![Netsurion logo]

Upgrade Guide

Upgrade the Netsurion Open XDR platform

From version 9.3 to 9.4

Publication Date:

April 07, 2023

Abstract

The purpose of this document is to help the existing users of the Netsurion Open XDR platform to upgrade to a newer version 9.4.

Note:

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

Audience

This guide is for all the admin users of the Netsurion Open XDR platform v9.3 who intend to upgrade to the Netsurion Open XDR platform v9.4.

Product Terminology

The following are the terms 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.

- The term "Data Source Integrations" refers to Knowledge Packs.

- The term "Sensor" refers to Agent.

Table of Contents

1 Introduction

This guide provides instructions for upgrading the existing Netsurion's Open XDR platform. Recommended to go through the entire procedures thoroughly before commencing the upgrade process.

1.1 System Requirements

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

1.1.1 Hardware Requirements

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

> **IMPORTANT**
>
> The Netsurion Open XDR platform version v9.4 installation is supported on 64-bit Operating System only.

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

> **Note**
>
> Recommended to have 2 Partitions in Disk 1 (SSD); Partition 1 for Operating System and Partition 2 for the Open XDR platform and Search cache. The Archives are stored in a NON-SSD disk (for example, Disk 2).

1.1.2 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 the Open XDR platform v9.4 Installation and all other protocols must be disabled.

Note:

Recommended not to install the Open XDR platform on a Domain Controller. Run the Open XDR Manager Console on a dedicated Microsoft Windows Server.

Note:

During the upgrade process, SQL and Elastic will be upgraded to the recommended version.

Note:

Only SQL Express edition is upgraded during the upgrade process. If the installed SQL version is not an Express edition, then the SQL needs to be upgraded manually before upgrading the Netsurion platform.

1.2 Supported Upgrade References

For more information on license keys or license certificates, contact Software-Support@Netsurion.com.

Only SQL 2019 (Express or licensed version) is supported when upgrading from v9.3 to v9.4. SQL Upgrade Link: https://learn.microsoft.com/en-us/sql/database-engine/install-windows/upgrade-sql-server?view=sql-server-ver15

Estimated time required for the upgrade and to monitor the successful upgrade.

It takes you between 60 and 90 minutes to complete the upgrade process.

1.3 Prerequisites

- Must have the latest Windows updates installed.
- The Netsurion Open XDR platform version below v9.3 must first be upgraded to v9.3.
- The Netsurion Open XDR platform version v9.3 must have the latest available updates.

1.4 Common Procedures for all Upgrades

Before beginning the upgrade process, make certain that you have all the necessary components in place.

1.4.1 Pre-upgrade process

- It is recommended to first export all the custom settings using Export Import Utility, and then install the latest Open XDR platform version v9.4.

  > **Note:**
  >
  > There is no need to export all policy settings because all the categories included in any earlier versions will be retained.

- Recommended to upgrade the Manager before proceeding with the upgrade of the sensors.

- For CM and CP set up, upgrade CM (Collection Master) first, and then upgrade CP (Collection point).

- Before the upgrade process, back up the DSI (Data Source Integration) integrator folder located in the Manager installed path **(Install path\Prism Microsystems\EventTracker\Agent).**

  > **Note:**
  >
  > Ensure to disable all the integrator related services, tasks from the windows service and the task manager as applicable. Refer to How to Reconfigure Integrator During Upgrade Netsurion for more details.

- For v9.3, back up the database from **the Open XDR platform Control Panel** > **Diagnostics** interface.

  > **Note:**
  >
  > Refer Generating a backup of the Database details section for more details.

- If your company logo is incorporated into the Open XDR platform, then take a backup of the .jpg file of your company logo before uninstalling the Open XDR platform. It is required to replace the backed up image file after installing the Open XDR platform.

- Backup all **Custom Categories** such as, Alerts (as well as verify the 'Export E-mail Settings' check box), Filters, and Reports using the Export Import Utility.

- Make note of the custom changes made in the 'Trusted List' (**Agent Configuration** > **Network Connections** > **Suspicious Traffic Only (SNAM)** > **Trusted List**).

1.4.2 Post-upgrade process

- If you had configured SSL (HTTPS) in the earlier version, then the configuration details will not get retained after the upgrade to v9.4.

  > **Note:**
  >
  > Ensure to reconfigure the SSL (HTTPS). Refer Securing IIS Web Server with SSL guide for more details.

- If the user has configured the JSON file in DLA Manager in the earlier version, the user will need to reconfigure it after upgrading.

- After upgrading the Collection Master, the user may notice inconsistencies in the Reports/ Log Search/ Cab received status (Admin > Collection Master > Archives status) until the database migration is complete.

- After upgrading the Collection Point, the user may not be able to view the exact cab transfer status in (Admin > Collection Point Configuration > Manage archives) until the database migration is complete.

> **Note:**
>
> It is important to spend some time verifying all the 'Scheduled Reports' that are generated.

2 Upgrading to the Netsurion Open XDR platform version v9.4

The Upgrade process is parted into two,

Upgrade Process - Quick View	is for the users who are quite familiar with the upgrade procedure and the fundamental system configuration details.
Upgrade Process - Detailed View	is for the users who are performing the upgrade for the first time and includes a step-by-step procedure.

2.1 Upgrade Process - Quick View

This section provides a quick insight to the upgrade process.

> **Note:**
>
> This section is for the system administrators and the experts familiar with the Open XDR platform and the upgrade process. It is presumed that the user has enough knowledge of the system and the configuration process.

Upgrading to the Netsurion Open XDR platform v9.4

1. Uninstall the previous version v9.3 of the Open XDR platform.

   > **Note:**
   >
   > Recommended to retain the old configuration and data before uninstalling the version v9.3. Refer to the Pre-upgrade process section for more details.

2. Restart the Open XDR manager server or system.

3. Run the v9.4 Open XDR installation package and click **Yes** to proceed with the upgrade.
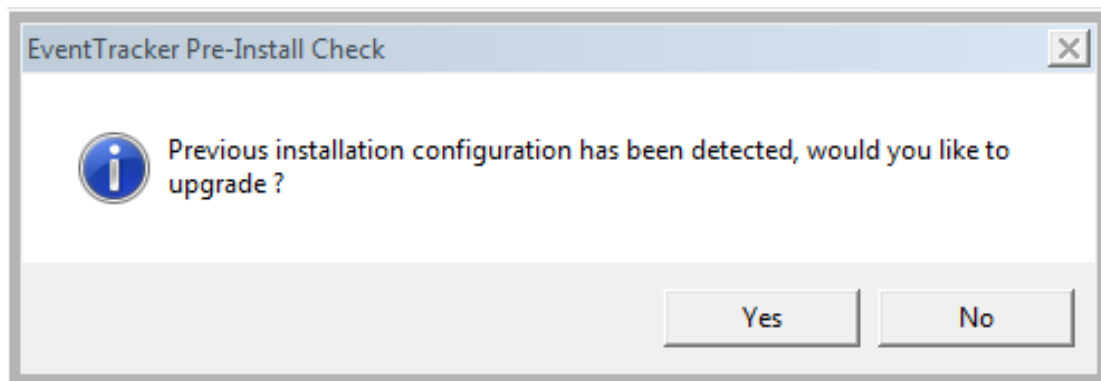
4. Configure the service accounts if the archives or reports are stored in the network path.

   > **Note:**
   >
   > Refer Configuring Service Accounts section for more details.

5. Update the Trusted List with the changes you noted before upgrading the Open XDR platform.

   > **Note:**
   >
   > Refer the procedure specified in Pre-upgrade process section for more details.

6. Upgrade all windows sensors using '**System Manager'**.

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

7. After upgrading to the Open XDR platform v9.4, place the DSI integrator folder retained prior to the upgrade process in the Manager installed location.

> **Note:**
>
> Ensure to start all the integrator related services, tasks from the windows service and the task manager as applicable. Refer to How to Reconfigure Integrator During Upgrade Netsurion for more details. Refer to the Pre-upgrade process section for more details.

2.2 Upgrade Process - Detailed View

This section describes the entire upgrade procedure.

> **Note:**
>
> This section is for the users upgrading the Open XDR platform for the first time.

2.2.1 Generating a backup of the Database
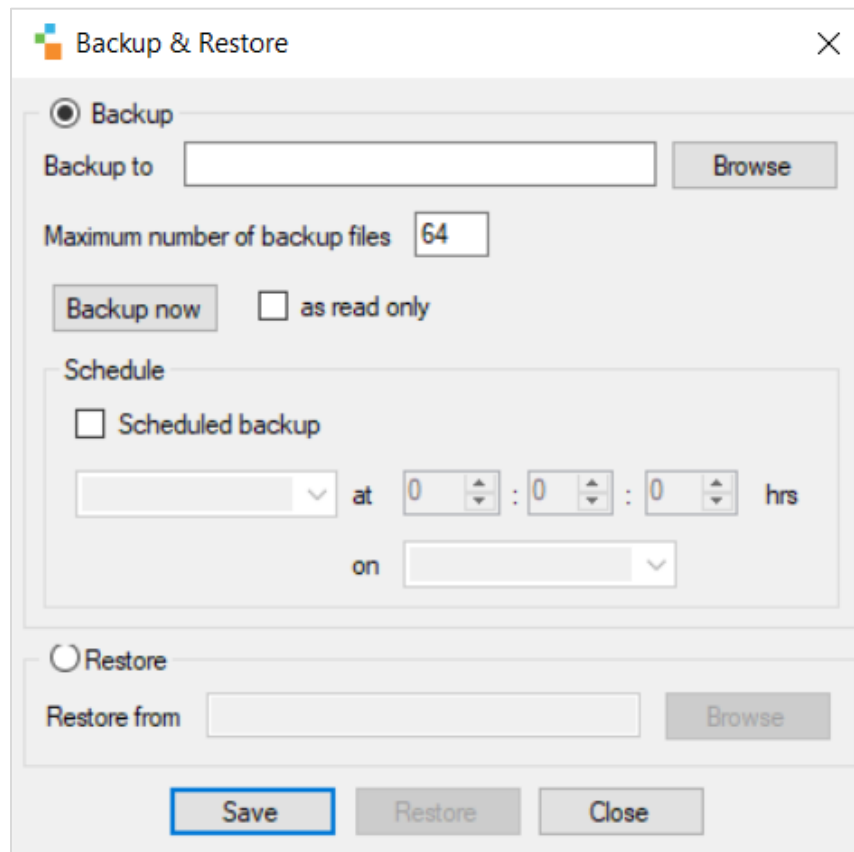
Perform the following procedure to back up the database.

> **Note:**
>
> Refer to the Pre-upgrade process section to retain the old configuration and data.

1. Go to the **Open XDR Control Panel** and double-click **Diagnostics**.

2. In **Diagnostics**, click **Backup** to go to the Backup & Restore window.

3. In **Backup & Restore**, click **Browse** and locate the folder you require to back up and click **Backup now**.

After the backup, navigate to the back up folder and the file generated with the .bkp extension is used for restoring the details.

Close/ terminate all the Open XDR platform components.

- Before upgrading the Open XDR platform to version v9.4, all Open XDR platform components present in the system, such as the Open XDR Control Panel and even RDP (Remote Desktop Protocol) sessions, must be closed or terminated.

