Abstract

This guide will help the users to install and configure EventTracker Enterprise, and verify the expected functionality of all its components.

EventTracker is a reliable, policy driven solution to monitor and manage critical events generated by Windows 7/8/8.1/2008/2008 R2/2012/2012 R2/10, Solaris BSM, Unix (SYSLOG), SYSLOG-NG and SNMP devices. EventTracker is an enterprise grade solution that provides real-time alerts, secure warehousing, and flexible reporting.

Audience

EventTracker users or system administrators, who wish to install the EventTracker Enterprise Manager.
Table of Contents

Abstract .................................................................................................................................................. 1

Audience .................................................................................................................................................. 1

Introduction ............................................................................................................................................. 4

Known Issues for v8.3 .............................................................................................................................. 4

System Requirements ............................................................................................................................ 6

Hardware Requirements [Min. Configuration] ....................................................................................... 6

Software Requirements .......................................................................................................................... 7

Pre-install instructions for Local Account and Active Directory authentication ................................. 8

Install EventTracker Manager ............................................................................................................... 9

Pre-install Checklist for EventTracker Manager .................................................................................. 9

IIS Settings ........................................................................................................................................... 9

User Permission on SQL Server ............................................................................................................... 11

Procedure to install EventTracker Manager - Custom ......................................................................... 11

Procedure to install EventTracker Manager - Standard / Collection Point Evaluation Version .......... 60

Deploy EventTracker Windows Agent .................................................................................................. 63

Pre-install Instructions for Windows Agent .......................................................................................... 63

Pre-install Checklist for Windows Agent .............................................................................................. 64

Different methods to install EventTracker Agents ............................................................................... 64

Deploy EventTracker Windows Agent via System Manager for Agent Based (full featured) ............ 64

Configure EventTracker Windows Agent ............................................................................................ 75

Configuring Agent-less collection via System Manager (limited features) .......................................... 77

Adding Systems for Agent-less monitoring ....................................................................................... 77

To add systems for Agent-less monitoring ....................................................................................... 77

Deploy EventTracker Windows Agent – Windows 7 and Above ........................................................... 85

Prerequisites for Windows Agent – Windows 7 and Above ................................................................ 85

Install / Uninstall Windows 7 and above Agent .................................................................................... 85

Agent Deployment ................................................................................................................................. 85

Secure EventTracker ............................................................................................................................. 85

Uninstall EventTracker Windows Agent ............................................................................................... 85
Uninstall EventTracker Windows Agent via Control Panel ................................................................. 85
Uninstall EventTracker Windows Agent via System Manager ........................................................... 86
Uninstall EventTracker ....................................................................................................................... 88
Ports to be used in EventTracker ...................................................................................................... 90
Frequently Asked Questions .............................................................................................................. 90
Introduction

EventTracker Enterprise provides a unique combination of capabilities, including:

- Enterprise-wide, Distributed Console Event Management
- Rapid Integration with Active Directory
- USB Device Monitoring
- Automatic Remediation
- Reporting
- Analytics
- Real-time Alerting
- File Integrity Monitoring
- Virtual Infrastructure Monitoring
- Status Tracker

This is the good time to familiarize you with the various product features as described on the Web site (http://www.eventtracker.com/eventtracker/enterprise/) in the brochure of this package. This installation guide is designed as an easy reference, since we recognize the imperative importance of error free and painless installation experience.

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

‘How To Install and Customize Web Server (IIS)’ document prior to installing EventTracker 8.3.

Known Issues for v8.3

The below mentioned issues are related to v8.2 Pre-Installer only.

Q1. I get the error “Failed to map the path ‘/app_GlobalResources/’.” in the browser interface.

