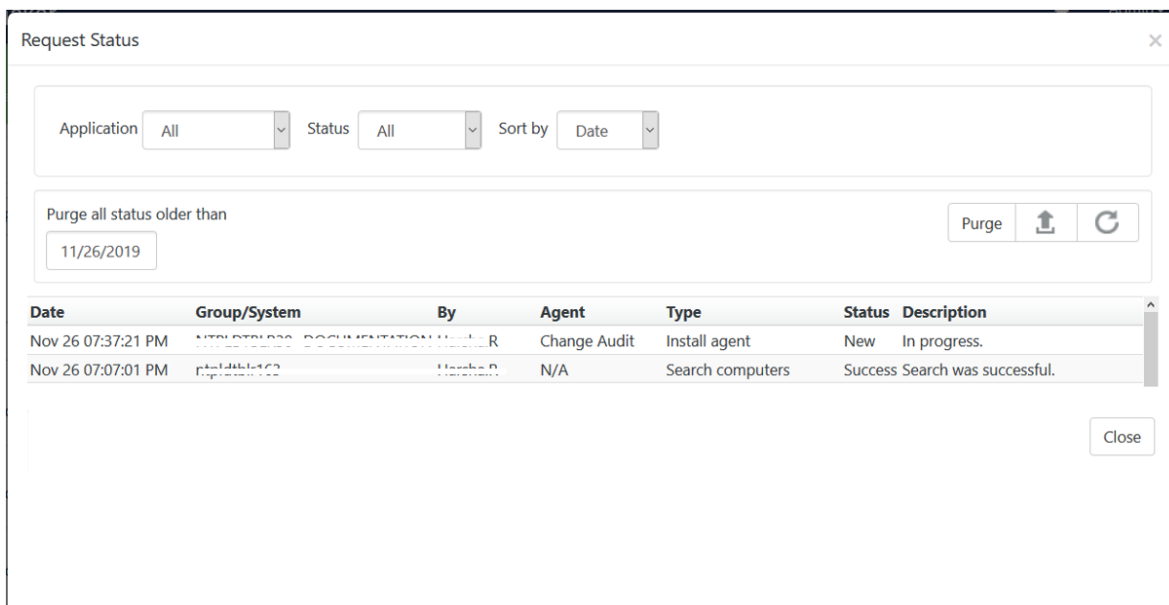
In case if you choose the Custom config option (and selected either **etaconfig\_Servers.ini**, **etaconfig\_Workstations.ini**) then configure the Manager.

- After providing the required details, click **Install**.

A message window pops-up stating *'Install in progress. Check the Request status screen for updates.'*




- Click **OK** and go to **Systems > Request Status** interface to view the installation status.



Select	To
Application	Sort the <b>Request Status</b> results by the application installed. Available options are EventTracker and Change Audit.
Status	Sort the <b>Request Status</b> results by the status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the <b>Request Status</b> results by <b>Date</b> of the application installed /on which <b>System</b> it is installed / <b>Type</b> of activity performed/ <b>Status</b> of the application.
Purge all status	Remove the older Request Status details from the list.

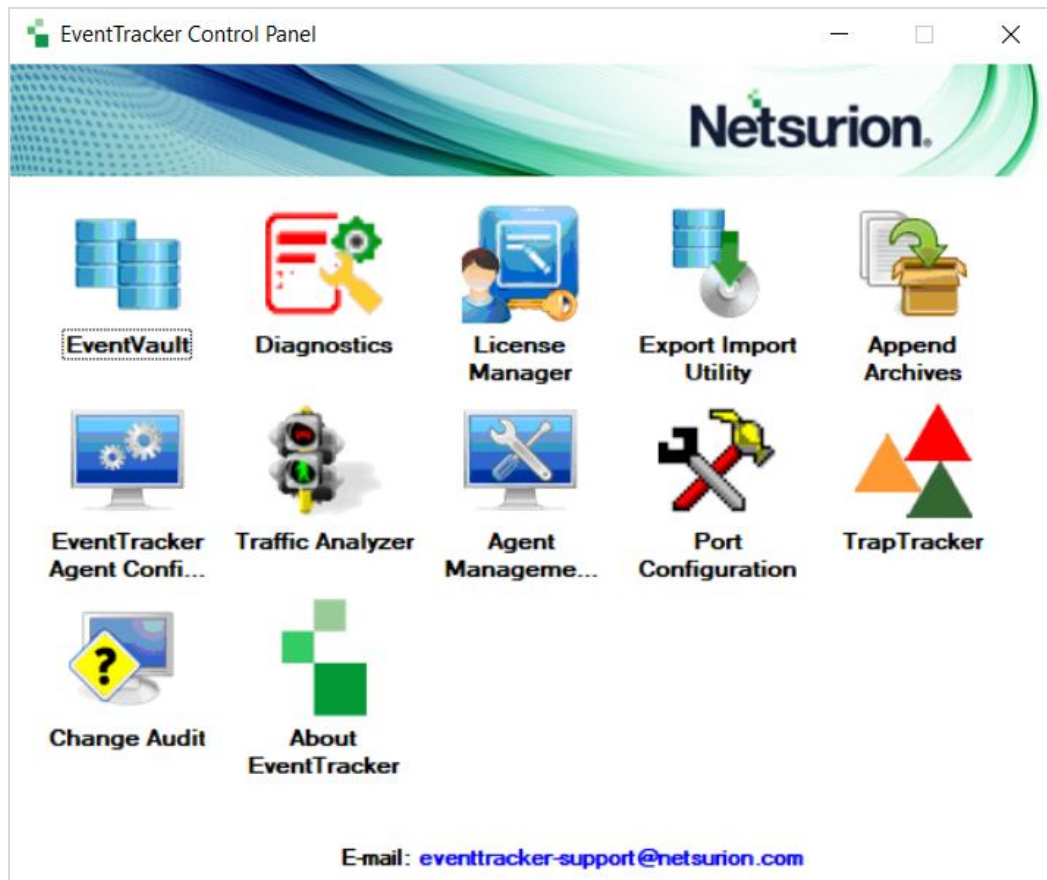
Select	To
older than	
Export	Export the 'System Status' into <b>Excel</b> format

- Click **Refresh**  to view the latest progress status or reopen the **Request Status** dialog box to see the updated status.