- If any of the previous Open XDR platform components is open during the uninstallation, the Open XDR platform prompts you to close the program and then click the **Retry** button to resume the uninstallation process.

2.2.2 Uninstalling the Netsurion Open XDR platform version v9.3

1. Uninstalling the Open XDR platform version v9.3 can be performed in any of the following two ways,

   ▪ Go to **Control Panel** > **Programs** > **Programs and Features**, right-click the Netusrion Open XDR platform **(EventTracker)**, and then click **Uninstall**. (OR),

   ▪ Go to **Start** > **Programs** > **Prism Microsystems**, click the Netusrion Open XDR platform **(EventTracker Control Panel\ EventTracker Configuration)**, and then right-click and click **Uninstall**.

   The Open XDR platform pops-up the **Uninstall EventTracker** window to confim to retain the data and configurations.

2. Keep the default selection to retain the data and configurations, and click **Clean** to proceed with the unistallation process.
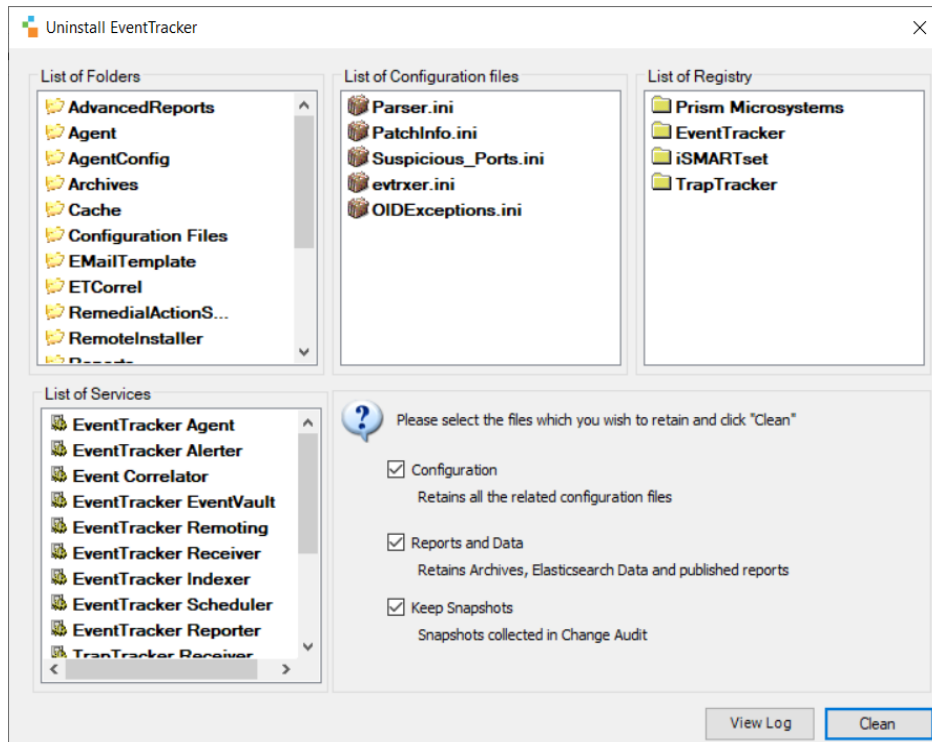
3. Then, click **Yes** to confirm and uninstall the Open XDR platform.
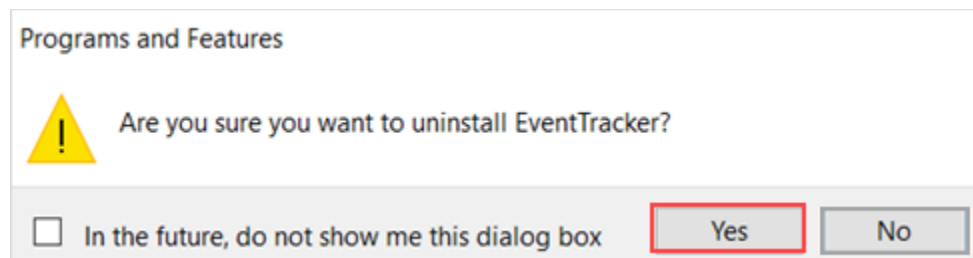
4. After the successful uninstallation of v9.3 Open XDR platform, in the **Uninstall EventTracker** window, click **View Log** to verify the log details.
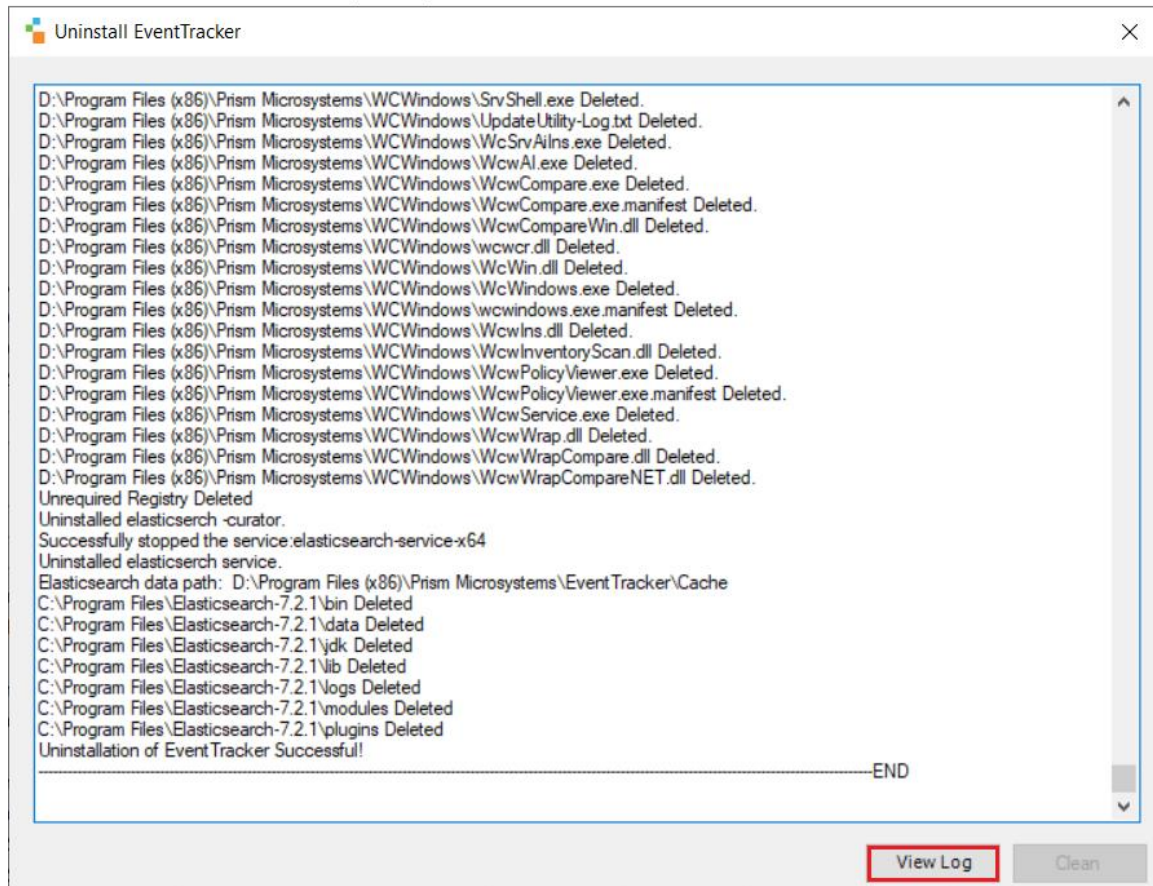
Rebooting the System/ Server

After the unistallation, it is required to restart the Open XDR Manager Server or the System.

Perform the following steps,

1. Close all the open applications on the desktop.

2. Go to **Start** > **Power** and click **Restart** from the drop-down list.

2.2.3 Installing the Netsurion Open XDR version v9.4

1. Run the v9.4 Open XDR installation package via **Run as Administrator**.

2. A pop-up window appears to upgrade the Open XDR platform setup with the previously installed configuration. Click **Yes** to proceed.
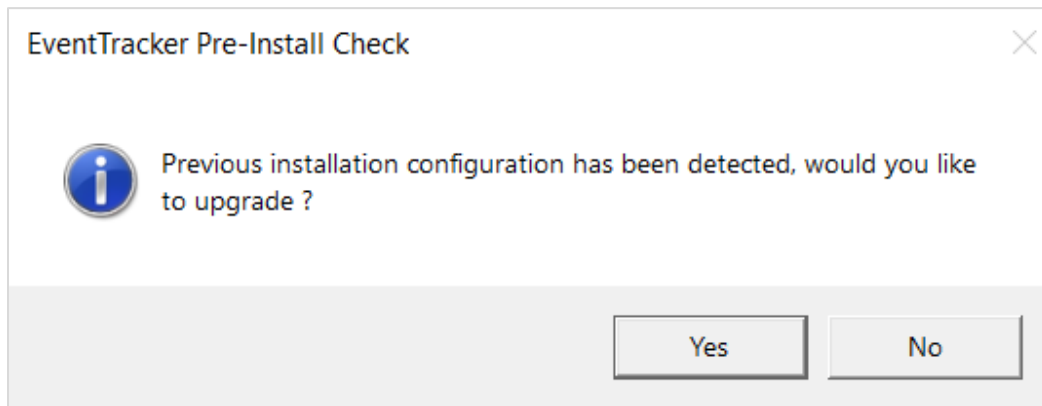
Installation Procedure

The Installation process involves the following procedures,

- ❖ Preinstallation checks
- ❖ EventTracker 9.4 Setup Program
- ❖ Configuring the Open XDR platform version v9.4
- ❖ Configuring Service Accounts