The workaround for this issue is to re-install IIS Express manually and later run the EventTracker Configuration once again. This error occurs if user has already installed IIS Express RC. Kindly follow the steps mentioned below.

   a. Uninstall IIS Express.
   b. Download IIS Express 8.1 from
      64 Bit:  
      http://download.microsoft.com/download/1/6/3/163BBBDE-5523-416D-A293-EA0492020E4A/iisexpress_8_1_RTM_x64_en-US.msi

      32 bit:
c. Install IIS Express 8.1.
d. To run EventTracker Configuration, search “EventTracker Configuration”.
e. In EventTracker Configuration, enter valid User Credentials, and then select the OK button.

Q2. If user X has finished pre-installation and user Y proceeds to finish the installation on the same machine, then below message is encountered, what should I do?

Please make sure 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 does not have permissions on respective SQL Instance. Please make sure that the logged in user and the system user are having sysadmin privileges on the SQL instance. For detail instructions to grant sysadmin privilege, please refer User Permission on MS SQL Server.

Q3. What should I do if the pre installer prompts to install IIS Express, even though it is installed?

(OR)
If SQL express is installed via pre-install check, then if you click ‘Back’, the installer shows SQL express is not installed.
What should I do if the message “A reboot is still pending” occurs?

![Figure 3](image)

Sometimes installer does not exit properly. This could be because of the pending reboot for Windows installer/.NET Framework/IIS. Quit the Pre-Installer, restart the machine and run the Pre-Installer once again.

Q4. What should I do, if some components do not work for UK region settings?

Please make sure that the Region settings have been applied to the MS SQL engine, (For Ex: UK region settings). Since EventTracker Setup does not install Microsoft SQL Management Studio, kindly download and install the same.

To configure UK Region settings in MS SQL, please refer [UK Region Settings Guide](#).

To know more such Known Issues, Refer: [Known Issues](#) Section in Install Guide-v8.2.

### System Requirements

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

#### Hardware Requirements [Min. Configuration]

Minimum hardware required to install and smoothly run EventTracker Enterprise.

**32-bit Installation:**

<table>
<thead>
<tr>
<th>CPU</th>
<th>2.80 GHz and above, 4 Core or equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>8GB</td>
</tr>
<tr>
<td>HDD</td>
<td>80 GB free SCSI 7,500 RPM (or) 75-100 IOPS RPM space for the application</td>
</tr>
</tbody>
</table>

**64-bit Installation:**
### Software Requirements

**EventTracker Manager**

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

Table 3

**Components:**
- Microsoft .NET Framework 3.5 SP1 and .NET Framework 4 or 4.5.2.
- IIS 7.0 -8.5. Also IIS Express is supported except **Win 2008** and above OS.
- Windows Management Framework 2.0
- Make sure **Windows updates** with all the latest service packs is installed.

**Web Browsers:**
- Internet Explorer 11 and above.
- Firefox Browser latest.

**NOTE**
1. It is recommended not to install EventTracker on Domain Controller.
2. It is recommended to run the EventTracker Manager Console on a Dedicated Windows Server.
3. EventTracker Enterprise installation on Windows 2012/2012 R2/2008/2008 R2 Server Core edition is not supported. We support 2012 r2 core minimal user interface.

### EventTracker Agent

<table>
<thead>
<tr>
<th>Windows Platforms</th>
<th>32 bit</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 2016</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 2012</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008 R2</td>
<td>Not Applicable</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2008</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2003 R2</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Server 2003</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</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 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**EventTracker Agent for Solaris: Solaris 9, Solaris 10**

Table 4

### Components:

- Microsoft .NET Framework 2.0 and above.

**NOTE**

Versions other than those specified above are not supported.

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

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

**NOTE:** If you wish to configure EventTracker users via Pre-installer then you can do so because the pre-install check performs the same steps and this entire process is automated. The details to configure via Pre-Installer are mentioned in [Procedure to Install EventTracker Manager](#). If you still wish to configure
Install EventTracker Manager

Prism recommends you to refer ‘EventTracker Architecture’ guide before you begin installation. This guide explains the architecture and sample deployment methods with illustrations.