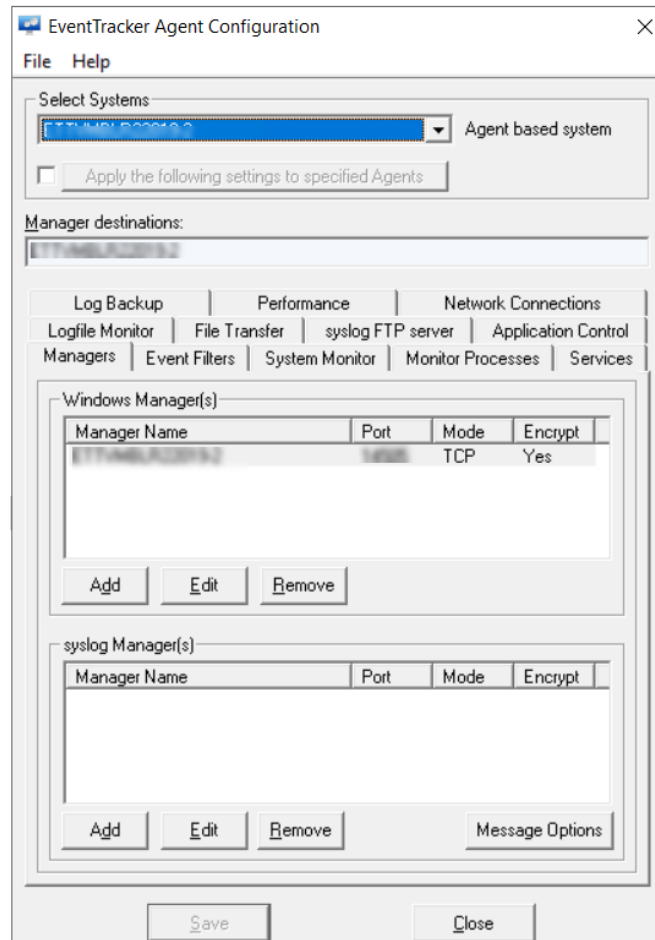
## 4.5 Configuring the Netsurion Open XDR Windows Sensors

All configurations for the sensor(s) are set by default during installation. Perform the following steps if you require to change the default configuration settings.

- Log in to the **Netsurion Open XDR Control Panel**.



2. Double-click **EventTracker Agent Configuration** and configure the sensor according to the requirement.



## 4.6 Configuring Sensor-less collection via System Manager (limited features)

If installing the Netsurion Open XDR Windows Sensor is not feasible or desirable, then Netsurion Open XDR can be set up to subscribe or poll remote computers' event logs over the network to collect new event log entries.

### Pros

- No sensor to deploy – Simple product deployment and trivial effort during planning, deployment, and upgrade.

### Cons

- Increased network traffic - Depending on the polling cycle or level of event generation that is chosen, network load is greater.
- Greater dependency and more critical points of failure - The Console becomes critical since it is polling target machines. Network choke points can impact performance.




- Limited to operation within a domain - The Console and target machine must be in the same domain so that domain privileges are preserved.
- Performance monitoring, Log file Monitoring, System Monitoring, Network Connection Monitoring, Software Install / Uninstall, Guaranteed Event Delivery, Process Monitoring, Application Monitoring, Service Monitoring, Software install/removal monitoring, Host-based intrusion detection, Monitoring external log files – The specified feature will not be available.
- Non-domain topologies not supported - This feature is only available when the Console and target machine are in the same Windows domain.

## Adding Systems for Sensor-less monitoring

This feature facilitates you to add systems from where you require to collect events periodically. The resource (CPU/memory/disk) usage, log file monitoring, and other Sensor-required features are disabled, in the Sensor-less monitoring systems. Additionally, the service account of the local Sensor should have administrative privileges on all the systems that are added for collecting events.

### Note:

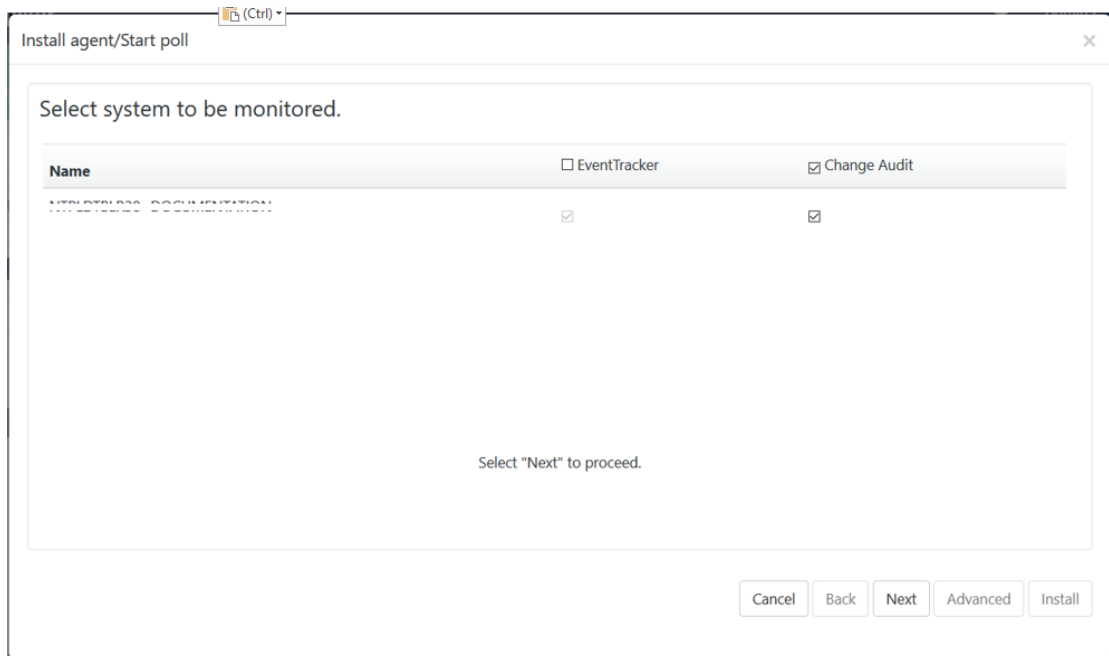
In Microsoft Windows Firewall, ensure that the Remote Event Log Management is added in the filter exception list, or else it will not connect to the target system.

1. In the **System** manager interface, select the gear  icon of the system in which you require to install the sensor and then click **Install agent/ Start poll** from the drop-down list.