The Netsurion Open XDR platform Preinstall Check

1. The Open XDR platform launches the Pre-Install Check window. Click **Next** to continue with the process.
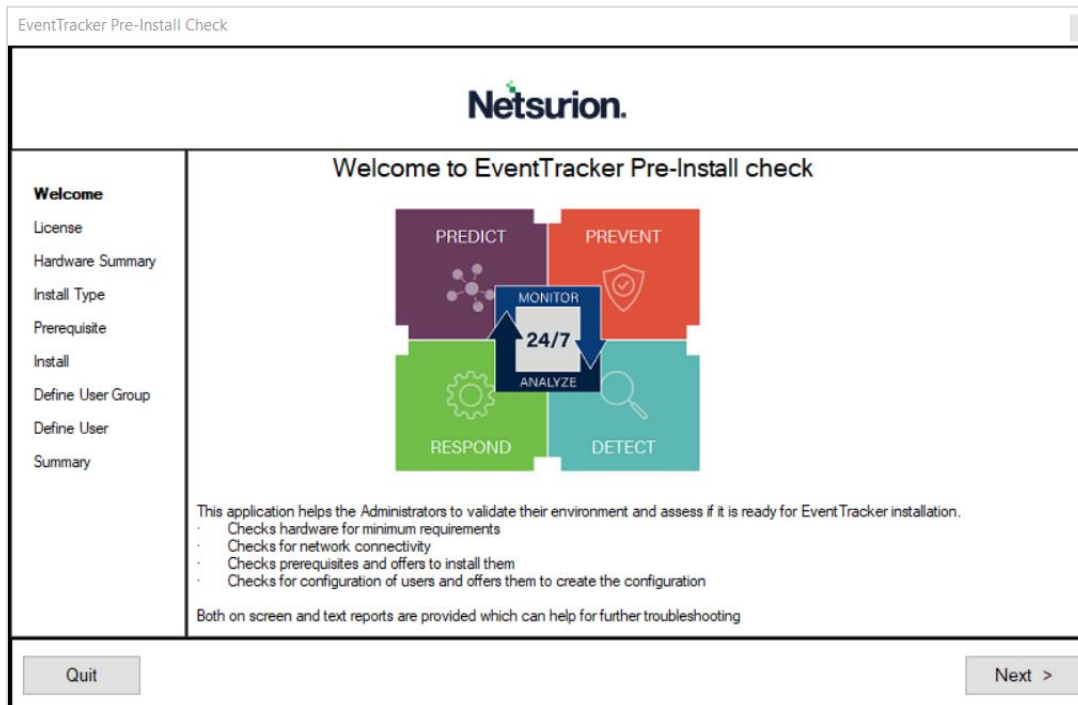
2. In the **License** section, (read the agreement,) click **Accept** to acknowledge and proceed with the process.
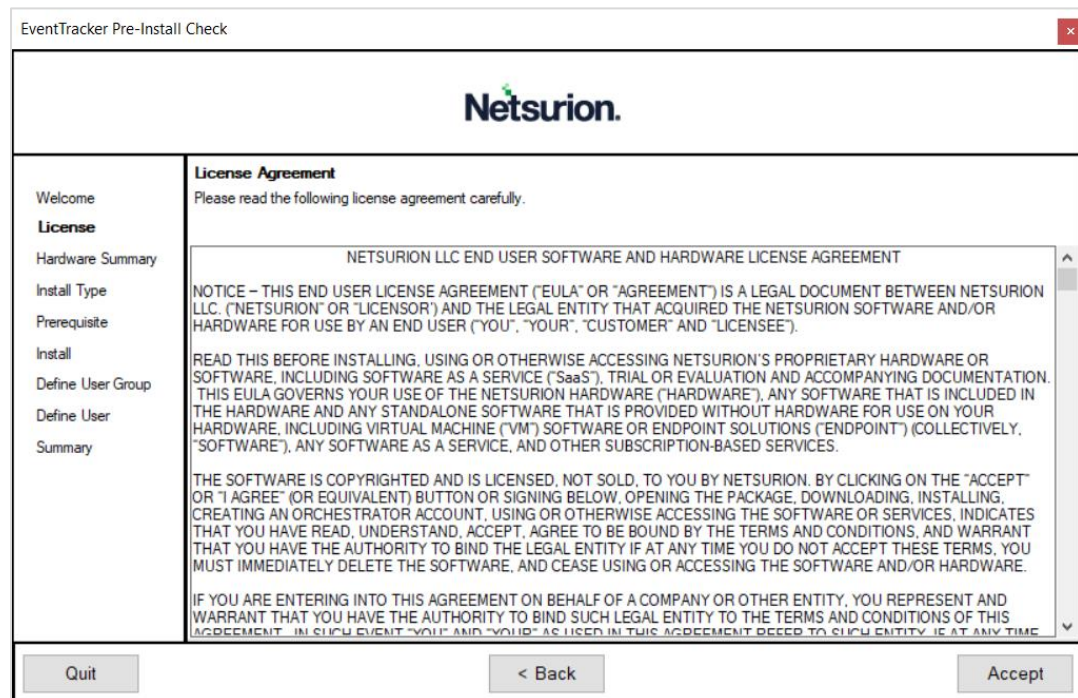
3. In the **Hardware Summary** section, it may take a few seconds to fetch the hardware details and a processing icon appears during the data collection process. Click **Next** to proceed.
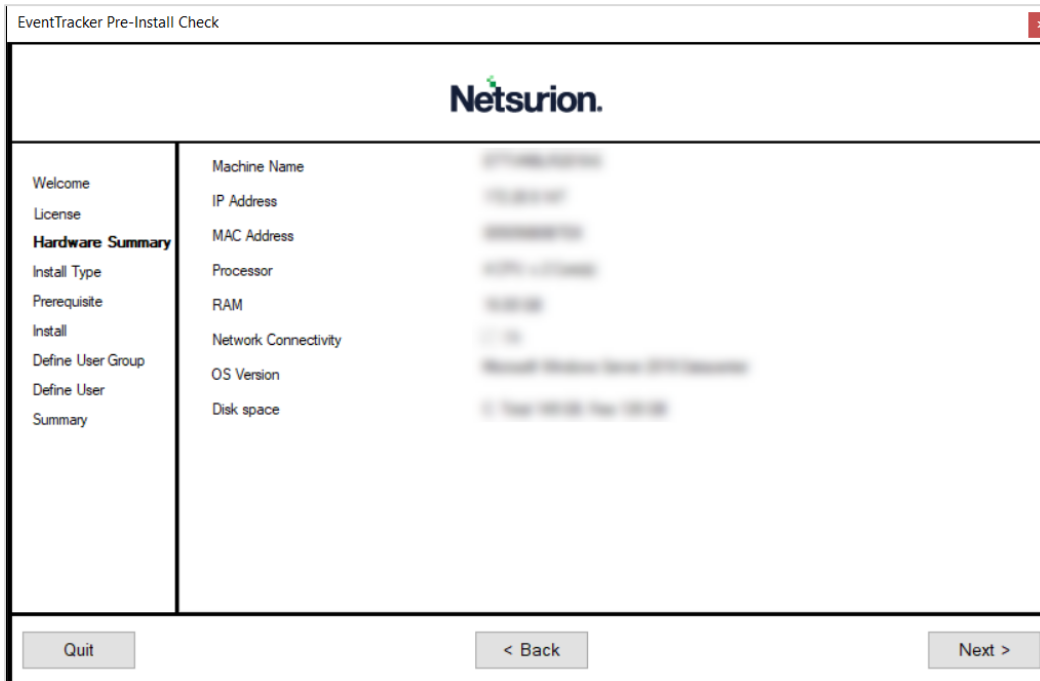
4. In the **Prerequisite** section, click **Next** to proceed with the installation of the softwares that are not installed.

Note:

The **Prerequisite** section lists all of the required softwares, as well as their status (Installed or Not Installed) adjacent to it.
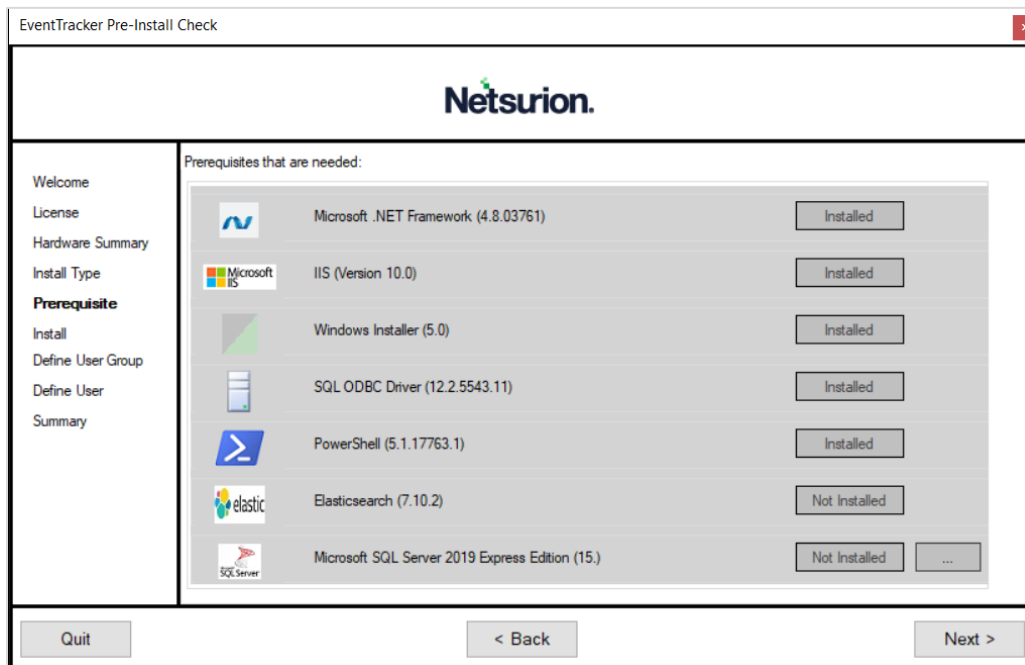
5. In the **Install** section, click **Next** to proceed with the installation of the requisite softwares.

As per the Prerequisite section (in the previous step), the installation status for the Elasticsearch and Microsoft SQL Server 2019 Express Edition is listed as **Not Installed**. As a result, the installation process is carried out for the Elasticsearch and Microsoft SQL Server 2019 Express Edition in the Install section.

