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 2012 R2/10/2016, 2019 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.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

1. Introduction .......................................................................................................................... 4
2. Requirements ......................................................................................................................... 4
  2.1 Known Issues while installing v9.3 ..................................................................................... 4
  2.2 System Requirements ......................................................................................................... 6
  2.3 Hardware Requirements [Min. Configuration] ................................................................. 6
  2.4 Software Requirements ..................................................................................................... 6
3. Installing EventTracker .......................................................................................................... 8
  3.1 Pre-install instructions for Local Account and Active Directory authentication .............. 8
  3.2 Installing EventTracker Manager ...................................................................................... 8
  3.3 Pre-install Checklist for EventTracker Manager ............................................................... 8
    3.3.1 IIS Settings ................................................................................................................. 9
    3.3.2 User Permission on SQL Server .................................................................................. 9
  3.4 Procedure to install EventTracker Manager - Custom ..................................................... 10
  3.5 Procedure to install EventTracker Manager - Standard / Collection Point Evaluation Version .... 39
4. Deploying EventTracker Windows Agent .............................................................................. 41
  4.1 Pre-install Instructions for Windows Agent ..................................................................... 41
  4.2 Pre-install checklist for Windows Agent ......................................................................... 42
  4.3 Different methods to install EventTracker Agents ............................................................ 42
  4.4 Deploying EventTracker Windows Agent via System Manager for Agent Based (full featured) .... 42
  4.5 Configuring EventTracker Windows Agent ..................................................................... 52
  4.6 Configuring Agent-less collection via System Manager (limited features) .................... 54
    4.6.1 Adding Systems for Agent-less monitoring ................................................................. 54
  4.7 Deploying EventTracker Windows Agent – Microsoft Windows 7 and Above .................. 62
    4.7.1 Prerequisites for Windows Agent – Microsoft Windows 7 and Above ......................... 62
    4.7.2 Installing / Uninstalling Microsoft Windows 7 and above Agent ................................. 62
5. Agent Deployment ................................................................................................................. 62
6. Securing EventTracker ........................................................................................................ 62
7. Uninstalling EventTracker Windows Agent .......................................................................... 62
  7.1 Uninstall EventTracker Windows Agent via Control Panel ............................................ 62
7.2 Uninstall EventTracker Windows Agent via System Manager .............................................................. 63
8. Uninstalling EventTracker ...................................................................................................................... 66
9. Ports used in EventTracker ..................................................................................................................... 68
10. Frequently Asked Questions .................................................................................................................. 68
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 (http://www.eventtracker.com/eventtracker/enterprise/) in the brochure of this package.

This installation guide helps you to install our product effortlessly.

**IMPORTANT:** EventTracker strongly recommends users to refer:

‘How To Install and Customize Web Server (IIS)’ document 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?
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?

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.

64-bit Installation:

<table>
<thead>
<tr>
<th></th>
<th>2.80 GHz and above, 8 Core or equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>16GB</td>
</tr>
<tr>
<td>HDD</td>
<td>200 GB (SSD) for application and search cache; 100 GB Non-SSD for storing archives (varies as per data retention needs)</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Microsoft Windows Platforms</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2019</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2012 R2</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2016</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Table 2

<table>
<thead>
<tr>
<th>SQL server</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 2017</td>
<td>Supported</td>
</tr>
<tr>
<td>SQL Server 2016</td>
<td>Supported</td>
</tr>
</tbody>
</table>

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

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

To install EventTracker Agent:

<table>
<thead>
<tr>
<th>Microsoft Windows Platforms</th>
<th>32 bit</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2019</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8, 8.1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008 R2</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2012</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2012 R2</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2016</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
</tbody>
</table>

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 to refer ‘EventTracker Architecture’ 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.

<table>
<thead>
<tr>
<th>ENSURE</th>
<th>User is a member of the ‘Local Administrators’ group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSI package installation is allowed</td>
</tr>
<tr>
<td></td>
<td>User has ‘Logon As Service’ rights</td>
</tr>
<tr>
<td></td>
<td>User has ‘Logon As Batch job’ rights</td>
</tr>
<tr>
<td></td>
<td>Network Discovery is enabled</td>
</tr>
<tr>
<td></td>
<td><strong>System cryptography</strong>: Use FIPS 140 compliant cryptographic algorithms, with encryption, hashing and signing algorithms disabled.</td>
</tr>
</tbody>
</table>
3.3.1 IIS Settings

Ensure that IIS Settings under Application Pools are as follows in Microsoft Windows 2012 R2/2016/10/2019.

![Advanced Settings](image)

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 Install Guide: v8.2

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.