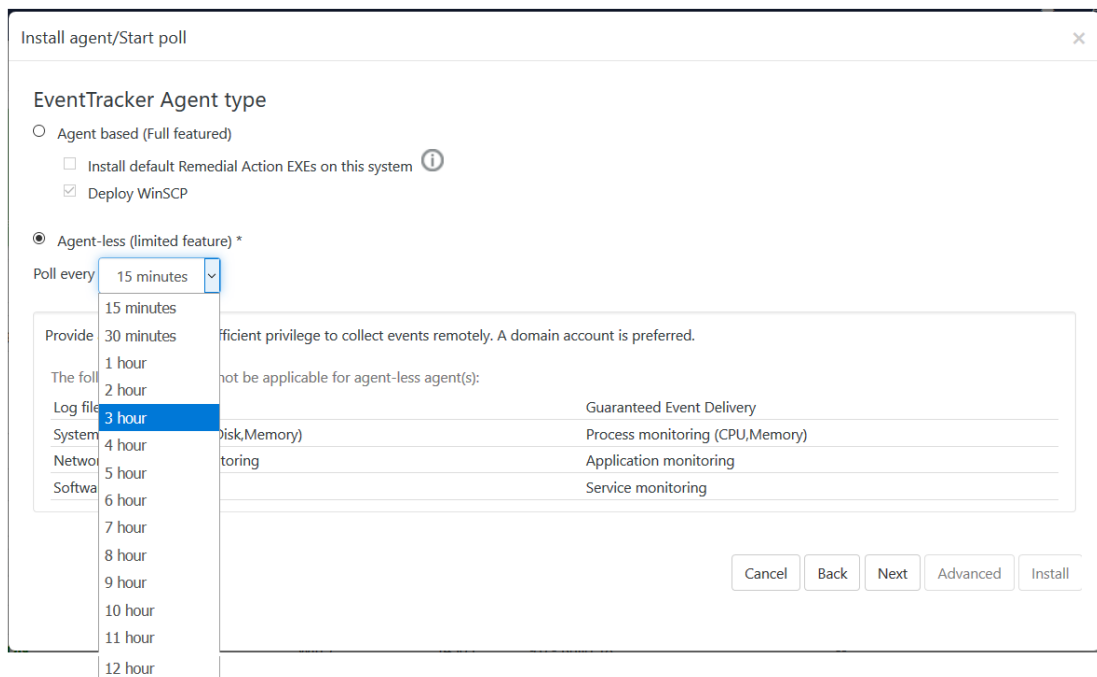
The screenshot shows the 'Systems' management interface. At the top, there are four summary cards: 'Non Reporting System' (0), 'Installation status' (0), 'Managed v/s default' (2), and 'Version' (1). Below these is a 'Groups' sidebar with 'TOONS' selected. The main area displays a table of systems under the 'TOONS - Enterprise Domain'. A dropdown menu is open for the system 'N2K81 \VM.', with 'Install agent/Start poll' highlighted in red.

Computer	Type	Port	EventTracker Version	Change Audit Version	Asset value
5X\ SERVE	2003	--	--	--	High
5X\ N10V1 01	Win 10	--	--	--	
5X\ N2K11 \ZVI 8	2012 R2	--	--	--	
5X\ N2K14 \M0	2016	--	--	--	
5X\ N2K14 \M0	2016	--	--	--	
5X\ N2K81 \VM	2008 R2	--	--	--	
5X\ N2K81 \VM.	2008 R2	--	--	--	
5X\ N2V1 \N7VM	2016	--	--	--	High

2. In the **Install Agent/Start poll** window, select the **EventTracker** check box to install the Netsurion Open XDR Sensor (Agent-less) and click **Next**.
  - a. Check the **Change Audit** option to install Change Audit Sensor (Only for Sensor-based option)



3. In the **EventTracker Agent Type** window, choose the **Agent-less (limited feature)\*** option.
4. **Poll Every** – Select the time frequency during which you want to get the events. By default, the frequency is set to 15 min to receive events from the remote Sensor system.



5. Netsurion Open XDR displays the Install agent/Start poll dialog box with the default client **Installation path** on the remote computer. Specify the appropriate details and click **Install**.

Field	Description
<b>Account</b>	Specify the valid username and password in Account, Password and Confirm Password fields respectively.
<b>Selected Systems</b>	This field displays the selected system list.

The sensor is installed on the selected machine with the default 'etaconfig.ini' configuration.

6. To set a more specific configuration, click **Advanced**.

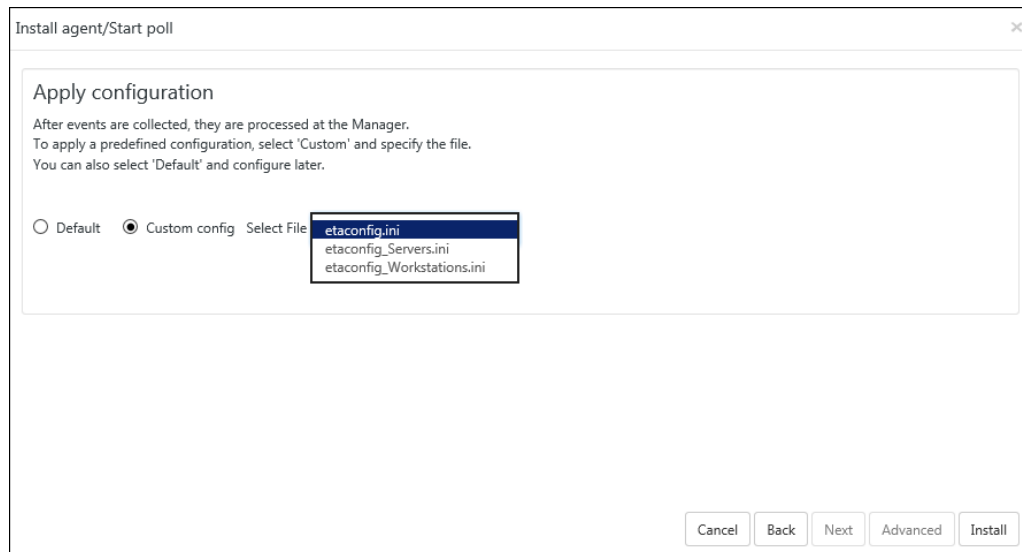
7. Choose the **Custom config** option to select a custom configuration file.

**Note:**

The **Default** option is selected by default to apply the manager side ‘Sensor configuration’ settings (etaconfig.ini).

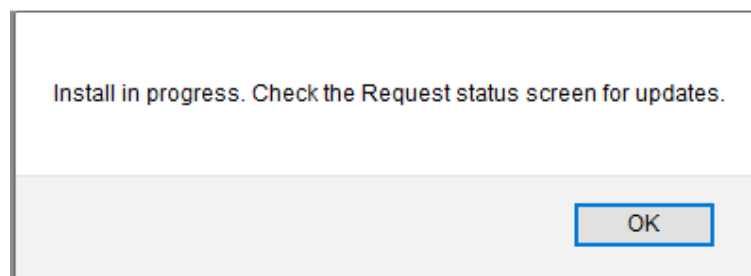
The custom configuration will provide the templates you created in Sensor configuration along with two more predefined templates.

etaconfig_Servers.ini	This predefined template contains the ideal server configurations which can be applied to the selected sensor system.
etaconfig_Workstations.ini	This predefined template contains the ideal workstation configurations which can be applied to the selected sensor system. This option disables the ‘Offline event sending’ option.