Sample Image representation for installing Elasticsearch
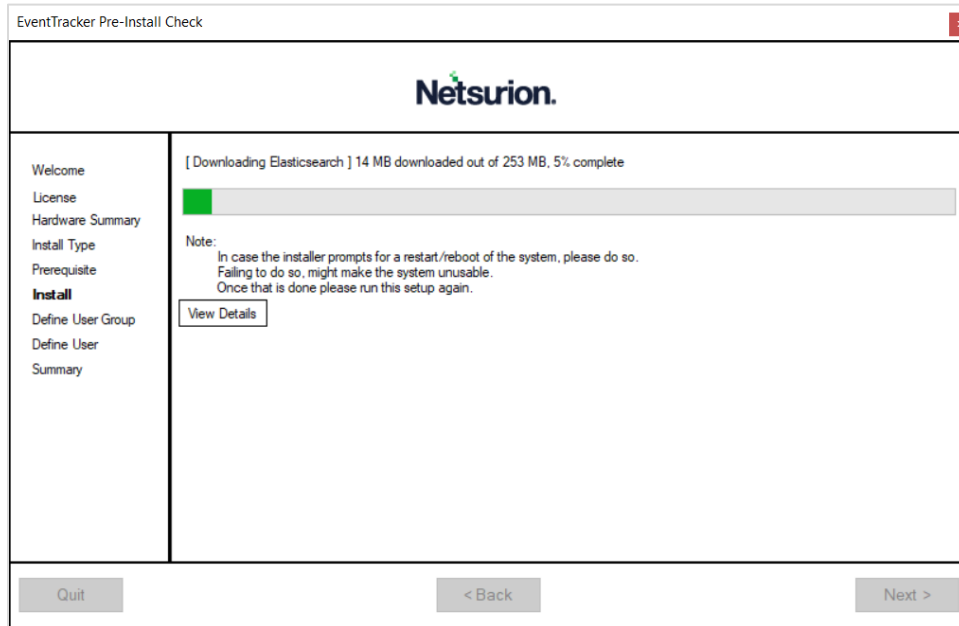
Sample Image representation for installing SQL Server
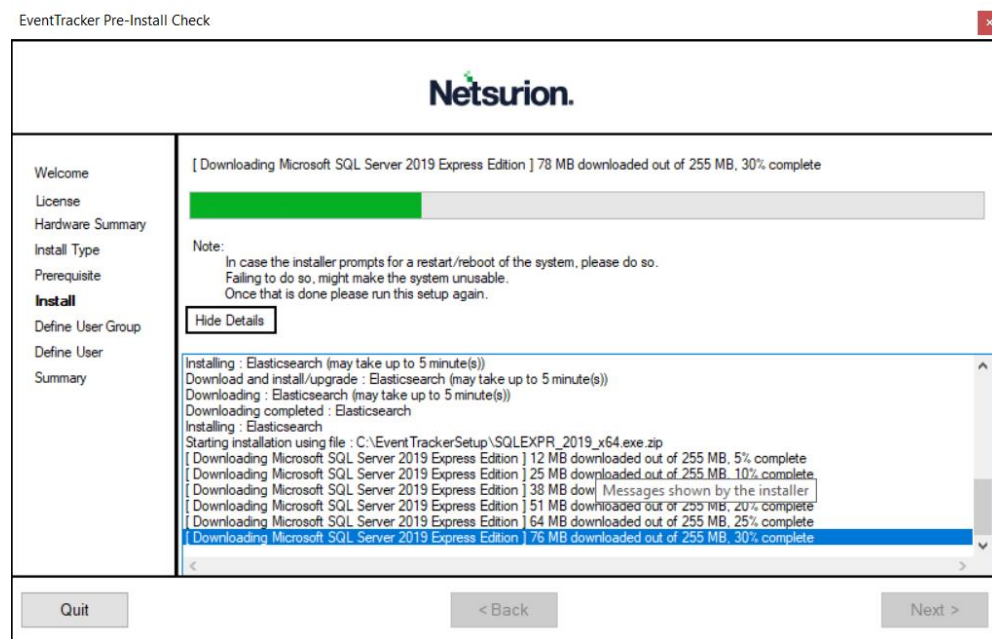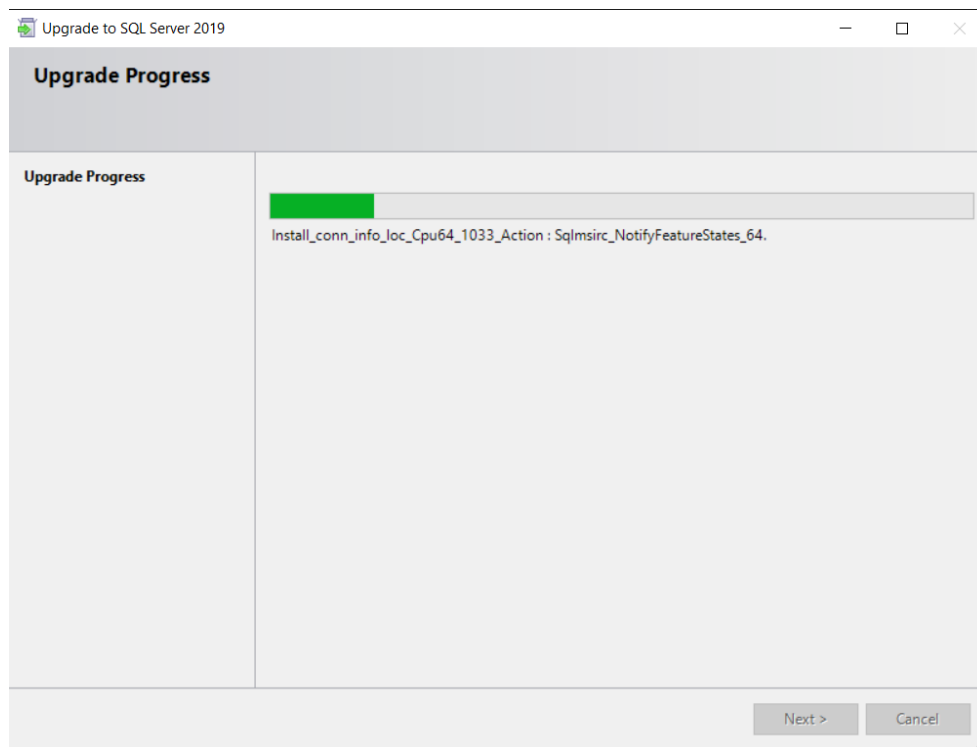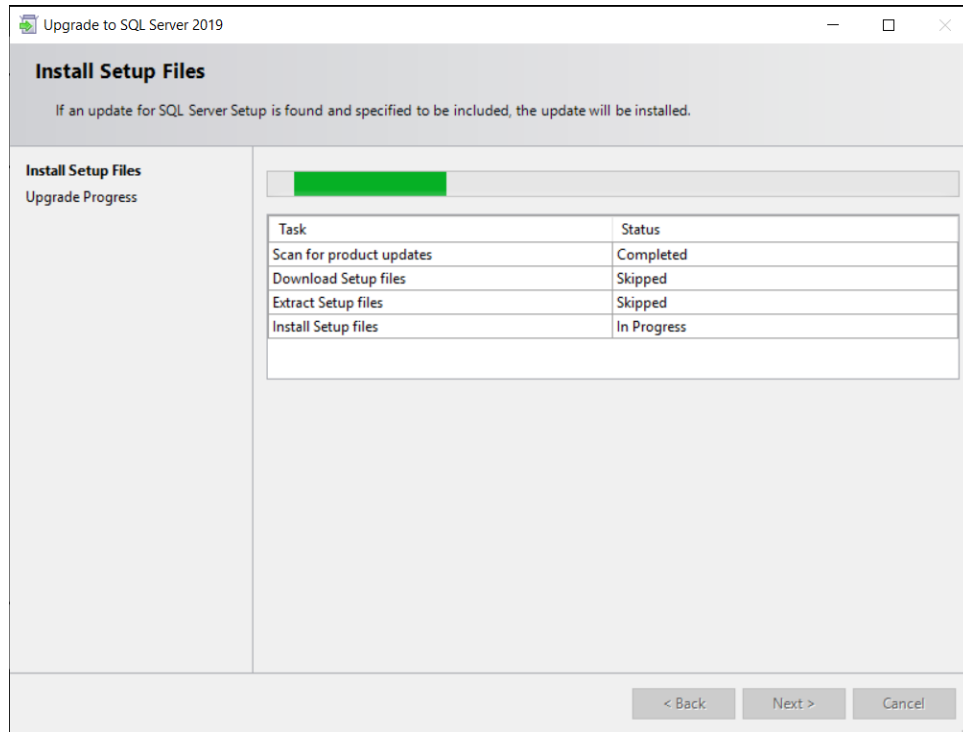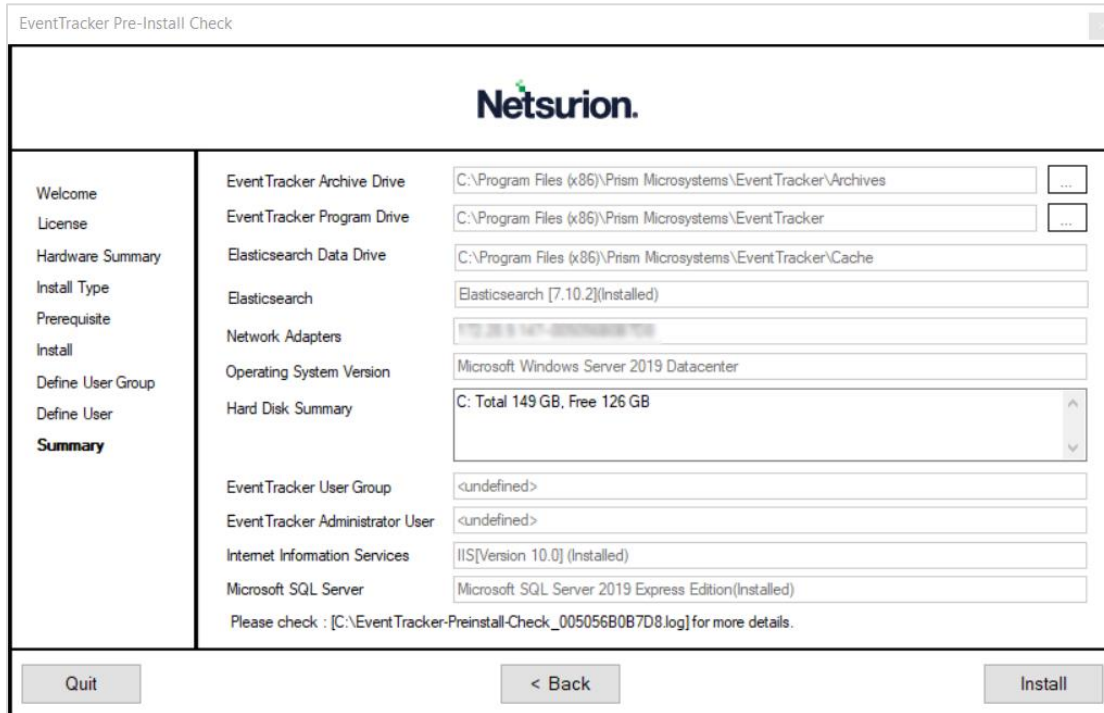
Note:

The **Installation process** varies for different softwares as we see above in the sample representations provided for the Elasticsearch and Microsoft SQL Server 2019 Express Edition.

---

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

EventTracker 9.4 Setup Wizard

The Open XDR platform displays the **EventTracker - InstallShield Wizard**.