Installation can be initiated by the following methods.

1. Launch the executable program. The installation is geared to be intuitive and friendly. During install you will be asked to provide the path of the digital certificate. Certificate is validated against the latest CRL. Installation proceeds further only if the Certificate found to be valid.

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

Pre-install Checklist for EventTracker Manager

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

| ENSURE | User is a member of ‘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 | User has permission on ‘Application install directory’ (Folders and sub folders). |
|        | User must have created service permission on the target system (SCM- service control manager). |
|        | User has Read/Write permission on windows registry. |

Table 5

IIS Settings

Please ensure that IIS Settings under Application Pools are as follows in Windows 2008/2008 R2/2012/2012 R2.
Figure 4 – 64 bit OS

Figure 5 – 32 bit OS
For details to configure the above settings, please refer Install and Customize IIS Web Server Guide.

User Permission on SQL Server

Users trying to install EventTracker should have sysadmin privilege on respective SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2012 R2 / 2014.

NOTE:
In SQL 2008 / 2008 R2 / 2012 / 2012 R2 / 2014, please make sure that sysadmin privilege has been granted to NT AUTHORITY\SYSTEM. If SQL server 2012 and above is used by the customer then the SQL service in the service control manager has to be changed from ‘NT Service\MSSQL$SSLEXPRESS’ to ‘Network Service’.
If 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

Procedure to install EventTracker Manager - Custom

If you are using EventTracker for the first time, launch the executable program and proceed. If you are a second time user, please uninstall the previous version of EventTracker and then proceed. The detail procedure to uninstall EventTracker is mentioned in Uninstall EventTracker.

The detail procedure to install EventTracker is given below.

NOTE: For Windows 7 and Windows 2008, if the Windows Management Framework 2.0 is not installed, the PowerShell 3.0 installation will fail, which is a pre-requisite for the EventTracker installation.

To download Windows Management Framework 2.0, click on the following link:

https://support.microsoft.com/en-us/kb/968929

1. Double-click the executable file.

NOTE: .NET 4.5. is enabled by default for Windows 8/8.1/2012.
NOTE: In case system doesn’t contain the latest windows updates with service packs then the following message will be displayed:

EventTracker Pre-Install Check window displays.
2. Click the Next > button. 
   Hardware Summary pane displays.

**NOTE:**

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

The processing symbol will be displayed only to the customers who are using EventTracker V 8.0 and later.
3. Click the **Next >** button. Install Type page displays.
4. Select Standard/Collection Point/Custom option, and then select the **Next >** button. In this section, Custom option is selected.
Prerequisite page displays.

NOTE:

- If the prerequisites are not installed, then a message ‘Install’ displays against the respective prerequisite.
a. Click the **Next >** button.

- For some Windows platforms, .NET Framework gets installed via Deployment Image Servicing Management Tool (DISM).

The instructions to install .NET Framework is given in detail in [How To - Install Microsoft .NET Framework](#).

If the system contains all latest service packs, then PowerShell will start installing.
a. Click the Install button.
b. Once the download is completed, it will search for updates in the computer. The Windows Update Standalone Installer page displays.
c. It will ask for applying the Windows Software updates.
d. Click Yes.

![Figure 14]

Figure 14

e. Accept the agreement by clicking the I Accept button.

f. The update package, Windows Management Framework 2.0 gets installed via Pre-installer as shown in the figure below:

![Figure 15]

Figure 15
NOTE: In case system doesn’t contain the latest Windows updates with service packs then the following message will be displayed:

![Windows Update Standalone Installer]

The update is not applicable to your computer.

Figure 16

Once prerequisites are installed, Database page displays.

5. If SQL server is running with multiple instances, EventTracker preinstaller will give a pop up message as shown below:

![EventTracker Pre-Install Check]

Figure 17
6. Select Appropriate Instance to proceed with the installation process.
7. If MSSQL Server – Express Edition 2005/2008/2008 R2/2012/2014 is already installed, then select one instance and click the Next > button.