![Figure 5](image)

IMPORTANT: Go to Internet Explorer -> Browser Settings -> Security -> Custom Level -> In the downloads -> File Download -> ensure the “enable” option is selected.
2. Once the .net framework 4.8 is installed a message appears, click **ok** and reboot manually.

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.
EventTracker Pre-Install Check window opens.

![EventTracker Pre-Install Check window](image)

**Figure 9**

Click Next.

![License Agreement](image)

**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.

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.
7. Prerequisite page opens.

8. If the SQL Server is running with multiple instances, click **Browse** and select appropriate Instance and proceed.
9. Click **Next**.
10. Once pre-requisites are installed, **Define User Group** page opens.

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**.

![Figure 16](image)

**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.

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.

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](image)

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’.

![Figure 20](image.png)

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

![Figure 21](image.png)
- 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.

![Figure 22](image)

- Click **OK**.

![Figure 23](image)

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

This User will manage EventTracker page opens.

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.

   ![Image of EventTracker Pre-Install Check interface](image)

   Figure 27

   b. Click **Next**.

   Summary page opens.

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

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

![EventTracker Pre-Install Check](image)

**Figure 29**

a. Click **Yes**.

15. In **Summary** page, verify all the data entered, and then click **Install**.
EventTracker - Install Shield Wizard opens.

EventTracker - InstallShield Wizard opens the **Welcome** screen.
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.
17. To locate the path of the certificate file, click **Browse**. Select File window opens.

![Select File Window](image)

**Figure 34**

18. Go to the appropriate folder, select the file and then click **Open**. The folder path is updated.

![Certificate File Selection](image)

**Figure 35**
19. Click **Next**.
Select Components screen opens.

![Select Components Screen](image-url)

**Figure 36**

<table>
<thead>
<tr>
<th><strong>EventTracker Components</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Console</td>
<td>Select this option to install the manager console on the target computer.</td>
</tr>
<tr>
<td>Change Audit</td>
<td>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.</td>
</tr>
<tr>
<td>Trap Tracker</td>
<td>Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.</td>
</tr>
</tbody>
</table>

**Table 6**
Click

To

Select a different destination folder to install EventTracker.

![Change Current Destination Folder screenshot](image1)

Figure 37

View **Select Component** conventions.

![Select Components Tips screenshot](image2)

Figure 38
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.
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.
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**.

![Configure Collection Point site](image)

**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](image)

**Figure 43**

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

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

![Image of Change Audit SnapShot dialog box](image)

**Figure 46**

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

(OR)

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

![Image of Change Current Destination Folder dialog box](image)

**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.

![Figure 48](image.png)

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.
25. Click **Install**.
InstallShield Wizard installs the selected components.

26. InstallShield Wizard opens the last screen.
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](image)

**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 Screen](image)

**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.
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.
2. Click **Next**.
   Hardware Summary pane opens.
3. Select **Standard/Collection Point** option, and then click **Next**.

![EventTracker Pre-Install Check](image)

**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.

<table>
<thead>
<tr>
<th>ENSURE</th>
<th>User is a member of the ‘Local Administrators’ group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MSI package installation is allowed</td>
</tr>
<tr>
<td></td>
<td>User has ‘Logon As Service’ rights</td>
</tr>
<tr>
<td></td>
<td>Network Discovery is enabled</td>
</tr>
<tr>
<td></td>
<td>File sharing is allowed</td>
</tr>
<tr>
<td></td>
<td>Access this computer from the network</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VERIFY</th>
<th>The user has permission on ‘Application install directory’ (Folders and sub folders).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The user must create service permission on the target system(SCM- service control manager)</td>
</tr>
<tr>
<td></td>
<td>The user has Read/Write permission on the Microsoft windows registry.</td>
</tr>
<tr>
<td></td>
<td>The user has permission to Admin share(C$) of Target systems and C$ should be accessible from the EventTracker Manager system.</td>
</tr>
</tbody>
</table>

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)


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.

![Figure 58](image)

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](image)
5. From the shortcut menu, click **Install agent/Start poll** option.

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

   ![Install agent/Start poll dialog box]

   **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.

<table>
<thead>
<tr>
<th>Option</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>All systems in the selected group</td>
<td>Click this option to install agents on all the systems present in the selected group.</td>
</tr>
<tr>
<td>Take systems from the text file</td>
<td>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.</td>
</tr>
<tr>
<td>Agent type</td>
<td>Select the agent type to be Installed</td>
</tr>
<tr>
<td>Specific systems in the selected group</td>
<td>Out of all the systems present in the group, select the specific system(s) to install the agent.</td>
</tr>
</tbody>
</table>

   **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.

![Image of EventTracker interface showing System manager page and the Install Agent/Start poll dialog box.]