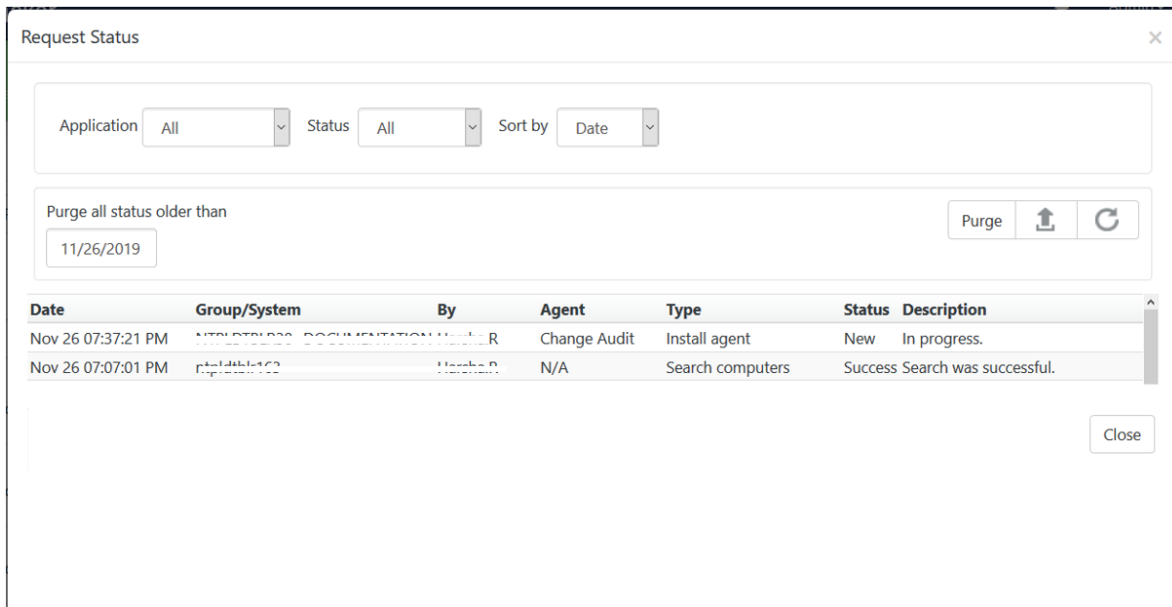


7. After providing the required details, click **Install**.


A message window pops-up stating **‘Install in progress. Check the Request status screen for updates.’**



8. Click **OK** and go to **Systems > Request Status** interface to view the installation status.

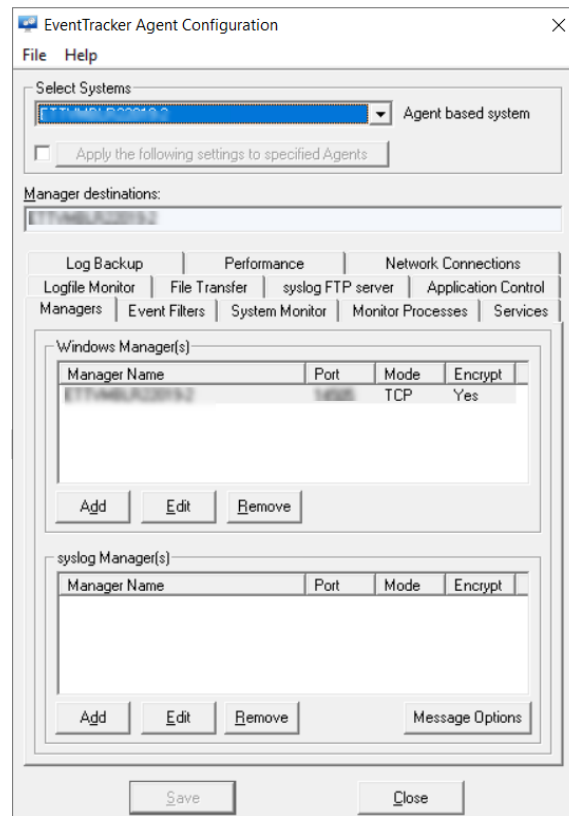


Select	To
Application	Sort the <b>Request Status</b> results by the application installed. Available options are EventTracker and Change Audit.
Status	Sort the <b>Request Status</b> results by the status of the application installed. Available options are All, New, Success, and Failed.
Sort by	Sort the <b>Request Status</b> results by <b>Date</b> of the application installed /on which <b>System</b> it is installed / <b>Type</b> of activity performed/ <b>Status</b> of the application.
Purge all status older than	Remove the older Request Status details from the list.
Export	Export the 'System Status' into <b>Excel</b> format

9. Click **Refresh**  to view the latest progress status or reopen the **Request Status** dialog box to see the updated status.

10. Then, go to the Netsurion Open XDR Control Panel, double-click the EventTracker Agent Configuration.

Only limited feature tabs are available as shown in the figure below:



## 4.7 Deploying the Netsurion Open XDR Windows Sensor - Microsoft Windows 10 and above

### 4.7.1 Prerequisites for Windows Sensor – Microsoft Windows 10 and above

Before deploying the Sensor, perform the following mandatory settings on Windows 10 or later system(s).

- By default, the Startup Type of Remote Registry is manual. Modify the **Startup Type** as Automatic and start the service.
- Enable **File** and **Printer Sharing**.
- Turn on and enable **Network Discovery**.
- To configure Sensor remotely, add port no 14506 TCP to Firewall Exceptions.
- The user must be domain administrator, member of domain admin, or must be added to the local administrator group where the Sensor must be deployed.

## 4.7.2 Installing / Uninstalling Microsoft Windows 10 and above Sensor

The installation and the uninstallation procedure for Windows 8.1 and above Sensor are identical to the procedures for other Windows Sensors. No other additional configuration settings are required.

## 5 Sensor Deployment

To install the Netsurion Open XDR Sensor and Change Audit Sensor, refer [EventTracker Agent Deployment – User Manual](#).

## 6 Securing Netsurion Open XDR

To secure Netsurion Open XDR, refer EventTracker Hardening Guide and [OWASP Complaint EventTracker Guide](#).