Database page displays.

- If MS SQL Express is not installed, then click **Next >**.

![Figure 18](image-url)

The pre-installer prompts to download SQL Server Express Edition.
a. Click the **Download** button.

Please select a location to download the SQL installer window displays.
b. Select the path to download SQL Express on a particular location and then click Save.

SQL Express starts downloading.
8. The Select SQL install and data directories screen will appear where you can choose the directory to which the SQL Server is to be installed.

![Select SQL install and data directories](image)

Figure 22

9. Select the browse button \(\ldots\) to choose the location and then click OK.

SQL Express will be installed in the background.

**NOTE:**
The option to choose the install directory is available only to the customers who are using EventTracker V 8.0 and later.

10. For SQL Express 2012/2014/2016 one needs to provide the user name and password of that person/account that will run the SQL service. This is to prevent the service from stopping since in some systems it is observed that the SQL service doesn’t execute under the default account in which it gets created.

![Figure 23](image1.png)

![Figure 24](image2.png)

After MS SQL Express is installed, Web Server page displays.

11. Select IIS/IIS Express option, and then select the **Next >** button.

**NOTE:**

- Only IIS Express will be displayed for installation, if IIS is not installed on the machine.
- If IIS is installed, it will display the installed IIS version along with IIS express option.
- We are supporting IIS Express since it is a lightweight tool. You can choose to install IIS Express/Manager based on the requirement.
- If you prefer to use IIS Manager, refer [install IIS](#) for detail instructions.
If IIS Express is already installed, on clicking **Next >**, **Disk Usage** page displays.

If IIS Express is not installed, proceed to install it.
a. If **IIS Express (Not Installed)** option is selected, then click the **Next >** button.

Installation of IIS Express proceeds.
b. Click the **Install** button.

After IIS Express is installed successfully.

Disk Usage page displays.
12. Click the **Next >** button.

   Installation Summary page displays.
13. Click the **Next >** button.

Define User Group page displays.
14. Select Local Machine or Active Directory option, and then select the Next > button.

If Local Machine option is selected, then You have selected to use local machine page displays. Please refer step 15 for further instructions.

NOTE:

While creating group and/or user, the user should be part of the administrators 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 displays. Please refer Step 16, for further instructions.

15. Select Create User Group EventTracker or Select existing User Group option, and then select the Next > button.

If local machine was selected earlier, then ‘You have selected to use local machine’ page displays.
NOTE:

When creating group,

➢ We encourage 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 will be to ‘Create User Group EventTracker’ else the default choice will be ‘Select Existing Group’.

   a. If Create User Group EventTracker is selected, click Next >.

      Members of this User Group can access EventTracker page displays.
The group name must be unique otherwise an error message displays stating that the group already exists.

Figure 32

b. Click the OK button.

c. To solve this issue, enter a unique **Group Name**, and then click the Next > button. Define User page displays. Please refer step 17 to continue installing EventTracker.

(OR)
a. If **Select existing User Group** option is selected, then select any group, and then click the **Next >** button.

![Define User page displays. Please refer step 17 to continue installing EventTracker.](image)

**NOTE:**

When creating group,
➢ We encourage 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 will be to ‘Create User Group EventTracker’ else the default choice will be ‘Select Existing Group’.

![EventTracker Pre-Install Check](image)

**Figure 35**

- If Create User Group EventTracker option is selected, then Members of this User Group can access EventTracker page displays.
➢ Enter unique and appropriate Group Name, and then click the Next > button.

NOTE:

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

A. Click the OK button.
❖ If Select existing User Group option is selected,

a. Select any group, and then select the Next > button.
Define User page displays.

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

❖ If **Create EventTrackerAdmin** option is selected, please refer Figure 34.

**NOTE:**

Administrator should have sufficient privileges on Active Directory machine as well as to create a group.

Figure 40

a. Click the Next > button.

