Installation guide

EventTracker v9.3

Publication Date:

May 9, 2022

Abstract

This EventTracker installation guide provides procedures to install and configure EventTracker version 9.3 and helps to verify the expected functionality of all its components.

EventTracker is a reliable, policy-driven SIEM solution to monitor and manage critical events generated by Windows Operating system, Solaris BSM, Unix (SYSLOG), SYSLOG-NG and SNMP devices. EventTracker 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.

Audience

This guide is intended for EventTracker users and network/system administrators responsible for installation and configuration of EventTracker v9.3.

Table of Contents

1. Introduction

EventTracker provides a unique combination of capabilities including:

- Real-time Log & Data Collection
- Log Correlation & Threat Intelligence
- Enterprise-wide, Distributed Console Event Management
- Rapid Integration with Active Directory
- USB Device Monitoring
- Automatic Remediation
- Reporting & Dashboards
- Prioritization & Analytics
- Real-time Notification & Alerting
- File Integrity Monitoring
- Virtual Infrastructure Monitoring
- Security workflows

To familiarize with the various product features, follow our web site, Threat Protection Platform in the brochure of this package.
This installation guide helps you to install our product effortlessly.

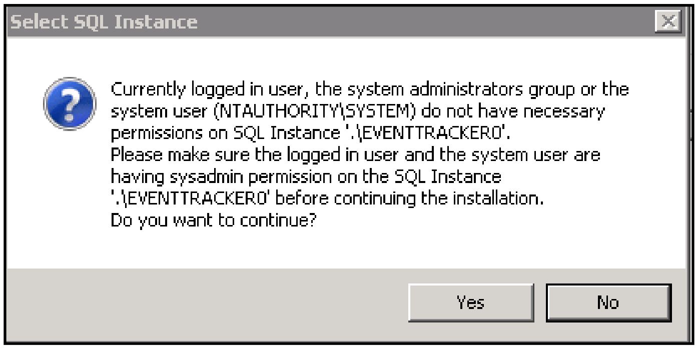
IMPORTANT: EventTracker strongly recommends users to refer the Install and Customize IIS Web Server v9x guide prior to installing EventTracker 9.3.

2. Requirements

2.1 Known Issues while installing v9.3

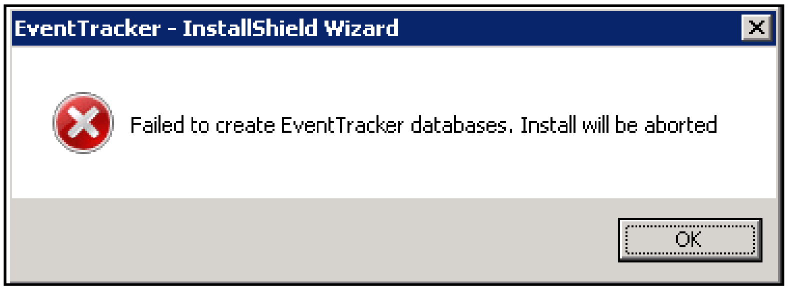
The below-mentioned issues are related to v9.3 Pre-Installer only.

1. If Admin X has finished pre-installation and user Y proceeds to finish the installation on the same machine, then below message is encountered, what should the user do?



Currently logged in user, the system administrators group or the system user (NTAUTHORITY\SYSTEM) do not have necessary permissions on SQL Instance '.\EVENTTRACKER0'.
Please make sure the logged in user and the system user are having sysadmin permission on the SQL Instance '.\EVENTTRACKER0' before continuing the installation.
Do you want to continue?

Figure 1



EventTracker - InstallShield Wizard

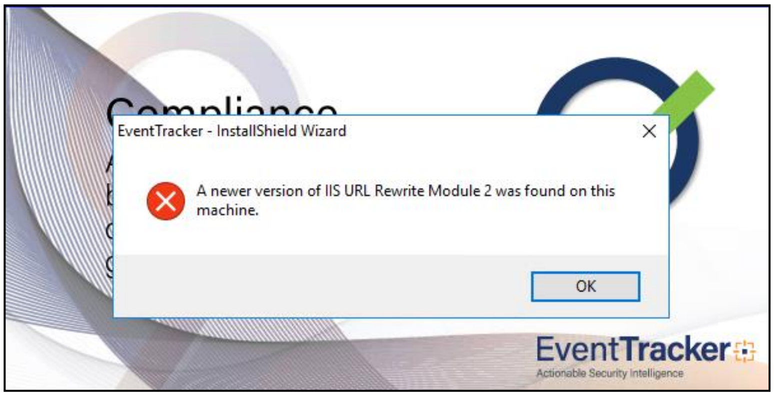
Failed to create EventTracker databases. Install will be aborted

Figure 2

Ensure that the user who has started the installation is an administrator, and the same user completes the installation. If two users switch between installing the application this issue arises.

The currently logged-in user, the system administrators' group, or the system user do not have permissions on the respective SQL instance. Ensure that the logged in user and the system user are having sysadmin privileges on the SQL instance. For detailed instructions to grant sysadmin privilege, please refer to User Permission on MS SQL Server.

2. What should I do if I get the below error message?



EventTracker - InstallShield Wizard

A newer version of IIS URL Rewrite Module 2 was found on this machine.

Figure 3

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

2.2 System Requirements

For optimal performance, the following are the hardware and software requirements to host EventTracker.

2.3 Hardware Requirements [Min. Configuration]

The minimum hardware required to install and smoothly run EventTracker.

EventTracker 9.3 installation is supported on 64-bit Operating System only.

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

Table 1

NOTE: It is recommended to have 2 partitions in Disk 1 (SSD), Partition 1 for Operating System and Partition 2 for EventTracker and search cache. The Archives are stored in a NON-SSD disk (example: Disk 2).

2.4 Software Requirements

To install EventTracker Manager :

Microsoft Windows Platforms	64 bit
Server 2022	Supported
Server 2019	Supported
Server 2016	Supported
Server 2012 R2	Supported

Table 2

SQL server	64 bit
SQL Server 2017	Supported
SQL Server 2016	Supported

Table 3

Components:

- **Elastic Search 7.2.1**.
- **Latest service packs of all Microsoft Windows update**.

Web Browsers:

- Internet Explorer 11 and above.
- Firefox Browser latest.
- Google Chrome latest.

NOTE

- Installing Elasticsearch 7.2.1 will automatically install the compatible OpenJDK version 12.0.1.

- **TLS-1.2** should be enabled for EventTracker v9.3 Installation and all other protocols must be disabled.
- It is recommended not to install EventTracker on a Domain Controller.
- It is recommended to run the EventTracker Manager Console on a dedicated Microsoft Windows Server.

To install EventTracker Agent:

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
Server 2012	Not Applicable	Supported
Server 2008 R2	Not Applicable	Supported
Server 2008	Supported	Supported
Windows 11	Not Applicable	Supported
Windows 10	Supported	Supported
Windows 8, 8.1	Supported	Supported
Windows 7	Supported	Supported
EventTracker Agent for Solaris: Solaris 9, Solaris 10 **Microsoft Windows 7 Embedded and Microsoft Windows 10 IOT Enterprise**		

Table 4

Components:

- Microsoft .NET Framework 3.5 and above.

NOTE: Versions other than those specified above are not supported.

3. Installing EventTracker

3.1 Pre-install instructions for Local Account and Active Directory authentication

EventTracker users are authenticated locally or against the Microsoft Windows Active Directory.

NOTE: You can also configure EventTracker via pre-installer, this entire process is automated. To configure via Pre-Installer, follow the link Procedure to Install EventTracker Manager. To configure manually, refer to Create Local User and Group Accounts or Create Active Directory User and Group Accounts

3.2 Installing EventTracker Manager

EventTracker recommends you refer Managing Billions of Logs Every Day guide before you begin the installation. This guide explains the architecture and sample deployment methods with illustrations.

Installation can be initiated by the following method.

- Launch the executable program. During install, you will be asked 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.

The installation procedure is identical for all operating system(s) as mentioned in Table 2 and Table 3.

3.3 Pre-install Checklist for EventTracker Manager

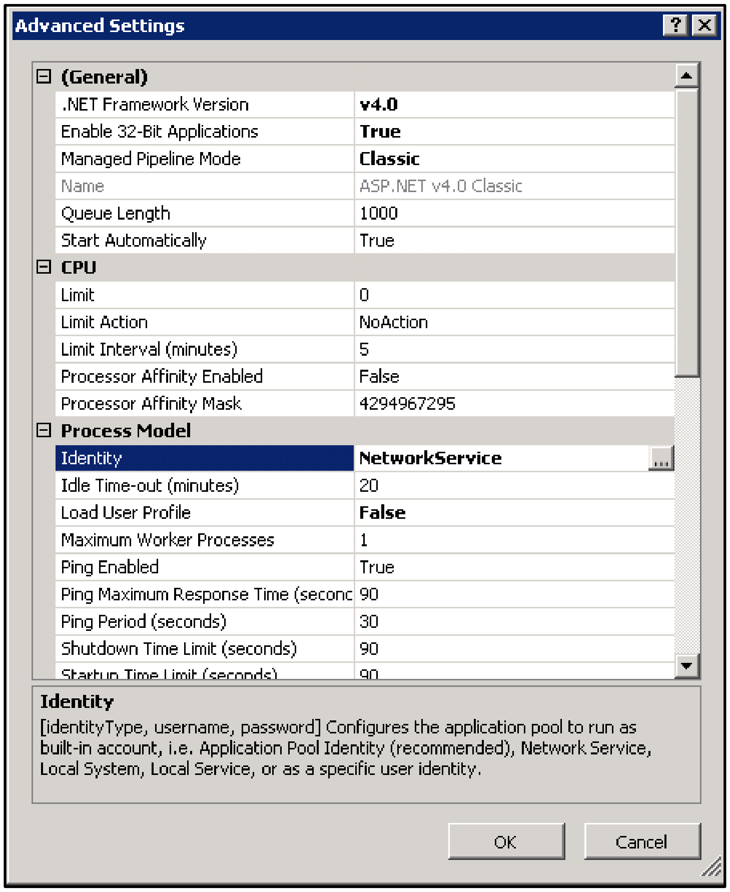
The pre-install checklist describes the specific settings, permissions, and privileges that are required for installing the EventTracker Manager. Read the checklist before installation to avoid installation failure.

ENSURE	**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
	System cryptography: Use FIPS 140 compliant cryptographic algorithms, with encryption, hashing and signing algorithms disabled.
VERIFY	The user has permission on 'Application install directory' (Folders and sub folders).
	The user must have created service permission on the target system (SCM - service control manager).
	User has Read/Write permission on the Microsoft windows registry.

Table 5

3.3.1 IIS Settings

Ensure that IIS Settings under Application Pools are as follows in Microsoft Windows operating system.



(General)	
.NET Framework Version	**v4.0**
Enable 32-Bit Applications	**True**
Managed Pipeline Mode	**Classic**
Name	ASP.NET v4.0 Classic
Queue Length	1000
Start Automatically	True
CPU	
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Process Model	
Identity	**NetworkService**
Idle Time-out (minutes)	20
Load User Profile	**False**
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconc	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Identity

[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

Figure 4

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 trying to install EventTracker should have sysadmin privilege on respective SQL Server 2016/2017.

NOTE:

In SQL Server 2016/2017, ensure that the sysadmin privilege has been granted to NT AUTHORITY\SYSTEM. **If SQL server 2016 and above** are used by the customer, then the SQL service in the service control manager has to be changed from '**NT Service\MSSQL$SQLEXPRESS**' to '**Network Service'.**

If the EventTracker SQL server is not running on Network services, then the user will have to change it manually.

For this, Refer: "**User Permission on SQL Server"** section in the EventTracker v9.3 Install Guide.

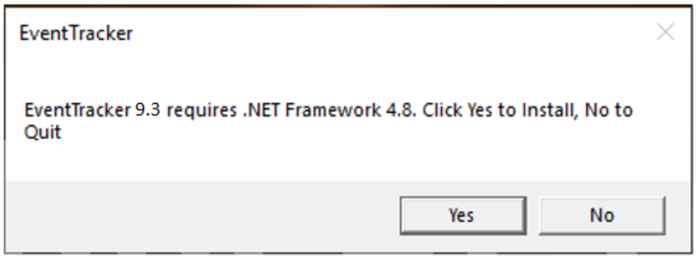
3.4 Procedure to install EventTracker Manager - Custom

If you are using EventTracker for the first time, launch the executable program and proceed. If you have the previous version of EventTracker, uninstall it and then proceed. The detailed procedure to uninstall EventTracker is mentioned in Uninstall EventTracker.

The detailed procedure to install EventTracker is given below.

1. Double-click the executable file.

NOTE: If .NET 4.8. is not installed, it will be installed during pre-install check.

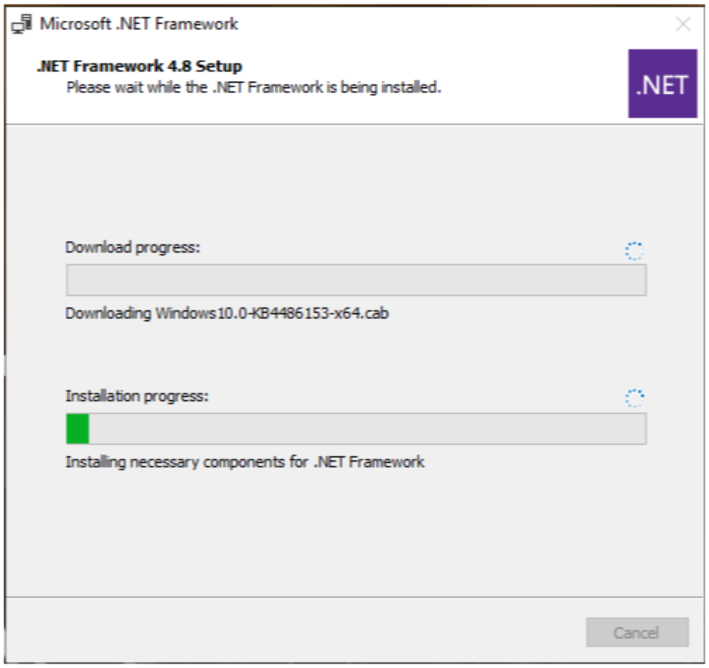


EventTracker

EventTracker 9.3 requires .NET Framework 4.8. Click Yes to Install, No to Quit

Figure 5

IMPORTANT: Go to Internet Explorer->Browser Settings->Security->Custom Level->In the downloads->File Download-> ensure the "enable" option is selected.



Microsoft .NET Framework

.NET Framework 4.8 Setup

Please wait while the .NET Framework is being installed.

Download progress:

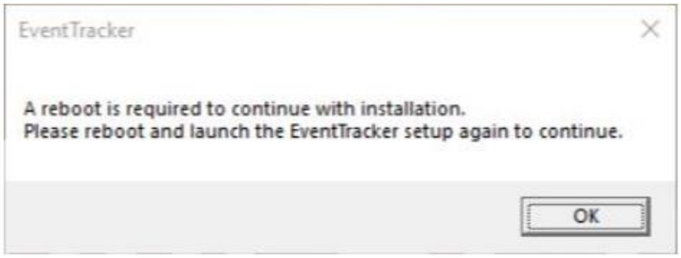
Downloading Windows10.0-KB4486153-x64.cab

Installation progress:

Installing necessary components for .NET Framework

Figure 6

2. Once the .net framework 4.8 is installed a message appears, click **ok** and reboot manually.

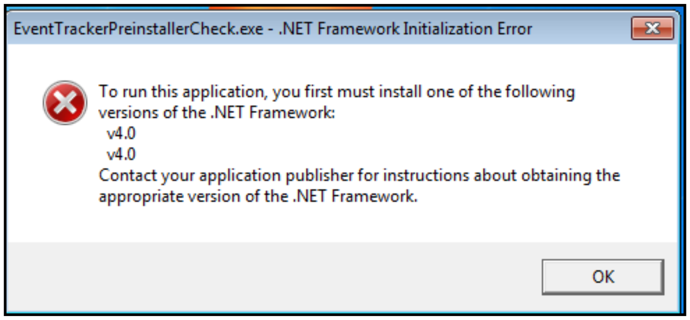


A reboot is required to continue with installation.
Please reboot and launch the EventTracker setup again to continue.

Figure 7

3. After the reboot relaunch the EventTracker setup.

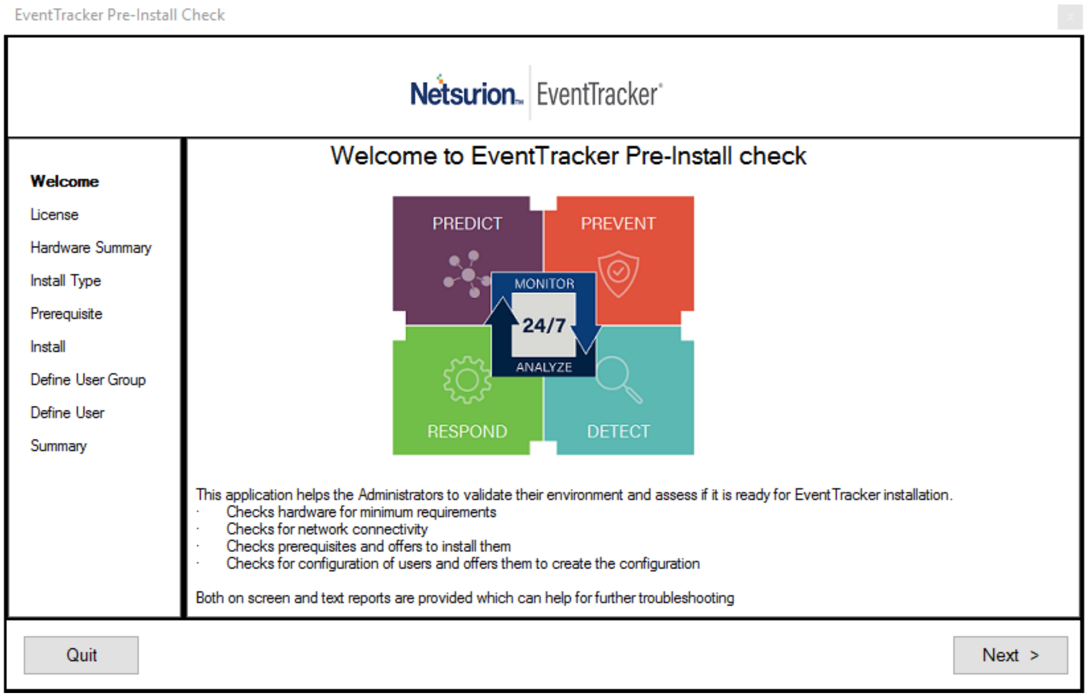
NOTE: If the system does not contain the latest Microsoft Windows updates with service packs then The following message appears.


EventTrackerPreinstallerCheck.exe - .NET Framework Initialization Error
OK

To run this application, you first must install one of the following versions of the .NET Framework:
v4.0
v4.0
Contact your application publisher for instructions about obtaining the appropriate version of the .NET Framework.

Figure 8

EventTracker Pre-Install Check window opens.

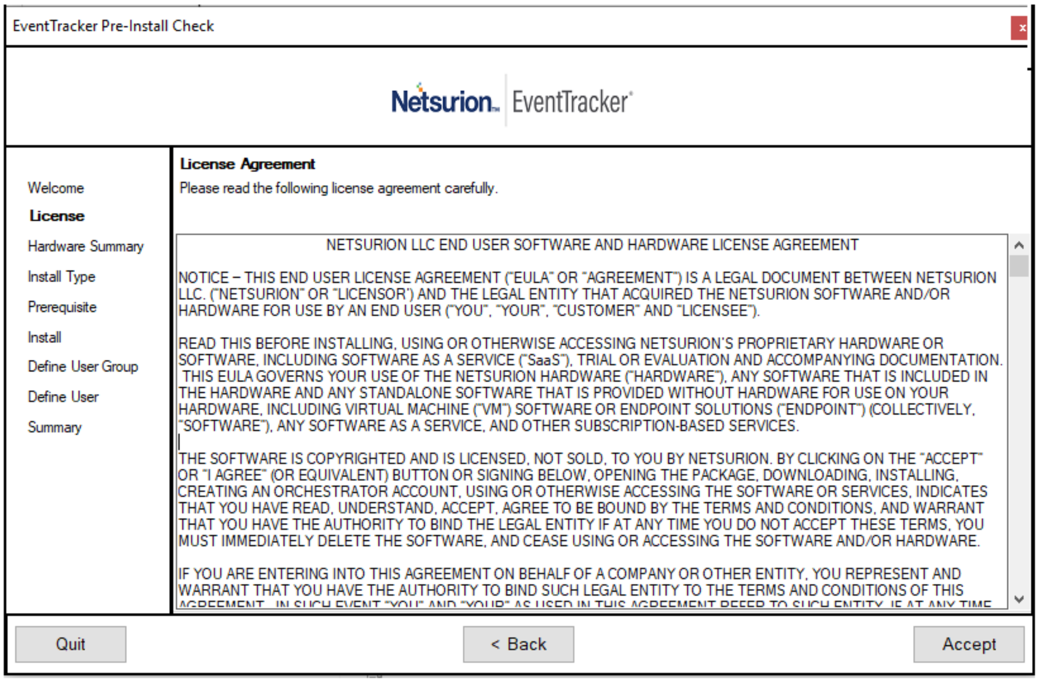


Welcome to EventTracker Pre-Install check

This application helps the Administrators to validate their environment and assess if it is ready for Event Tracker installation.
- Checks hardware for minimum requirements
- Checks for network connectivity
- Checks prerequisites and offers to install them
- Checks for configuration of users and offers them to create the configuration

Both on screen and text reports are provided which can help for further troubleshooting

Figure 9



License Agreement

Please read the following license agreement carefully.

NETSURION LLC END USER SOFTWARE AND HARDWARE LICENSE AGREEMENT

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

READ THIS BEFORE INSTALLING, USING OR OTHERWISE ACCESSING NETSURION'S PROPRIETARY HARDWARE OR SOFTWARE, INCLUDING SOFTWARE AS A SERVICE ("SaaS"), TRIAL OR EVALUATION AND ACCOMPANYING DOCUMENTATION. THIS EULA GOVERNS YOUR USE OF THE NETSURION HARDWARE ("HARDWARE"), ANY SOFTWARE THAT IS INCLUDED IN THE HARDWARE AND ANY STANDALONE SOFTWARE THAT IS PROVIDED WITHOUT HARDWARE FOR USE ON YOUR HARDWARE, INCLUDING VIRTUAL MACHINE ("VM") SOFTWARE OR ENDPOINT SOLUTIONS ("ENDPOINT") (COLLECTIVELY, "SOFTWARE"), ANY SOFTWARE AS A SERVICE, AND OTHER SUBSCRIPTION-BASED SERVICES.

THE SOFTWARE IS COPYRIGHTED AND IS LICENSED, NOT SOLD, TO YOU BY NETSURION. BY CLICKING ON THE "ACCEPT" OR "I AGREE" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, CREATING AN ORCHESTRATOR ACCOUNT, USING OR OTHERWISE ACCESSING THE SOFTWARE OR SERVICES, INDICATES THAT YOU HAVE READ, UNDERSTAND, ACCEPT, AGREE TO BE BOUND BY THE TERMS AND CONDITIONS, AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THE LEGAL ENTITY IF AT ANY TIME YOU DO NOT ACCEPT THESE TERMS, YOU MUST IMMEDIATELY DELETE THE SOFTWARE, AND CEASE USING OR ACCESSING THE SOFTWARE AND/OR HARDWARE.

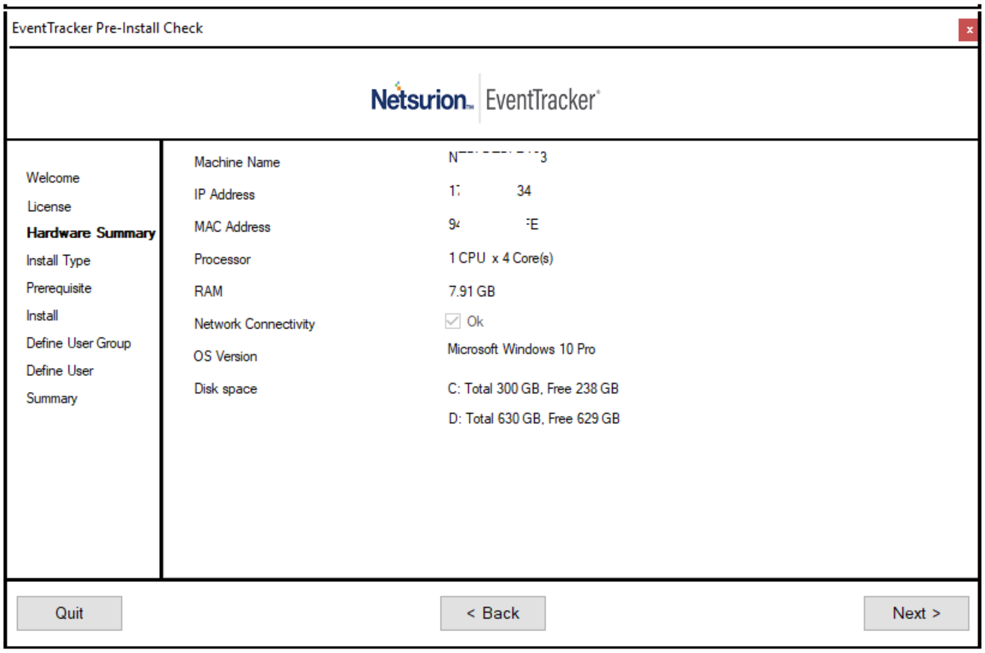
IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND SUCH LEGAL ENTITY TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IN SUCH EVENT "YOU" AND "YOUR" AS USED IN THIS AGREEMENT REFER TO SUCH ENTITY. IF AT ANY TIME

Figure 10

4. Click **Next**.
   Hardware Summary pane opens.

NOTE:

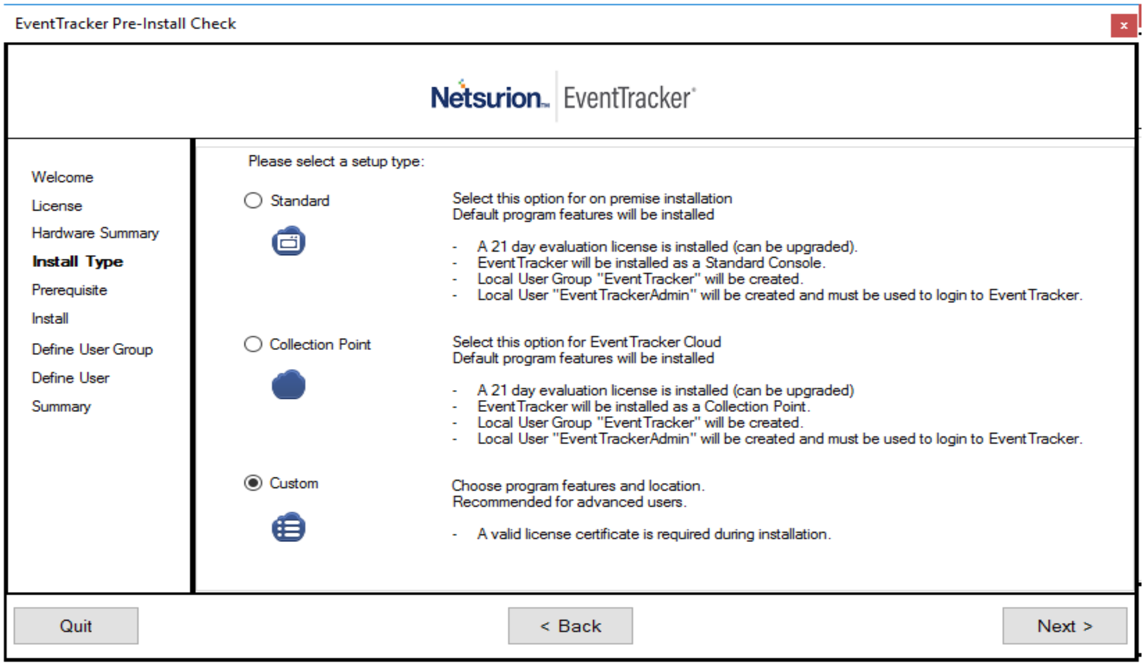
It may take a few seconds to fetch the hardware details and a processing symbol will appear during the data collection process.



Machine Name	N[redacted]3
IP Address	1[redacted]34
MAC Address	9[redacted]E
Processor	1 CPU x 4 Core(s)
RAM	7.91 GB
Network Connectivity	☑ Ok
OS Version	Microsoft Windows 10 Pro
Disk space	C: Total 300 GB, Free 238 GB D: Total 630 GB, Free 629 GB

Figure 11

5. Click **Next**.
   Install Type page opens.
6. Select Standard/Collection Point/Custom option, and then click **Next**.
   By default, the **custom** option is selected.



Please select a setup type:

○ Standard

Select this option for on premise installation
Default program features will be installed

- A 21 day evaluation license is installed (can be upgraded).
- EventTracker will be installed as a Standard Console.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.

○ Collection Point

Select this option for EventTracker Cloud
Default program features will be installed

- A 21 day evaluation license is installed (can be upgraded)
- EventTracker will be installed as a Collection Point.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.