## 7 Uninstalling the Netsurion Open XDR Windows Sensor

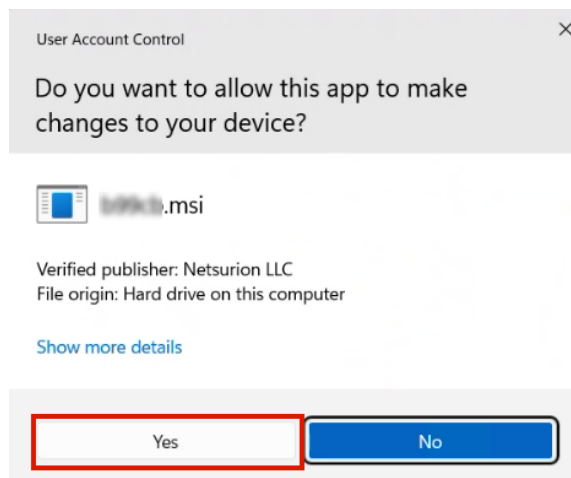
There are different methods to uninstall the Netsurion Open XDR Windows Sensor.

- Uninstalling via Control Panel.
- Uninstalling via System Manager.

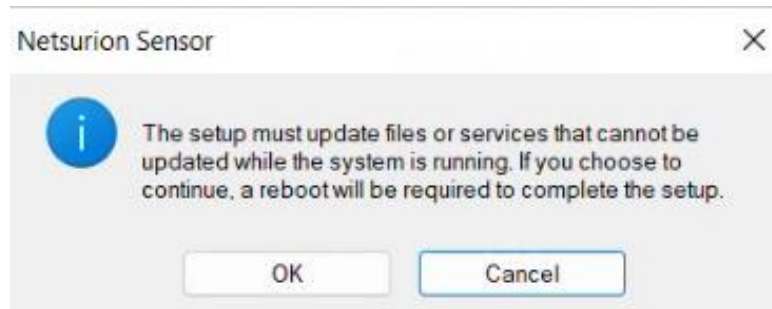
### 7.1 Uninstalling via Control Panel

Perform the following procedure to uninstall the Netsurion Open XDR Windows Sensor via Control Panel.

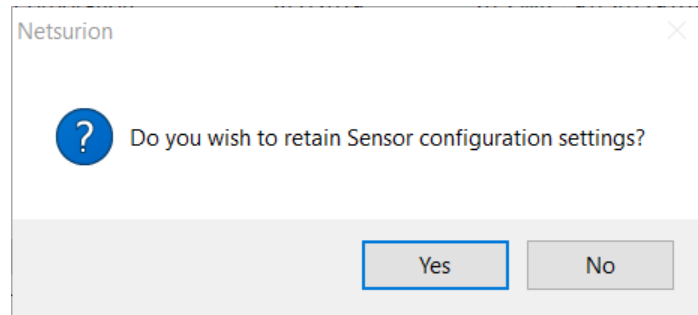
1. Go to **Start > Control Panel > Programs and Features**.
2. In the **Uninstall or change a program**, search, and right-click **Netsurion Sensor**, and then click **Uninstall** to uninstall the Netsurion Open XDR Windows Sensor.
3. A message window pops up to permit and confirm the process. Click **Yes** to confirm.



- Another message window pops-up to proceed with the uninstallation process. Click **OK** to update the setup and proceed with the uninstallation.



- Netsurion Open XDR pops up a message window stating whether to retain the Sensor configuration settings. Click either **Yes** to retain or **No** to rule out as per the requirement.



Thus, by carrying out the specified procedure, the Netsurion Open XDR sensor will be successfully uninstalled.

## 7.2 Uninstalling via System Manager

Perform the following procedure to uninstall the Netsurion Open XDR Windows Sensor via System Manager.

- Log in to **Netsurion Open XDR**, hover over **Admin** and click **Systems** to go to the Systems Manager interface.
- In the **Systems** interface, select the required group or system to uninstall the sensor.



- Then, click the gear icon of the group or system and then click **Uninstall agent/ Stop poll** from the drop-down list.

Type	Port	EventTracker version	Change audit version	Asset value
Unknown	05	9.1 - Build 19	--	Undefined
2008 R2	92	--	--	Undefined
Win 10	--	--	--	Undefined
Win 7	05	9.0 - Build 18	--	Low
2016	05	9.2 - Build 8	9.2 - Build 8	Serious
2016	05	--	--	Serious
Unknown	05	--	--	Undefined
Unknown	05	--	--	Undefined
2008 R2	05	--	--	Undefined

- In the **Uninstall agent/ Stop poll** window, choose the required function from the available option, and click **Next**.

Uninstall Remote agent(s)/Stop poll

Select systems and agent type

All systems in the selected group

Take systems from text file

(One system per line)

Agent Type  EventTracker  Change Audit

Specific systems in the selected group

5. Select the required **EventTracker**, **Change Audit** options and then click **Next**.

Uninstall Remote agent(s)/Stop poll

Select system to be monitored.

Name	<input type="checkbox"/> EventTracker	Change Audit <input type="checkbox"/>
ESSENTIAL	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Select "Next" to proceed.

Cancel Back Next Advanced Install

6. Specify the valid credentials and then click **Uninstall**.

Uninstall Remote agent(s)/Stop poll

Account  ⓘ

Password

Confirm Password

**EventTracker:** ESSENTIAL

Select 'Uninstall' to proceed.

Cancel Back Next Uninstall

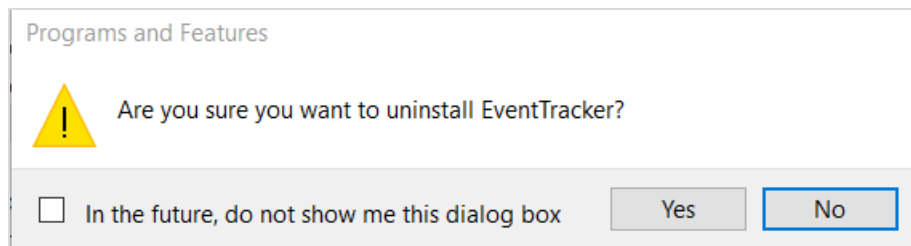
## 8 Uninstalling Netsurion Open XDR

Perform the following procedure to uninstall Netsurion Open XDR via Control Panel.