Figure 61

EventTracker displays the Install Agent/Start poll dialog box.
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.
Agent based (Full featured)

<table>
<thead>
<tr>
<th>Install default Remedial Action EXEs on this system</th>
<th>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.</th>
</tr>
</thead>
</table>

| 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](image)

   **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.
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)

- 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).
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.
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.

13. Click OK.

EventTracker displays Request Status screen.
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**.

![EventTracker Control Panel](image)

Figure 70

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

EventTracker Agent Configuration window opens.
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**.

![Figure 72](image)

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

![Figure 73](image)
• 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.

![EventTracker Agent type](image-url)

*Figure 74*
### Agent less (limited feature)

<table>
<thead>
<tr>
<th>Select this option to add the system with limited EventTracker Agent features.</th>
<th>In the Agent-less type, the following features are not available:</th>
</tr>
</thead>
</table>
|  | • Log file Monitoring  
|  | • System Monitoring  
|  | • Network Connection Monitoring  
|  | • Software Install / Uninstall  
|  | • Guaranteed Event Delivery  
|  | • Process Monitoring  
|  | • Application Monitoring  
|  | • Service Monitoring  

<table>
<thead>
<tr>
<th>Poll Every</th>
<th>By default, the frequency is set to 15 min to receive events from the remote agent system.</th>
</tr>
</thead>
</table>

Table 11

e) Click **Next**. EventTracker displays the Install agent/Start poll dialog box with the default client installation path on the remote computer.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling frequency</td>
<td><strong>Poll Every</strong> Select the time frequency for which you want to get the events</td>
</tr>
<tr>
<td>Domain Admin account</td>
<td>Type valid user name and password in Account, Password and Confirm Password fields respectively.</td>
</tr>
<tr>
<td>Selected Systems</td>
<td>This field displays the selected system list.</td>
</tr>
</tbody>
</table>

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.
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.](image)

**Figure 77**

h) Click **OK**. EventTracker opens **Request Status** screen.
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>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Sort the Request Status results by the application installed. Available options are EventTracker &amp; Change Audit.</td>
</tr>
<tr>
<td>Status</td>
<td>Sort the Request Status results by the status of the application installed. Available options are All, New, Success, and Failed.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Sort the Request Status results by Date application was installed /on which System it is installed / Type of activity</td>
</tr>
<tr>
<td>Purge all status older than</td>
<td>Remove the older Request Status details from the list.</td>
</tr>
<tr>
<td>Export</td>
<td>Export the ‘System Status’ into Excel format</td>
</tr>
</tbody>
</table>

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 on **EventTracker Agent Configuration**. Only limited feature tabs are available as shown in the figure below:

![EventTracker Agent Configuration](image)

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

![Image of Programs and Features window]

3. **Figure 80**

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

![Figure 82](image)

![Figure 83](image)
4. Select the required **EventTracker, Change Audit** options and then click **Next**. Uninstall Remote agent(s)/Stop poll window opens.

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**.

   ![Figure 86](image)

   Windows Installer window appears.

3. Click **Yes**.

   ![Figure 87](image)

   EventTracker window displays a message.

4. Click **Ok**.

   Uninstall EventTracker window opens.

   ![Figure 88](image)
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**

<table>
<thead>
<tr>
<th>EventTracker Module</th>
<th>Port(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Agent</td>
<td>14506/TCP</td>
</tr>
<tr>
<td>Windows Receiver</td>
<td>14505(TCP/UDP) - Optional and multiple VCP’s can be configured</td>
</tr>
<tr>
<td>Syslog Receiver</td>
<td>514(UDP/TCP) can be configured to any number of ports</td>
</tr>
<tr>
<td>Collection Master</td>
<td>14507/TCP - Optional and can be configured to any TCP port</td>
</tr>
<tr>
<td>Correlation Receiver</td>
<td>14509/TCP</td>
</tr>
<tr>
<td>EventTracker – Change Audit Agent</td>
<td>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.</td>
</tr>
<tr>
<td>License Server</td>
<td>14503/TCP</td>
</tr>
<tr>
<td>EventTracker Active WatchList</td>
<td>14504</td>
</tr>
</tbody>
</table>

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

c. Modify it as shown below.

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

d. Right click `<Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url` (Internet Shortcut) and select properties.
e. Click on the Web Document tab.

![Figure 90](image)

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

![Figure 91](image)

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.
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.

![Figure 92: Edit Site Binding window](image)

**Figure 92**

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

![Image of Default Web Site stopped and EventTracker site started](image)

**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.

![Image of EventTrackerWeb Properties](image)

**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.