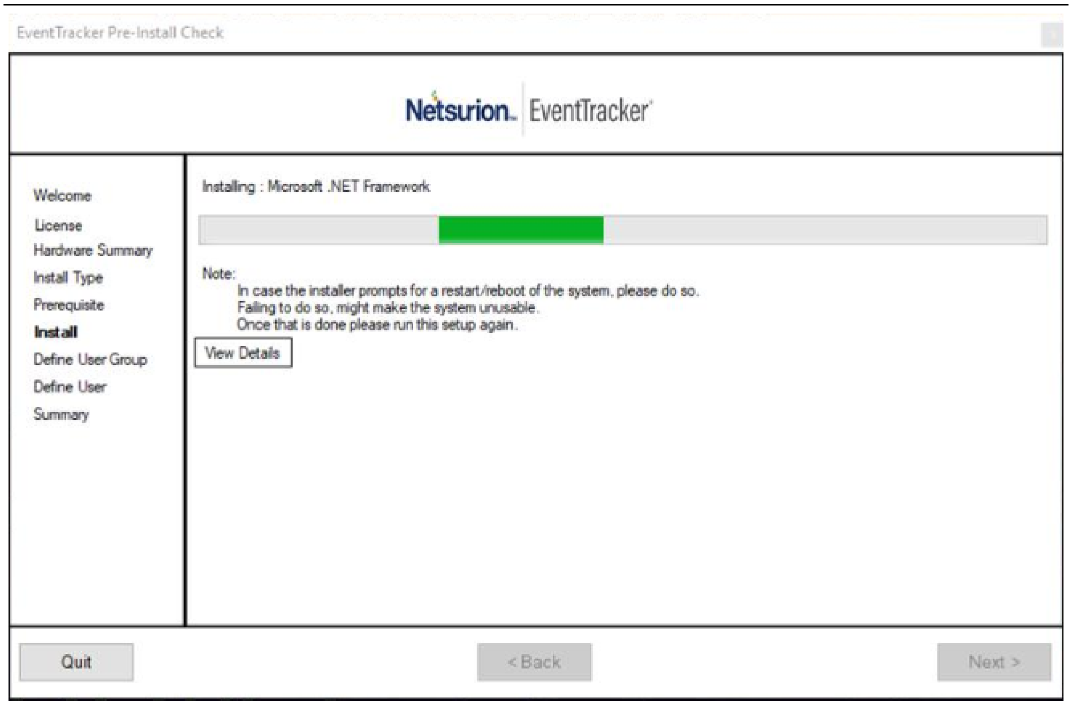
● Custom

Choose program features and location.
Recommended for advanced users.

- A valid license certificate is required during installation.

Figure 12

7. Prerequisite page opens.

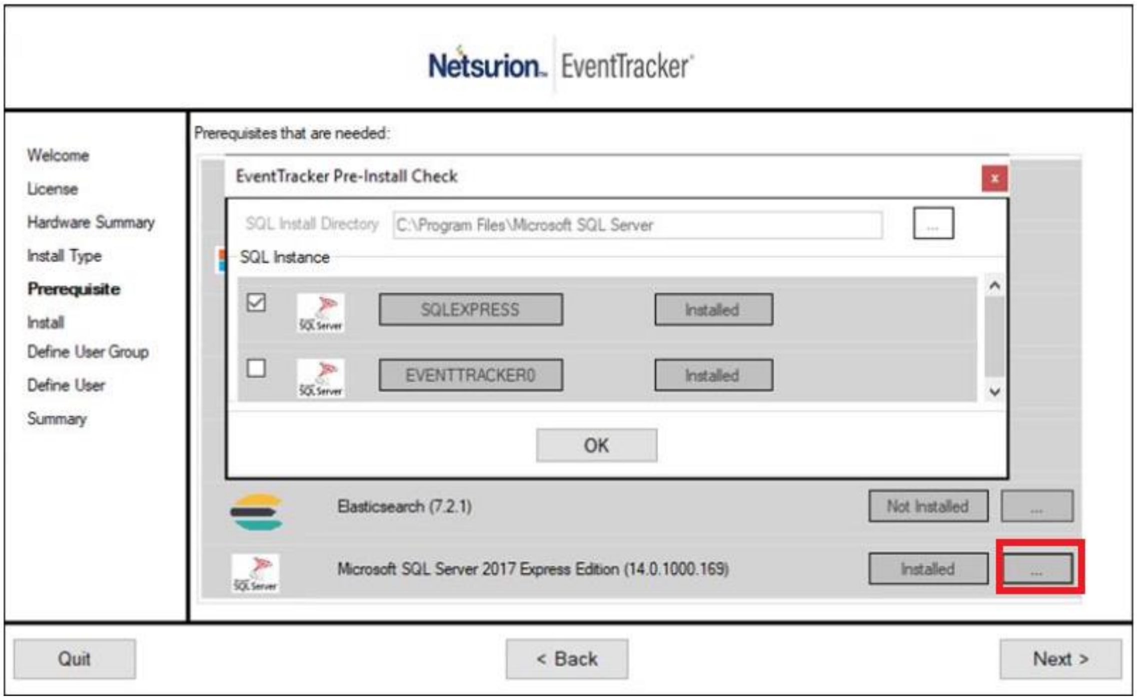


Installing : Microsoft .NET Framework

Note:
In case the installer prompts for a restart/reboot of the system, please do so.
Failing to do so, might make the system unusable.
Once that is done please run this setup again.

Figure 13

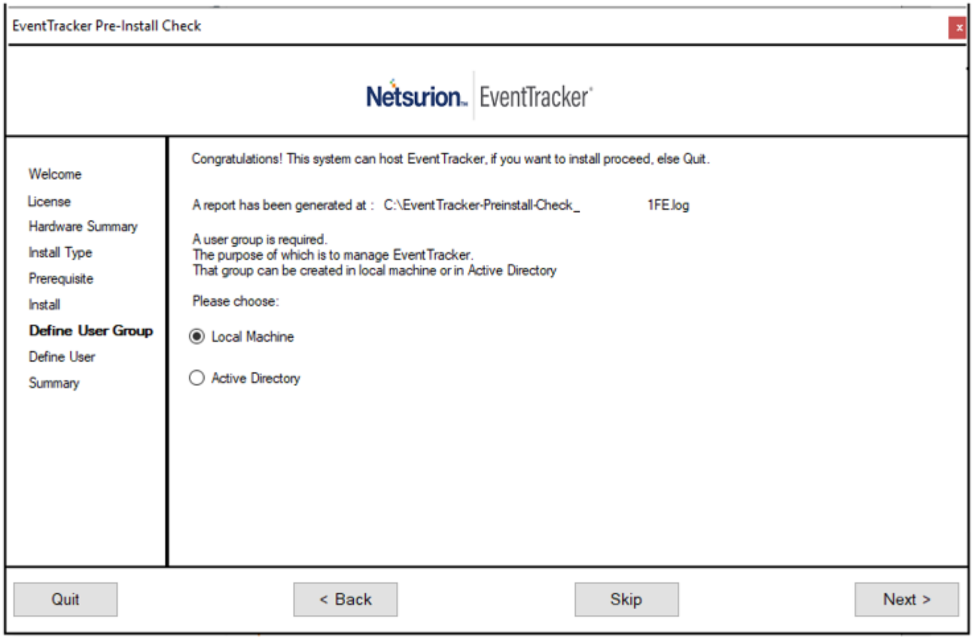
8. If the SQL Server is running with multiple instances, click **Browse** ... and select appropriate Instance and proceed.



Netsurion. EventTracker
Welcome
License
Hardware Summary
Install Type
Prerequisite
Install
Define User Group
Define User
Summary
Prerequisites that are needed:
EventTracker Pre-Install Check
x
SQL Install Directory C:\Program Files\Microsoft SQL Server
...
SQL Instance
☑ SQLEXPRESS Installed
☐ EVENTTRACKER0 Installed
OK
Elasticsearch (7.2.1) Not Installed ...
Microsoft SQL Server 2017 Express Edition (14.0.1000.169) Installed ...
Quit
< Back
Next >

Figure 14

9. Click **Next**.
10. Once pre-requisites are installed, **Define User Group** page opens.



Congratulations! This system can host EventTracker, if you want to install proceed, else Quit.

A report has been generated at : C:\EventTracker-Preinstall-Check_ 1FE.log

A user group is required.
The purpose of which is to manage EventTracker.
That group can be created in local machine or in Active Directory

Please choose:

● Local Machine

○ Active Directory

Figure 15

11. Select Local Machine or Active Directory option, and then click **Next.**

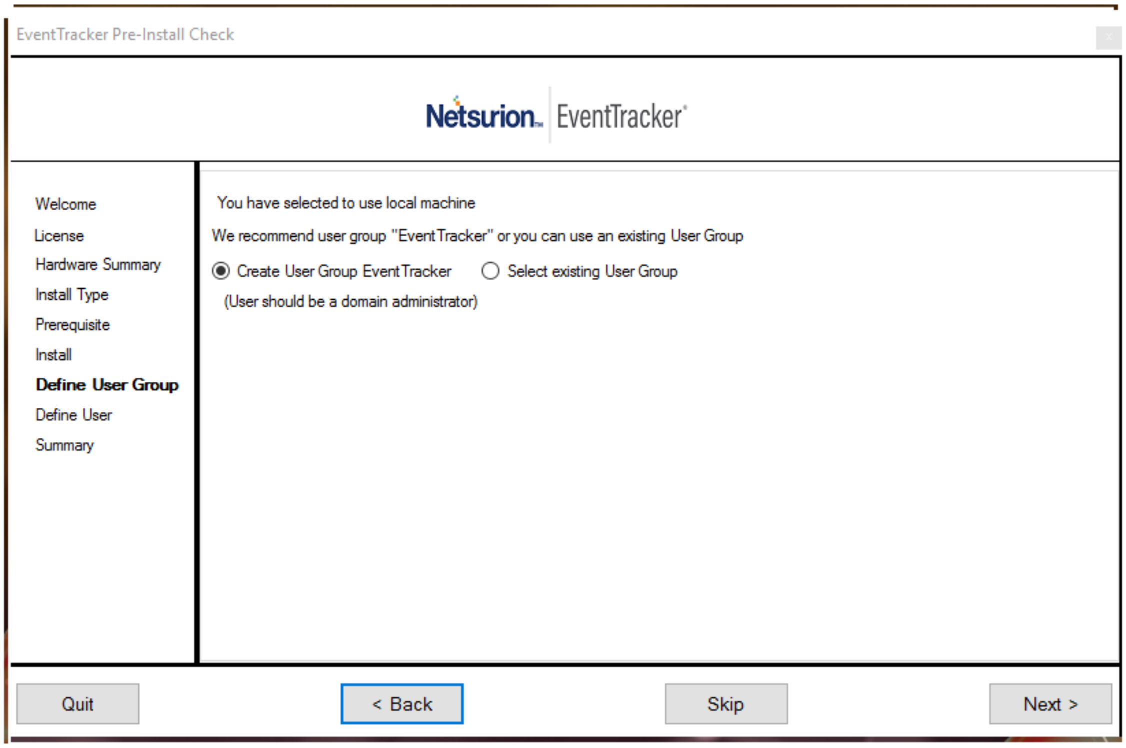
- If the **Local Machine** option is selected, then **You have selected to use local machine** page opens. Refer to **step 12** for further instructions.

  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.

- If **Active Directory** option is selected, then **You have selected Active Directory domain:** page opens. Please refer to **step 13** , for further instructions.

If the local machine was selected earlier, then 'You have selected to use local machine' page opens.

12. Select Create User Group EventTracker or Select existing User Group option, and then click **Next**.



You have selected to use local machine

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

● Create User Group EventTracker ○ Select existing User Group

(User should be a domain administrator)

Figure 16

NOTE:

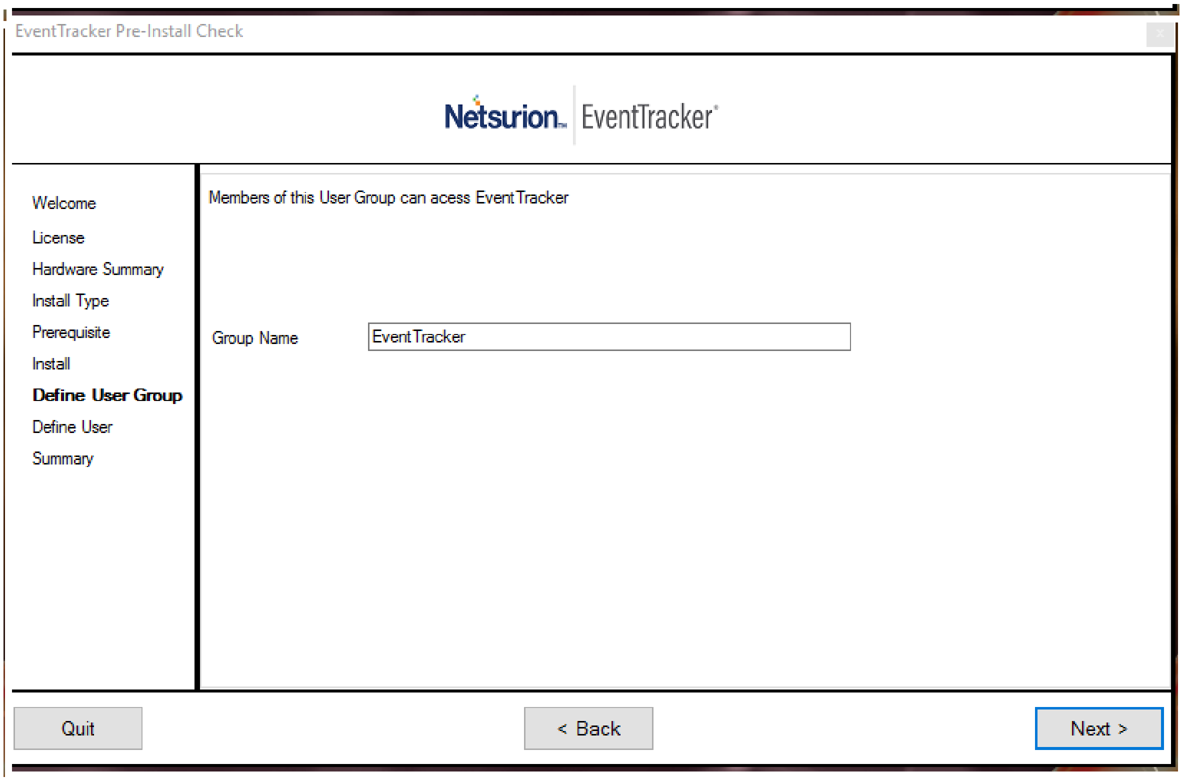
When creating a group,

- We suggest the users to use the group name as 'EventTracker', though EventTracker works with any group name.
- In case this group name does not exist then the default choice is to 'Create User Group EventTracker' else the default choice is 'Select Existing Group'.

If Create User Group EventTracker is selected

a. After selecting **Create User Group EventTracker**, click **Next**.

Members of this User Group can access EventTracker page opens.



EventTracker Pre-Install Check

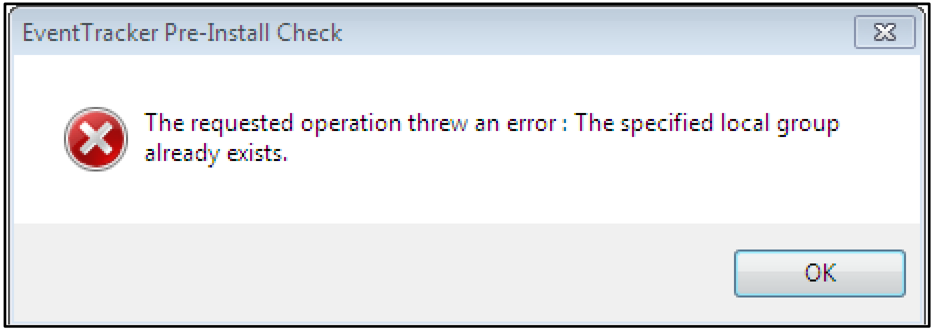
Members of this User Group can acess EventTracker

Group Name: EventTracker

Figure 17

In the Group Name box, enter a unique Group Name and then click **Next**.

Note: The group name must be unique if not **The local group already exists** message appears.



EventTracker Pre-Install Check

The requested operation threw an error : The specified local group already exists.

Figure 18

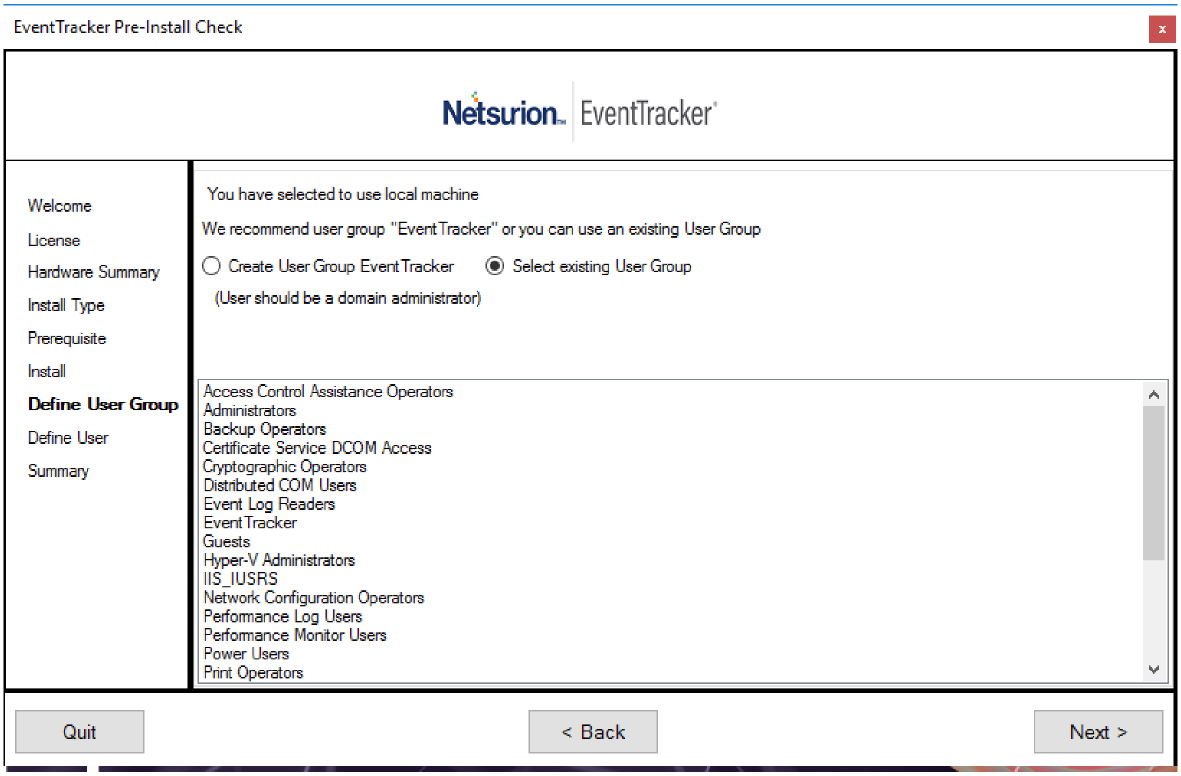
b. Click **OK**.

Define User page opens. Please refer **step 14** to continue installing EventTracker.

(OR)

If Select existing User Group option is selected

a. If **Select existing User Group** option is selected, then select any group, and then click **Next**.



EventTracker Pre-Install Check

You have selected to use local machine

We recommend user group "EventTracker" 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
Distributed COM Users
Event Log Readers
EventTracker
Guests
Hyper-V Administrators
IIS_IUSRS
Network Configuration Operators
Performance Log Users
Performance Monitor Users
Power Users
Print Operators

Figure 19

b. Define User page opens. Please refer **step 14** to continue installing EventTracker.

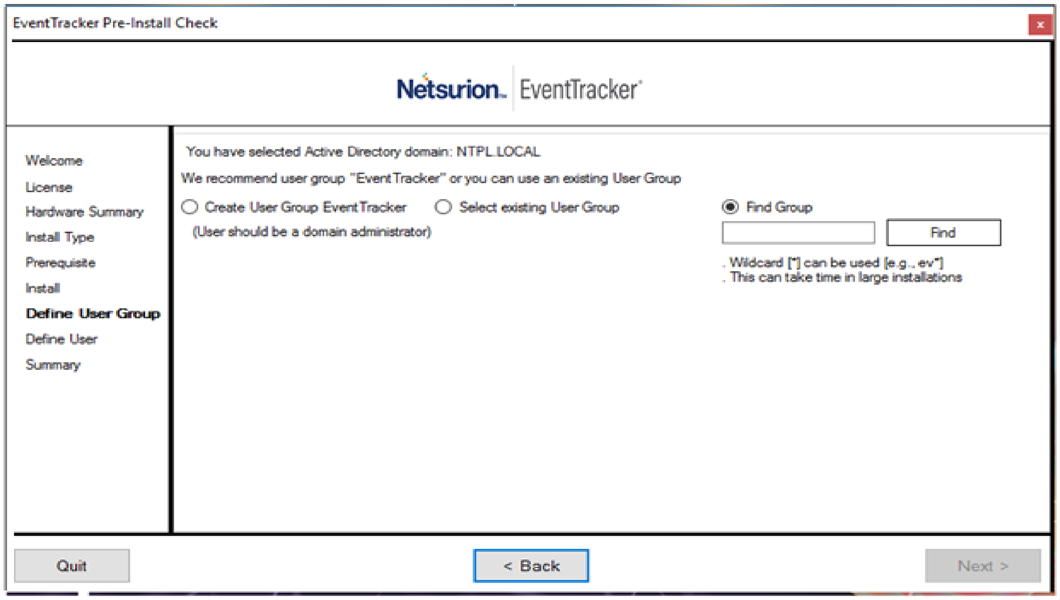
If Active Directory is selected earlier, (please refer **Figure 15**) You have selected Active Directory domain: page opens.

13. Select **Create User Group EventTracker** or **Select existing User Group** option, and then click **Next**.

NOTE:

When creating a group,

- We suggest users to use the group name as ‘EventTracker’, though EventTracker works with any group name.
- In case this group name does not exist then the default choice is to ‘Create User Group EventTracker’ else the default choice is ‘Select Existing Group’.



You have selected Active Directory domain: NTPL.LOCAL

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

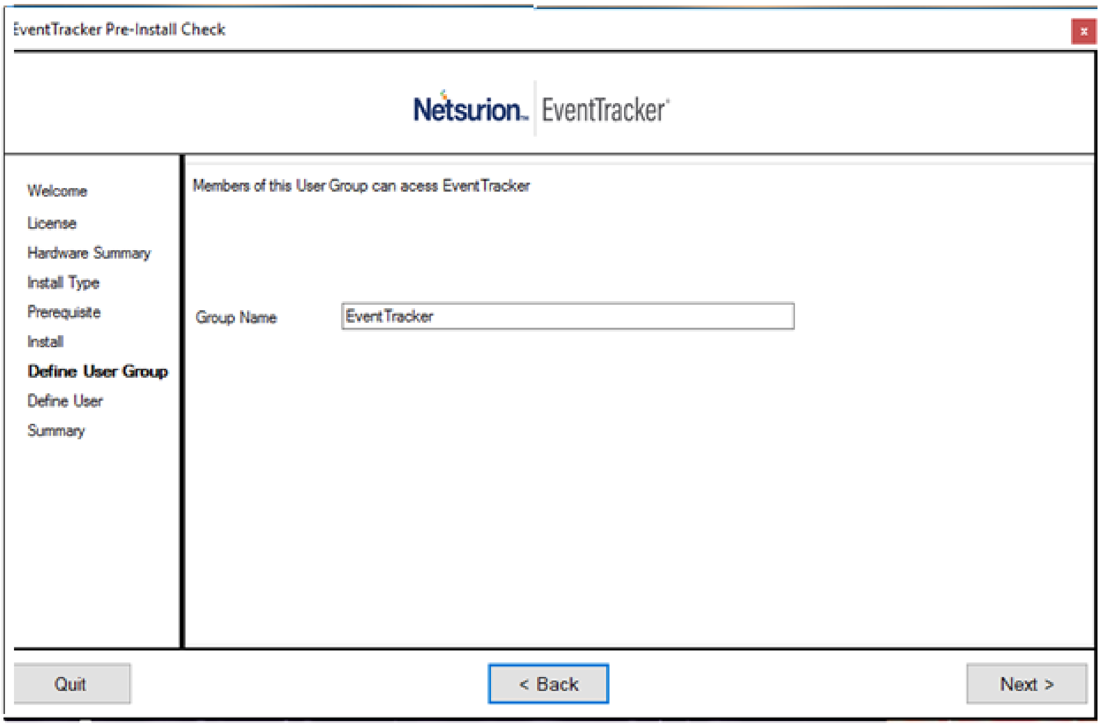
○ Create User Group EventTracker ○ Select existing User Group ● Find Group

(User should be a domain administrator)

. Wildcard [*] can be used [e.g., ev*]
. This can take time in large installations

Figure 20

- If **Create User Group EventTracker** option is selected, then **Members of this User Group can access EventTracker** page opens.



Members of this User Group can acess EventTracker

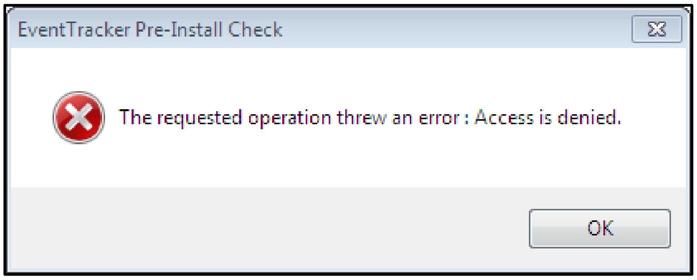
Group Name: EventTracker

Figure 21

  - Enter a unique name in **Group Name box,** and then click **Next**.

NOTE:

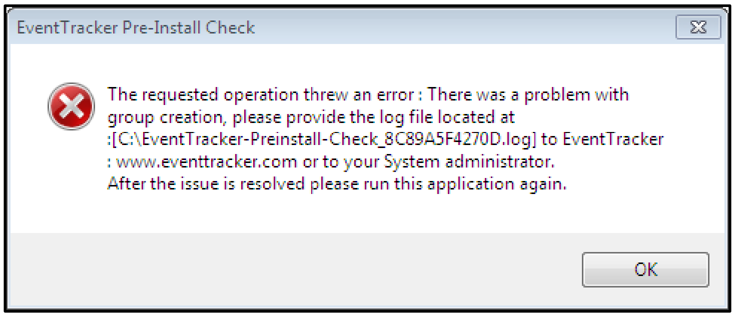
If you do not have appropriate permissions to create a group on the Active Directory machine, then error message ‘Access Denied’ opens. Please contact the administrator if you do not have sufficient permissions.



The requested operation threw an error : Access is denied.

Figure 22

- Click **OK**.

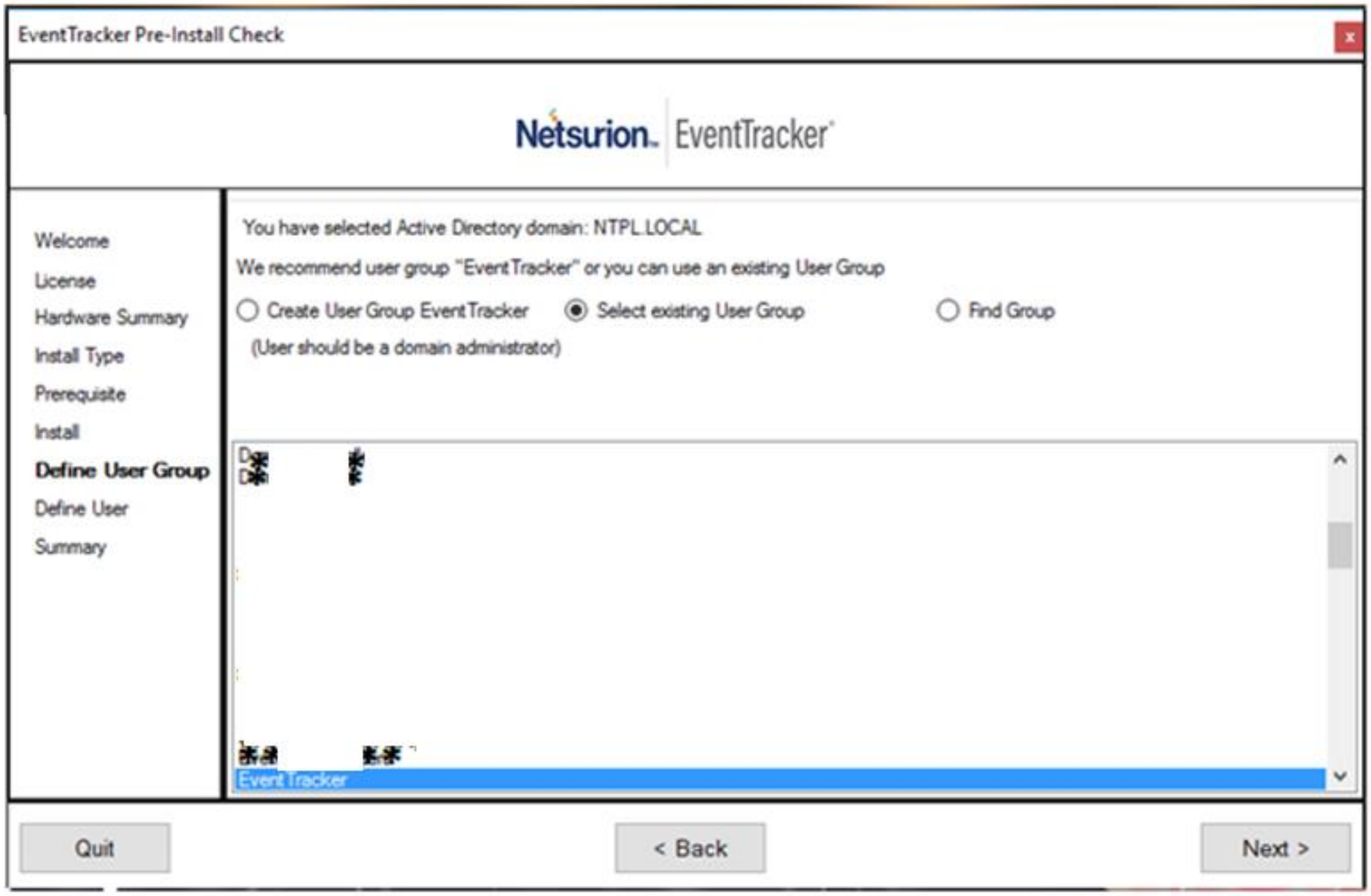


The requested operation threw an error : There was a problem with group creation, please provide the log file located at :[C:\EventTracker-Preinstall-Check_8C89A5F4270D.log] to EventTracker : www.eventtracker.com or to your System administrator.
After the issue is resolved please run this application again.