This User will manage EventTracker page displays.
b. Enter relevant credentials, and then click the **Next >** button. Summary page displays.

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

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

**NOTE:** A wildcard can also be entered.
b. Click the **Next >** button.

   Summary page displays.

   - If **Select existing User** option is selected, select an appropriate user, and then select the **Next >** button.
Summary page displays.

If user is not EventTracker Administrator then below message displays.

![EventTracker Pre-Install Check](image)

Figure 44

a. Click the **Yes** button.
18. In **Summary** page, verify all the data entered, and then click the **Install** button.

![EventTracker Pre-Install Check](image)

**Figure 45**

19. Click the **Yes** button.

EventTracker - Install Shield Wizard displays.
EventTracker - InstallShield Wizard displays the **Welcome** screen.
20. Click Next >.
21. In case of multiple SQL instances, select the appropriate instance name from Instance name dropdown, and then click the OK button.

NOTE: If default instance of SQLEXPRESS is present in the system, then EventTracker won’t prompt for this screen. If the selected SQL Instance is not running then EventTracker Installation wizard will display a message.

InstallShield Wizard displays the License Agreement screen.
22. Read the license agreement, and then click ‘I accept the terms in the license agreement’ option to accept the terms and condition.

23. Click the Next > button.

Select a Certificate File page displays.

**NOTE:**

If the user has selected **Custom** option in EventTracker Pre Install Check, then the installer prompts to add the certificate file.
24. To locate the path of the certificate file, click the Browse button. Select File window displays.
25. Go to the appropriate folder, select the file and then click Open. The folder path is updated.

Figure 51
26. Click Next >.
Select Components screen displays.
### EventTracker Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Console</td>
<td>Select this option to install manager console on 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. Agent component will also be installed along with the Manager Console. You can also deploy 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>
<tr>
<td>Status Tracker</td>
<td>Optional component. Installing this component enable you to monitor and manage TCP/IP networks, Web sites, applications, and ports in mission critical environment.</td>
</tr>
</tbody>
</table>

Click to Select different destination folder to install EventTracker.

[Image of destination folder selection dialog box]
27. Click **Next >**.
InstallShield Wizard displays 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.

![Standard Console Diagram](image)

**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 displays Configure Collection Point site page.

b) Enter **Site name:** and then select the **Next >** button.
**NOTE:**
Some special characters are not allowed while providing site/group name. InstallShield Wizard displays a pop-up window if site or group name is provided with such special characters.

![EventTracker](image)

**Figure 119**

c) Enter **Collection Master**: name or IP Address, and then select the **Next >** button.

![EventTracker](image)

**Figure 57**

**Collection Master:**

Used in hierarchical network topologies where collection points replicate their event log archives to a Collection Master.
27. Select a console type, and then select the **Next >** button.

If you have selected **Change Audit** component, then InstallShield Wizard displays **Change Audit SnapShot** dialog box.
28. Click the **Next** > button to keep the default store location.

(OR)

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

![Figure 60](image)

29. Browse the destination folder, and then click the **OK** button.

**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 upgrade, if the change audit snapshots are retained during product un-installation, then the snapshot store location path cannot be changed.
If you have not selected to install **Change Audit**, then InstallShield Wizard displays the **Ready to Install the Program** screen.

30. The **Ready to Install the Program** screen displays the summary of the installation path, console type and the selected features.
31. Click the **Install** button. InstallShield Wizard installs the selected components.

InstallShield Wizard initializes the configuration settings required for proper operation of EventTracker. After initializing the necessary configuration settings, InstallShield[R] Wizard displays the **Basic configuration** dialog box.
32. Select appropriate options, and then click **OK**.

InstallShield Wizard displays the last screen.
a. Click **Import existing event log entries** option to import event logs of EventTracker. Windows Security Alert message will be displayed if Firewall is on.
Firewall blocks the incoming network connection, if `getallevt.exe` does not exist in the Program and Services Exceptions and displays a notification.