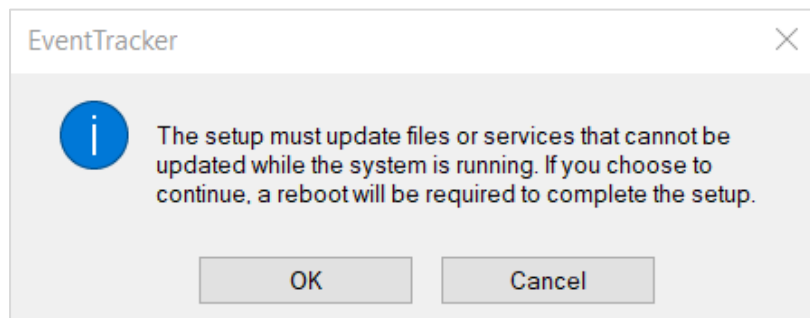
1. Go to **Start > All Programs > Control Panel** and click **Add or Remove Programs**.
2. In the **Add or Remove Programs**, search, and right-click **EventTracker**, and then click **Uninstall** to uninstall Netsurion Open XDR.

Name	Publisher	Installed On	Size	Version
Azure Data Studio	Microsoft Corporation	7/19/2022	567 MB	1.36.2
Browser for SQL Server 2019	Microsoft Corporation	1/12/2023	11.0 MB	15.0.2000.5
EventTracker	Netsurion LLC	1/12/2023	684 MB	9.4
Google Chrome	Google LLC	1/11/2023		109.0.5414.75
IIS URL Rewrite Module 2	Microsoft Corporation	1/12/2023	1.80 MB	7.2.1952
Microsoft Access database engine 2010 (English)	Microsoft Corporation	1/12/2023	110 MB	14.0.7015.1000
Microsoft Help Viewer 2.3	Microsoft Corporation	1/12/2023	12.1 MB	2.3.28307

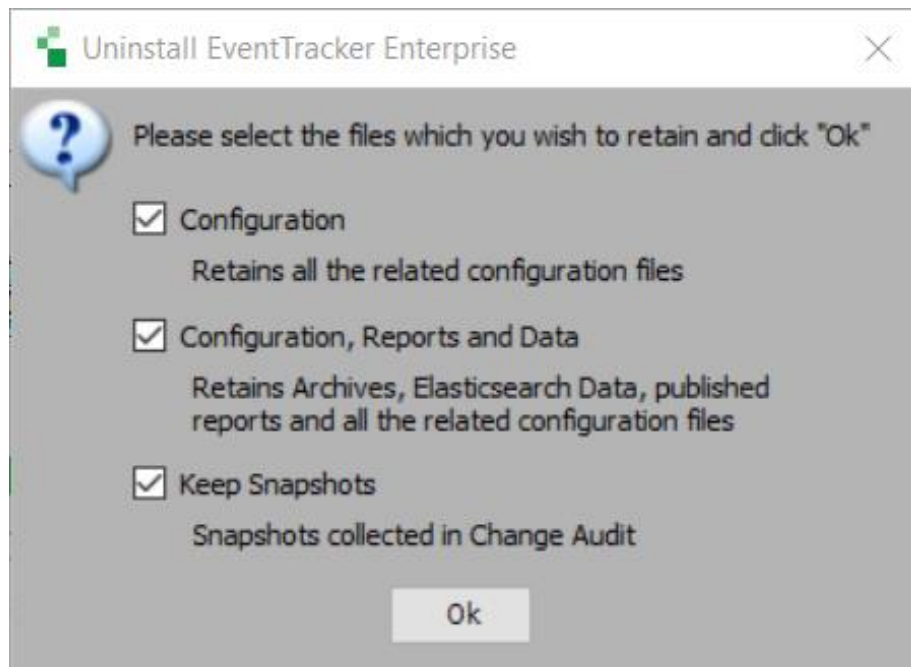
3. A message window pops up to confirm the uninstallation. Click **Yes** to confirm.



4. Netsurion Open XDR pops up a message window stating reboot the system to complete the setup. Click **OK** to proceed.



- In the Uninstall EventTracker Enterprise window, select the required configuration files check boxes to retain the **Configuration, Reports, Elastic Data and Snapshots** files and click **OK**.



## 9 Ports in Netsurion Open XDR

Netsurion Open XDR Module	Port(s)
Netsurion Open XDR Sensor	14506/TCP
Windows Receiver	14505(TCP/UDP) - Optional and multiple VCP's can be configured
Syslog Receiver	514(UDP/TCP) can be configured to any number of ports
Collection Master	14507/TCP - Optional and can be configured to any TCP port
Correlation Receiver	14509/TCP
EventTracker – Change Audit Sensor	14502 (TCP) - To transfer snapshot between client and Server. 14508 (TCP) - Used for real-time comparison of any system with the golden snapshot located at the server.
License Server	14503/TCP
EventTracker Active WatchList	14504

### Note:

In case the user creates multiple Virtual Collection Points, ensure the port used does not contradict with the Default ports used.