Figure 23

❖ If **Select existing User Group** option is selected,

a. Select any group, and then click **Next**.



EventTracker Pre-Install Check

Netsurion. EventTracker

You have selected Active Directory domain: NTPL.LOCAL

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

○ Create User Group EventTracker ● Select existing User Group ○ Find Group

(User should be a domain administrator)

[redacted]

Event Tracker

Figure 24

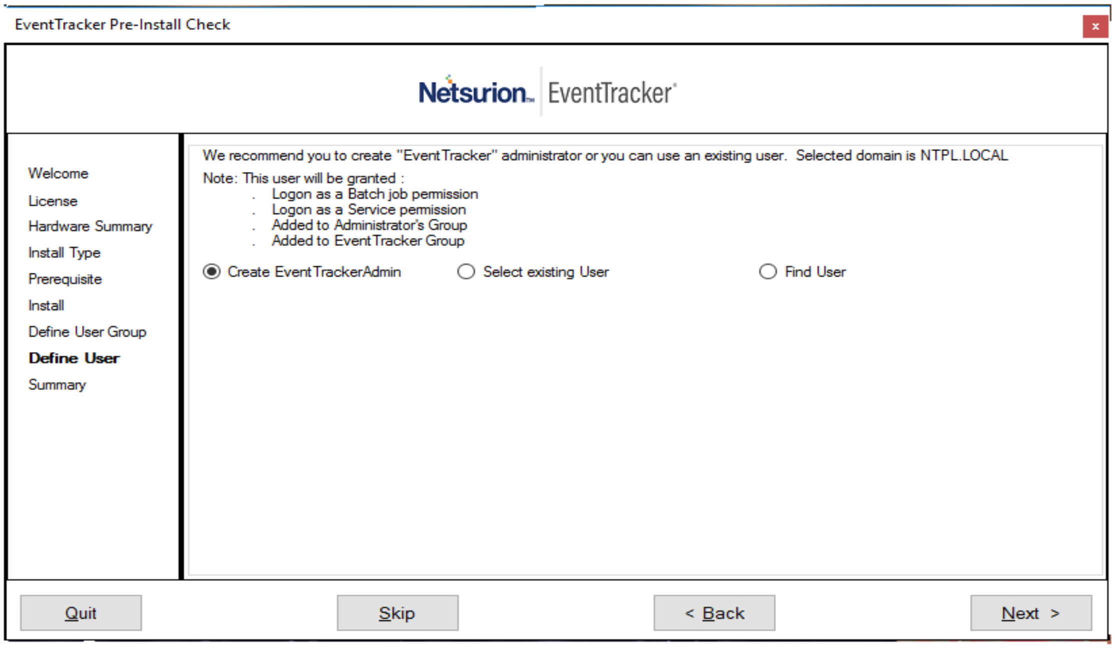
Define User page opens.

14. Select **Create EventTrackerAdmin/Find User/Select existing User** option.

   ❖ If **Create EventTrackerAdmin** option is selected, please refer to **Figure 25.**

NOTE:

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



We recommend you to create "EventTracker" administrator or you can use an existing user. Selected domain is NTPL.LOCAL

Note: This user will be granted :

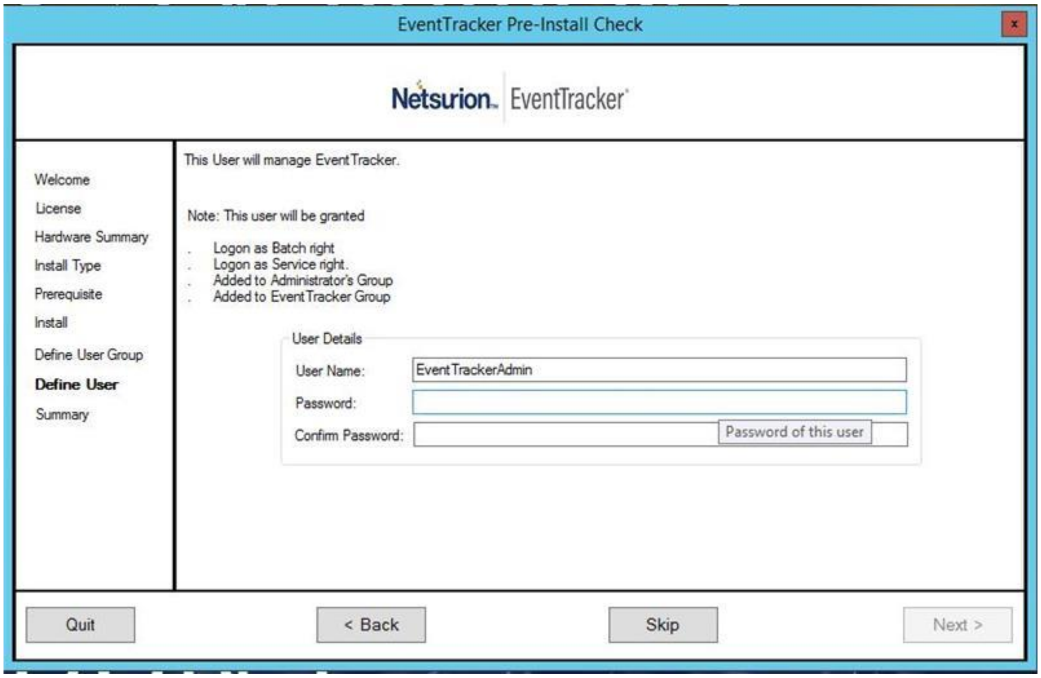
- Logon as a Batch job permission
- Logon as a Service permission
- Added to Administrator's Group
- Added to EventTracker Group

● Create EventTrackerAdmin ○ Select existing User ○ Find User

Figure 25

a. Click **Next**.

This User will manage EventTracker page opens.



This User will manage EventTracker.

Note: This user will be granted

- Logon as Batch right
- Logon as Service right.
- Added to Administrator's Group
- Added to EventTracker Group

User Details

User Name: EventTrackerAdmin

Password:

Confirm Password:

Figure 26

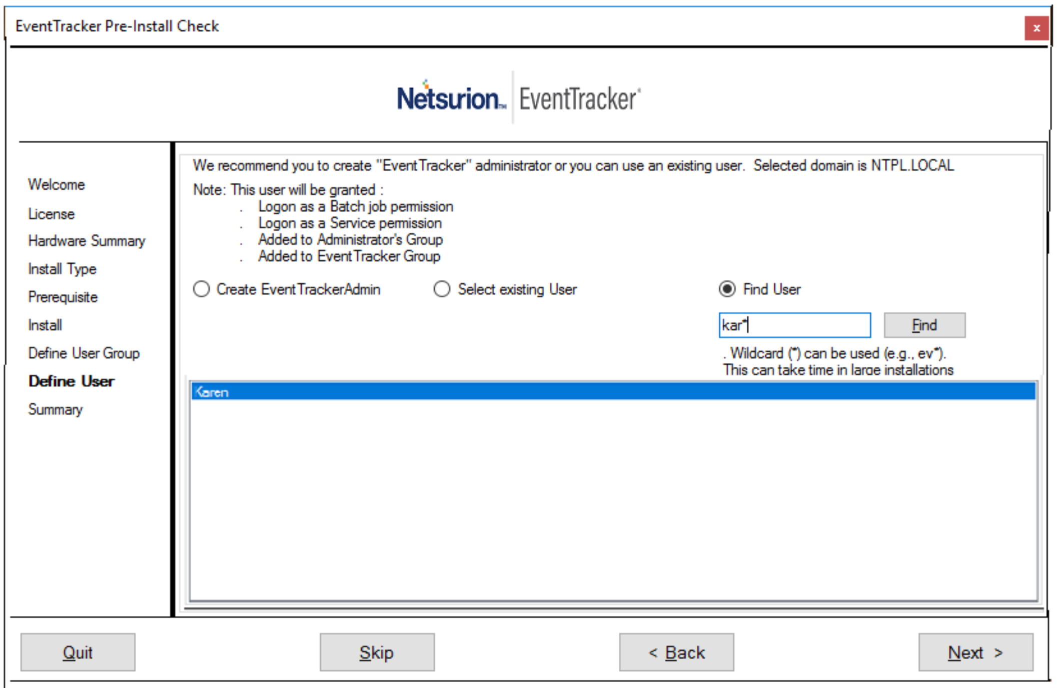
b. Enter relevant credentials, and then click **Next**.

Summary page opens.

❖ If **Find User** option is selected,

a. Enter a name in the box, and then click **Find**.

NOTE: A wildcard can also be entered.



We recommend you to create "EventTracker" administrator or you can use an existing user. Selected domain is NTPL.LOCAL

Note: This user will be granted :

- Logon as a Batch job permission
- Logon as a Service permission
- Added to Administrator's Group
- Added to EventTracker Group

○ Create EventTrackerAdmin ○ Select existing User ● Find User

kar*

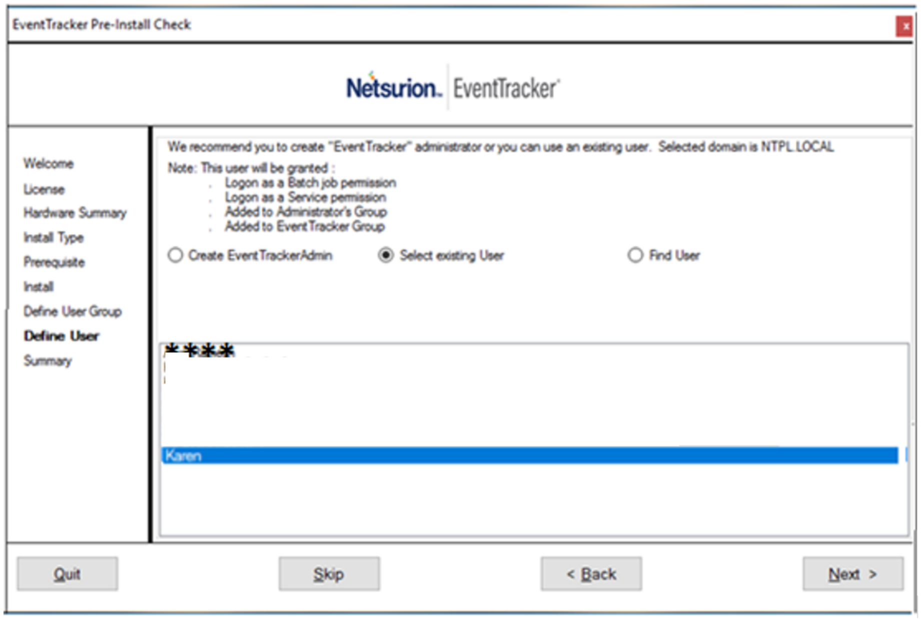
. Wildcard (*) can be used (e.g., ev*).
This can take time in large installations

Karen

Figure 27

b. Click **Next**.
Summary page opens.

❖ If **Select existing User** option is selected, select an appropriate user, and then select **Next**.



We recommend you to create "EventTracker" administrator or you can use an existing user. Selected domain is NTPL.LOCAL

Note: This user will be granted :

- Logon as a Batch job permission
- Logon as a Service permission
- Added to Administrator's Group
- Added to EventTracker Group

○ Create EventTrackerAdmin ● Select existing User ○ Find User

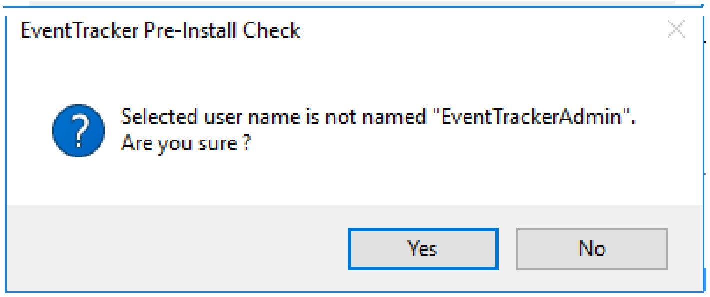
****

Karen

Figure 28

Summary page opens.

If you are not EventTracker Administrator then you get the below message.



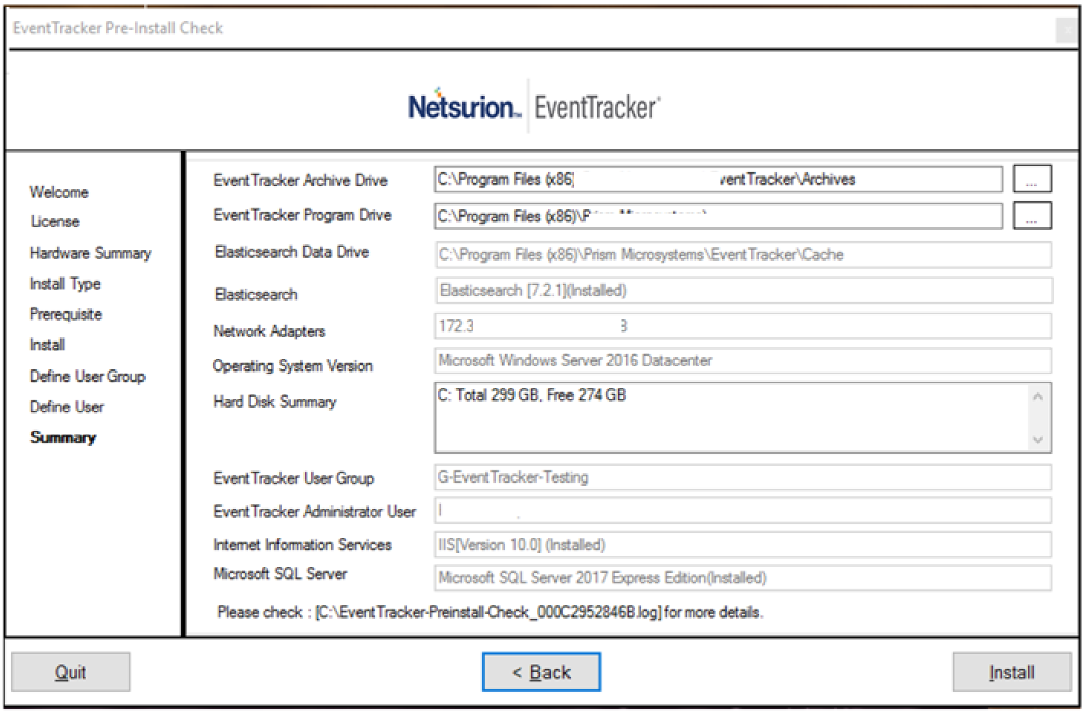
EventTracker Pre-Install Check

Selected user name is not named "EventTrackerAdmin".
Are you sure ?

Figure 29

a. Click **Yes**.

15. In **Summary** page, verify all the data entered, and then click **Install**.



EventTracker Pre-Install Check

EventTracker Archive Drive: C:\Program Files (x86) ventTracker\Archives

EventTracker Program Drive: C:\Program Files (x86)\P

Elasticsearch Data Drive: C:\Program Files (x86)\Prism Microsystems\EventTracker\Cache

Elasticsearch: Elasticsearch [7.2.1](Installed)

Network Adapters: 172.3 3

Operating System Version: Microsoft Windows Server 2016 Datacenter

Hard Disk Summary: C: Total 299 GB, Free 274 GB

EventTracker User Group: G-EventTracker-Testing

EventTracker Administrator User: I

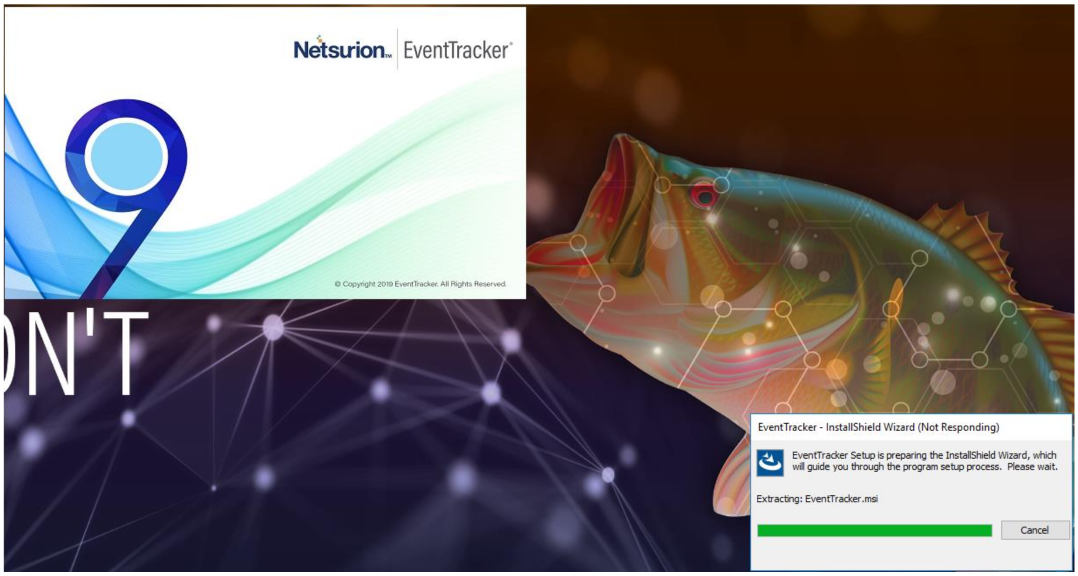
Internet Information Services: IIS[Version 10.0] (Installed)

Microsoft SQL Server: Microsoft SQL Server 2017 Express Edition(Installed)

Please check : [C:\EventTracker-Preinstall-Check_000C2952846B.log] for more details.

Figure 30

EventTracker - Install Shield Wizard opens.



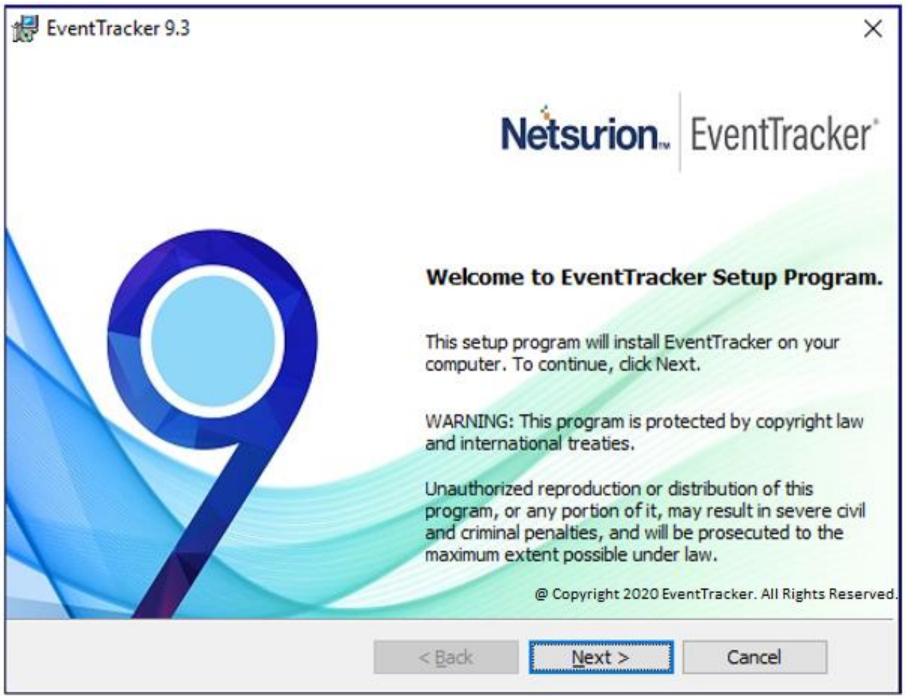
EventTracker - InstallShield Wizard (Not Responding)

EventTracker Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.

Extracting: EventTracker.msi

Figure 31

EventTracker - InstallShield Wizard opens the **Welcome** screen.



Welcome to EventTracker Setup Program.

This setup program will install EventTracker on your computer. To continue, click Next.

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

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

@ Copyright 2020 EventTracker. All Rights Reserved.

Figure 32

16. Click **Next**.

    Select a Certificate File page opens.

NOTE:

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

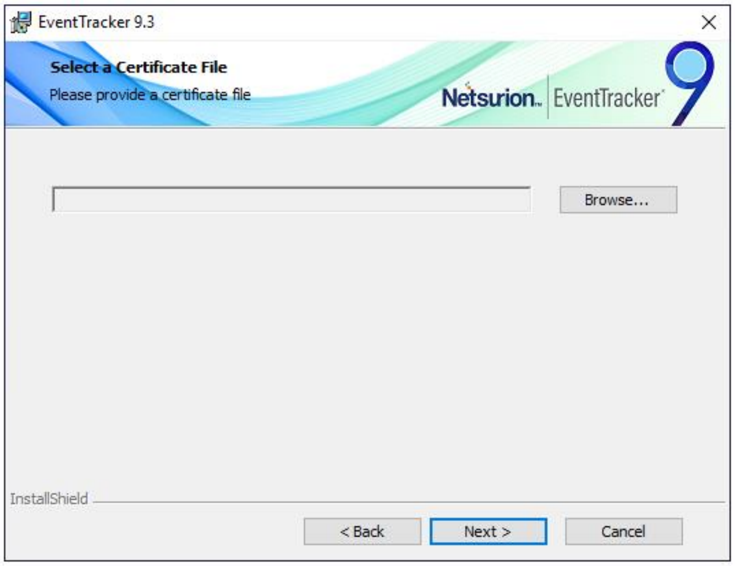

EventTracker 9.3
Select a Certificate File
Please provide a certificate file
Netsurion. EventTracker 9
Browse...
InstallShield
< Back
Next >
Cancel

Figure 33

17. To locate the path of the certificate file, click **Browse**.

 Select File window opens.

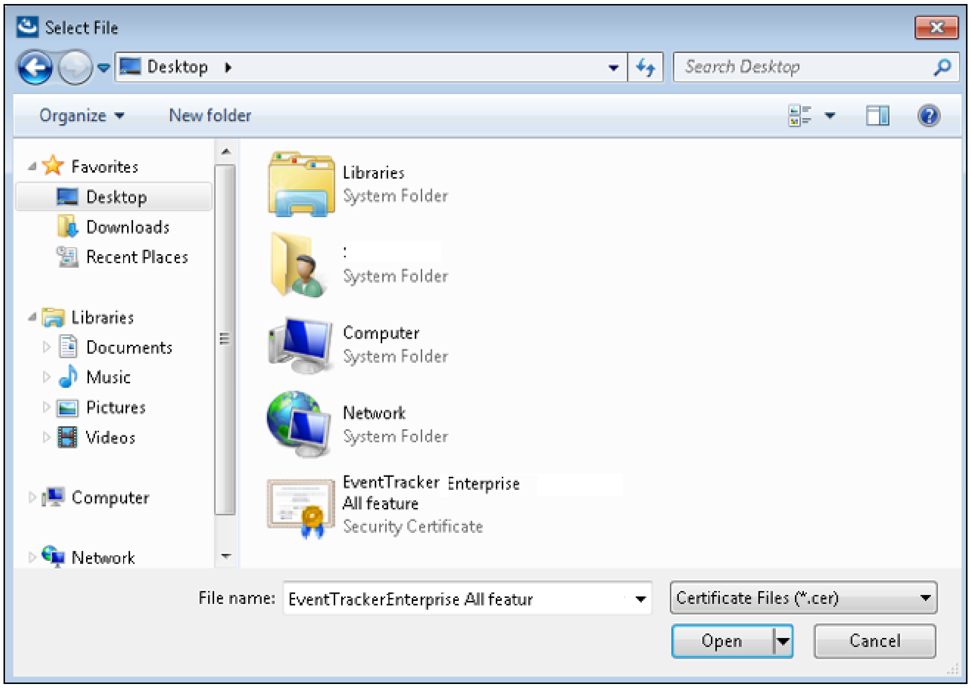
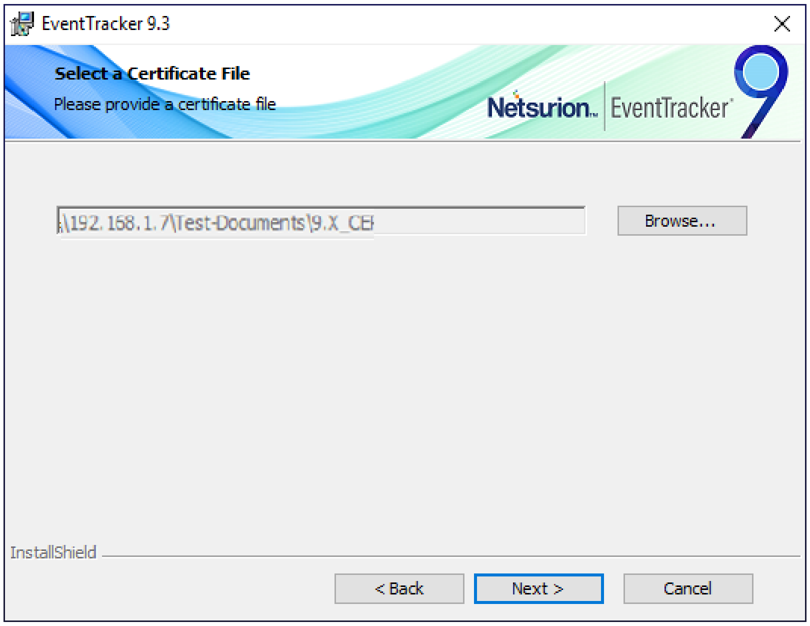


Figure 34

18. Go to the appropriate folder, select the file and then click **Open**.

 The folder path is updated.



EventTracker 9.3

Select a Certificate File

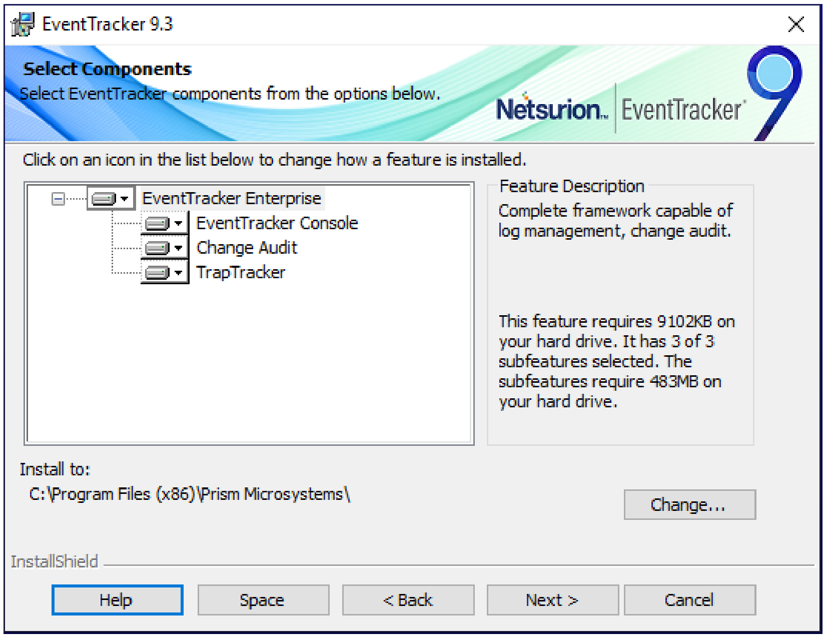
Please provide a certificate file

\\192.168.1.7\Test-Documents\9.X_CEI

Figure 35

19. Click **Next**.

    Select Components screen opens.



EventTracker 9.3

Select Components

Select EventTracker components from the options below.

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

- EventTracker Enterprise
  - EventTracker Console
  - Change Audit
  - TrapTracker

Feature Description

Complete framework capable of log management, change audit.

This feature requires 9102KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 483MB on your hard drive.