1. In EventTracker - InstallShield **Welcome** window, click **Next** to proceed with the Open XDR platform setup process.
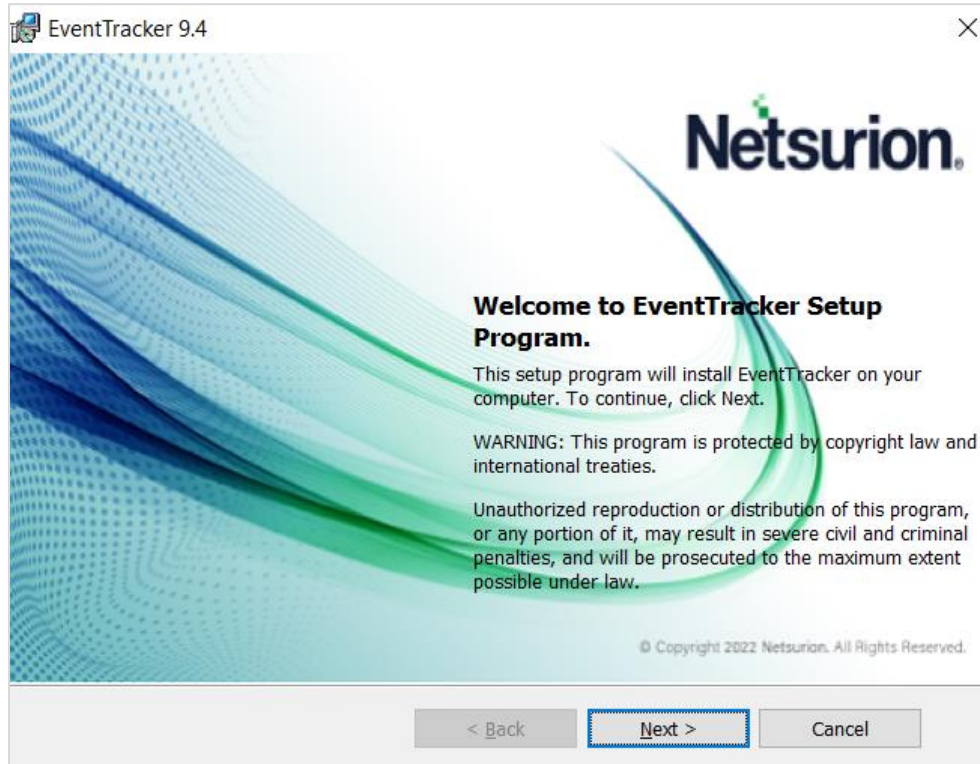
2. In **Select a Certificate File** window, click **Browse** and locate the appropriate certificate file (the file with **.cer** extension), and then click **Next**.
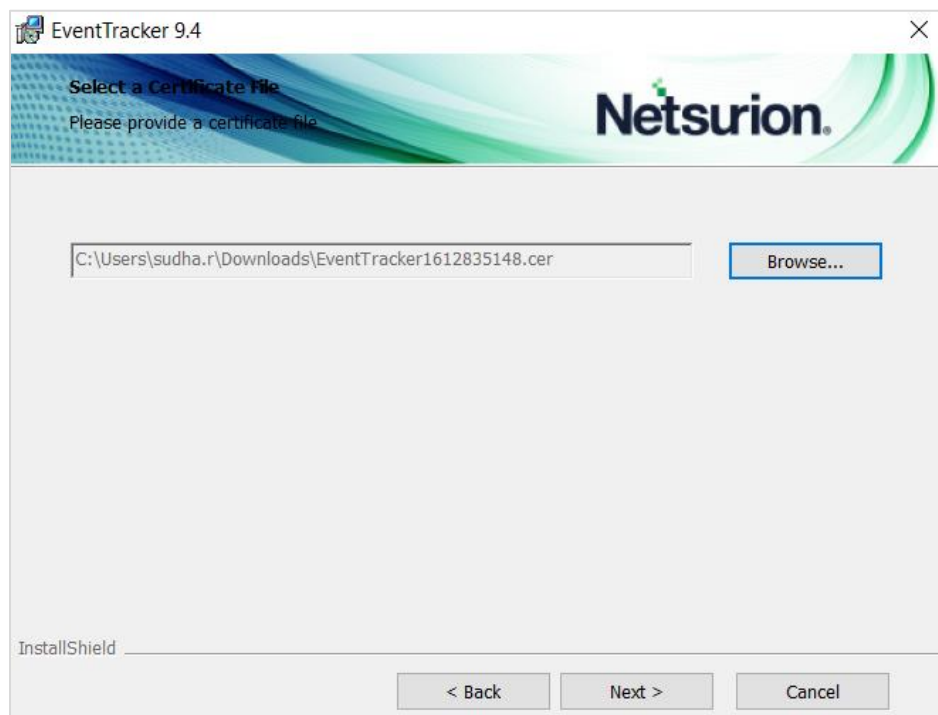
3. In **Select Components** window, select the required component details and click **Next**.
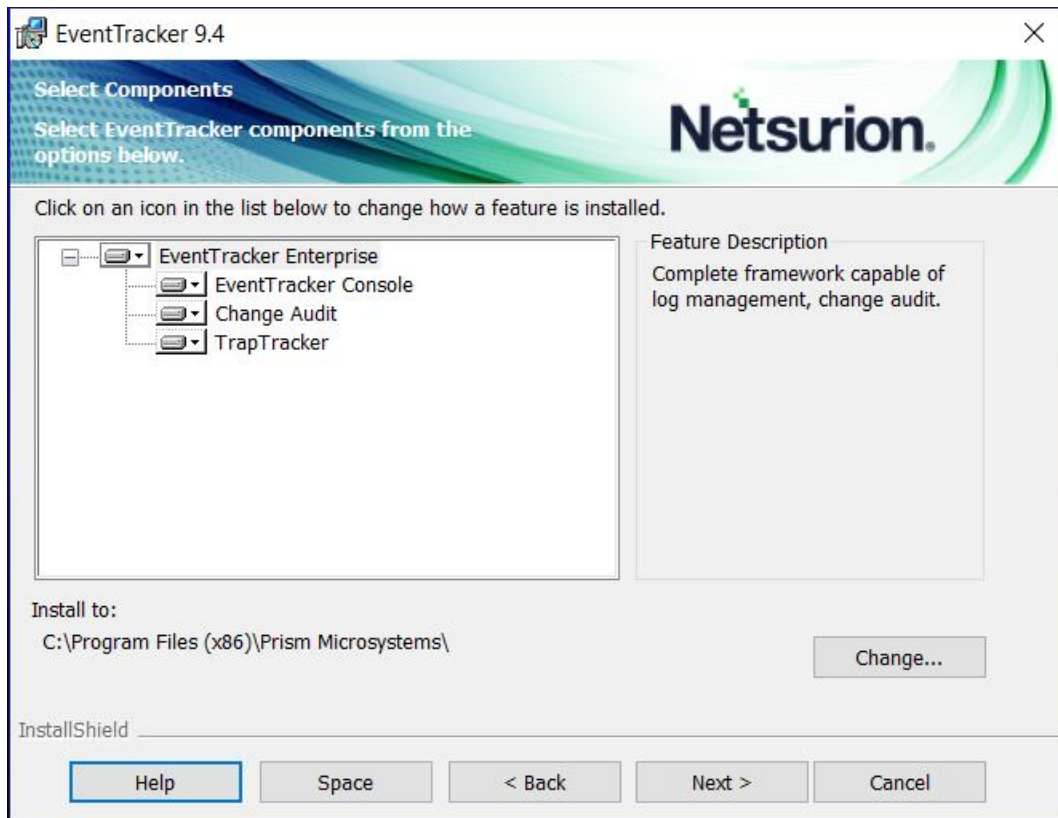
Components	Description
EventTracker Console	Select this component to install the manager console on the target computer.
Change Audit	**Optional component.** ▪ Installing this component enables you to monitor and manage change over the enterprise. ▪ The sensor component will also be installed along with 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.

4. In **Select EventTracker Console Type** window, the previously selected Console Type option will be selected by default (retains the option as opted in version v9.3). Click **Next** to proceed.
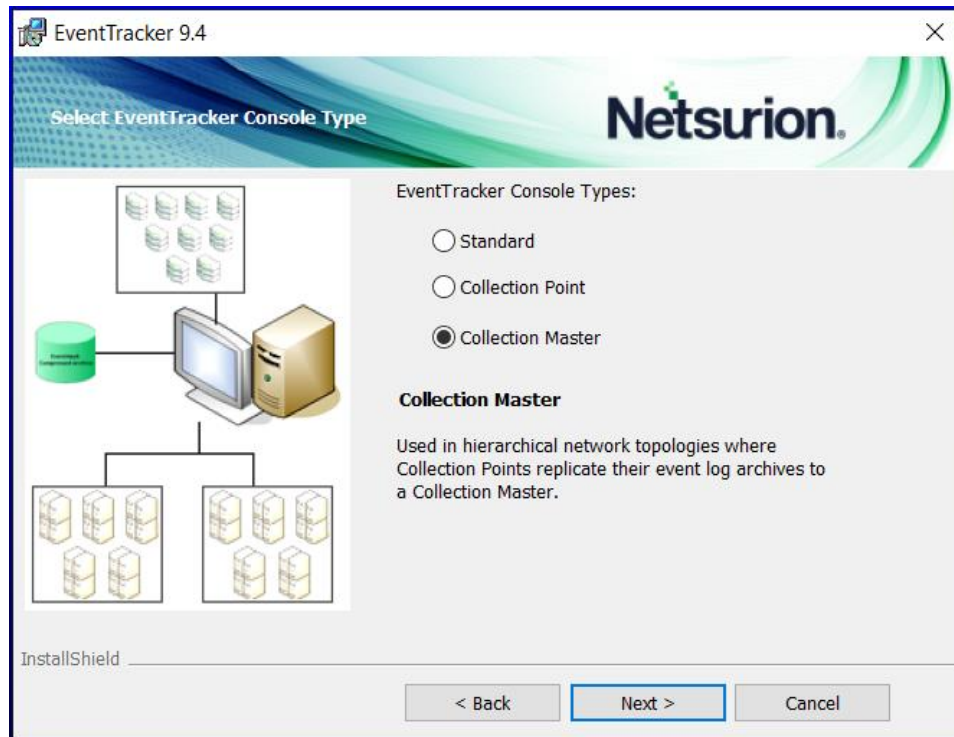
5. The **Ready to Install the Program screen** provides the summary of the details, the installation path, console type, and the selected features. Verify and click **Install** to install the selected components.
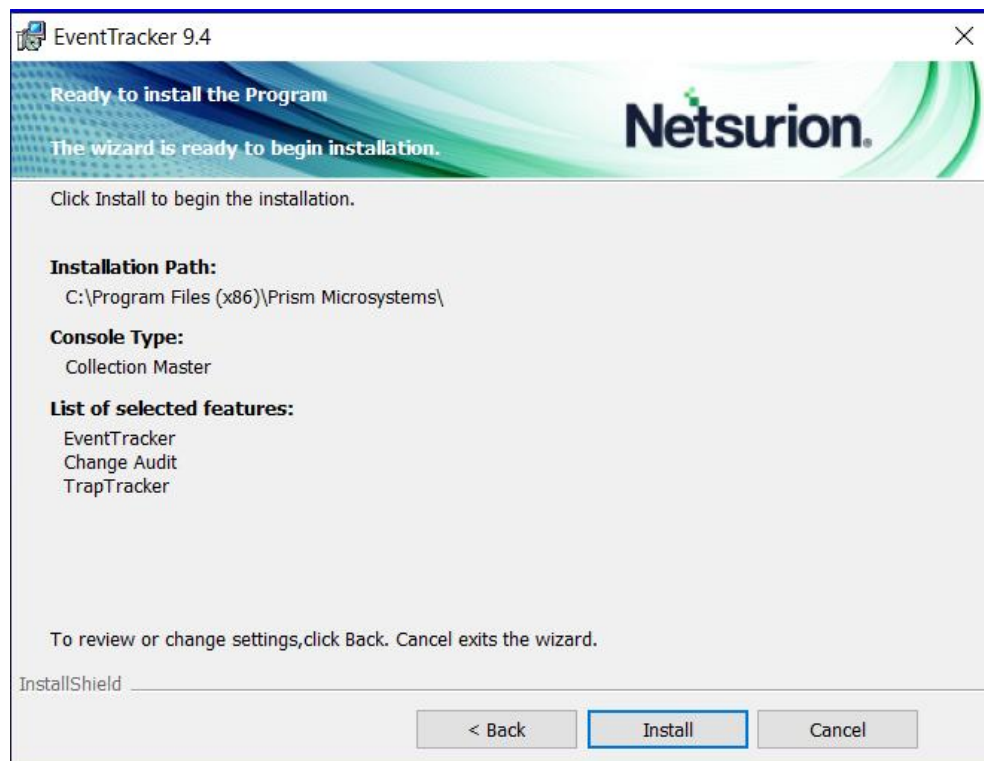
6. In the **Installation is finished** window, select the required option details and click **Finish** to conclude the installation process.
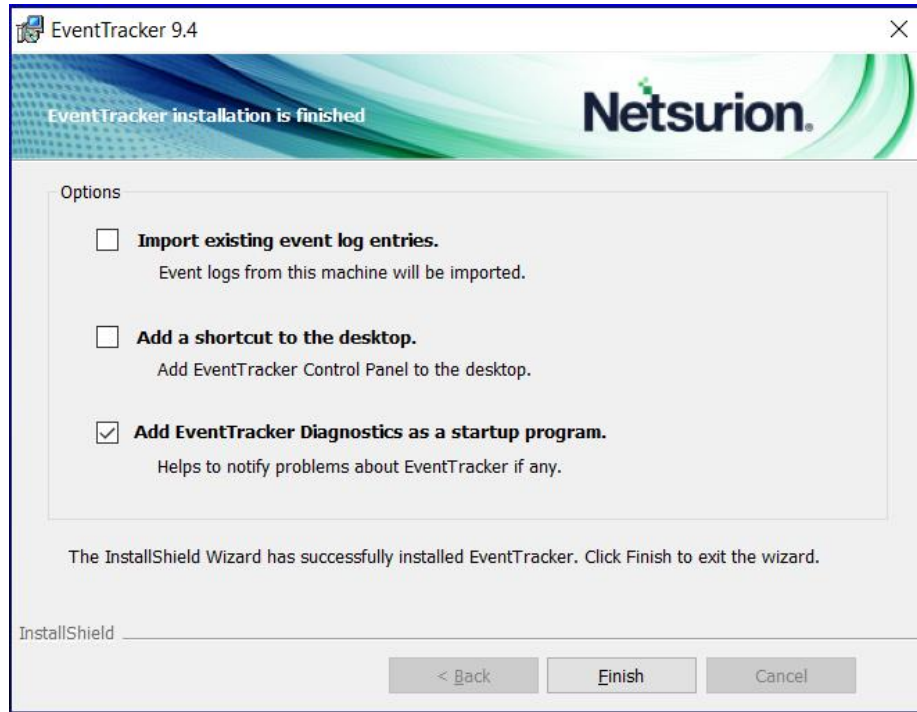
Configuring the Netsurion Open XDR platform version v9.4