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

b. Check **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.

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

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

![EventTracker Configuration screen](image)

**Figure 67**

**NOTE:**
Make sure that you select/enter the correct **User Credentials, User Authentication and EventTracker Group** in order to login successfully. The user name/authentication that is done in EventTracker Preinstall Check, reflects in this screen, but user has the option to override it.

34. 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.

35. Select a **User Authentication** option.

  - **Local Account:** Authentication is done locally on the computer where EventTracker is being installed.
  - **Active Directory:** Authentication is done in the Active Directory.
36. Type the EventTracker group name in the **EventTracker Group** field.

37. Click **OK**.

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

   ![EventTracker Configuration](image)

   **Figure 68**

38. Click **OK**.

**NOTE:**

If the password is changed for the above configured user, it is mandatory to re-run the EventTracker Configuration (Figure: 67) with the updated password.

   i. To find ‘EventTracker Configuration’, select the **Start** button, select **All Programs**.
   ii. Select **Prism Microsystems**, select **EventTracker**, and then select **EventTracker Configuration**.
   iii. Enter appropriate credentials and then select the **OK** button.

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

**NOTE:**

If **Standard** or **Collection Point** is selected, then

- The archive path will be the drive with the maximum free space
- Local machine authentication will be used
- Group will be created as ‘EventTracker’
- User name will be ‘EventTrackerAdmin’
- This user will be local machine admin

- This user will be given ‘Logon as batch user’ rights, and ‘Logon as Service’ rights
- Only express versions of IIS and SQL can be used.

To install EventTracker 21 day trial – Standard/Collection Point, please follow the steps given below.
10. Double-click the executable file. EventTracker Pre-Install Check window displays.

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

**Figure 69**

11. Click the **Next >** button. Hardware Summary pane displays.
12. Select **Standard/Collection Point** option, and then select the **Next >** button.
To proceed with the further installation, refer the ETLM-Install Guide.

**NOTE:** After logging into EventTracker Enterprise, 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.

## Deploy EventTracker Windows Agent

### 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.
- Make sure that the systems that 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 a 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.

Pre-install Checklist for Windows Agent

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

<table>
<thead>
<tr>
<th>ENSURE</th>
<th>Verify</th>
</tr>
</thead>
<tbody>
<tr>
<td>User is a member of ‘Local Administrators’ group</td>
<td>User has permission on ‘Application install directory’ (Folders and sub folders).</td>
</tr>
<tr>
<td>MSI package installation is allowed</td>
<td>User must have create service permission on the target system(SCM- service control manager)</td>
</tr>
<tr>
<td>User has ‘Logon As Service’ rights</td>
<td>User has Read/Write permission on windows registry.</td>
</tr>
<tr>
<td>Network Discovery is enabled</td>
<td>User has permission to Admin share(C$) of Target systems and C$ should be accessible from EventTracker Manager system.</td>
</tr>
<tr>
<td>File sharing is allowed</td>
<td></td>
</tr>
<tr>
<td>Access this computer from network</td>
<td></td>
</tr>
</tbody>
</table>

Table 6

Different methods to install EventTracker Agents

There are 2 methods to deploy EventTracker Agents

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.

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


1. Select the Start button, select All Programs, and then select Prism Microsystems.
2. Select EventTracker, and then select EventTracker Enterprise. EventTracker displays the login page.

3. Logon with valid user credentials. EventTracker displays the Incident dashboard.

4. Click the Admin drop-down list at the upper-right corner, and then select Systems. EventTracker displays the Systems manager page.

![Figure 72](image)

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

1. Right-click the system group on the right-pane in which the target systems exist. EventTracker displays the shortcut menu.
2. From the shortcut menu, click the **Install agent/Start poll** option. EventTracker displays the **Install agent/Start poll** dialog box.