## 10 URL or Domain Accessed by Netsurion Open XDR

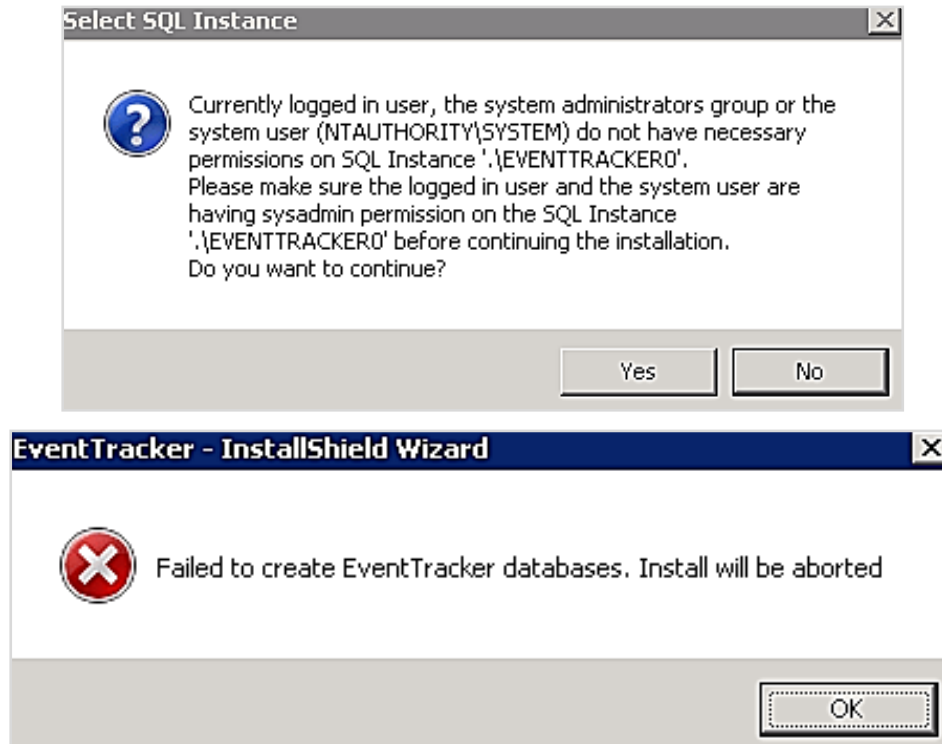
URL/Domain	Port/Protocol/Direction	Purpose
*.eventtracker.com *.netsurion.com	443/TCP/Outbound	Download the XDR platform updates and DSI
threatcenter.netsurion.com threatcenter.eventtracker.com	443/TCP/Outbound	Netsurion Threat Center
nsrl.eventtracker.com	9120/TCP/Outbound	Netsurion NSRL server (Hash IOC Lookup)
certificates.eventtracker.com	443/TCP/Outbound	Netsurion Licensing server
ipinfo.io	443/TCP/Outbound	Load the map in Machine Learning dashboard
geolite.maxmind.com	80/TCP/Outbound	Download the Geolocation details in the Attackers Dashboard
maps.google.com	443/TCP/Outbound	Load the map in the Attackers Dashboard
virustotal.com	443/TCP/Outbound	IOC lookup from Application Control
hybrid-analysis.com	443/TCP/Outbound	IOC lookup from Application Control
whois.domaintools.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
exchange.xforce.ibmcloud.com api.xforce.ibmcloud.com xforce-api.mybluemix.net	443/TCP/Outbound	IOC lookup from Threat Dashboard
rules.emergingthreats.net	443/TCP/Outbound	IOC lookup from Threat Dashboard
otx.alienvault.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
ipvoid.com	80/TCP/Outbound	IOC lookup from Threat Dashboard
senderbase.org talosintelligence.com	443/TCP/Outbound	IOC lookup from Threat Dashboard
app.recordedfuture.com	443/TCP/Outbound	IOC lookup from Threat Dashboard

## 11 Troubleshooting

### 11.1 Known Issues while installing Netsurion Open XDR 9.4

The following issues are related to Netsurion Open XDR 9.4 Pre-Installer only.

1. After the admin (A) completes the pre-installation tasks, the user (B) continues to complete the installation on the same system and encounters the following message.



#### Solution

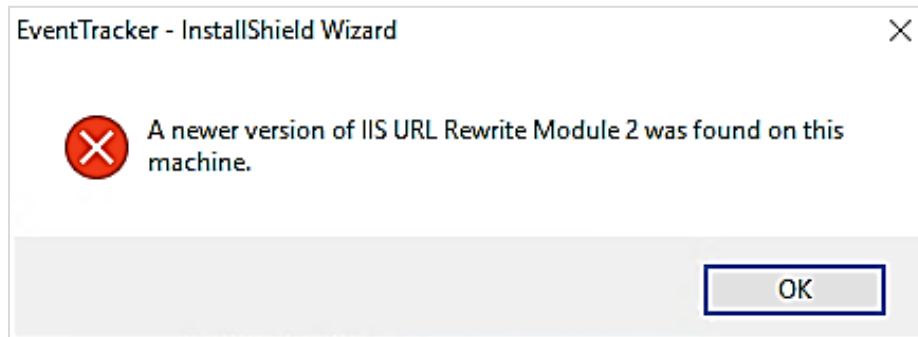
This issue arises when two users alternate while installing the application. As a result,

- make sure the admin user who started the installation finishes installing the application.
- make sure that the logged in user and the system user have the sysadmin privileges on the SQL instance.

#### Note

Refer to [User Permission on MS SQL Server](#) for detailed instructions on granting sysadmin privilege.

- Steps to follow for the below error message.



### Solution

Click **OK** and proceed with the installation.

## 11.2 Frequently Asked Questions

<b>Query</b>	User unable to login to Netsurion Open XDR.
<b>Cause</b>	Issue with querying Active Directory to authenticate the user
<b>Solution</b>	<p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Go to the &lt;INSTALL_PATH&gt;\EventTrackerWeb\Bin folder.</li> <li>Run the executable “<b>ActiveDirectoryAuthenticationTypes.exe</b>” file.</li> <li>Select the following flags and click <b>Apply</b>. <ul style="list-style-type: none"> <li><b>Delegation, Secure and Signing</b> (in the section “<b>Use the below flags to authenticate while logging in from Web GUI</b>”)</li> <li><b>Negotiate, Signing and Sealing</b> (in the section “<b>Use the below flags to authenticate while using “EventTracker Configuration” or “Update Users List” utility</b>”)</li> </ul> </li> <li>Then, re-run the EventTracker Configuration utility.</li> </ol>

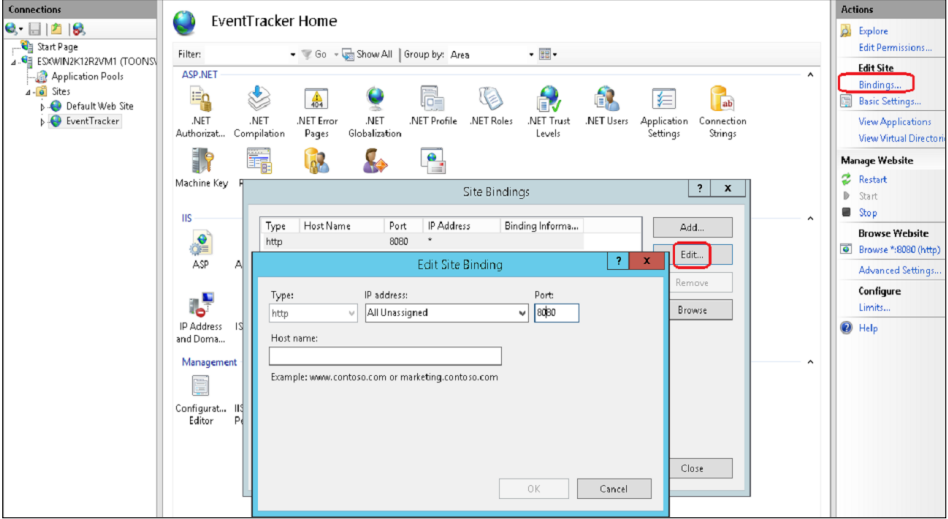
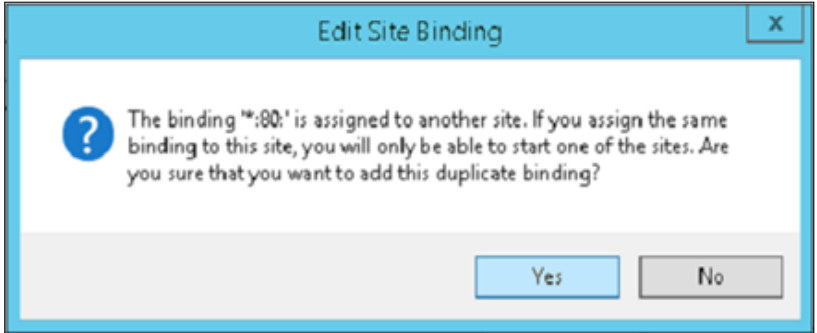
<b>Query</b>	User unable to login to Netsurion Open XDR
<b>Cause</b>	Identity impersonation
<b>Solution</b>	<p>Perform the following steps.</p> <ol style="list-style-type: none"> <li>Verify if the “HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\ASPNET_SETREG” registry hive has values (such as, Impersonate, username, and password) present in it.</li> <li>If not, then run the following command by launching the Microsoft Windows Command Prompt via “<b>Run as administrator</b>”. <ul style="list-style-type: none"> <li>Go to &lt;INSTALL_PATH&gt;\EventTrackerWeb\Bin directory.</li> </ul> </li> </ol>