1. In the **EventTracker Configuration** interface, specify the appropriate user credentials (the existing) in the **User Name** and **Password** fields, and then click **OK.**
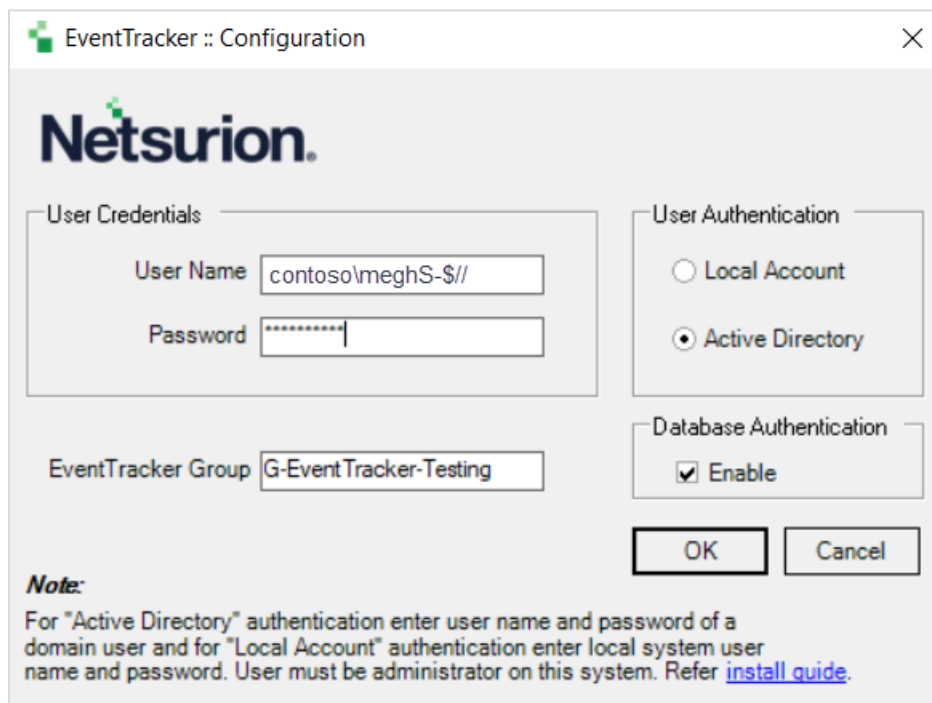
Note:

If required, in **Database Authentication,** select the **Enable** check box to allow authentication for the database.

After successful validation, a message window pops-up stating the credentials successfully validated.

2. Click **OK** to coninue with configuring the application settings.
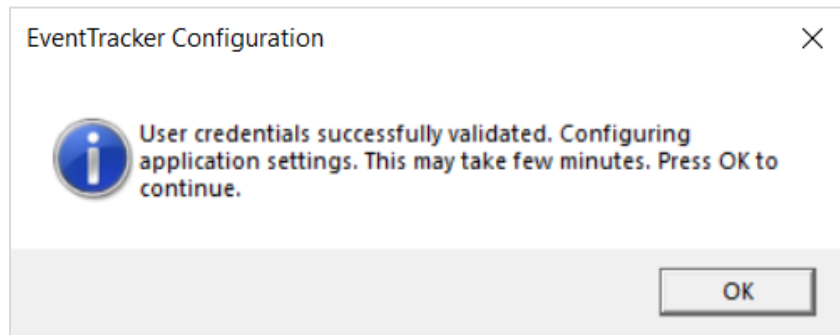
3. Configure the service accounts if the archives or reports are stored in the network path.

Note:

Refer the Configuring Service Accounts section for more details.

4. Verify that the Categories, Alerts, Filters, are updated and intact.

5. After upgrading to the Open XDR platform v9.4, place the DSI integrator folder retained prior to the upgrade process in the Manager installed location.

Note:

Ensure to start all the integrator related services, tasks from the windows service and the task manager as applicable. Refer to How to Reconfigure Integrator During Upgrade Netsurion for more details. Refer to the Pre-upgrade process section for more details.

6. Upgrade all the Windows sensors using the System manager.

Note:

The Open XDR sensor upgrade is necessary to keep the sensors up to date with the manager system.

Note:

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

7. Log in to **the Open XDR platform**, hover over the **Admin** menu and click **Systems** to go to the Systems Manager interface.

---

8. In the **Systems** interface, select the required group or system to upgrade the sensor.
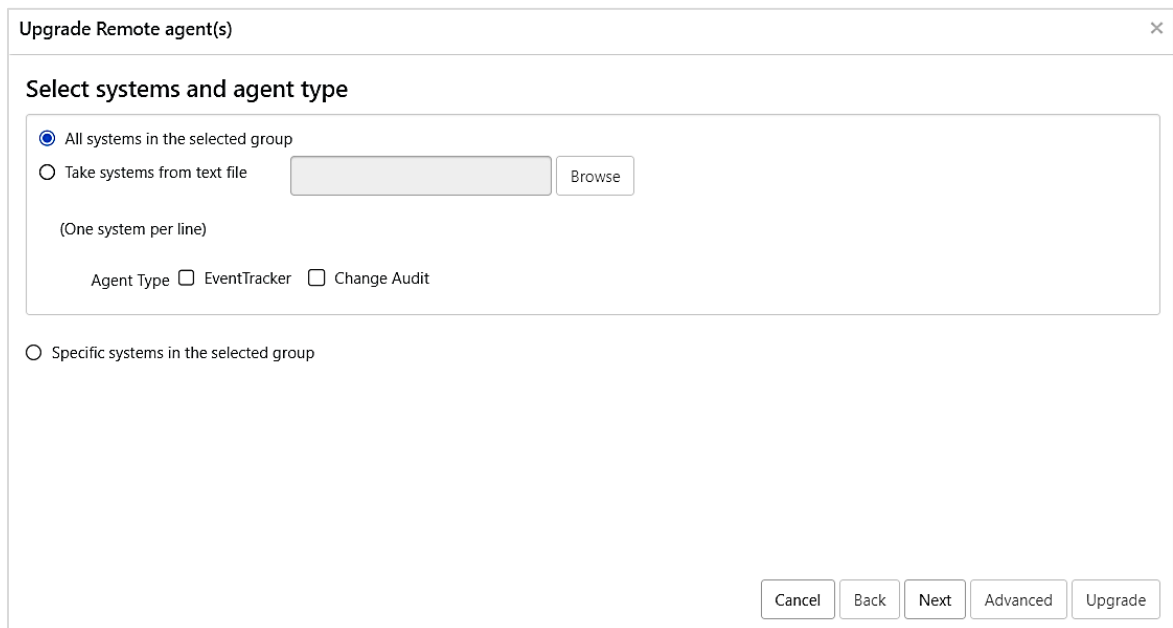
> **Note:**
>
> Refer Upgrading Sensors for a Group section to upgrade the sensors for a group or the Upgrading Sensor for a System section to upgrade the sensor for a system, and then proceed with the next step.

- **Upgrading 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 **Upgrade agent** from the drop-down list.
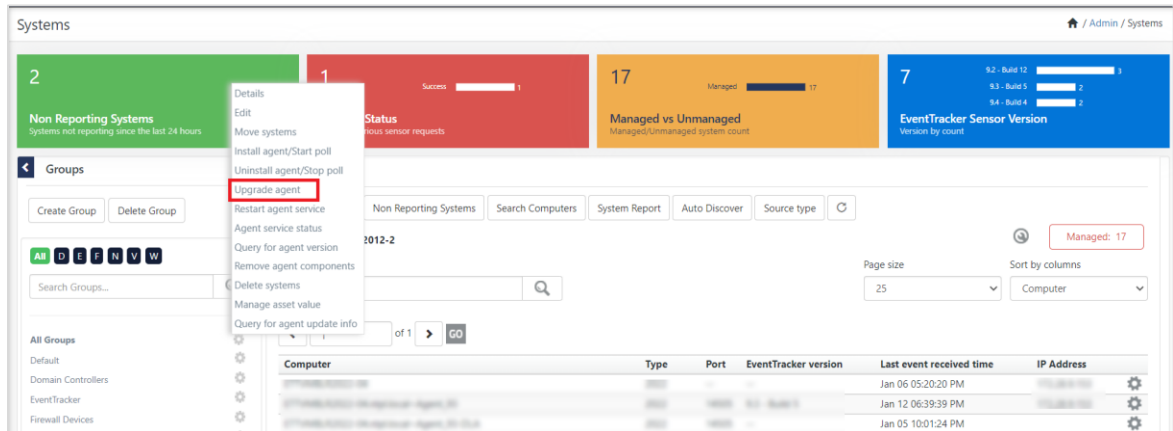
In the **Upgrade Remote agent(s)** window, the following three options are available,

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

Options	Description
All systems in the selected group	• Click this option to upgrade all the sensors available in the selected group.
Take systems from the text file	• 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. • If you desire to select this option, then create the text file to select the sensor system names.
Agent Type	Select the appropriate sensor type to upgrade. • EventTracker • Change Audit
Specific systems in the selected group	Out of all the sensor systems available in the group, select a specific sensor system(s) to upgrade.