![Figure 73](image1)

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

![Figure 74](image2)
• All Systems in the selected group
• Take systems from 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 specific system(s) to install the agent.</td>
</tr>
</tbody>
</table>

Table 7

1. Click **Next**.

![Figure 75](image)

2. To install **EventTracker/Change Audit Agent** on all the system present in the domain, select the respective **EventTracker/Change Audit** option.
   (OR)
   Select the respective check box against the systems where you wish to deploy the EventTracker/Change Audit agent.
In the **System** manager page, move the mouse pointer over the system where you wish to install the agent.

a) Click the dropdown.
   EventTracker displays the drop-down list.

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

---

EventTracker displays the **Install Agent/Start poll** dialog box.
c) Check the **EventTracker** option to install EventTracker agent.

d) Check the **Change Audit** option to install Change Audit agent.

3. Click **Next**.
4. 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 will be 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>
<tbody>
<tr>
<td>Deploy SCAP</td>
<td>Provides an option to install SCAP components to remote machines while deploying agent(s).</td>
</tr>
<tr>
<td>Deploy WinSCP</td>
<td>Provides an option to install WinSCP components to remote machines while deploying agent(s).</td>
</tr>
</tbody>
</table>

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 8

13. 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)

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

   ![OK Cancel](image)

   Figure 79

   **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 default client installation path on the remote computer.
14. 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.
15. Check the **Create ‘Program Menu’ shortcuts** option to create shortcuts.
16. Enter valid **Account** name and **Password**.
17. Reenter the password in **Confirm Password**.
18. Click **Install**.

The agent will be 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 manager side ‘Agent configuration’ settings (etaconfig.ini).
b) Select **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.
NOTE:

In case you select `etaconfig_Servers.ini`, `etaconfig_Workstations.ini`, 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.

To configure Manager Name follow the steps given below.

i. Select **Admin** drop-down in EventTracker home page.

ii. Select **Windows Agent Config** and then select **Load Template**.

iii. Select the required file name i.e. `etaconfig_Servers/etaconfig_Workstations` accordingly. Select **Load**.

iv. In **EventTracker Managers** tab, select **Add**.

v. In **Add Destination** window, enter the relevant **Destination** and **Port**.

vi. In **Connect to Manager using** box, select **High Performance Mode (UDP)** or **Guaranteed Delivery Mode (TCP)** and then select the **OK** button.

c) Select the configuration file from the **File** dropdown, and then click the **Install** button. EventTracker displays the pop-up window with appropriate message.
5. Click **OK**. 
EventTracker displays **Installation Status** screen.

![Figure 84](image)

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

Table 9

6. Click **Refresh** to view the current status.

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

15. Click **Close**.
16. Refresh the **System** manager.
Configure EventTracker Windows Agent

All configurations for 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 85**

2. Double-click EventTracker Agent Configuration.
   
   EventTracker Agent Configuration window displays.
3. Click appropriate tabs and configure the agent as you wish.
Configuring Agent-less collection via System Manager (limited features)

In cases where 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.

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

To add systems for Agent-less monitoring

In the System manager page, move the mouse pointer over the system where you wish to install the agent.
a) Click the dropdown icon. EventTracker displays the drop-down list.

b) Click Install agent/Start poll.

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

---

**Figure 89**

**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
By default, the frequency is set to 15 min to receive events from the remote agent system.

Table 10

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling frequency</td>
<td>Poll Every 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>

Table 11

e) Click **Next**.

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

![Install agent/Start poll dialog box](image)

**Figure 90**

f) Click **Install**.

The agent will be 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 manager side ‘Agent configuration’ settings (etaconfig.ini).

2. Select **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.

   ![Figure 91](image)

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

   ![Figure 92](image)
h) Click **OK**.

EventTracker displays **Installation Status** screen.