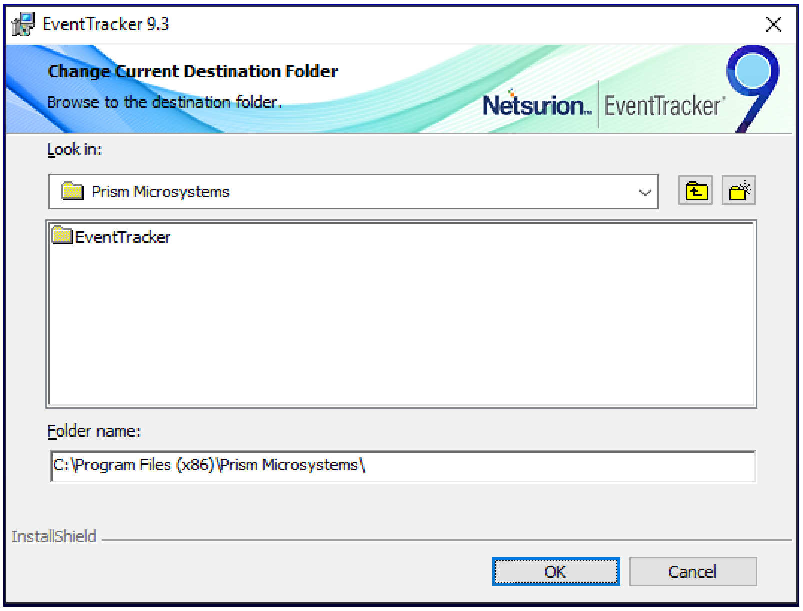
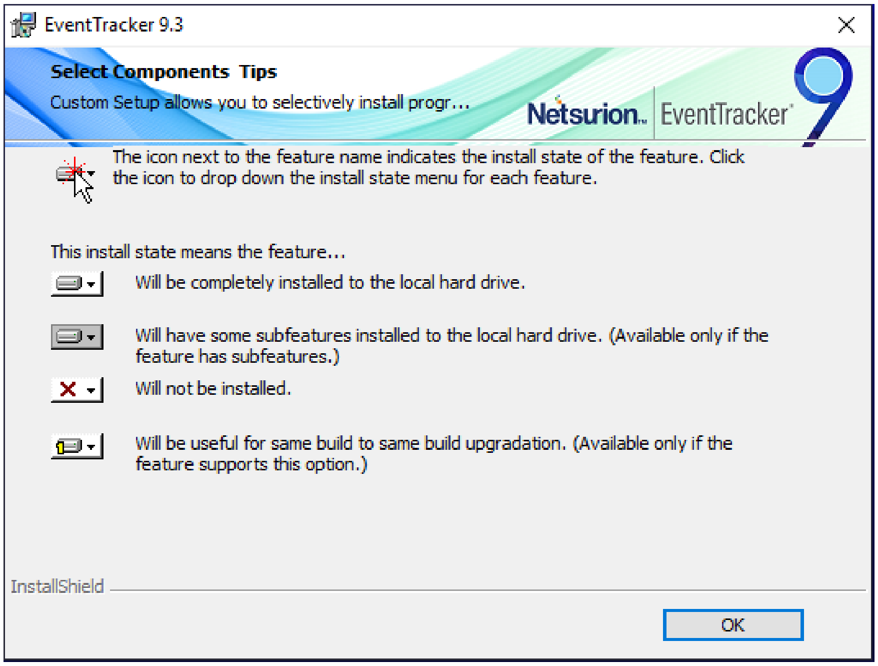
Install to:

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

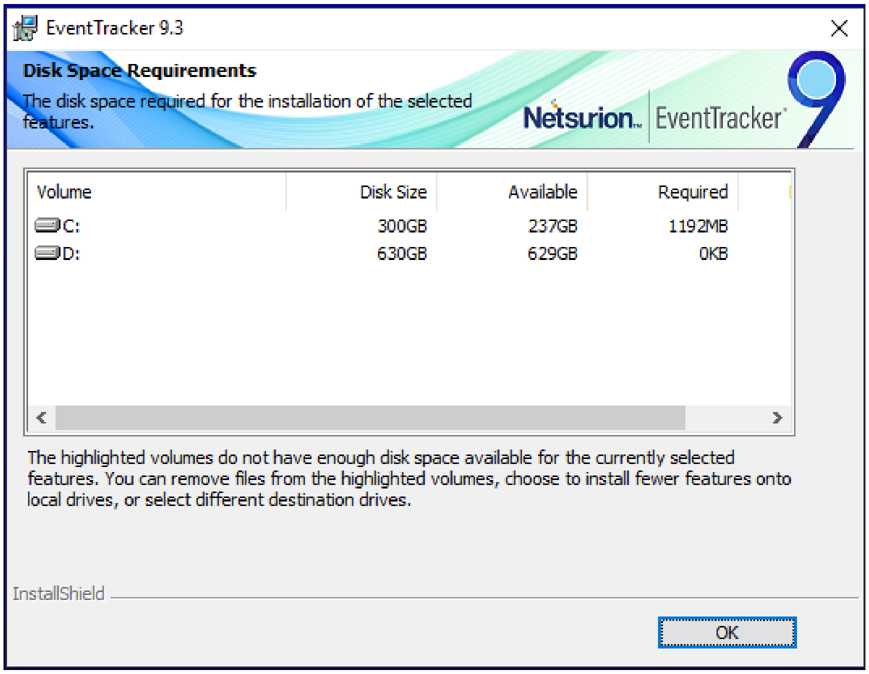
Figure 36

EventTracker Components	Description
EventTracker Console	Select this option 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 agent component will also be installed along with the Manager Console. You can also deploy the agent 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.

Table 6

Click	To
Change…	Select a different destination folder to install EventTracker.  EventTracker 9.3 Netsurion. EventTracker InstallShield OK Cancel **Change Current Destination Folder** Browse to the destination folder. Look in: Prism Microsystems EventTracker Folder name: C:\Program Files (x86)\Prism Microsystems\ Figure 37
Help	View **Select Component** conventions.  EventTracker 9.3 Netsurion. EventTracker InstallShield OK **Select Components Tips** Custom Setup allows you to selectively install progr… The icon next to the feature name indicates the install state of the feature. Click the icon to drop down the install state menu for each feature. This install state means the feature… Will be completely installed to the local hard drive. Will have some subfeatures installed to the local hard drive. (Available only if the feature has subfeatures.) Will not be installed. Will be useful for same build to same build upgradation. (Available only if the feature supports this option.) Figure 38

Check the disk space available on the target computer.



Disk Space Requirements

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

Volume	Disk Size	Available	Required
C:	300GB	237GB	1192MB
D:	630GB	629GB	0KB

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.

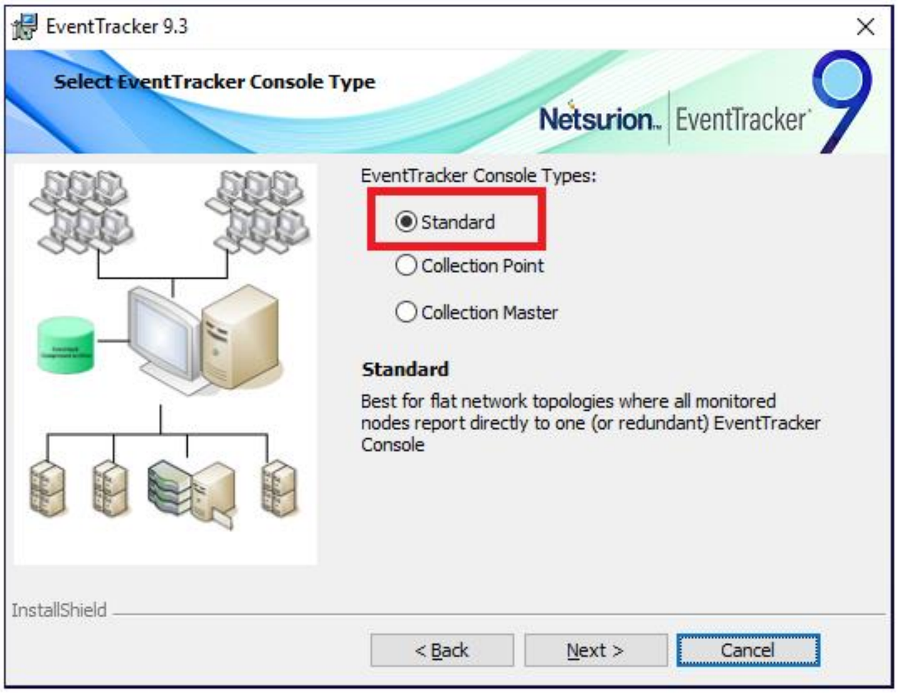
Figure 39

20. Click Next.

    InstallShield Wizard opens the **Select EventTracker Console Type** screen.

Standard Console:

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



EventTracker 9.3

Select EventTracker Console Type

EventTracker Console Types:

● Standard

○ Collection Point

○ Collection Master

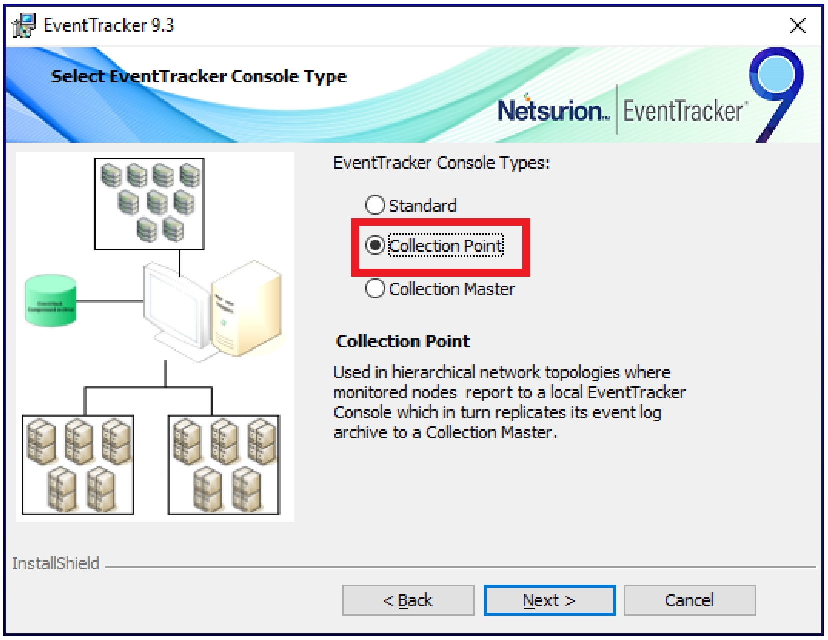
Standard

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

Figure 40

Collection Point:

Used in hierarchical network topologies where monitored nodes report to a local EventTracker Console which in turn replicates its event log archive to a Collection Master.



EventTracker 9.3

Select EventTracker Console Type

EventTracker Console Types:

○ Standard

● Collection Point

○ Collection Master

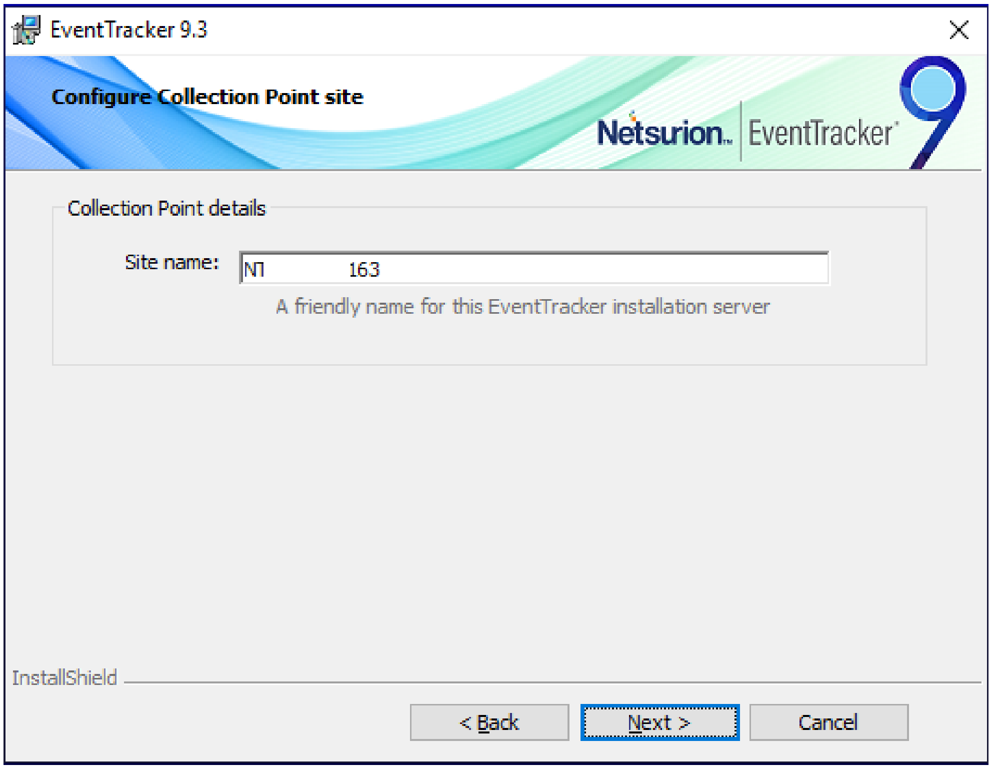
Collection Point

Used in hierarchical network topologies where monitored nodes report to a local EventTracker Console which in turn replicates its event log archive to a Collection Master.

Figure 41

a) Select the console type as **Collection Point**, and then click **Next**.
   InstallShield Wizard opens the Configure Collection Point site page.

b) Enter **Site name:** and then click **Next**.



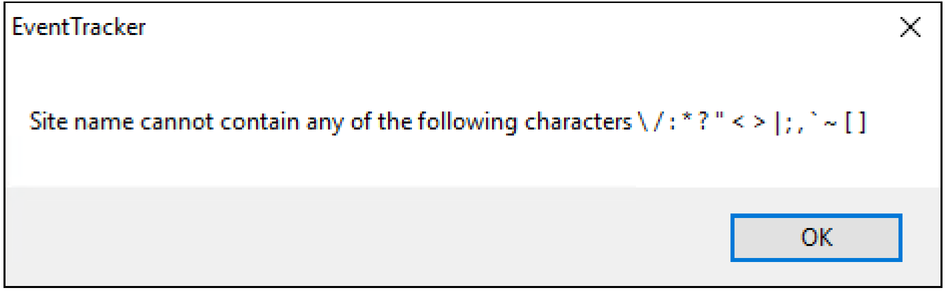
Site name: NT 163

A friendly name for this EventTracker installation server

Figure 42

NOTE:

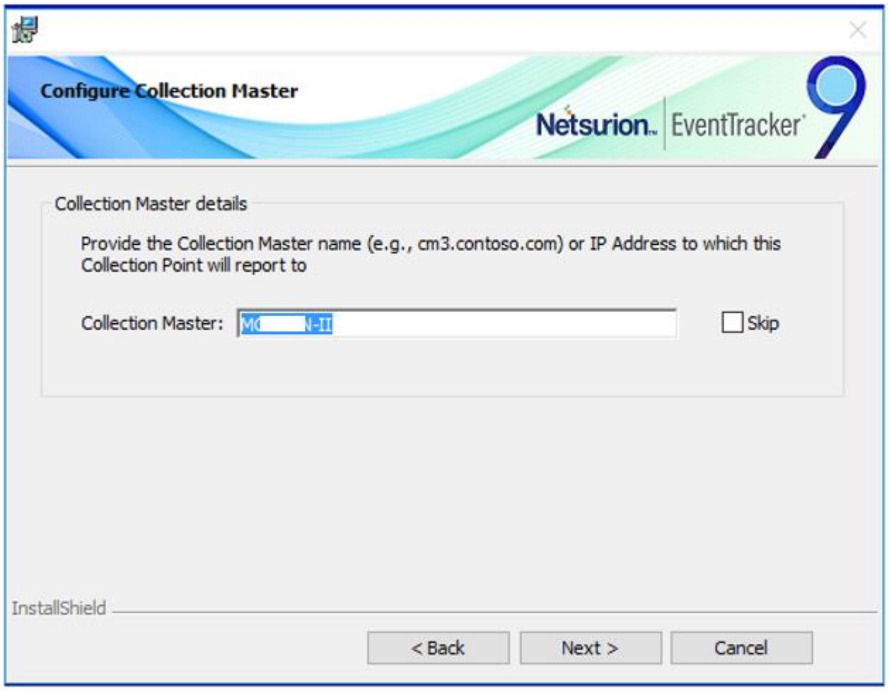
Some special characters are not allowed while providing site/group name. InstallShield Wizard displays a message if the site or group name is provided with such special characters.



Site name cannot contain any of the following characters \ / : * ? " < > | ; , ` ~ [ ]

Figure 43

c) Enter **Collection Master:** name or IP Address, and then click **Next**.



Configure Collection Master

Collection Master details

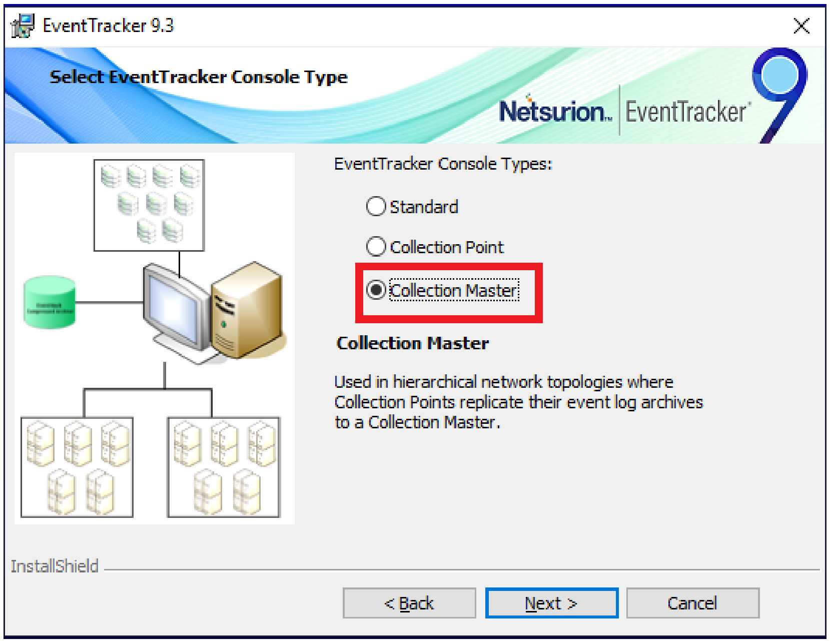
Provide the Collection Master name (e.g., cm3.contoso.com) or IP Address to which this Collection Point will report to

Collection Master: MC[redacted]N-II ☐ Skip

Figure 44

Collection Master:

Used in hierarchical network topologies where collection points replicate their event log archives to a Collection Master.



EventTracker 9.3

Select EventTracker Console Type

EventTracker Console Types:

○ Standard

○ Collection Point

● Collection Master

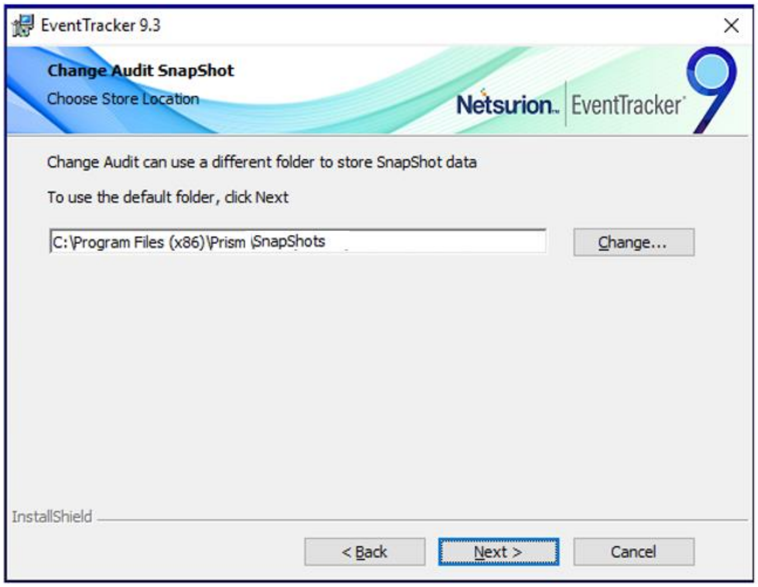
Collection Master

Used in hierarchical network topologies where Collection Points replicate their event log archives to a Collection Master.

Figure 45

21. Select a console type, and then click **Next**.

If you have selected the **Change Audit** component**,** then InstallShield Wizard opens the **Change Audit SnapShot** dialog box.



EventTracker 9.3

Change Audit SnapShot

Choose Store Location

Change Audit can use a different folder to store SnapShot data

To use the default folder, click Next

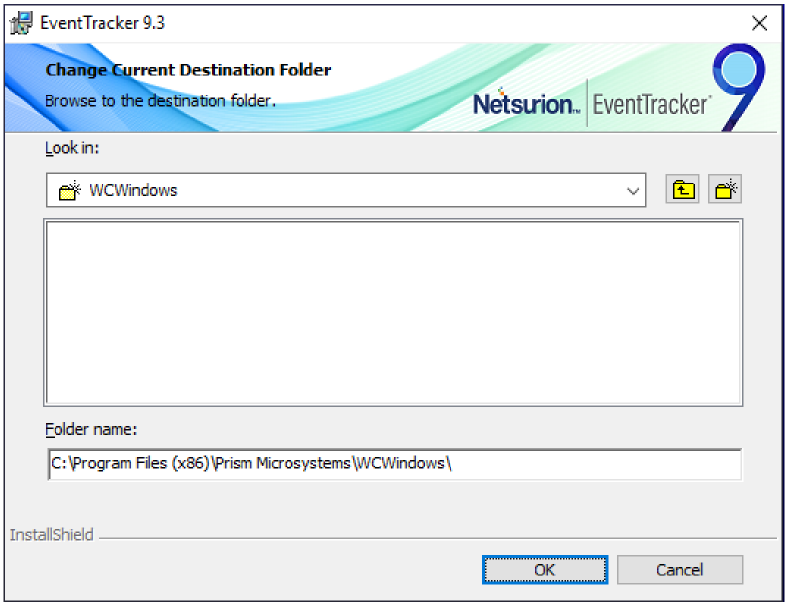
C:\Program Files (x86)\Prism \SnapShots

Figure 46

22. Click **Next** to keep the default store location.

(OR)

Click **Change** to change the snapshot store location.



EventTracker 9.3

Change Current Destination Folder

Browse to the destination folder.

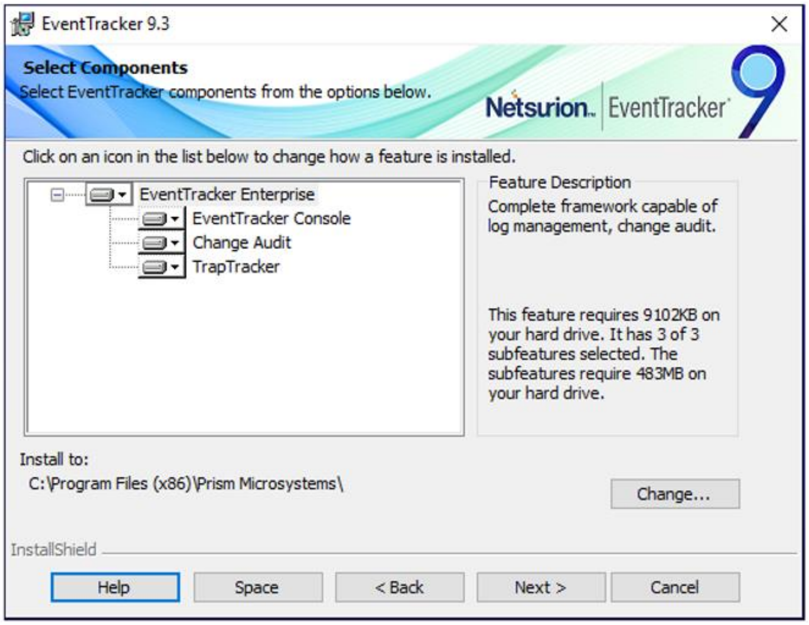
Look in: WCWindows

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

Figure 47

23. Browse the destination folder, and then click **OK**.

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.


EventTracker 9.3
Select Components
Select EventTracker components from the options below.
Netsurion. EventTracker 9

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

- EventTracker Enterprise
  - EventTracker Console
  - Change Audit
  - TrapTracker

Feature Description
Complete framework capable of log management, change audit.

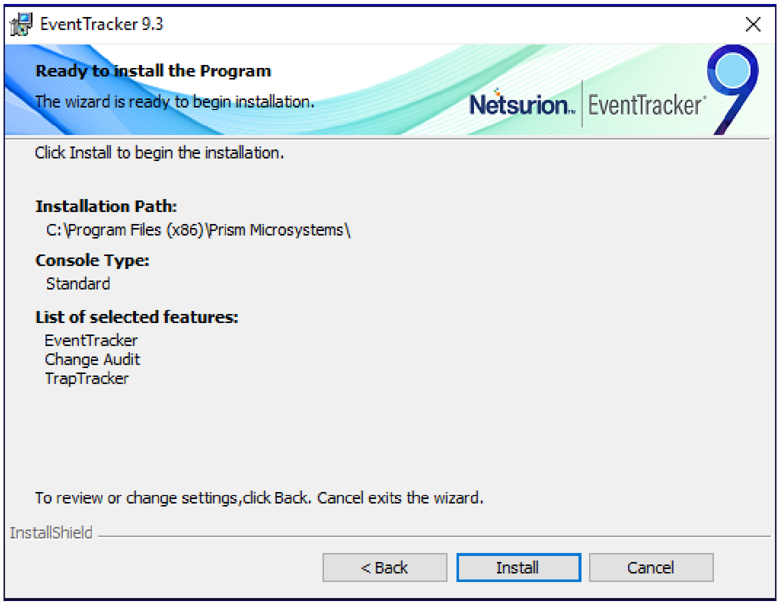
This feature requires 9102KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 483MB on your hard drive.

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

Figure 48

If you have not selected to install **Change Audit,** then InstallShield Wizard opens the **Ready to Install the Program** screen.

24. The **Ready to Install the Program** screen displays the summary of the installation path, console type, and the selected features.


EventTracker 9.3
Ready to install the Program
The wizard is ready to begin installation.
Netsurion. EventTracker 9

Click Install to begin the installation.

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

Console Type:
Standard

List of selected features:
EventTracker
Change Audit
TrapTracker

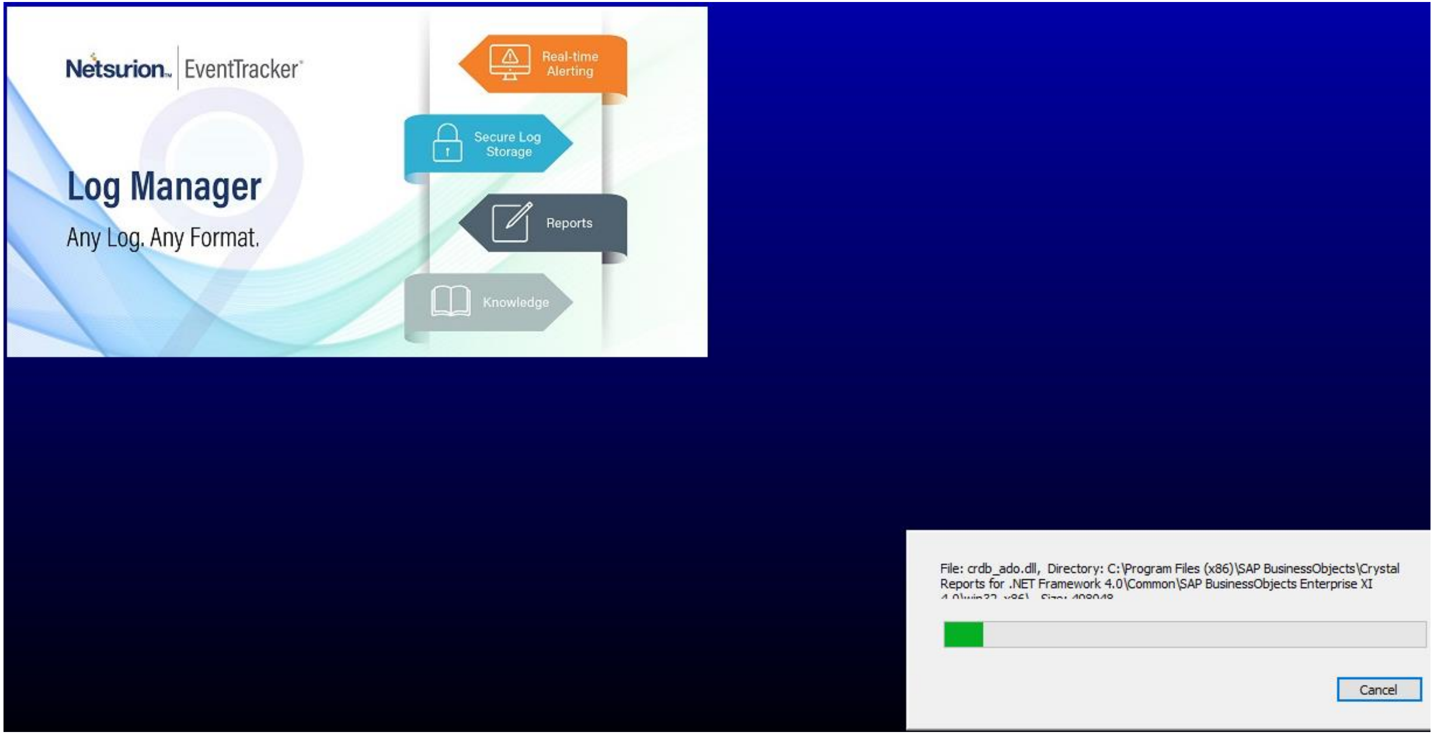
To review or change settings,click Back. Cancel exits the wizard.