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

- **Upgrading 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 upgrade the sensor, and then click **Upgrade Agent** from the drop-down list.

b. In the **Upgrade Remote agent(s)** pop-up window, select the required sensor type check box, and then click **Next**.

9. Next, select the appropriate option for the method of upgrade.

- Choose the **Windows Domain Network** option and specify the details for user credentials;

- (OR) choose the **Upgrade over IP (Non-Windows Domain)** option if the remote sensor is in a non-trusted domain or the remote system is not accessible using Windows file sharing.

10. Select the following check box to install as required (which is optional).

   a. Select **Install default Remedial Action EXEs on this system** check box to install the remedial action scripts.

   > **Note:**
   >
   > Remedial Action are scripts or executable files launched at either the sensor or the manager side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the manager side. This may be installed at the sensor side also, during deployment via the System manager.

   - Click **OK** or **Cancel** in the pop-up message window to enable or disable the above selected feature and click **Upgrade**.
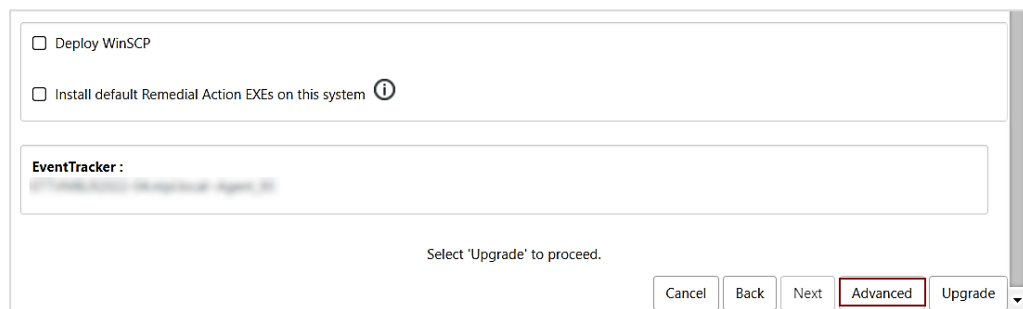
   The sensor will be upgraded on the selected machine with the default **etaconfig.ini** configurations.

b. Select **Deploy WinSCP** check box to install the WinSCP exe.

> **Note:**
>
> If this option is enabled, a WinSCP exe will get installed on the remote agent in the below directory \EventTracker\Agent.

11. If required, in the **Upgrade Remote Agent** window, click **Advanced** (located below) to set a more specific configuration while upgrading the sensor.

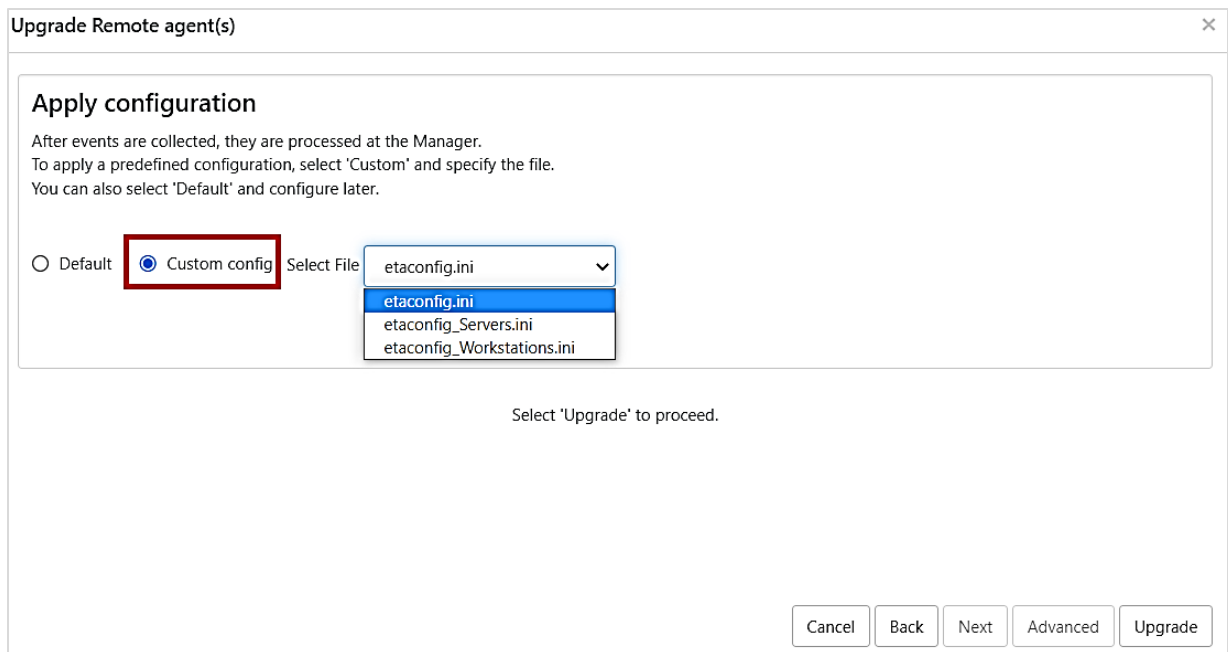12. Choose the **Custom config** option to select a custom configuration file.

> **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 holds 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

13. Select the required **Custom config** file from the drop-down list and click **Upgrade**.
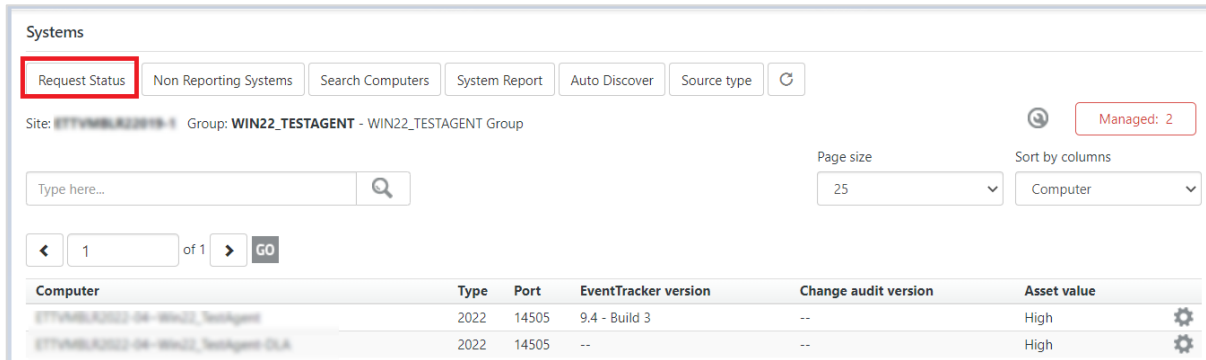
A message window pops-up stating '***Agent upgrade is in progress. Check the Request status screen for updates.***'.

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

The **Request Status** interface displays all the group or system status and description details for which the sensor upgrade process is being taken care.

15. Click the **Refresh** ⟳ button located on the (top right corner of the interface) to see the latest installation status.
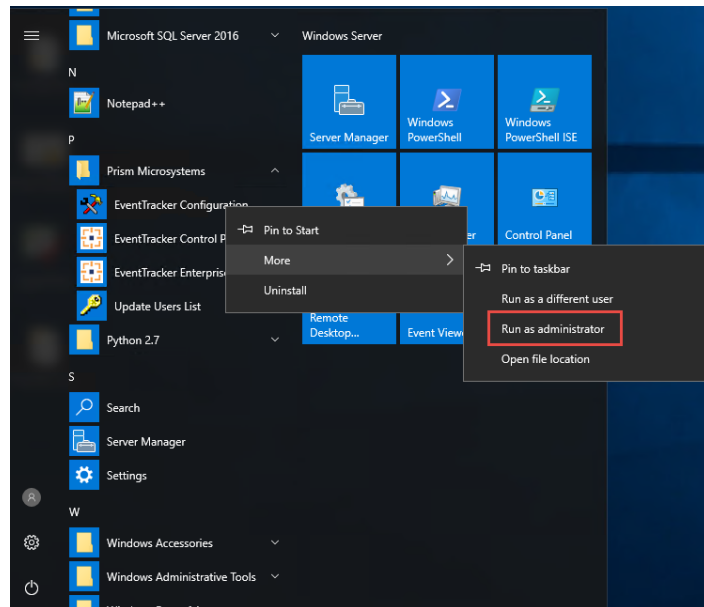

Note:

It may take few minutes to load the status.

Configuring Service Accounts

If you require to set a UNC path (Uniform Naming Convention) for storing Archives/Reports, then you must run the service account of EventTracker Scheduler, EventTracker EventVault, EventTracker Reporter, EventTracker Indexer, and Event Correlator (if available) on the user account having full permission on the set UNC path.
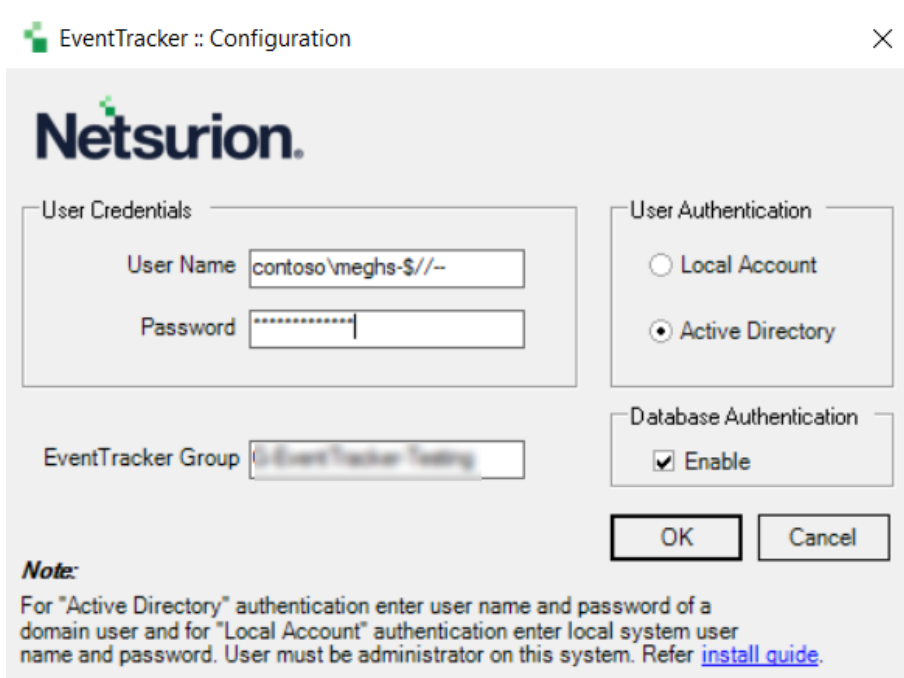
1. Go to **Start**, right-click **EventTracker Configuration** and click **Run as administrator**.