![Installation Status screen](image)

**Figure 93**

<table>
<thead>
<tr>
<th>Select</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Sort the <em>Installation Status</em> results by the application installed. Available options are EventTracker &amp; Change Audit.</td>
</tr>
<tr>
<td>Status</td>
<td>Sort the <em>Installation Status</em> results by status of the application installed. Available options are All, New, Success, and Failed.</td>
</tr>
<tr>
<td>Sort by</td>
<td>Sort the <em>Installation Status</em> 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 installation status details from the list.</td>
</tr>
<tr>
<td>Export</td>
<td>Export the ‘System Status’ into Excel format</td>
</tr>
</tbody>
</table>

**Table 12**

i) Click **Refresh** to view the current status.

(OR)

Reopen the **Installation 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 will be available as shown in the figure below:

![EventTracker Agent Configuration](image)

**Figure 94**

Go to **EventTracker Web**,  
1. Click the **Admin** drop-down list at the upper-right corner.  
2. Click the **Windows Agent Config**.
3. Click the Search system button to select the system.

**NOTE:** For Agent-less (limited feature)* option, all the above mentioned feature tabs will be displayed but only limited feature will be available.

*Agent-less (limited feature)* refers to a version with restricted features compared to the full-fledged version.
Deploy EventTracker Windows Agent – Windows 7 and Above

Prerequisites for Windows Agent – Windows 7 and Above

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.

Install / Uninstall Windows 7 and above Agent

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

Agent Deployment

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

Secure EventTracker

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

Uninstall EventTracker Windows Agent

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

Uninstall EventTracker Windows Agent via Control Panel

1. Select the Start button, select All Programs, and then select Control Panel.
2. Select Add or Remove Programs, select EventTrackerAgent, and then select Remove. Windows Installer displays.
3. Select the **Yes** button.
   EventTracker window displays.
4. Select **Yes/No** as per the requirement.

**NOTE:**

If you wish to retain the agent configuration settings, select the **Yes** button. If you do not wish to retain agent configuration settings, select the **No** button.

**Uninstall EventTracker Windows Agent via System Manager**

1) Click **Admin** drop down, select **Systems**.
2) Select the **Groups** or **Computer** name on which un-installation is required.
3) Select **Uninstall agent/Stop poll.**

Uninstall Remote agent(s)/Stop poll displays.

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

![Uninstall Remote agent(s)/Stop poll window](image)

Figure 100

5) Enter valid credentials and then select **Uninstall**.

**Uninstall EventTracker**

1. Select the **Start** button, select **Control Panel-> Programs and Features**.
2. Select **EventTracker**, and then select **Uninstall**.

![Uninstall or change a program](image)

Figure 101

Windows Installer window appears displays.
3. Select the **Yes** button.

EventTracker window displays.

4. Select the **Ok** button.

Uninstall EventTracker Enterprise window displays.

**NOTE:**

In case you wish to retain **Configuration, Reports and Data, Snapshots** files then select the respective check box otherwise uncheck the options.

5. Select the **Ok** button.
Ports to be 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>14504</td>
<td>EventTracker Active WatchList (For v8.2 and v8.3)</td>
</tr>
</tbody>
</table>

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

Frequently Asked Questions

1. How to change webserver port used by EventTracker?

   If the EventTracker installation is using IISEXRPRESS follow the below 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 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. Select Web Document tab.

f. Modify URL: as shown below.

g. Restart IISExpress service.
If the EventTracker installation is using IIS please follow the below steps to use port 80:

a. Open IIS Manager and expand Sites. Select EventTracker site.
b. In the Actions pane, click Bindings.
c. Select the listed entry and then select Edit as shown below.

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

   Edit Site Binding window displays confirmation message.

   ![Figure 108](image)

   e. Click the Yes button.

**NOTE:**
If user gets a message stating that changes cannot be applied to the shortcut, user has to copy the "Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url" to some other location, modify the same and update the same file under "Prism Microsystems\EventTrackerWeb\EventTrackerWeb.url".

Figure 109

f. Stop the **Default Web Site** and start **EventTracker** site as shown below.

Figure 110

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

Figure 111
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.