InstallShield
< Back
Install
Cancel

Figure 49

25. Click **Install**.

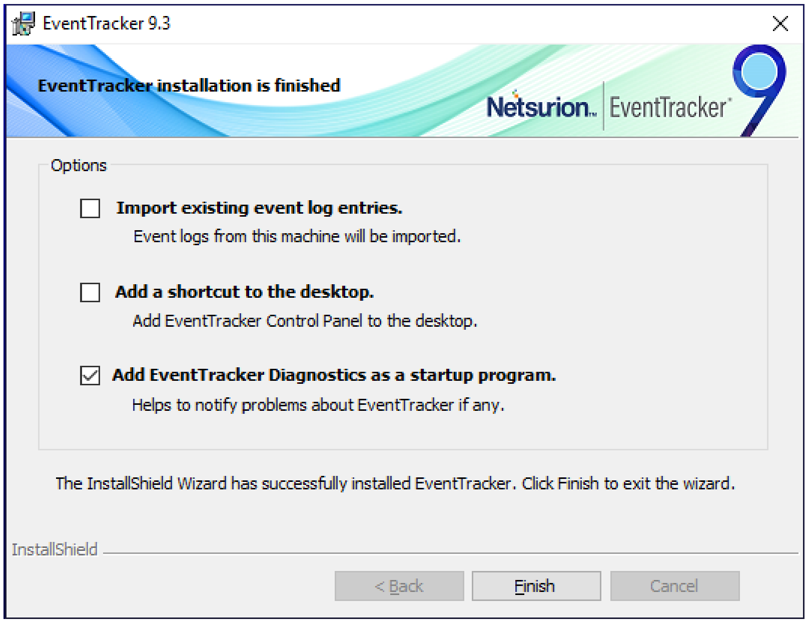
    InstallShield Wizard installs the selected components.



File: crdb_ado.dll, Directory: C:\Program Files (x86)\SAP BusinessObjects\Crystal Reports for .NET Framework 4.0\Common\SAP BusinessObjects Enterprise XI 4.0\win32_x86\, Size: 408048

Figure 50

26. InstallShield Wizard opens the last screen.



EventTracker installation is finished

☐ **Import existing event log entries.**
Event logs from this machine will be imported.

☐ **Add a shortcut to the desktop.**
Add EventTracker Control Panel to the desktop.

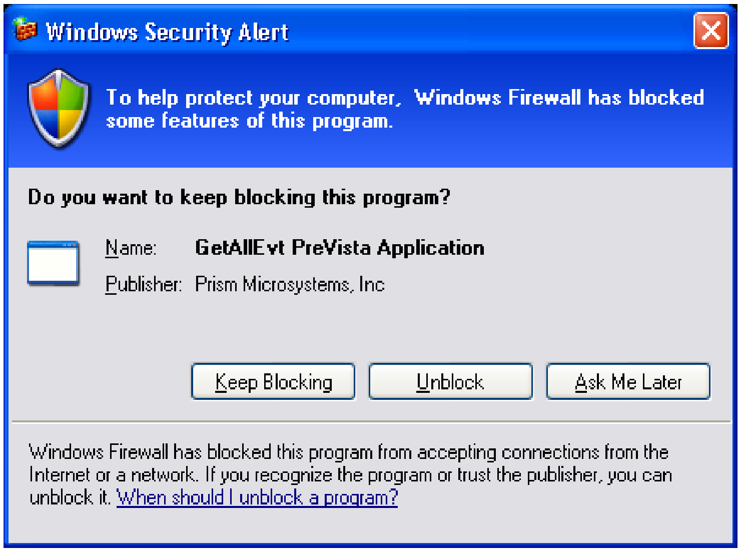
☑ **Add EventTracker Diagnostics as a startup program.**
Helps to notify problems about EventTracker if any.

The InstallShield Wizard has successfully installed EventTracker. Click Finish to exit the wizard.

Figure 51

a. Click **Import existing event log entries** option to import event logs of EventTracker.

   You will get a Microsoft Windows Security Alert message if the firewall is on.



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: GetAllEvt PreVista Application

Publisher: Prism Microsystems, Inc

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Figure 52

Firewall blocks the incoming network connection, if the **getallevt.exe** does not exist in the Program and Services Exceptions and shows a notification.

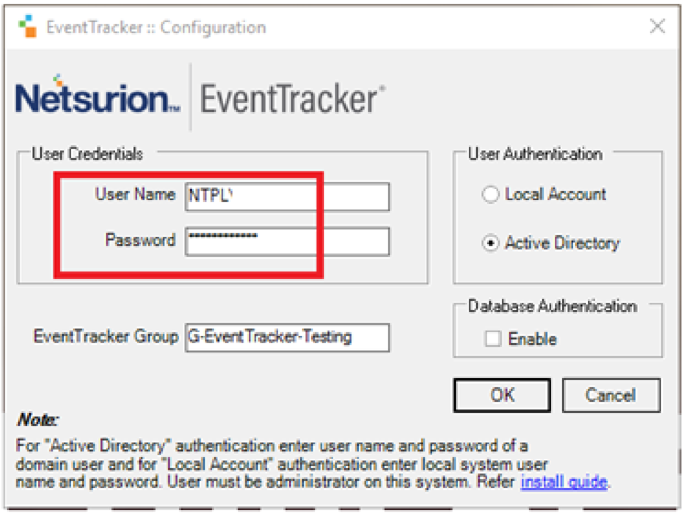
- Click **Unblock** for the **getallevt.exe** to import event logs.

b. Check to **Add a shortcut to the desktop** option, to add the shortcuts to the EventTracker application on the desktop.

- **Add EventTracker diagnostics as a startup program** option is selected by default to notify problems about EventTracker if any.

27. Click **Finish** to conclude the installation process.

InstallShield Wizard opens the **EventTracker Configuration** screen.



EventTracker :: Configuration

User Credentials

User Name: NTPL\

Password: *************

User Authentication

○ Local Account

● Active Directory

Database Authentication

□ Enable

EventTracker Group: G-EventTracker-Testing

Note:

For "Active Directory" authentication enter user name and password of a domain user and for "Local Account" authentication enter local system user name and password. User must be administrator on this system. Refer install guide.

Figure 53

NOTE:

Select/enter the correct **User Credentials, User Authentication and EventTracker Group** to log in successfully. The username/authentication that is done in EventTracker Preinstall, Check reflects in this screen, but the user has the option to override it.

28. Type valid user credentials in the **User Name** and **Password** fields respectively.

NOTE:
EventTracker services run under this account. By default, this user is assigned the 'EventTracker Administrator' role and can login to EventTracker.

29. Select a **User Authentication** option.

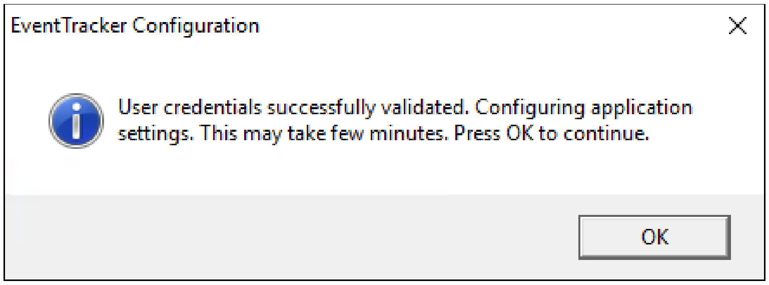
    Local Account: Authentication is done locally on the computer where EventTracker is installed.

    Active Directory: Authentication is done in the Active Directory.

30. Type the EventTracker group name in the **EventTracker Group** field.

31. Click **OK**.

After successfully validating the user credentials, InstallShield[R] Wizard displays the **EventTracker Configuration** message box.



EventTracker Configuration

User credentials successfully validated. Configuring application settings. This may take few minutes. Press OK to continue.

Figure 54

32. Click **OK**.

NOTE:
If the password is changed for the above-configured user, it is mandatory to re-run the EventTracker Configuration (Figure: 72) with the updated password.

1. To find '**EventTracker Configuration'**, click **Start**, point to **All Programs**.
2. Click **Prism Microsystems**, click **EventTracker** and then click **EventTracker Configuration.**
3. Enter appropriate credentials and then click **OK.**

3.5 Procedure to install EventTracker Manager - Standard / Collection Point Evaluation Version

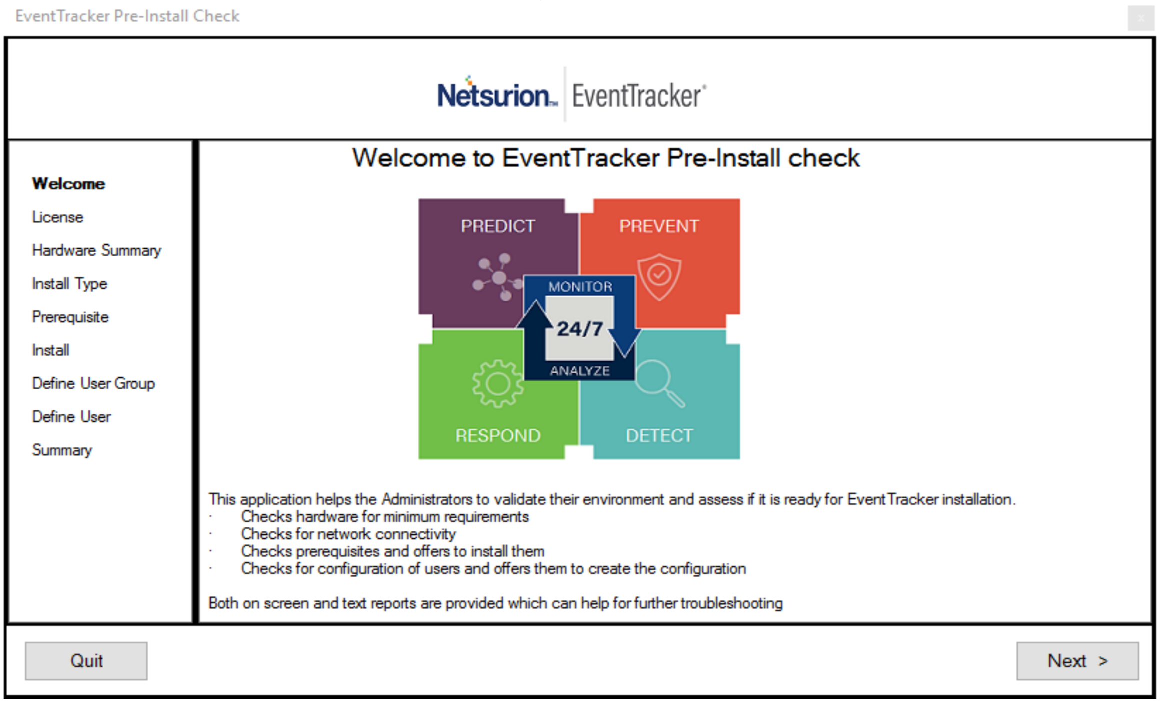
NOTE:

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 is 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 the EventTracker 21-day trial – Standard/Collection Point.

1. Double-click the executable file.
   EventTracker Pre-Install Check window opens.



Welcome to EventTracker Pre-Install check

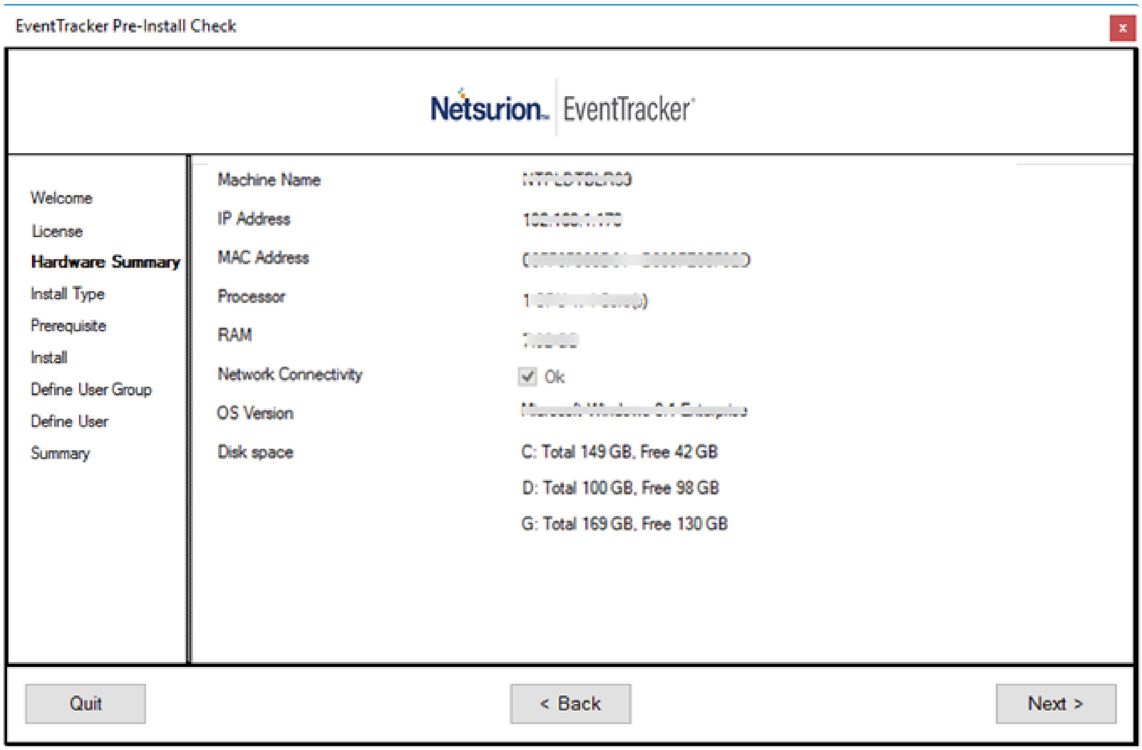
This application helps the Administrators to validate their environment and assess if it is ready for Event Tracker installation.

- Checks hardware for minimum requirements
- Checks for network connectivity
- Checks prerequisites and offers to install them
- Checks for configuration of users and offers them to create the configuration

Both on screen and text reports are provided which can help for further troubleshooting

Figure 55

2. Click **Next**.
   Hardware Summary pane opens.



EventTracker Pre-Install Check

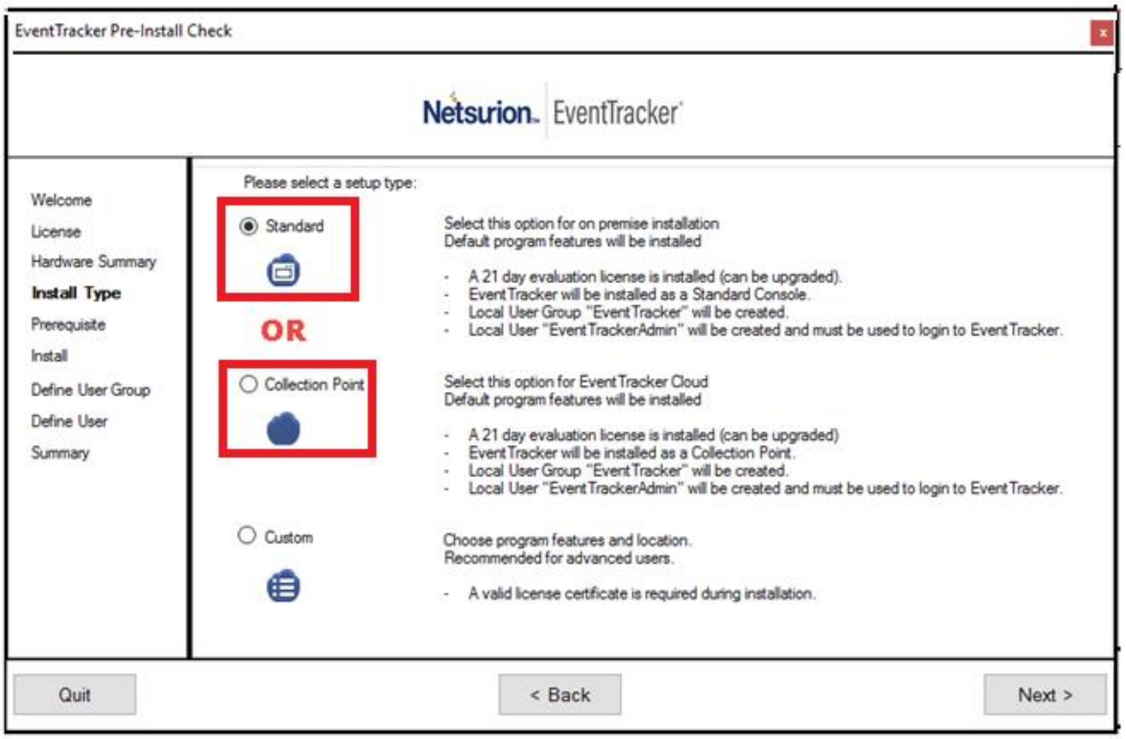
Netsurion. EventTracker

- Welcome
- License
- **Hardware Summary**
- Install Type
- Prerequisite
- Install
- Define User Group
- Define User
- Summary

Machine Name	[redacted]
IP Address	[redacted]
MAC Address	[redacted]
Processor	[redacted]
RAM	[redacted]
Network Connectivity	☑ Ok
OS Version	[redacted]
Disk space	C: Total 149 GB, Free 42 GB D: Total 100 GB, Free 98 GB G: Total 169 GB, Free 130 GB

Figure 56

3. Select **Standard/Collection Point** option, and then click **Next**.



EventTracker Pre-Install Check

Netsurion. EventTracker

- Welcome
- License
- Hardware Summary
- **Install Type**
- Prerequisite
- Install
- Define User Group
- Define User
- Summary

Please select a setup type:

● Standard

Select this option for on premise installation
Default program features will be installed

- A 21 day evaluation license is installed (can be upgraded).
- EventTracker will be installed as a Standard Console.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.

OR

○ Collection Point

Select this option for EventTracker Cloud
Default program features will be installed

- A 21 day evaluation license is installed (can be upgraded)
- EventTracker will be installed as a Collection Point.
- Local User Group "EventTracker" will be created.
- Local User "EventTrackerAdmin" will be created and must be used to login to EventTracker.

○ Custom

Choose program features and location.
Recommended for advanced users.

- A valid license certificate is required during installation.

Figure 57

To proceed with the further installation, refer to the ETLM-Install Guide.

NOTE: After logging into EventTracker, some of the components are not available as it is a trial version.

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

4. Deploying EventTracker Windows Agent

4.1 Pre-install Instructions for Windows Agent

- You must have **Local Admin** privileges on the remote systems where you want to remotely install the **Agents**.
- You can also install **Agents** 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 50MB that can be used by the **Agent**.
- If the remote system is accessed through a **VPN** with slow line speed, the install may take time and it is recommended that you schedule your activities accordingly.
- To monitor a system that supports syslog messages (e.g. Unix, Linux, and Cisco, etc.) configure that specific system to forward the syslog messages to EventTracker Manager.

4.2 Pre-install checklist for Windows Agent

The pre-installation checklist describes the specific settings, permissions, and privileges that are required for deploying the EventTracker agent. Read the checklist before installation to ensure safe and smooth agent installation.

ENSURE	**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
VERIFY	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 EventTracker Manager system.

Table 7

4.3 Different methods to install EventTracker Agents

There are 2 methods to deploy EventTracker Agents. This can be done by:

a. Using the **System Manager** that is installed as part of the EventTracker Manager. From this **System Manager**, EventTracker Agents can be deployed onto all computers identified as EventTracker Agents.
(OR)
b. Using the **Manual Agent** Installation package on all computers identified as EventTracker Agents.

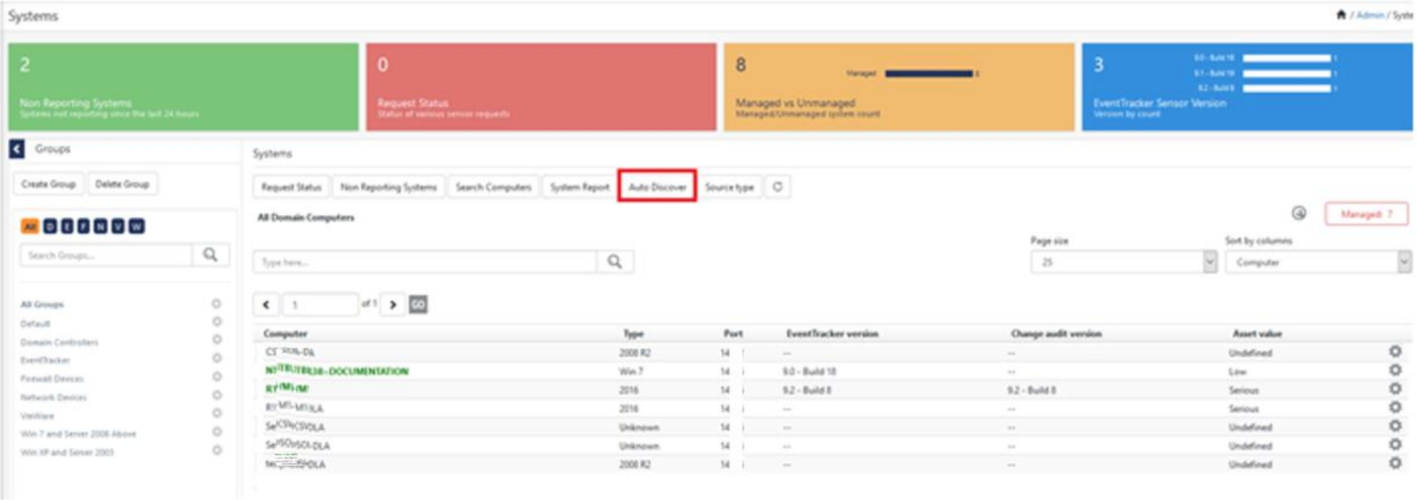
4.4 Deploying EventTracker Windows Agent via System Manager for Agent Based (full featured)

The installation procedure is identical for all supported Microsoft Windows operating systems.

1. Log into EventTracker web.
   EventTracker opens the login page.

2. Logon with valid user credentials.
   EventTracker opens the Incident dashboard.

3. Click the Admin drop-down list at the upper-right corner, and then click Systems.
   EventTracker opens the Systems manager page.



Computer	Type	Port	EventTracker version	Change audit version	Asset value
CT [illegible]-DL	2008 R2	14	--	--	Undefined
N[illegible]TBR38-DOCUMENTATION	Win 7	14	9.0 - Build 18	--	Low
RY[illegible]	2016	14	9.2 - Build 8	9.2 - Build 8	Serious
RY[illegible]XLA	2016	14	--	--	Serious
Se[illegible]SVDLA	Unknown	14	--	--	Undefined
Se[illegible]SOI-DLA	Unknown	14	--	--	Undefined
te[illegible]DLA	2008 R2	14	--	--	Undefined

Figure 58

This console displays the list of systems that are members of all trusted domains provided if **Auto Discover** is ON. Otherwise only the EventTracker Manager system is opens. It also indicates the operating system type, asset value, port number, and managed system status through which the agent communicates with the 'EventTracker Receiver'.

4. Click the Gear ⚙ icon in the system group on the right-pane in which the target systems exist. EventTracker displays the shortcut menu.

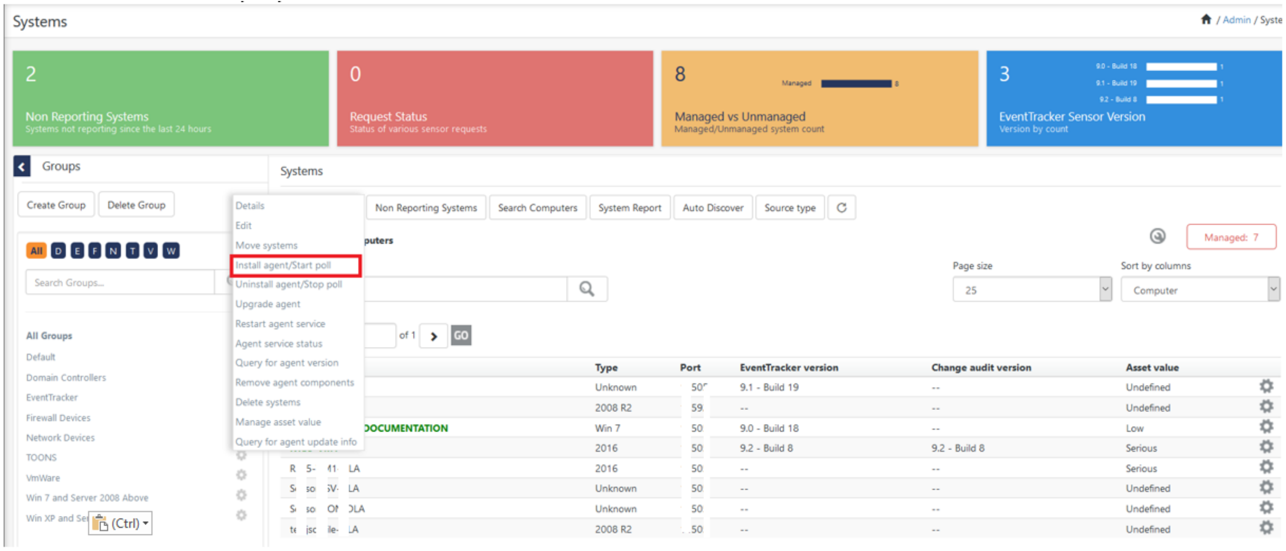
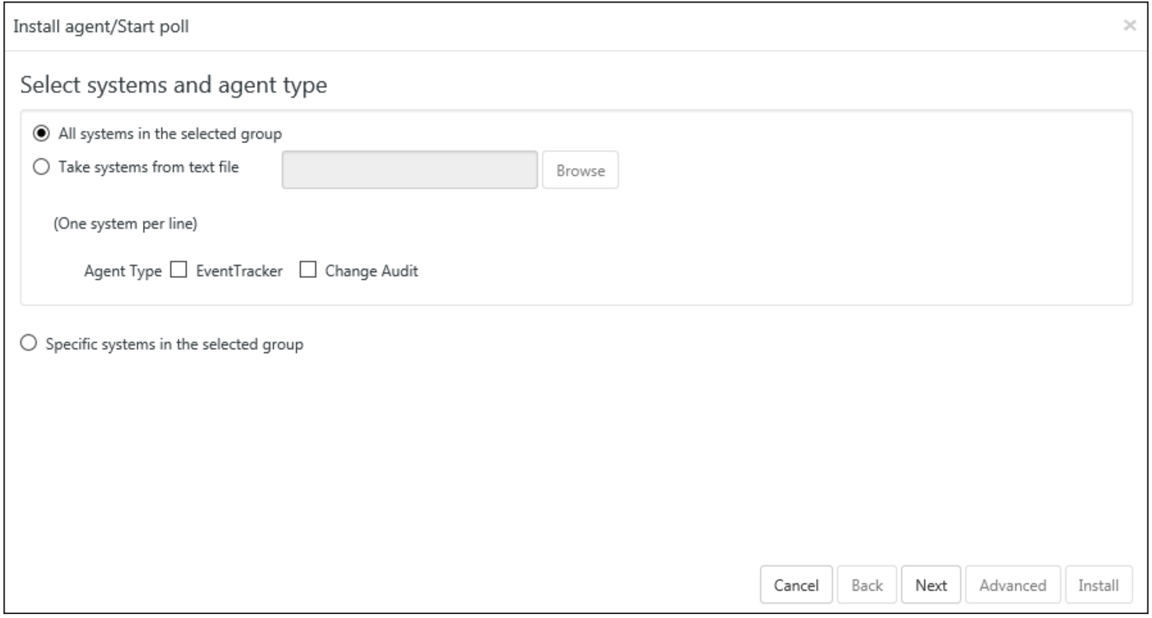


Figure 59

5. From the shortcut menu, click **Install agent/Start poll** option. EventTracker opens the **Install agent/Start poll** dialog box.


Install agent/Start 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

Figure 60

There are various options to **Select systems and agent types.** They are

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

Details are given in the below table.

Option	***To***
All systems in the selected group	Click this option to install agents on all the systems present in the selected group.
Take systems from the text file	Create a text file containing agent system names on which the agent is to be installed. The text file should contain one system name per line. If you select this option, then browse the text file to select the agent system names.
Agent type	Select the agent type to be Installed
Specific systems in the selected group	Out of all the systems present in the group, select the specific system(s) to install the agent.

Table 8

6. Click **Next.**
7. To install the EventTracker/Change Audit Agent on all the systems present in the domain, select the respective EventTracker/Change Audit option.

   (OR)

   Select the respective check box against the systems where you want to deploy the EventTracker/Change Audit agent.

   (OR)

In the **System** manager page, move the mouse pointer over the system where you want to install the agent.