- Run `aspnet_setreg.exe -k:"SOFTWARE\\Prism Microsystems\\EventTracker\\Temp" -u:"username" -p:"password"`.

**Note:**

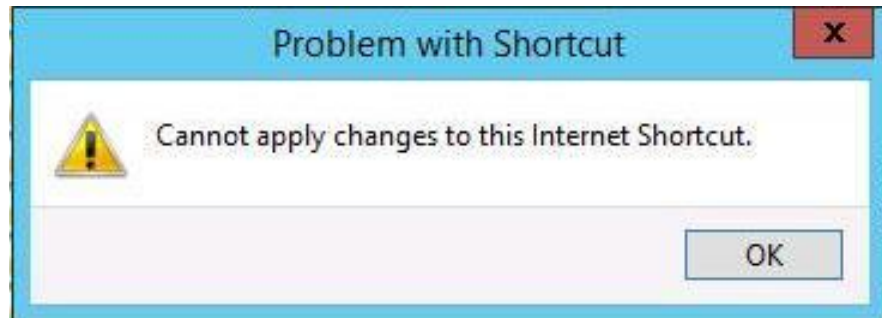
Replace “username” and “password” with either domain or local admin credentials.

- Then, re-run the EventTracker Configuration utility.

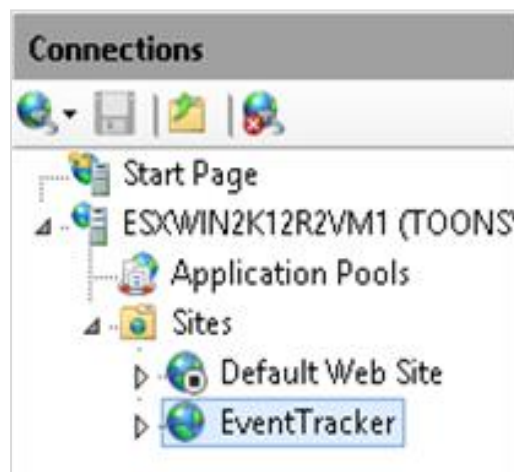
<p><b>Query</b></p>	<p>How to modify Netsurion Open XDR webserver port</p>
<p><b>Scenario</b></p>	<p>If Netsurion Open XDR installation is using IIS, follow the steps to use port 80:</p>
<p><b>Solution</b></p>	<ol style="list-style-type: none"> <li>Go to <b>IIS Manager</b> and expand <b>Sites</b> and click the <b>EventTracker</b> site.</li> <li>In the <b>Actions</b> panel located on the right, in the <b>Edit site</b>, click <b>Bindings</b>.</li> <li>In the <b>Site Binding</b> Window, select the listed entry and click <b>Edit</b>.</li> <li>In the <b>Edit Site Binding</b> window, modify the existing port number from <b>8080</b> to <b>80</b> and click <b>OK</b>.</li> </ol>  <ol style="list-style-type: none"> <li>A message window pops up to confirm the modified site binding details. Click <b>Yes</b> to confirm.</li> </ol> 



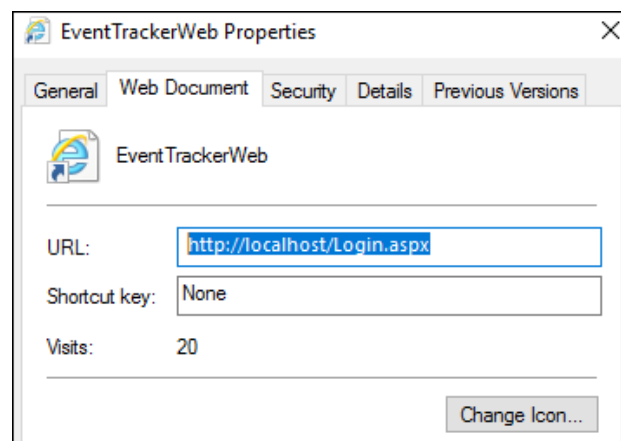
If the issue occurs with Shortcut message stating **Cannot apply changes to this Internet Shortcut**,



6. Then copy the path...\**Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url** to a different location. Modify and update the file in the ...\**Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url**.
7. Next, stop the **Default Web Site** and start the **EventTracker** site as illustrated in the following image.



8. Then, go to...\**Prism Microsystems\EventTrackerWeb** and right-click **EventTrackerWeb.url** (Internet Shortcut) and click **Properties**, and then modify the URL as illustrated in the following image.



<b>Query</b>	Prerequisites for displaying the Attacks Dashboard.
<b>Required</b>	Access needs to be provided for these websites.
<b>Solution</b>	<p>Attackers Dashboard feature uses the following websites:</p> <ul style="list-style-type: none"> <li>▪ <b>maps.google.com</b></li> <li>▪ <b>Ipvoid.com</b></li> <li>▪ <b>IBM XFE</b></li> </ul>

## About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Netsurion Open XDR 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](http://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	<a href="mailto:SOC@Netsurion.com">SOC@Netsurion.com</a>
Managed XDR Enterprise MSPs	<a href="mailto:SOC-MSP@Netsurion.com">SOC-MSP@Netsurion.com</a>
Managed XDR Essentials	<a href="mailto:Essentials@Netsurion.com">Essentials@Netsurion.com</a>
Software-Only Customers	<a href="mailto:Software-Support@Netsurion.com">Software-Support@Netsurion.com</a>

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