2. Provide the user credentials having the full permissions to access the shared archives folder.
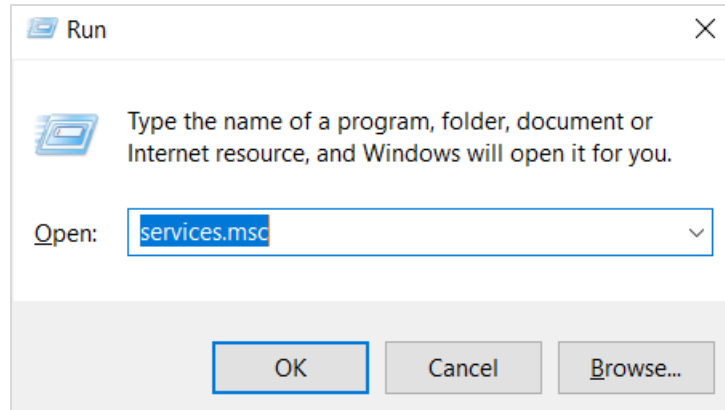
> **Note:**
> Make sure the specified user credentials has the full permissions to access the archives UNC path. Ignore the above procedure if you had already configured with the required user account.

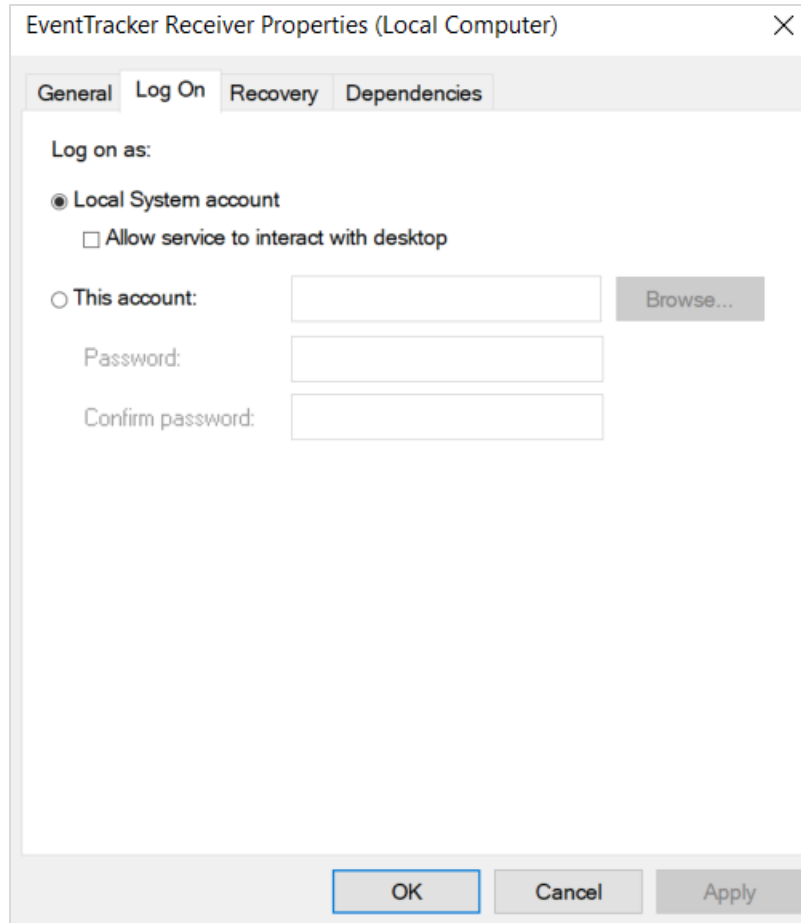3. Then go to **Start** > **Run**, type **services.msc** and click **OK**.

In the **Services** window, search for EventTracker services (such as EventTracker Scheduler, EventTracker EventVault, EventTracker Reporter, EventTracker Indexer, and Event Correlator).

4. Then, right-click the service name (for example, **EventTracker EventVault** service) and click **Properties**.
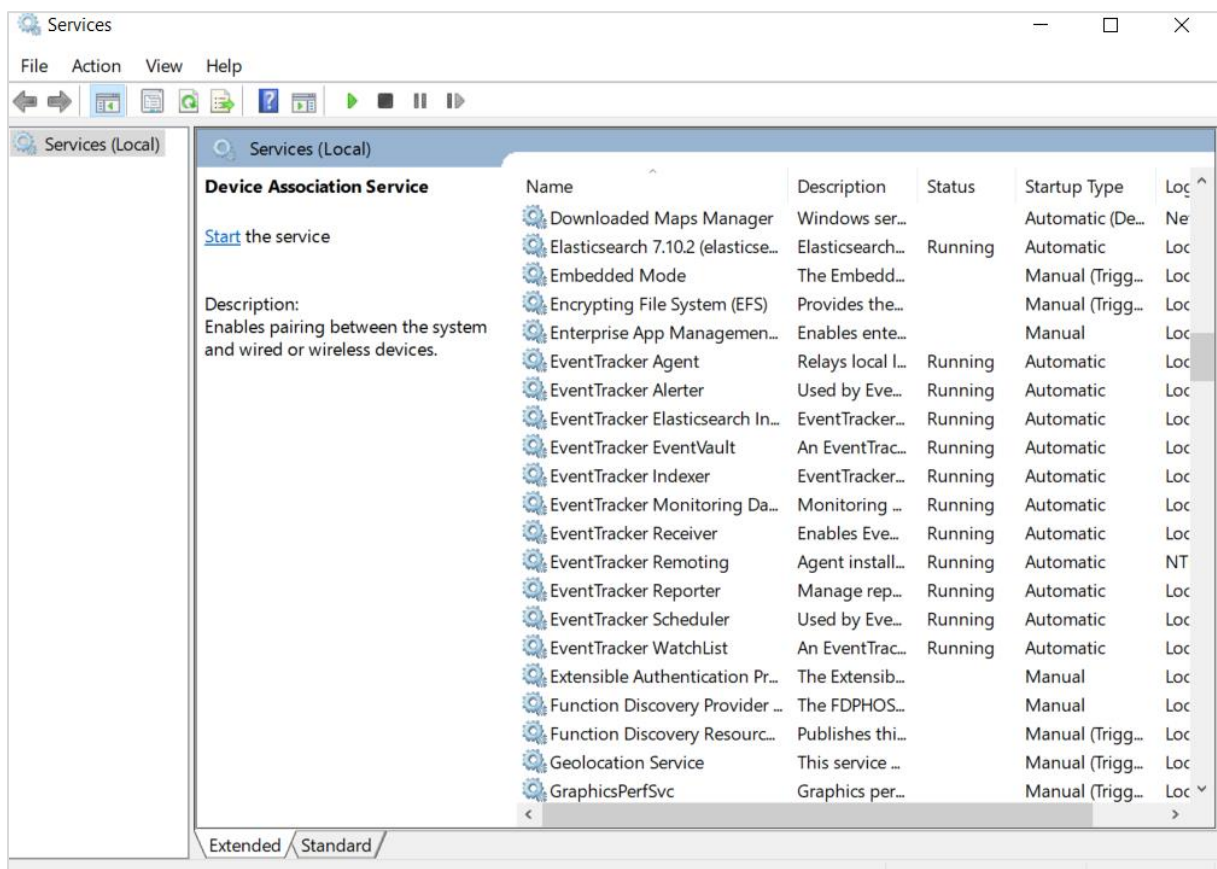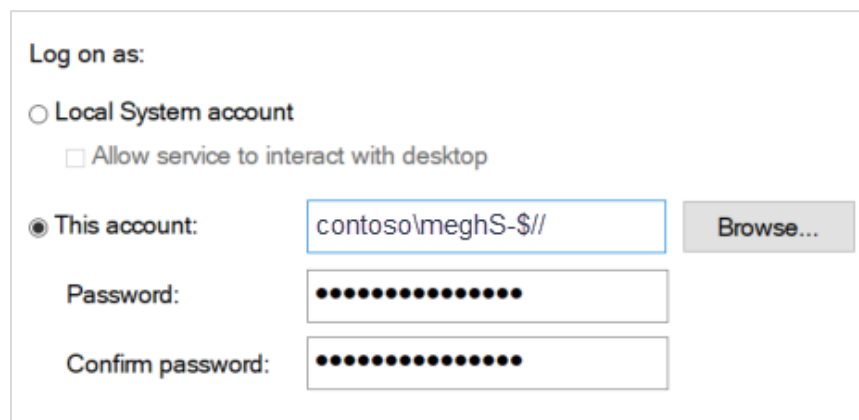
5.   In the **Properties** window, go to the **Log On** tab and choose the **This account** option.
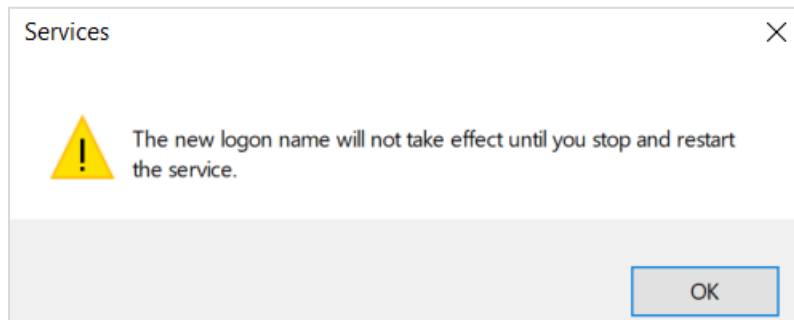

6.   In **This account**, provide the appropriate user credentials and click **Apply**.

> **Note:**
>
> In the **This account** field, the user's name must be specified in the 'domain name\username' format.

7. A warning message pops-up specifying to stop and restart the service to amend the logon details. Click **OK**.

8. Then, go to the services window and stop and start the services (such as EventTracker Scheduler, EventTracker EventVault, EventTracker Reporter, EventTracker Indexer, and Event Correlator) to run the services with the new log on name.

The **Log On As** column will display the updated service account name.

Name	Description	Status	Startup Type	Log On As
EventTracker Alerter	Used by Eve…	Running	Automatic	Local System
EventTracker Elasticsearch In…	EventTracker…	Running	Manual	Local System
EventTracker EventVault	An EventTrac…	Running	Automatic	Local System
EventTracker Indexer	EventTracker…	Running	Automatic	contoso\me(
EventTracker Monitoring Da…	Monitoring …	Running	Automatic	Local System
EventTracker Receiver	Enables Eve…	Running	Automatic	Local System
EventTracker Remoting	Agent install…	Running	Automatic	contoso\me(
EventTracker Reporter	Manage rep…	Running	Automatic	contoso\me(
EventTracker Scheduler	Used by Eve…	Running	Automatic	contoso\me(
EventTracker WatchList	An EventTrac…	Running	Automatic	Local System

Note:

If you encounter any issues during the upgrade process, contact the Software-Support@Netsurion.com support team for prompt and thorough assistance.

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 www.netsurion.com.

Contact Us

Corporate Headquarters

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

Contact Numbers

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

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

https://www.netsurion.com/support