1. Click **dropdown**.
   EventTracker displays the drop-down list.
2. Click **Install agent/ Start poll**.

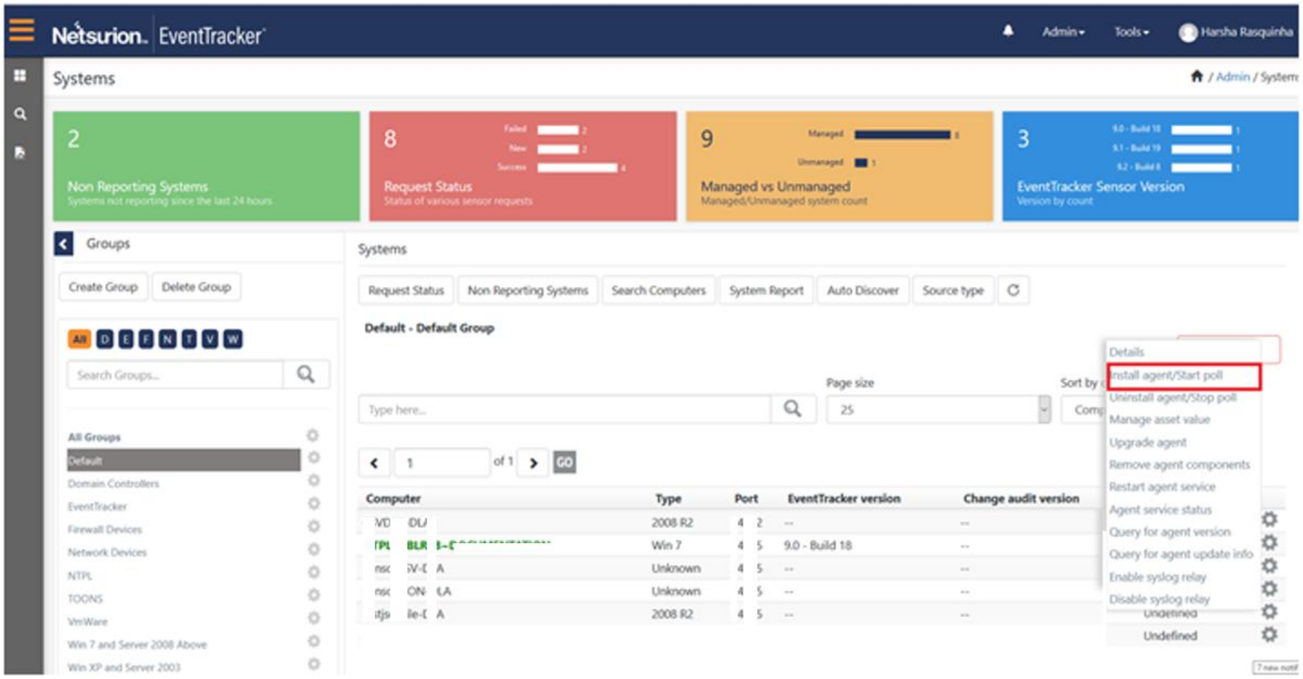
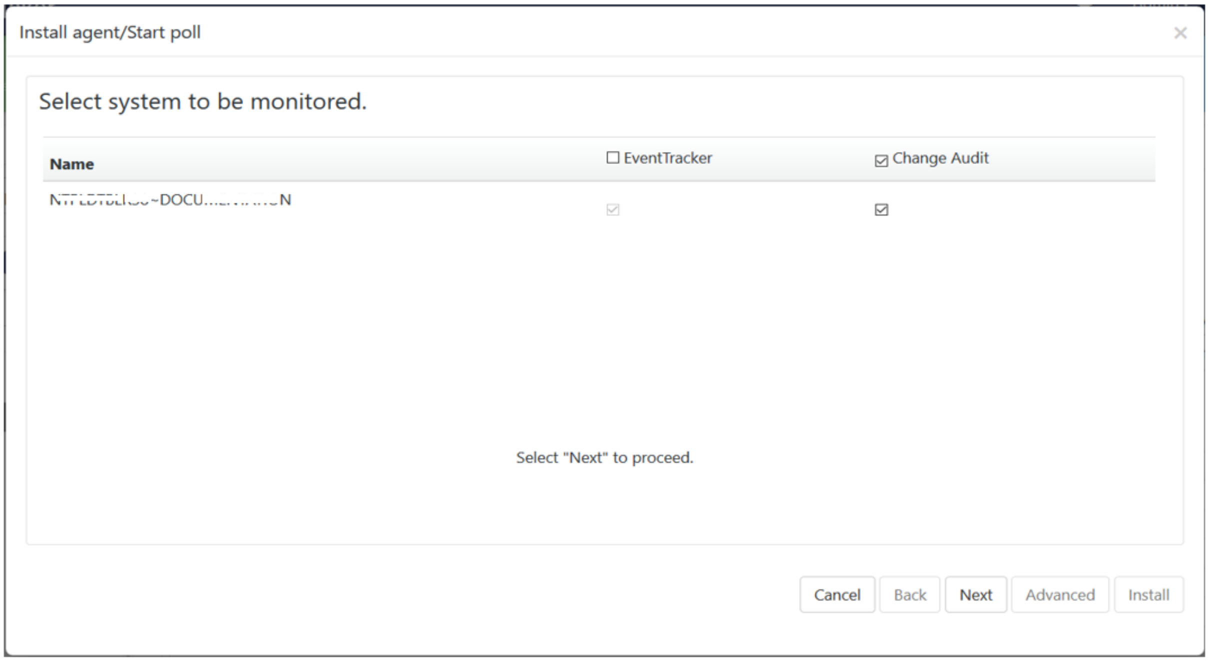


Figure 61

EventTracker displays the **Install Agent/Start poll** dialog box.


Install agent/Start poll

Select system to be monitored.

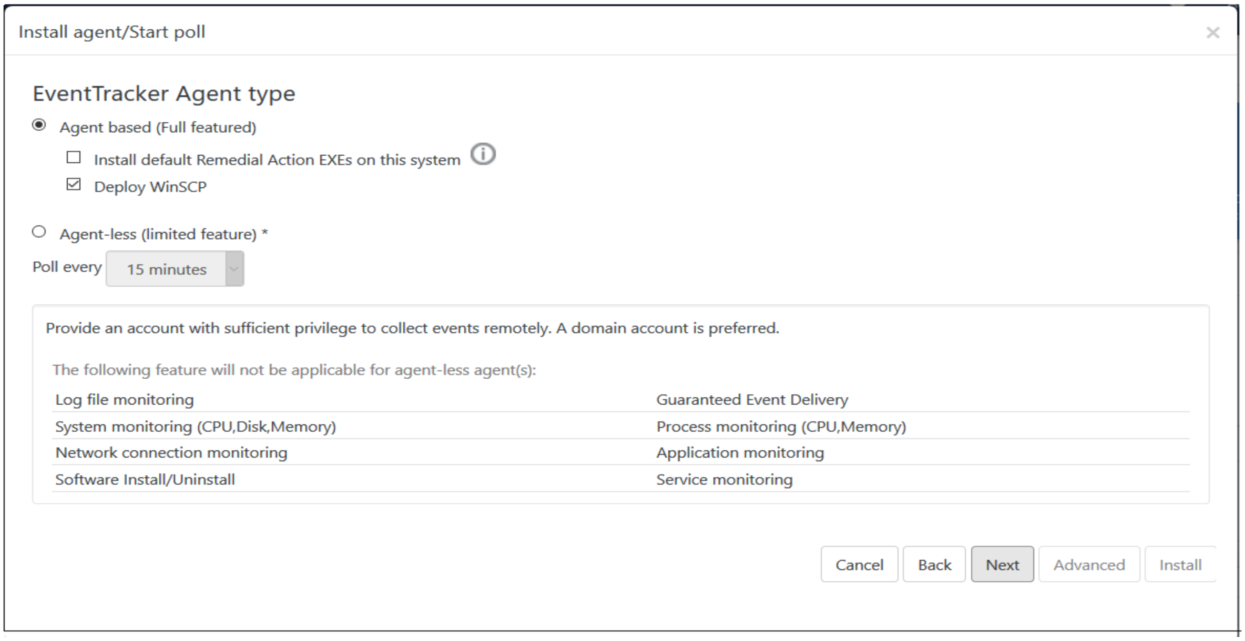
Name	☐ EventTracker	☑ Change Audit
[redacted]	☑	☑

Select "Next" to proceed.

Figure 62

3. Check the **EventTracker** option to install the EventTracker agent.
4. Check the **Change Audit** option to install the Change Audit agent.
5. Click **Next**.

6. Select **EventTracker Agent Type i.e. Agent based (Full Featured) / Agent-less (limited feature)*** option.



Install agent/Start poll

EventTracker Agent type

● Agent based (Full featured)

□ Install default Remedial Action EXEs on this system

☑ Deploy WinSCP

○ Agent-less (limited feature) *

Poll every 15 minutes

Provide an account with sufficient privilege to collect events remotely. A domain account is preferred.

The following feature will not be applicable for agent-less agent(s):

Log file monitoring	Guaranteed Event Delivery
System monitoring (CPU,Disk,Memory)	Process monitoring (CPU,Memory)
Network connection monitoring	Application monitoring
Software Install/Uninstall	Service monitoring

Figure 63

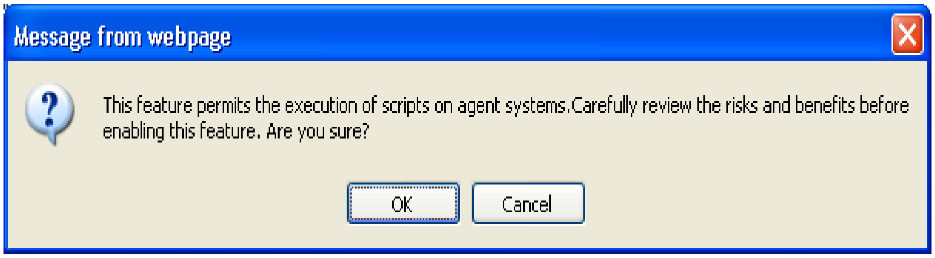
Agent based (Full featured)	
Install default Remedial Action EXEs on this system	**Remedial Actions** are scripts or executable files that can be launched at either the agent or the manager side, in response to events. If this option is enabled, predefined scripts are placed in the EventTracker\Agent\Script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

Table 9

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

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

      EventTracker displays a message box.



Message from webpage

This feature permits the execution of scripts on agent systems.Carefully review the risks and benefits before enabling this feature. Are you sure?

Figure 64

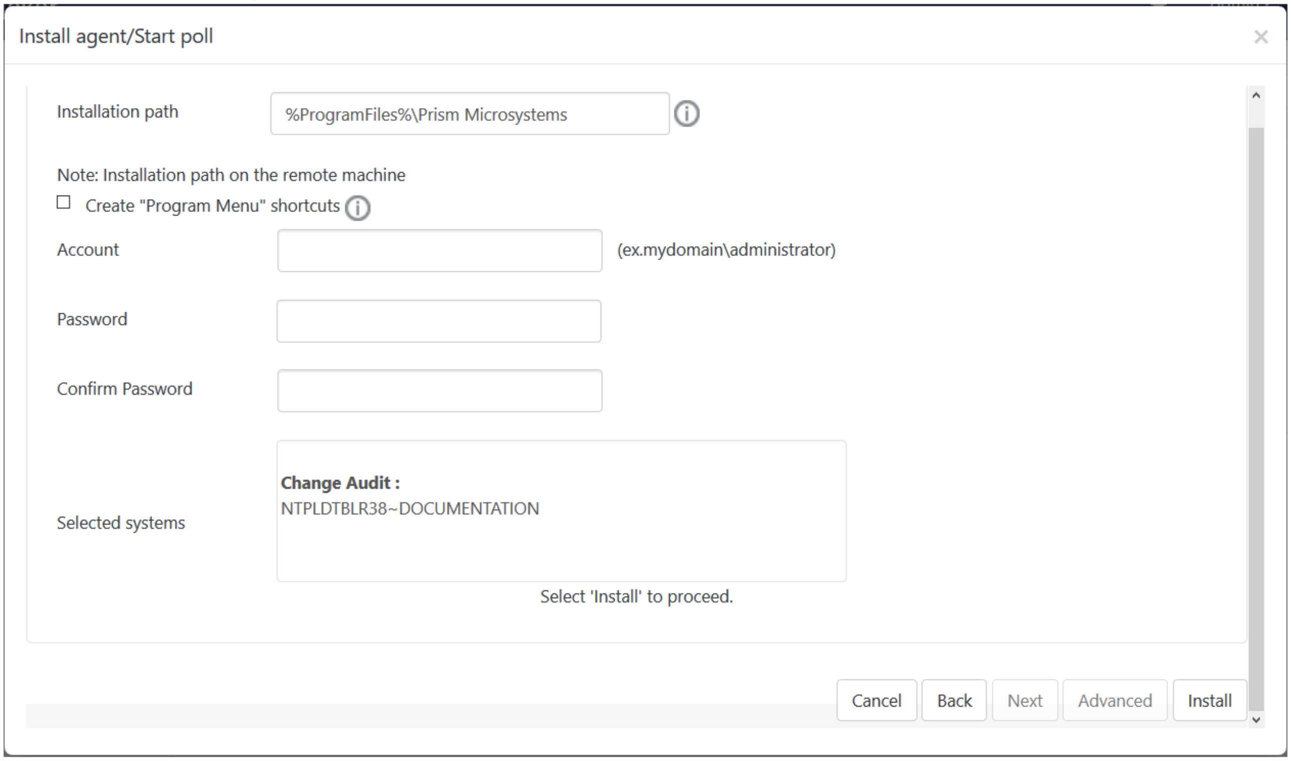
NOTE:

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

ii. Click **OK** to install remedial action EXEs
(OR)
Click **Cancel** to not to install remedial action EXEs.

iii. Click **Next**.

EventTracker displays the Install agent/Start poll dialog box with the default client installation path on the remote computer.



Install agent/Start poll

Installation path: %ProgramFiles%\Prism Microsystems

Note: Installation path on the remote machine

□ Create "Program Menu" shortcuts

Account: (ex.mydomain\administrator)

Password:

Confirm Password:

Selected systems: **Change Audit :** NTPLDTBLR38~DOCUMENTATION

Select 'Install' to proceed.

Figure 65

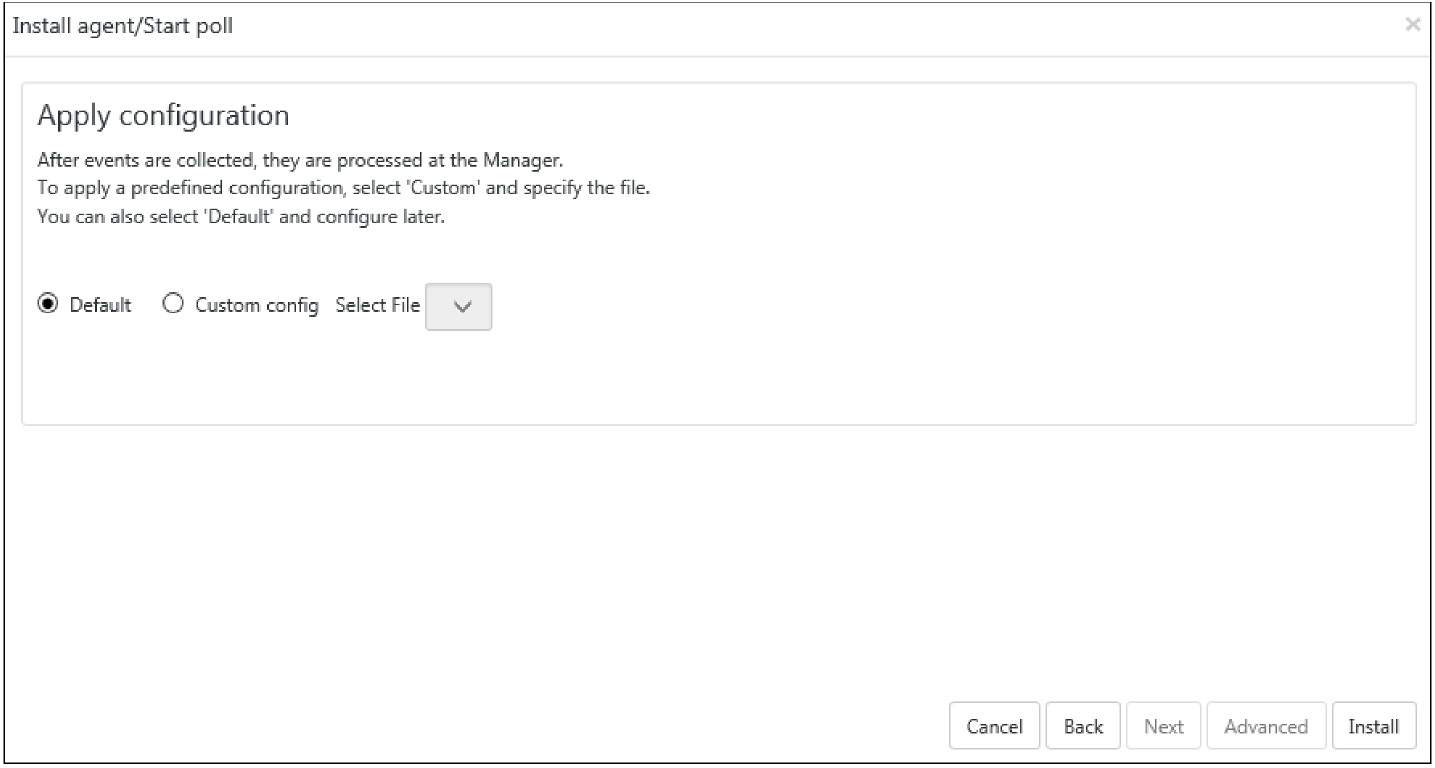
8. To install the agent in a different drive apart from the default one, type the new installation path in the **Select installation path on the remote machines** field.
9. Check the **Create 'Program Menu' shortcuts** option to create shortcuts.
10. Enter valid **Account** name and **Password**.

11. Reenter the password in **Confirm Password**.
12. Click **Install**.

The agent is installed on the selected machine with the default ‘etaconfig.ini’ configuration.
(OR)

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

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



Install agent/Start poll

Apply configuration

After events are collected, they are processed at the Manager.
To apply a predefined configuration, select 'Custom' and specify the file.
You can also select 'Default' and configure later.

● Default ○ Custom config Select File

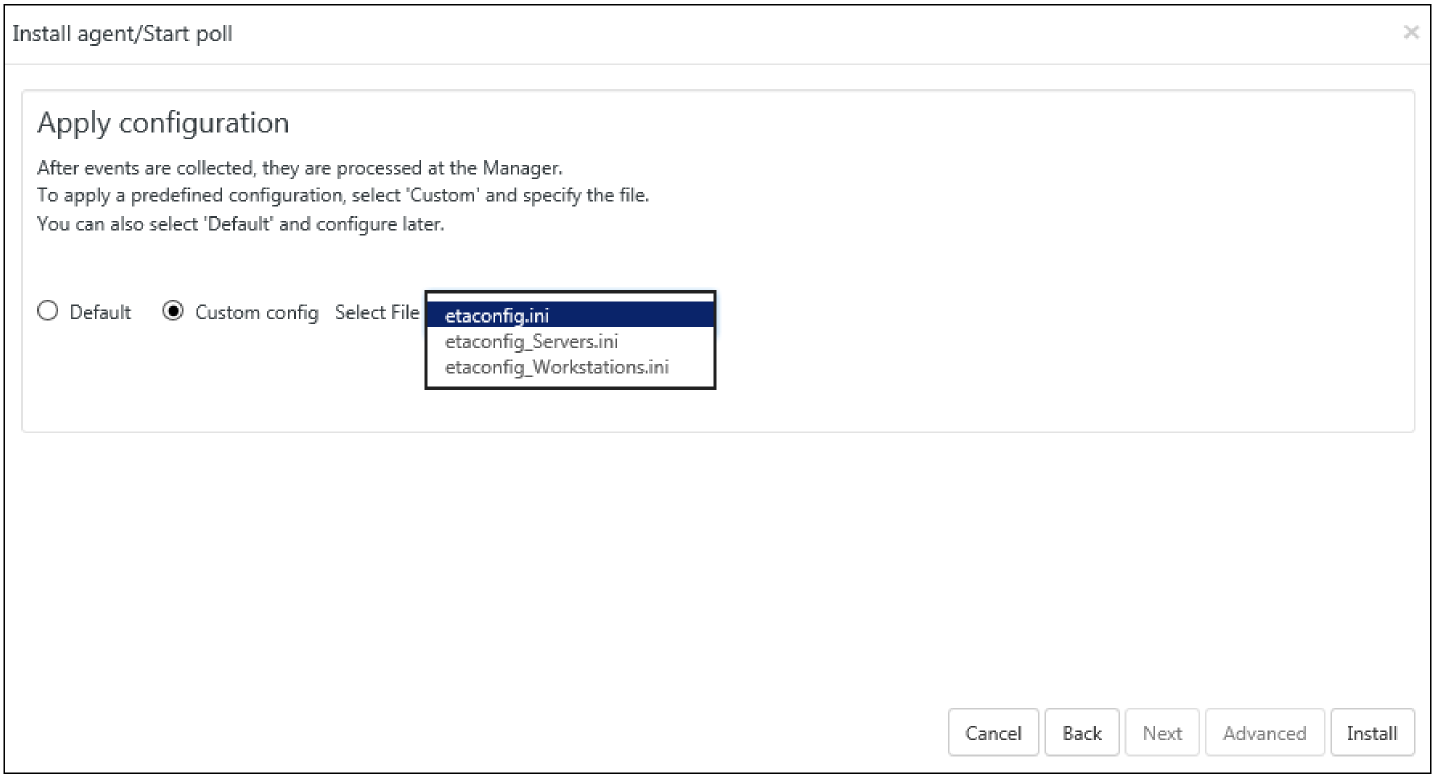
Figure 66

b) Select the **Default** or **Custom config** option to select a custom configuration file as per the requirement.

The custom configuration will provide you the templates that you have created in Agent configuration and two more predefined templates.

You can select the template of your choice.

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



Install agent/Start poll

Apply configuration

After events are collected, they are processed at the Manager.
To apply a predefined configuration, select 'Custom' and specify the file.
You can also select 'Default' and configure later.

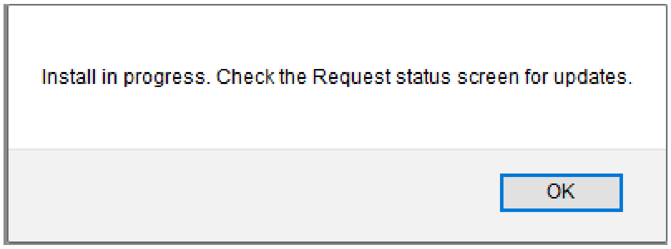
○ Default ● Custom config Select File etaconfig.ini

Figure 67

NOTE:

In case you select **etaconfig_Servers.ini, etaconfig_Workstations.ini,** The Manager Name will be empty after installation. If you want to use any of the pre-defined configuration (i.e. **etaconfig_Servers.ini, etaconfig_Workstations.ini**) you have to configure the Manager.

c) Select the configuration file from the **File** dropdown, and then click **Install**. EventTracker displays the pop-up window with the appropriate message.

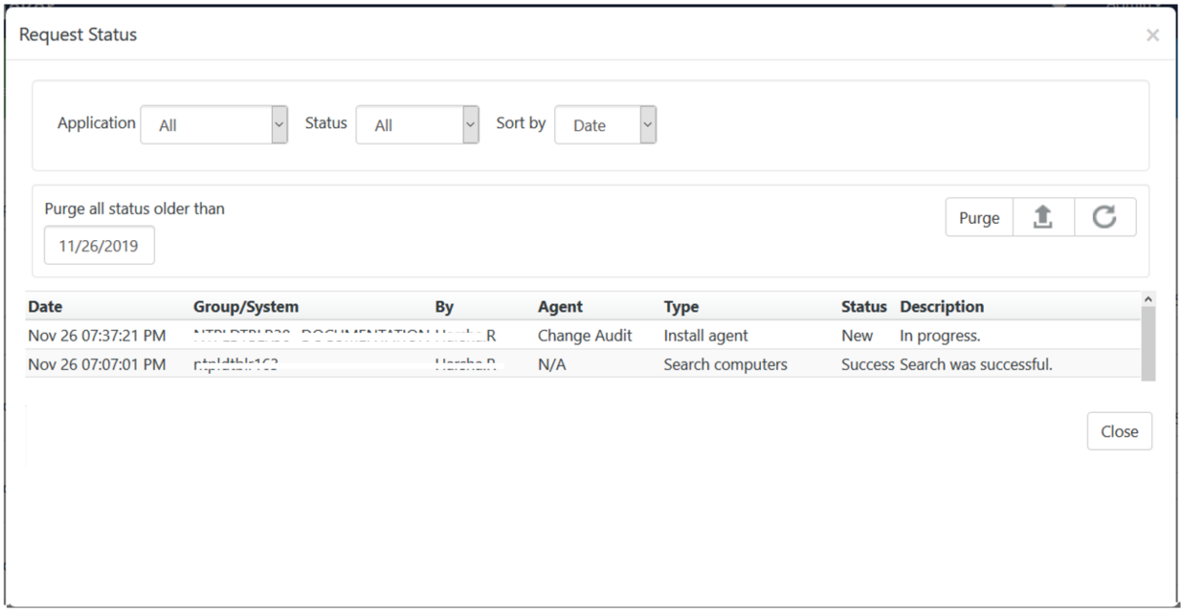


Install in progress. Check the Request status screen for updates.

Figure 68

13. Click **OK.**

    EventTracker displays **Request Status** screen.



Request Status

Application: All | Status: All | Sort by: Date

Purge all status older than: 11/26/2019

Date	Group/System	By	Agent	Type	Status	Description
Nov 26 07:37:21 PM	[redacted]	[redacted]	Change Audit	Install agent	New	In progress.
Nov 26 07:07:01 PM	[redacted]	[redacted]	N/A	Search computers	Success	Search was successful.

Figure 69

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

Table 10

14. Click **Refresh** ⟳ to view the current status.

(OR)
Reopen the **Request Status** dialog box to see the updated status.

15. Click **Close.**
16. Refresh the **System** manager.

4.5 Configuring EventTracker Windows Agent

All configurations for the agent(s) are set by default during installation. If you are interested in changing the default configuration settings, then

1. Open **EventTracker Control Panel**.

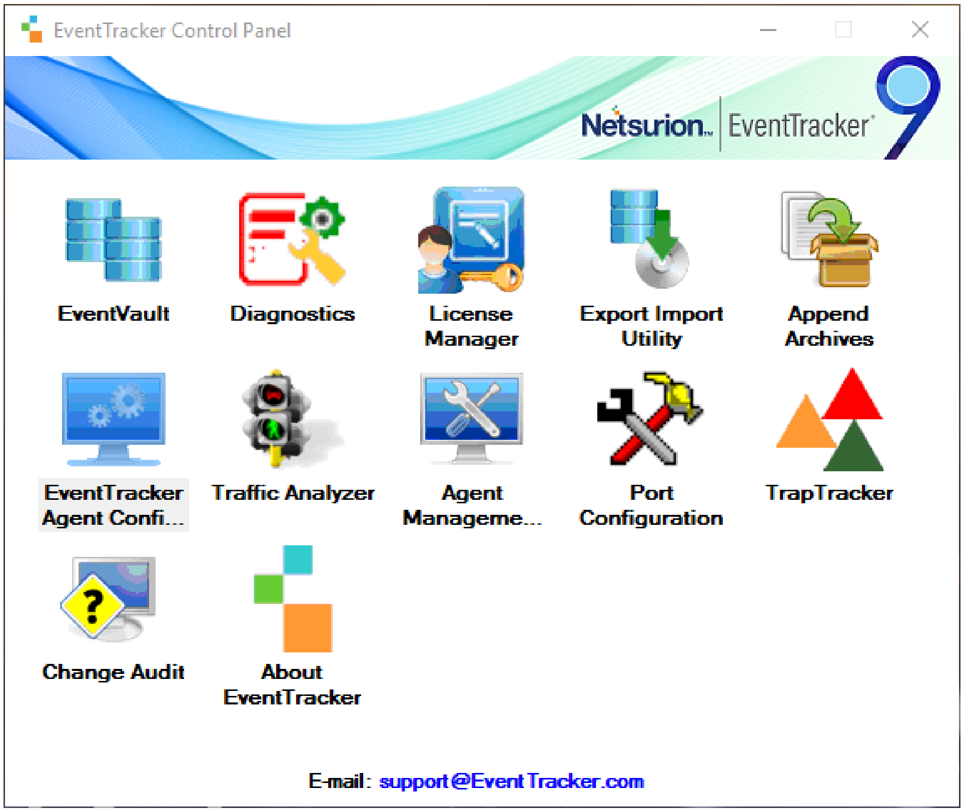
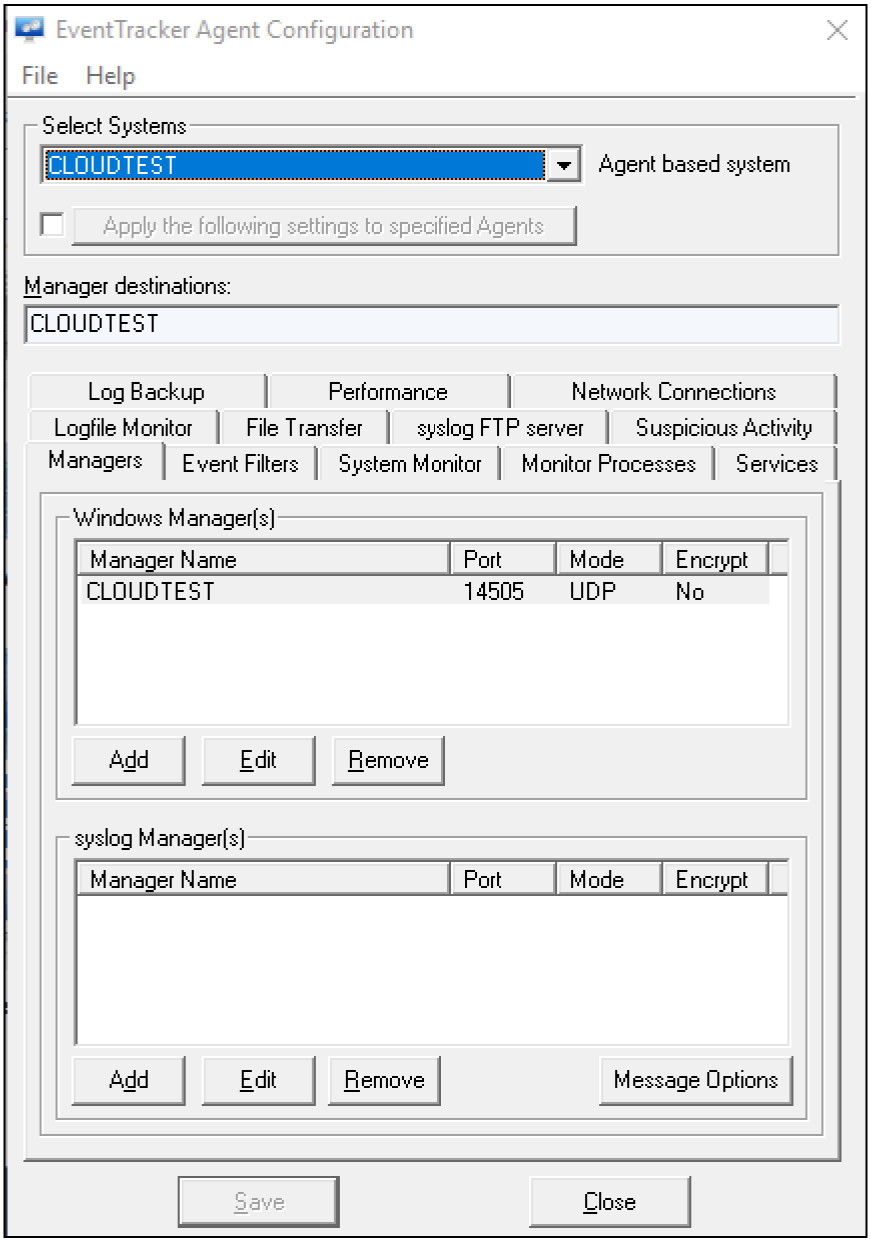


Figure 70

2. Double-click **EventTracker Agent Configuration**.

   EventTracker Agent Configuration window opens.



Select Systems: CLOUDTEST ▾ Agent based system

□ Apply the following settings to specified Agents

Manager destinations:
CLOUDTEST

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
CLOUDTEST	14505	UDP	No

syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 71

3. Click appropriate tabs and configure the agent as your requirement.

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

In case if it is not possible or desirable to install the EventTracker Windows Agent, EventTracker can be configured to subscribe/poll the event log of remote computers over the network to collect new event log entries.

Pros

No agent to deploy – Simpler product deployment. There is lesser effort during planning, deployment and upgrade.

Cons

- Increased network load – Depending on the selected polling cycle or level of event generation, network load is greater.
- Greater dependency, 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 – This feature is not available.
- Application monitoring – This feature is not available.
- Software install/removal monitoring – This feature is not available.
- Service monitoring – This feature is not available.
- Monitoring external log files – This feature is not available.
- Host-based intrusion detection – This feature is not available.
- Non-domain topologies not supported – This feature is only available when the Console and target machine are in the same Windows domain.

4.6.1 Adding Systems for Agent-less monitoring

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

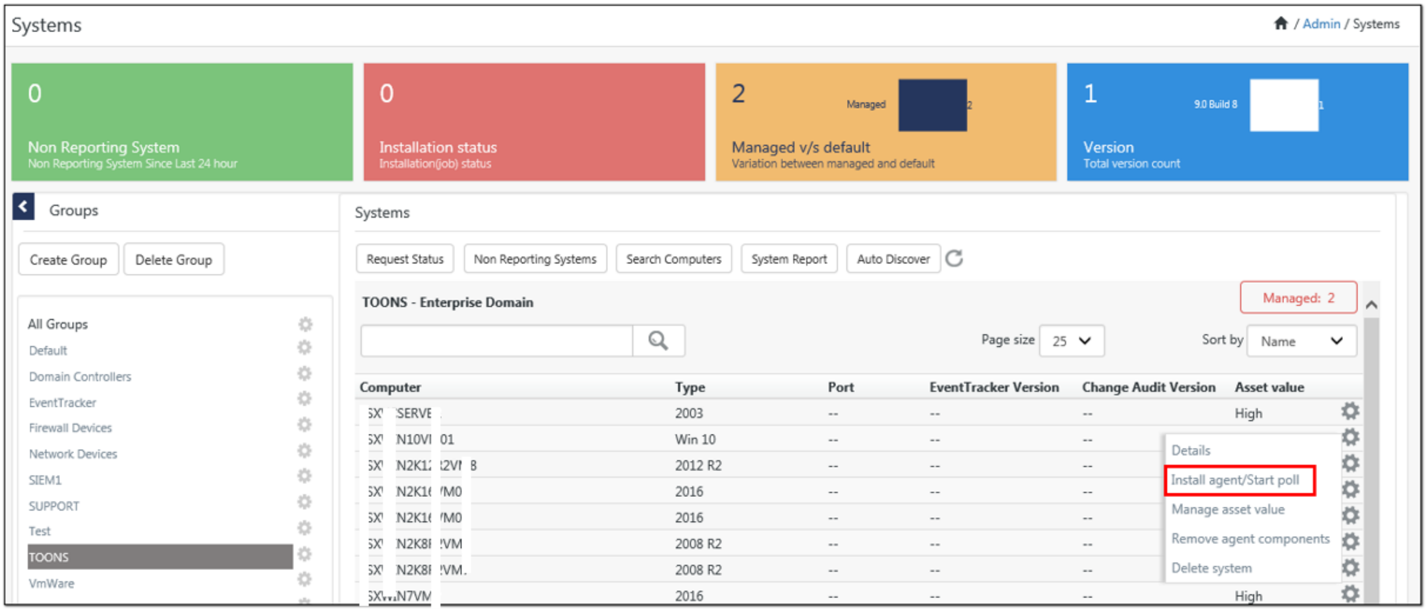
NOTE: Ensure that the Remote Event Log Management is added in the filter exception list in Microsoft Windows Firewall, or else it will not connect to the target system.

In the **System** manager page, move the mouse pointer over the system where you want to install the agent.

a) Click **Dropdown** ⚙.

EventTracker opens the drop-down list.

b) Click **Install agent/ Start poll**.

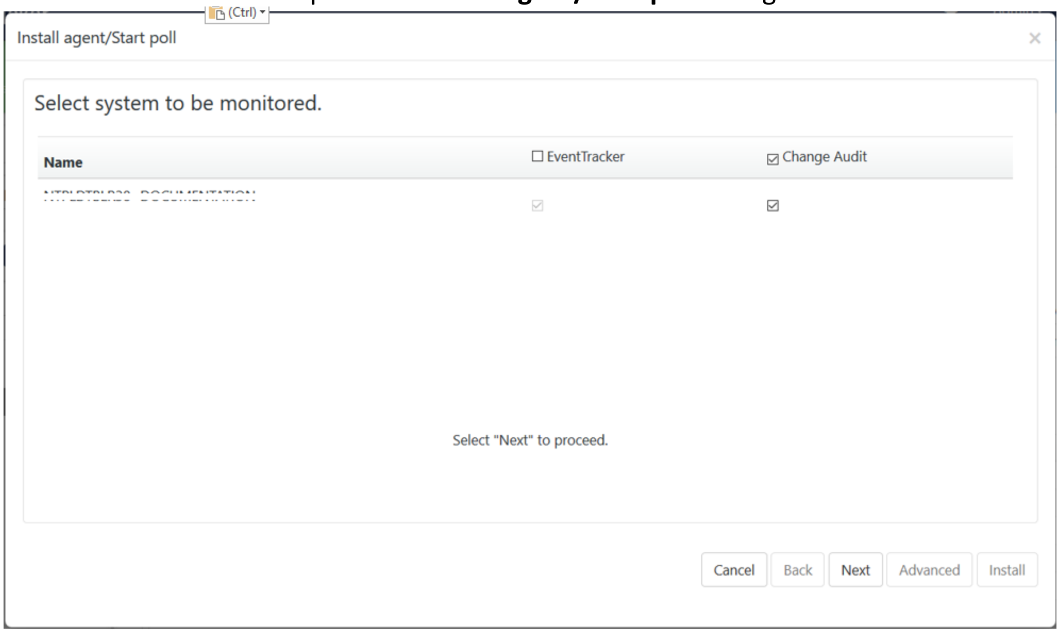


TOONS - Enterprise Domain

Computer	Type	Port	EventTracker Version	Change Audit Version	Asset value
5X SERVE	2003	--	--	--	High
5X N10VI 01	Win 10	--	--	--	
5X N2K12 2VI B	2012 R2	--	--	--	
5X N2K1(/M0	2016	--	--	--	
5X N2K1(/M0	2016	--	--	--	
5X N2K8I !VM	2008 R2	--	--	--	
5X N2K8I !VM.	2008 R2	--	--	--	
5X...N7VM	2016	--	--	--	High

Figure 72

EventTracker opens the **Install Agent/Start poll** dialog box.



Install agent/Start poll

Select system to be monitored.

Name	□ EventTracker	☑ Change Audit
NTPLDTBLR20 - DOCUMENTATION	☑	☑

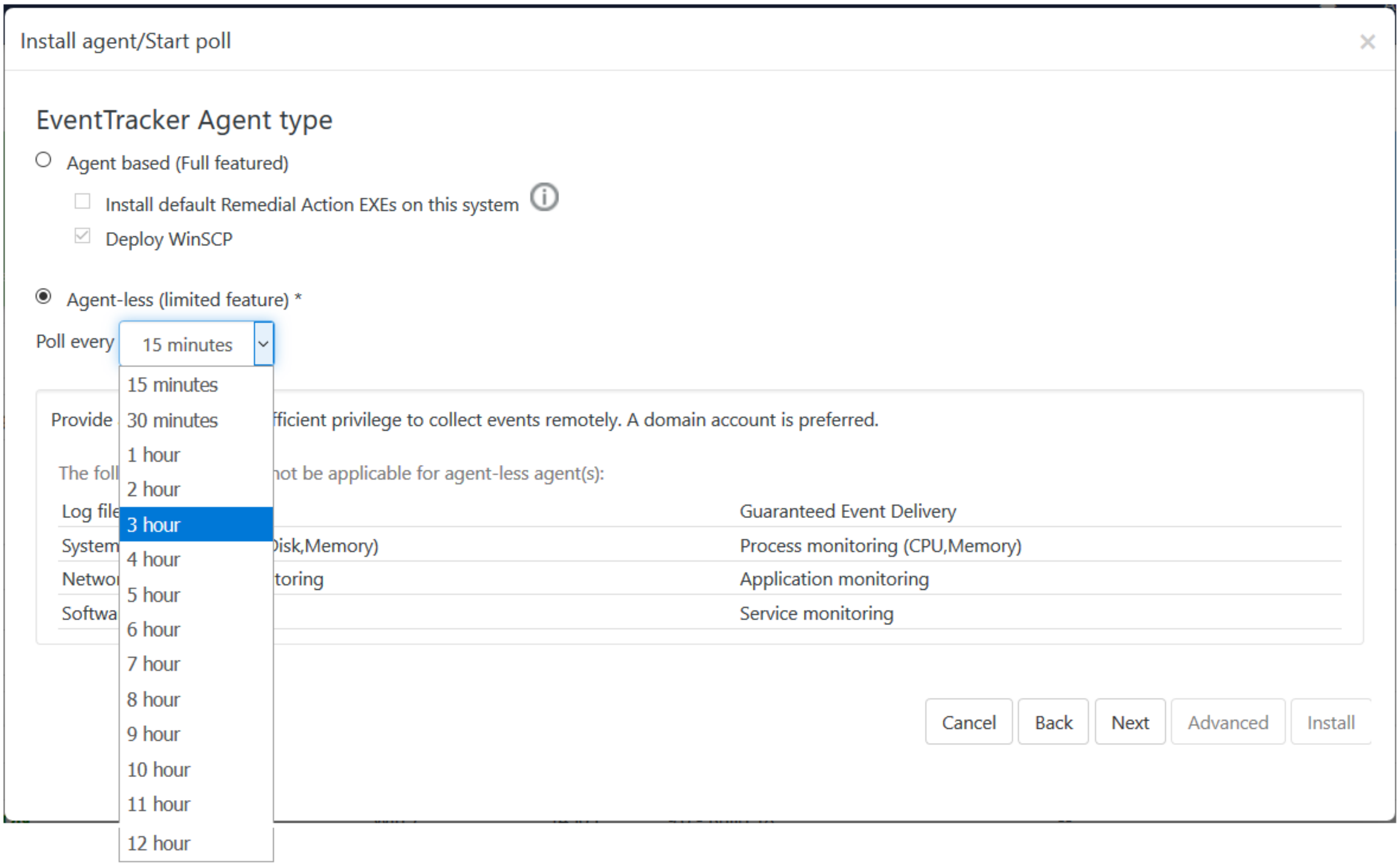
Select "Next" to proceed.

Figure 73

- Check the **EventTracker** option to install EventTracker agent (Agent-less).
- Check the **Change Audit** option to install Change Audit agent (Only for agent-based option)

c) Click **Next**.

d) Select **EventTracker Agent Type i.e. Agent-less (limited feature)*** option.



Install agent/Start poll

EventTracker Agent type

○ Agent based (Full featured)

□ Install default Remedial Action EXEs on this system

☑ Deploy WinSCP

● Agent-less (limited feature) *

Poll every 15 minutes

Provide ... fficient privilege to collect events remotely. A domain account is preferred.

The foll ... not be applicable for agent-less agent(s):

Log file ...	Guaranteed Event Delivery
System ... Disk,Memory)	Process monitoring (CPU,Memory)
Netwo ... toring	Application monitoring
Softwa ...	Service monitoring

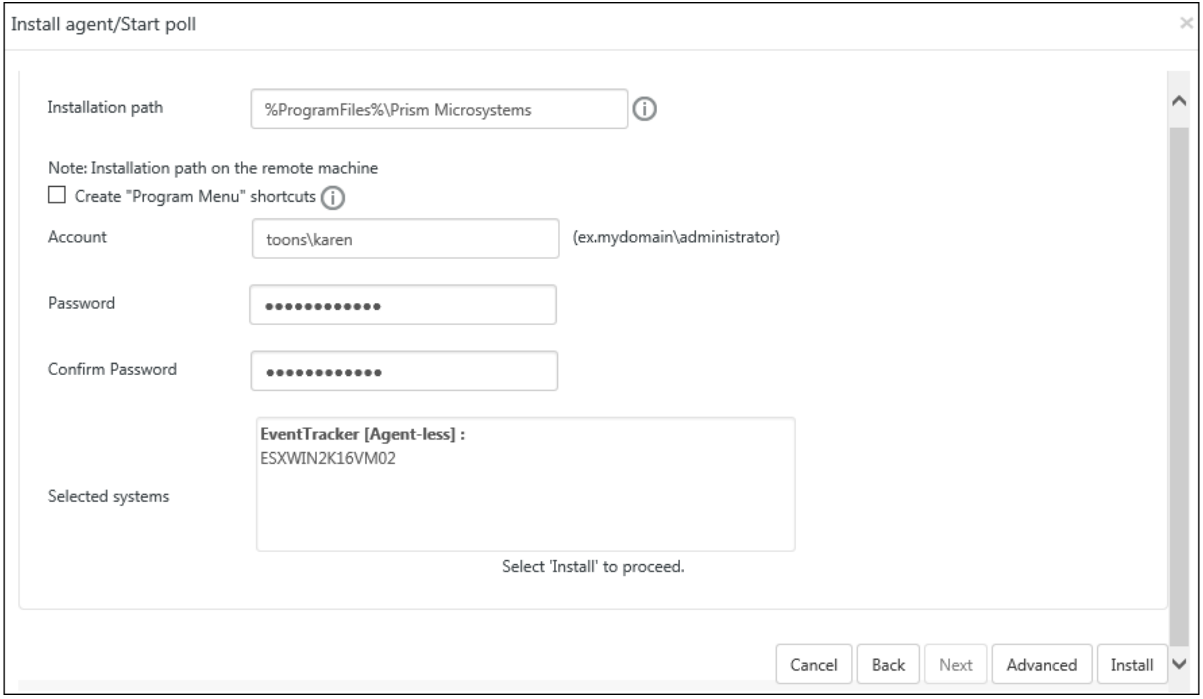
Figure74

Agent less (limited feature)	
Select this option to add the system with limited EventTracker Agent features.	In the Agent-less type, the following features are not available: • Log file Monitoring • System Monitoring • Network Connection Monitoring • Software Install / Uninstall • Guaranteed Event Delivery • Process Monitoring • Application Monitoring • Service Monitoring
Poll Every	By default, the frequency is set to 15 min to receive events from the remote agent system.

Table 11

e) Click **Next**.

EventTracker displays the Install agent/Start poll dialog box with the default client installation path on the remote computer.



Install agent/Start poll

Installation path: %ProgramFiles%\Prism Microsystems

Note: Installation path on the remote machine

□ Create "Program Menu" shortcuts

Account: toons\karen (ex.mydomain\administrator)

Password: ••••••••••••

Confirm Password: ••••••••••••

Selected systems: **EventTracker [Agent-less] :** ESXWIN2K16VM02

Select 'Install' to proceed.

Figure 75

Field	***Description***
Polling frequency	**Poll Every** Select the time frequency for which you want to get the events
Domain Admin account	Type valid user name and password in Account, Password and Confirm Password fields respectively.
Selected Systems	This field displays the selected system list.

Table 12

f) Click **Install**.

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

(OR)

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

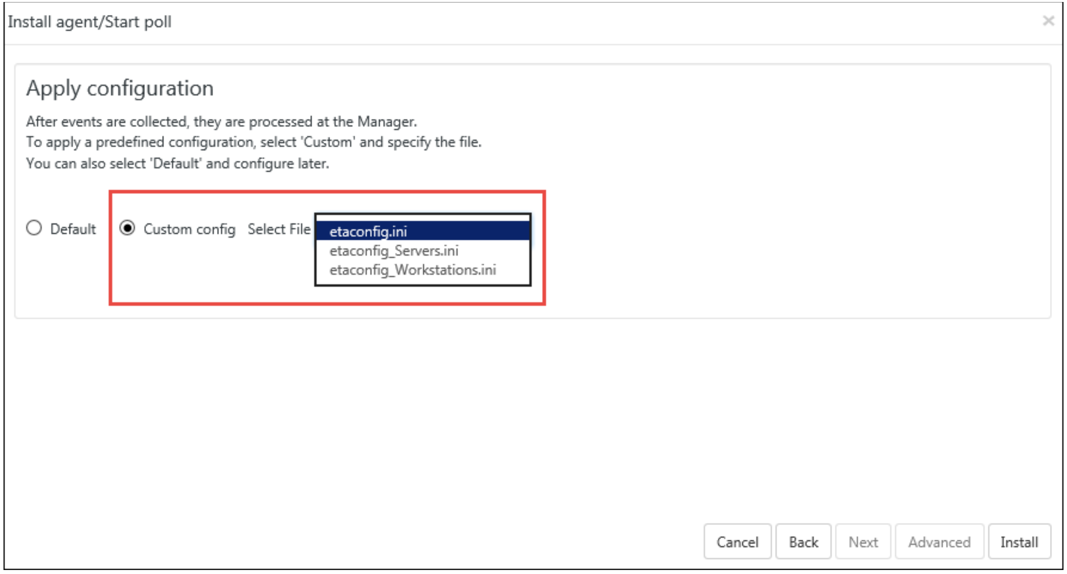
The **Default** option is selected by default to apply the manager side 'Agent configuration' settings (etaconfig.ini).

2. Select the **Default** or **Custom config** option to select a custom configuration file as per the requirement.

The custom configuration will provide you the templates which you have created in Agent configuration and two more predefined templates.

You can select the template of your choice:

- **etaconfig_Servers.ini:** This predefined template contains the ideal server configurations which can be applied to the selected agent system.
- **etaconfig_Workstations.ini:** This predefined template contains the ideal workstation configurations which can be applied to the selected agent system. This option disables the 'Offline event sending' option.


Install agent/Start poll

Apply configuration

After events are collected, they are processed at the Manager.
To apply a predefined configuration, select 'Custom' and specify the file.
You can also select 'Default' and configure later.

○ Default ● Custom config Select File etaconfig.ini

Figure 76

g) Select the configuration file from the **File** dropdown, and then click **Install**.
EventTracker displays the pop-up window with the appropriate message.

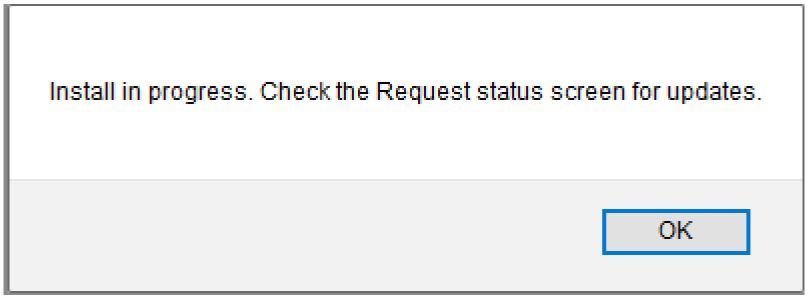
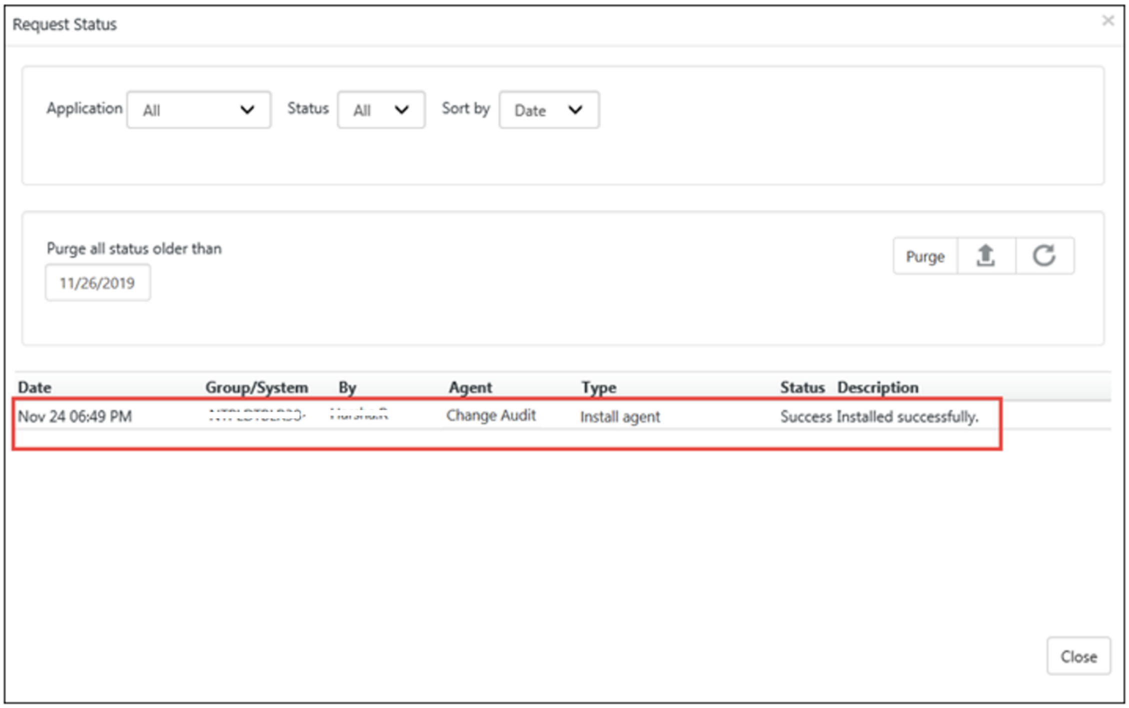

Install in progress. Check the Request status screen for updates.

Figure 77

h) Click **OK.**
EventTracker opens **Request Status** screen.



Request Status

Application: All | Status: All | Sort by: Date

Purge all status older than 11/26/2019

Date	Group/System	By	Agent	Type	Status	Description
Nov 24 06:49 PM	[redacted]	[redacted]	Change Audit	Install agent	Success	Installed successfully.

Figure 78

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

Table 13

i) Click **Refresh** ↻ to view the current status.
(OR)
Reopen the **Request Status** dialog box to see the updated status.

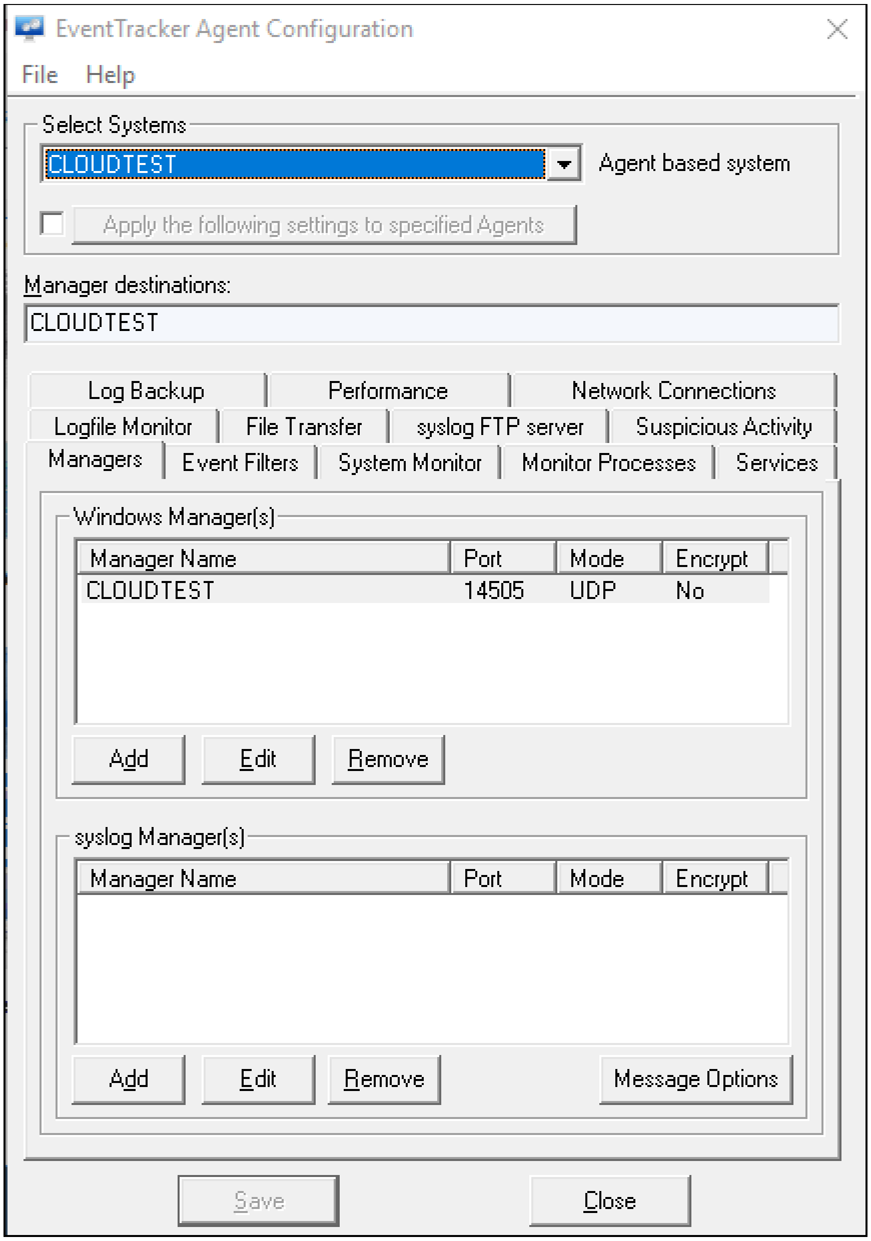
j) Click **Close.**

k) Refresh the **System** manager.

Now,

1. Open **EventTracker Control Panel**.
2. Double-Click the **EventTracker Agent Configuration**.

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



Select Systems: CLOUDTEST — Agent based system

Manager destinations: CLOUDTEST

Windows Manager(s)

Manager Name	Port	Mode	Encrypt
CLOUDTEST	14505	UDP	No

syslog Manager(s)

Manager Name	Port	Mode	Encrypt

Figure 79

4.7 Deploying EventTracker Windows Agent – Microsoft Windows 7 and Above

4.7.1 Prerequisites for Windows Agent – Microsoft Windows 7 and Above

The following are the mandatory settings you ought to do on Win 7 and above system(s) before you deploy an Agent.

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

4.7.2 Installing / Uninstalling Microsoft Windows 7 and above Agent

Install and uninstall procedure for Windows 7 and above agent is identical to the procedures for other Windows Agents. No other additional configuration settings are required.

5. Agent Deployment

To install EventTracker Agent and Change Audit Agent refer EventTracker Agent Deployment – User Manual.

6. Securing EventTracker

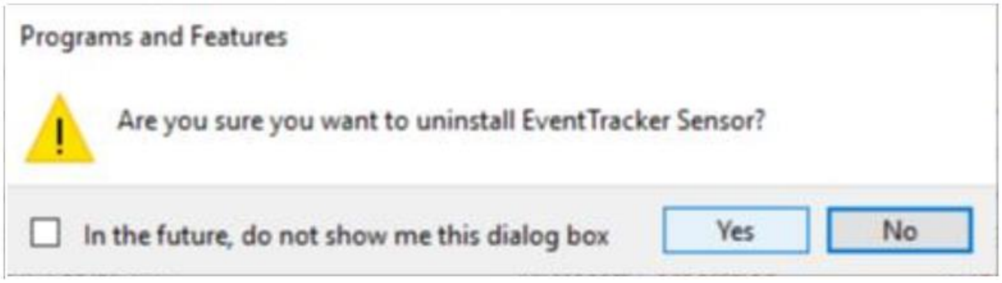
To secure EventTracker, refer EventTracker Hardening Guide and OWASP Complaint EventTracker Guide.

7. Uninstalling EventTracker Windows Agent

There are several methods to uninstall EventTracker Windows Agent. Few methods are mentioned below:

7.1 Uninstall EventTracker Windows Agent via Control Panel

1. Click **Start**, point to **All Programs**, and then click **Control Panel**.
2. Click **Add or Remove Programs**, select **EventTrackerAgent**, and then click **Remove**.
   Windows Installer message opens.

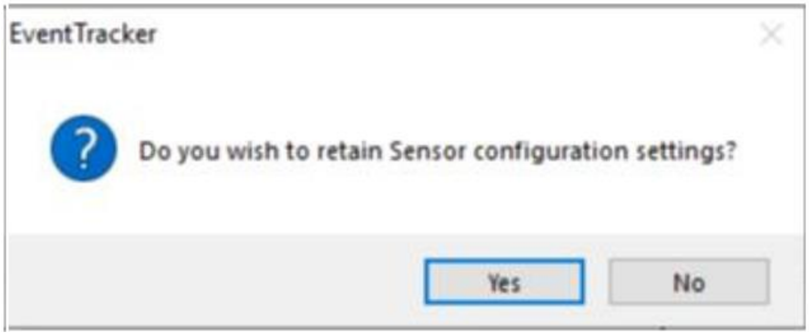


Programs and Features

Are you sure you want to uninstall EventTracker Sensor?

Figure 80

3. Select **Yes**.
   EventTracker window opens.
4. Select **Yes or No** as per the requirement.



Do you wish to retain Sensor configuration settings?

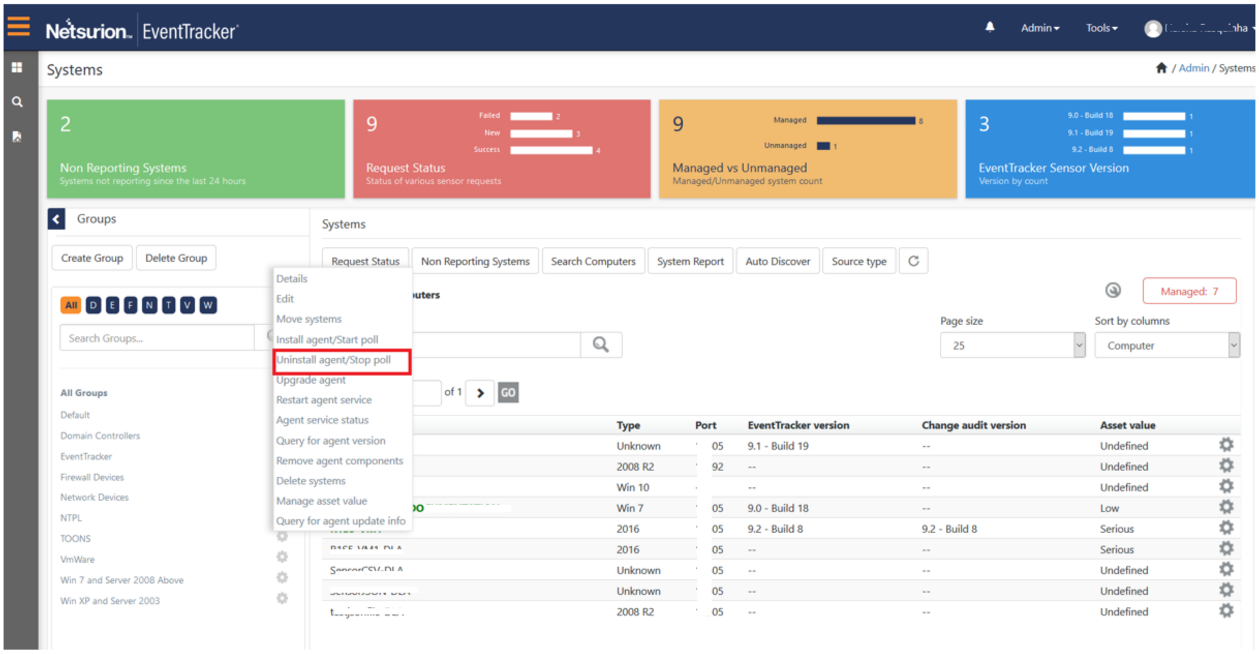
Figure 81

NOTE:

To retain the agent configuration settings, click **Yes**. To delete click **No.**

7.2 Uninstall EventTracker Windows Agent via System Manager

1. Click **Admin** drop down and select **Systems**.
2. Select the **Groups** or **Computer** name on which un-installation is required.



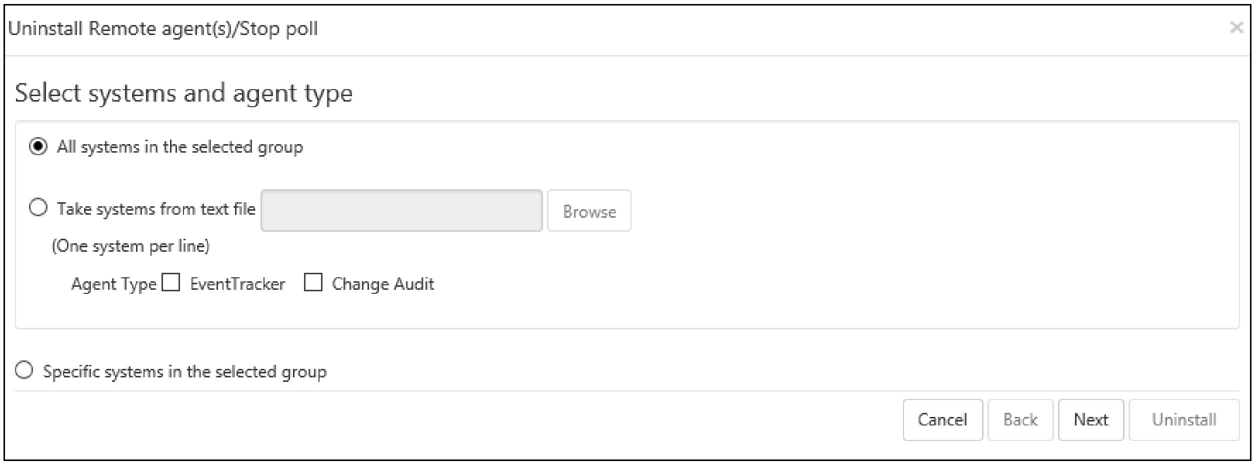
Page size: 25

Sort by columns: Computer

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

Figure 82

3. Select the **Uninstall agent/Stop poll.**
   Uninstall Remote agent(s)/Stop poll opens.



Uninstall Remote agent(s)/Stop poll ×

Select systems and agent type

● All systems in the selected group

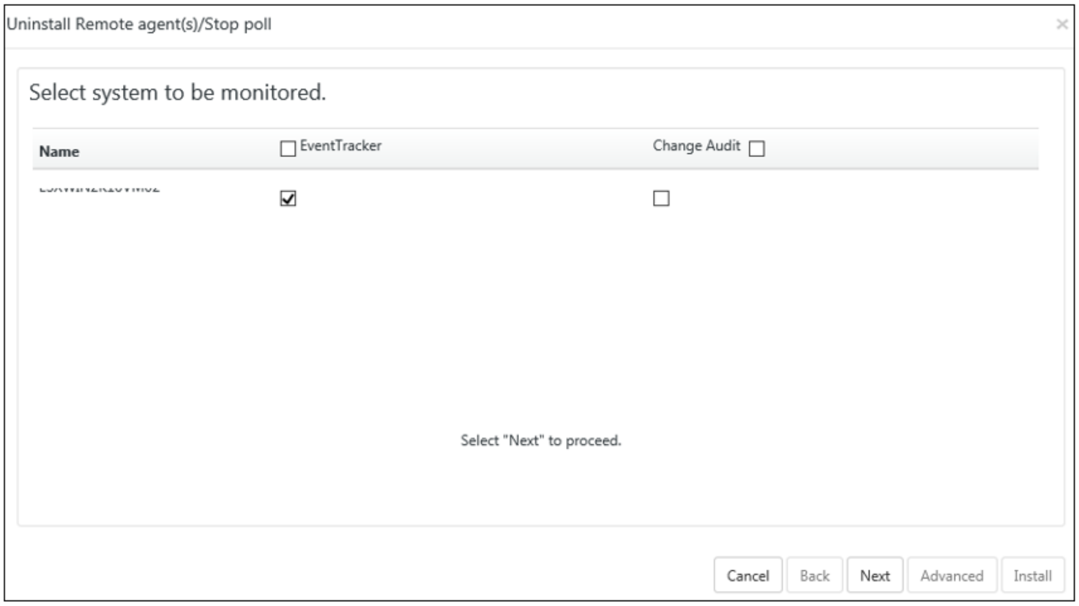
○ Take systems from text file [ ] Browse

(One system per line)

Agent Type □ EventTracker □ Change Audit

○ Specific systems in the selected group

Figure 83



Uninstall Remote agent(s)/Stop poll ×

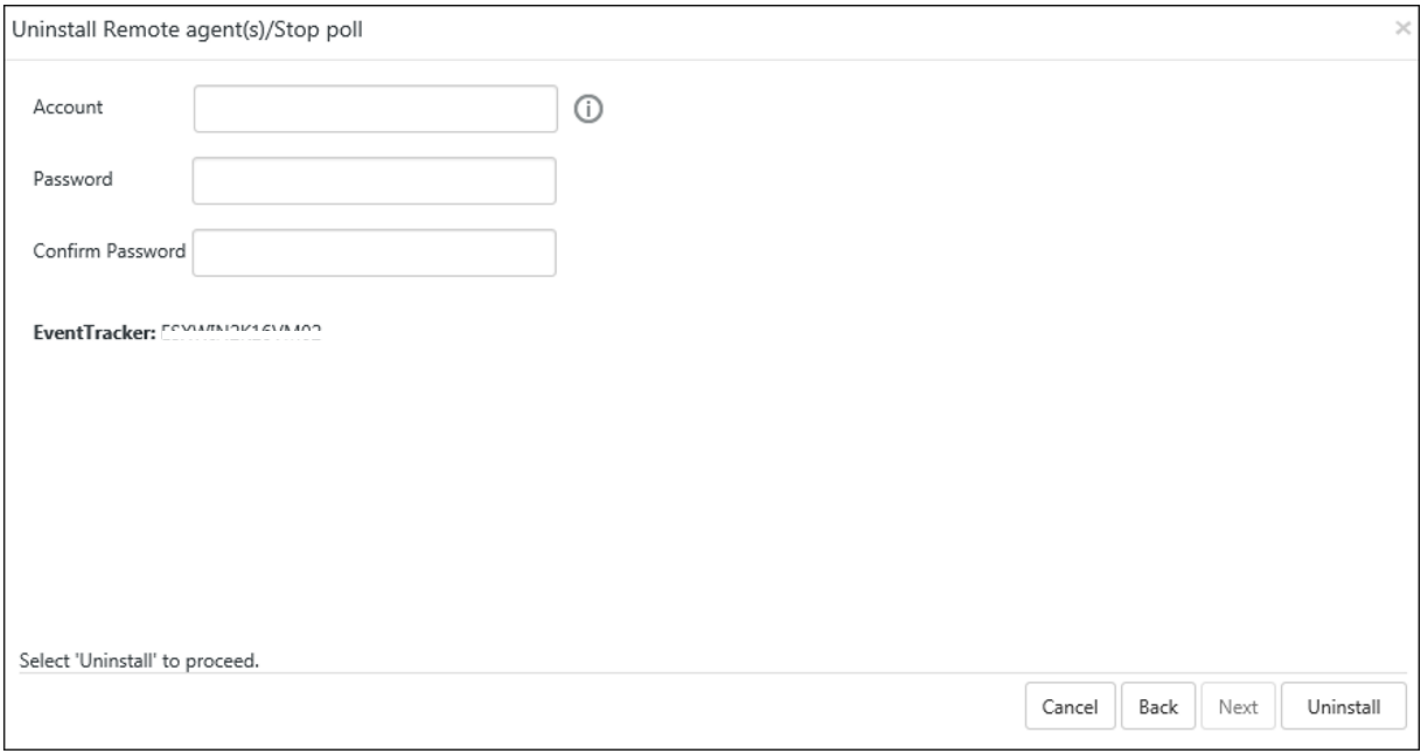
Select system to be monitored.

Name	□ EventTracker	Change Audit □
[illegible]	☑	□

Select "Next" to proceed.

Figure 84

4. Select the required **EventTracker**, **Change Audit** options and then click **Next**.
   Uninstall Remote agent(s)/Stop poll window opens.



Uninstall Remote agent(s)/Stop poll

Account

Password

Confirm Password

EventTracker: [redacted]

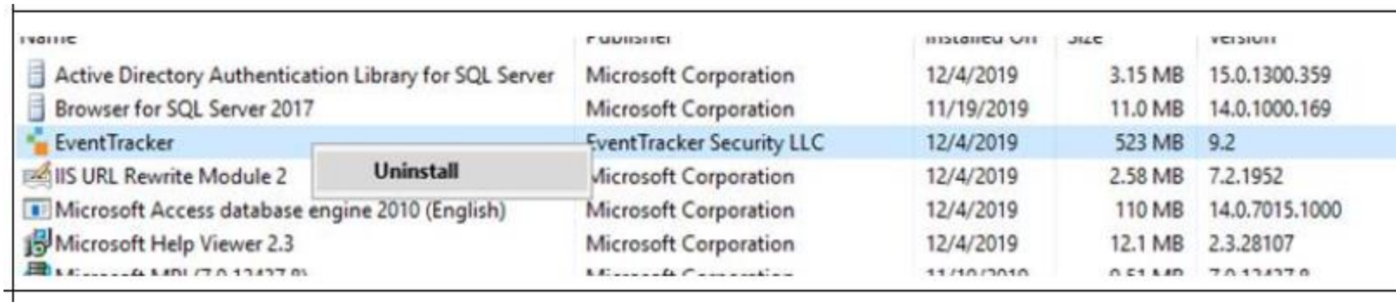
Select 'Uninstall' to proceed.

Figure 85

5. Enter valid credentials and then click **Uninstall**.

8. Uninstalling EventTracker

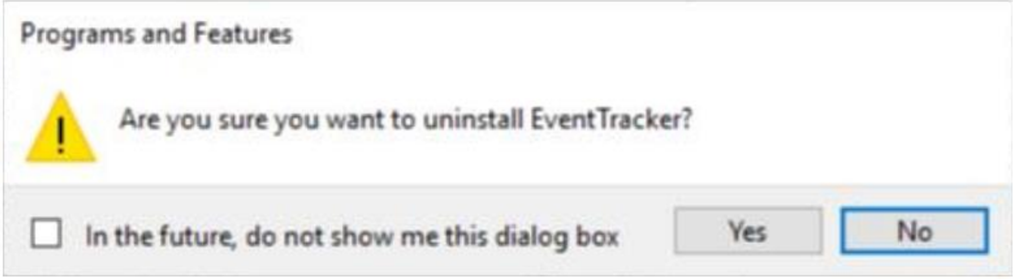
1. Click **Start**, then click **Control Panel and** click **Programs and Features**.
2. Select **EventTracker**, and then click **Uninstall**.



Name	Publisher	Installed On	Size	Version
Active Directory Authentication Library for SQL Server	Microsoft Corporation	12/4/2019	3.15 MB	15.0.1300.359
Browser for SQL Server 2017	Microsoft Corporation	11/19/2019	11.0 MB	14.0.1000.169
EventTracker	EventTracker Security LLC	12/4/2019	523 MB	9.2
IIS URL Rewrite Module 2	Microsoft Corporation	12/4/2019	2.58 MB	7.2.1952
Microsoft Access database engine 2010 (English)	Microsoft Corporation	12/4/2019	110 MB	14.0.7015.1000
Microsoft Help Viewer 2.3	Microsoft Corporation	12/4/2019	12.1 MB	2.3.28107
Microsoft MPI (7.0.12437.8)	Microsoft Corporation	11/19/2019	9.51 MB	7.0.12437.8

Figure 86

Windows Installer window appears.



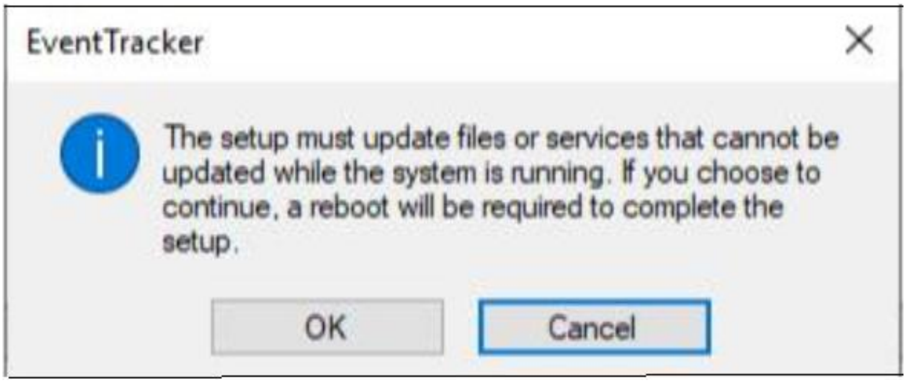
Are you sure you want to uninstall EventTracker?

☐ In the future, do not show me this dialog box

Figure 87

3. Click **Yes**.

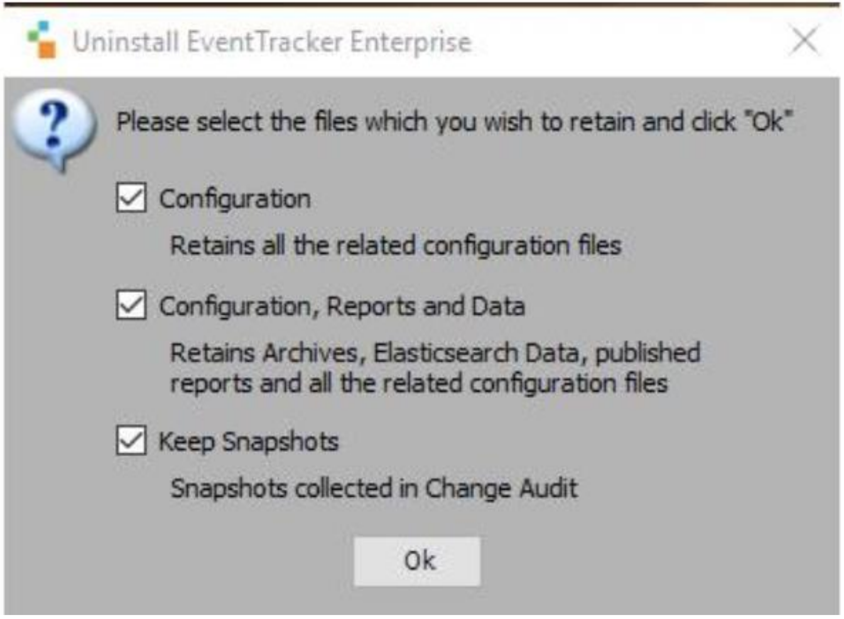
   EventTracker window displays a message.



The setup must update files or services that cannot be updated while the system is running. If you choose to continue, a reboot will be required to complete the setup.

Figure 88

4. Click **Ok**.
   Uninstall EventTracker window opens.



Please select the files which you wish to retain and click "Ok"

☑ Configuration

Retains all the related configuration files

☑ Configuration, Reports and Data

Retains Archives, Elasticsearch Data, published reports and all the related configuration files

☑ Keep Snapshots

Snapshots collected in Change Audit

Figure 89

NOTE:

To retain **Configuration, Reports, Data, and Snapshots** files, select the respective check box otherwise uncheck the options.

5. Select **Ok**.

9. Ports used in EventTracker

EventTracker Module	Port(s)
EventTracker Agent	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 Agent	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

Table 14

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

10. Frequently Asked Questions

1. What if the user is unable to login to EventTracker?

Issue 1: Issue with querying Active Directory to authenticate the user.

To do this:

- Run the executable "**ActiveDirectoryAuthenticationTypes.exe**" found under <INSTALL_PATH>\EventTrackerWeb\Bin folder.

- Put a check mark against the below flags,

   a. **Delegation**, **Secure** and **Signing** (in the section "**Use the below flags to authenticate while logging in from Web GUI**)
   b. **Negotiate**, **Signing** and **Sealing** (in the section "**Use the below flags to authenticate while using "EventTracker Configuration"** or **"Update Users List" utility**)

- Click "**Apply**".

- Re-run the EventTracker Configuration utility.

Issue 2: Identity impersonation

To fix this:

- Check whether "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Prism Microsystems\EventTracker\ASPNET_SETREG" registry hive has values (i.e. **Impersonate**, **username**, and **password**) present in it.

- If not, then run the below command by launching the Microsoft Windows command prompt as "**Run as administrator**".
   a. Go to <INSTALL_PATH>\EventTrackerWeb\Bin directory.
   b. 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.

- Re-run the EventTracker Configuration utility.

2. How to change the webserver port used by EventTracker?

   If the EventTracker installation is using IISEXRPESS follow the steps to use port 80:

   a. Open **…\Prism Microsystems\EventTrackerWeb\applicationhost.config** file.

   b. Find the below two lines.

      <binding protocol="http" bindingInformation=":8080:xxx.xxx.xxx.xxx" /> (xxx.xxx.xxx.xxx is the IP Address of the server)

      <binding protocol="http" bindingInformation=":8080:localhost" />

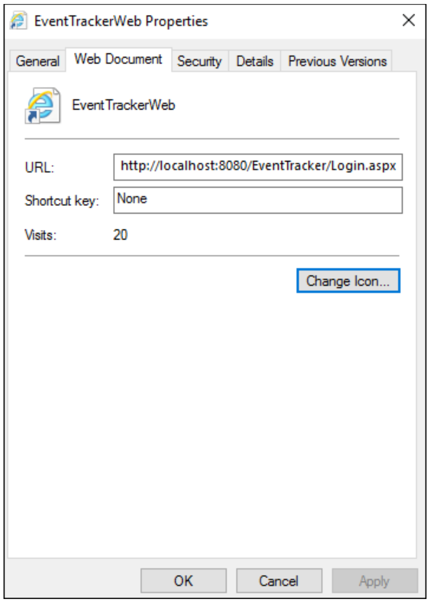
   c. Modify it as shown below.

      <binding protocol="http" bindingInformation=":80: xxx.xxx.xxx.xxx " /> (xxx.xxx.xxx.xxx is the IP Address of the server)

      <binding protocol="http" bindingInformation=":80:localhost" />

   d. Right click **…\Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url** (Internet Shortcut) and select properties.

e. Click the **Web Document** tab.



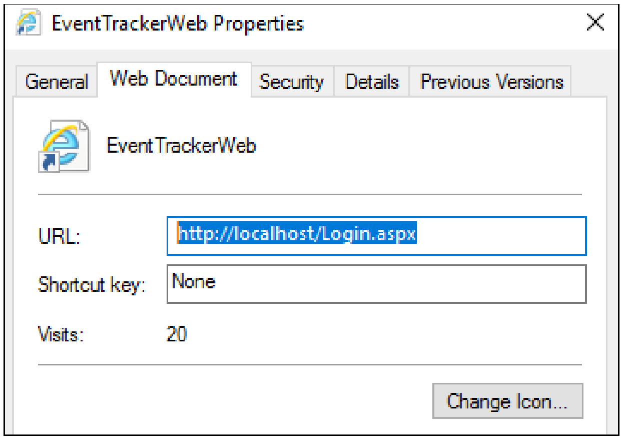
URL: http://localhost:8080/EventTracker/Login.aspx

Shortcut key: None

Visits: 20

Figure 90

f. In the **URL box, modify the entry** as shown below.



URL: http://localhost/Login.aspx

Shortcut key: None

Visits: 20

Figure 91

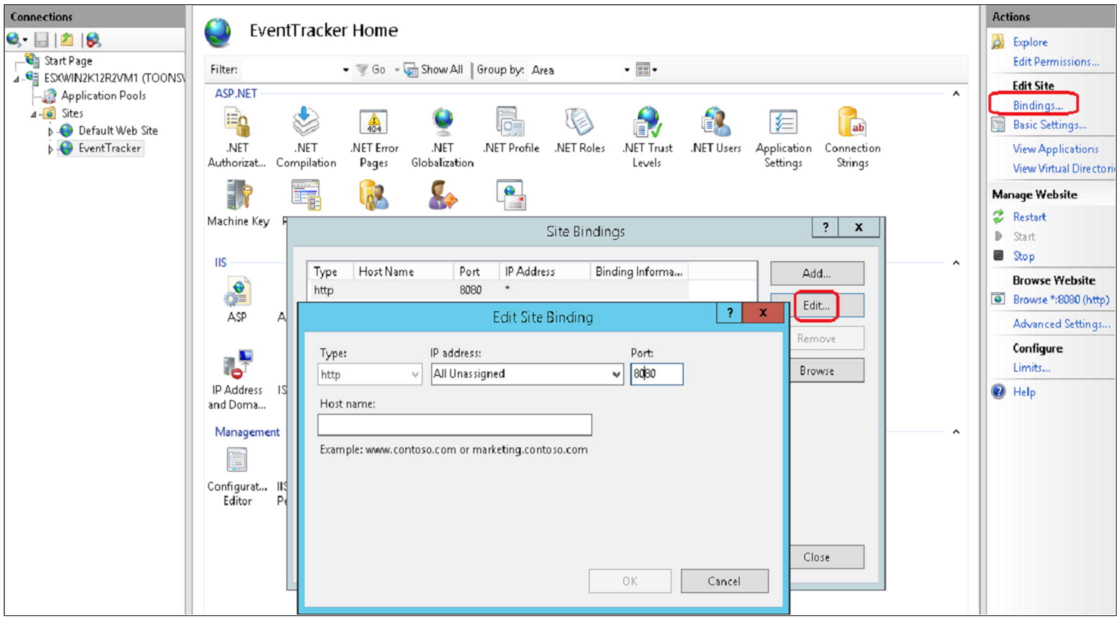
g. Restart the **IISExpress** service.

If the EventTracker installation is using IIS, follow the steps to use port 80:

a. Open IIS Manager and expand **Sites**. Select the **EventTracker** site.

b. In the **Actions** pane, click **Bindings** on the right.

c. In the **Site Binding** Window (Select the listed entry and then) Click **Edit**.



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http		8080	*	

Edit Site Binding

Type: http

IP address: All Unassigned

Port: 8080

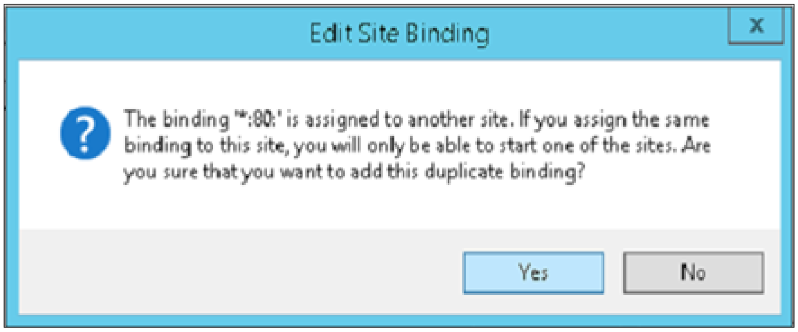
Host name:

Example: www.contoso.com or marketing.contoso.com

Figure 92

d. **Edit Site Binding** window opens, modify the existing port number from **8080** to **80** and click **OK**.

Edit Site Binding window displays a confirmation message.



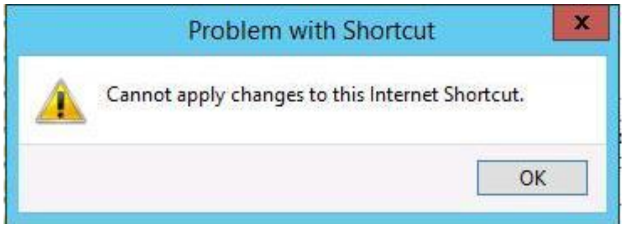
The binding '*:80:' is assigned to another site. If you assign the same binding to this site, you will only be able to start one of the sites. Are you sure that you want to add this duplicate binding?

Figure 93

e. Click **Yes**.

NOTE:

If issue occurs with Shortcut message you have to copy the path…\Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url to a different location, modify and update the file under …\Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url.



Cannot apply changes to this Internet Shortcut.

Figure 94

f. Stop the **Default Web Site** and start the **EventTracker** site as shown in the following figure.

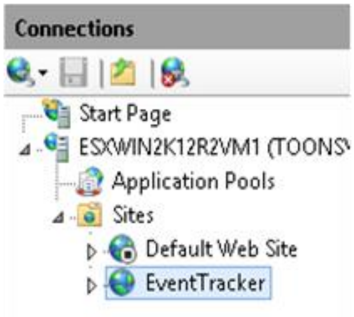
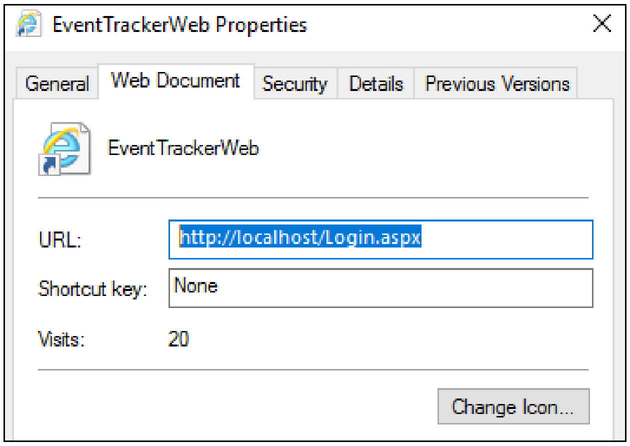


Figure 95

g. Right click ...\Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url (Internet Shortcut) and select **Properties** and modify the URL as shown in the following figure.



URL: http://localhost/Login.aspx

Shortcut key: None

Visits: 20

Figure 96

2. What are the prerequisites for displaying the Attacks Dashboard?

Attackers Dashboard feature uses the following websites:

- **maps.google.com**
- **Ipvoid.com**
- **IBM XFE**

Access needs to be provided for these websites.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both.
Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn.

Contact Us

Corporate Headquarters

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

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support