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 XP/Vista/Win 7/2003/2008/2008R2/2012/Win 8, 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.

Target Audience

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

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

System Requirements ................................................................................................................................ 5

Hardware Requirements [Min. Configuration]..................................................................................... 5

Software Requirements .......................................................................................................................... 5

Pre-install instructions for Local Account and Active Directory authentication ...................... 7

Create Local User and Group Accounts ................................................................................................. 7

Create EventTracker User Group ........................................................................................................... 9

Create User ........................................................................................................................................ 12

Add User to EventTracker Group ...................................................................................................... 14

Create Active Directory User and Group Accounts .......................................................................... 19

Create EventTracker Group ................................................................................................................. 20

Create User ........................................................................................................................................ 23

Add User to EventTracker Group ...................................................................................................... 27

Add User to Local Administrators group ......................................................................................... 31

Add cross-domain users ...................................................................................................................... 32

Add cross-forest users .......................................................................................................................... 33

Install EventTracker Manager .................................................................................................................. 34

Pre-install Checklist for EventTracker Manager ................................................................................ 34

User Permission on SQL Server ....................................................................................................... 35

Procedure to install EventTracker Manager ...................................................................................... 45

Deploy EventTracker Windows Agent ..................................................................................................... 67

Pre-install Instructions for Windows Agent ....................................................................................... 67

Pre-install Checklist for Windows Agent ............................................................................................ 67

Different methods to install EventTracker Agents ........................................................................... 68

Deploy EventTracker Windows Agent via System Manager ............................................................. 68

Configure EventTracker Windows Agent ............................................................................................... 78

Deploy EventTracker Windows Agent – Vista and Above ................................................................. 81

Prerequisites for Windows Agent – Vista and Above ..................................................................... 81

Install / Uninstall Vista and above Agent ............................................................................................ 81
Agent Deployment .................................................................81
Secure EventTracker ..........................................................81
Uninstall EventTracker Windows Agent ..............................82
     Uninstall EventTracker Windows Agent via Control Panel   82
     Uninstall EventTracker Windows Agent via System Manager 83
Uninstall EventTracker ........................................................85
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: Prism strongly recommends users to refer ‘How To Install and Customize Web Server (IIS)’ document prior to installing EventTracker 7.4.
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>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2GHz, 32-bit (x86) Xeon ® Quad Core or equivalent</td>
</tr>
<tr>
<td>RAM</td>
<td>3 GB</td>
</tr>
<tr>
<td>HDD</td>
<td>10 GB Free Hard disk space for the application</td>
</tr>
</tbody>
</table>

64-bit Installation:

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2.80 GHz, 64-bit (x64) Xeon ® Dual Core or equivalent</td>
</tr>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>HDD</td>
<td>10 GB Free Hard disk space for the application</td>
</tr>
</tbody>
</table>

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 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>
</tbody>
</table>

Components:
- Microsoft .NET Framework 3.5 SP1
• IIS 6.0 and above

**Web Browsers:**
• Internet Explorer 8.0 and above
• Firefox Browser 3.5 and above

**Note:** EventTracker Enterprise installation on Windows 2012/2008/2008R2 Server Core edition not supported.

**EventTracker Agent**

<table>
<thead>
<tr>
<th>Windows Platforms</th>
<th>32 bit</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<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 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>2000 Server</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>2000 Professional</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Vista</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th></th>
<th>32 bit</th>
<th>64 bit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

**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.
- If you want ‘Local Account’ authentication, then user accounts and group accounts should preexist on the target computer where EventTracker Enterprise is to be installed. So, create user accounts and group accounts on the target computer before you attempt to install EventTracker Enterprise.
- If you want ‘Active Directory’ authentication, then user accounts and group accounts should preexist in the Active Directory. So, create user accounts and group accounts in the Active Directory before you attempt to install EventTracker Enterprise.

Create Local User and Group Accounts

**NOTE:**
To perform this procedure, you must be a member of the administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, then members of the ‘Local Admin’ group might be able to perform this procedure.

**Summary**
- What is the significance of creating ‘EventTracker’ user group?
  - To log on to EventTracker Enterprise, the user must be a member of ‘EventTracker’ group.
  - EventTracker Enterprise user authentication operates locally, that is confined to a particular computer or within Active Directory context.
- Create a local user group ‘EventTracker***’ on the computer where EventTracker Enterprise is to be installed.
  - Create a local user e.g. ETKaren**.
  - Add ETKaren user to EventTracker group. Members of this group can log on to EventTracker Enterprise.
  - Add ETKaren user to local Administrators group on the computer where EventTracker Enterprise is to be installed.

*** You can name user group and user with any name you prefer and need not necessarily be EventTracker and ETKaren.
Figure 1
Create EventTracker User Group

1. Select the **Start** button, select **Control Panel**, and then select **Administrative Tools**.
2. Select **Computer Management**, and then select **Local Users and Groups**.

![Figure 2](image)

3. Expand the **Local Users and Groups** node. Right-click **Groups**, and then select **New Group**. Refer Figure 3.
4. Type the name of the group in the **Group name** field.

5. Select **Create**, and then select **Close**.
Event Tracker group is created.
Create User

1. In Local Users and Groups node, right-click Users, and then select New User.

   ![Figure 6](image)

2. Type appropriate user credentials.
   For example, you can type ‘ETKaren’ as user name.
3. Provide a strong password and confirm the same.
4. Select the Password never expires check box.
   Refer Figure 7.

   ![Figure 7](image)
NOTE:
It is not mandatory to check **Password never expires** option. In order to avoid password expiry of EventTracker every now and then, we recommend you to check this option.

5. Select **Create**, and then select **Close**.

![Figure 8](image)

ETKaren user is created.
Add User to EventTracker Group

1. Right-click the newly created user group, and then select **Properties**.

![EventTracker Properties window displays.](image)

**Figure 9**

**EventTracker Properties** window displays.

![EventTracker Properties](image)

**Figure 10**
2. Select the **Add** button. Select Users, Computers, Service Accounts or Groups window displays.

![Select Users, Computers, Service Accounts, or Groups](image)

**Figure 11**

3. Select the **Locations** button. Locations window displays.

![Locations](image)

**Figure 12**

4. Select the location, typically the name of the computer. In this example, name of the computer is SPIDER-II. Refer Figure 13.
5. Select the **OK** button.

6. Type the user name in the **Enter the object names to select** field.
7. Select the **Check Names** button.

8. Select the **OK** button.
9. Select **Apply**, and then select the **OK** button.
Create Active Directory User and Group Accounts

**NOTE:**
To perform this procedure, you must be a member of the ‘Account Operators’ group, ‘Local Admin’ group, or the ‘Enterprise Admin’ group in Active Directory, or you must have been delegated the appropriate authority.

Summary:

a. Create a user group e.g. EventTracker Test** in the domain where EventTracker Enterprise is to be installed.

b. Create a domain user e.g. ETKaren**:
   Add ETKaren user to EventTracker Test group. Members of this group can log on to EventTracker Enterprise.

c. Add ETKaren user to local Administrators group on the computer where EventTracker Enterprise is to be installed.

** You can name user group and user with any name you prefer and need not necessarily be EventTracker Test and ETKaren.

![Diagram](image18.png)

*Figure 18*
Create EventTracker Group

1. Select the **Start** button, select **Settings**, and then select **Control Panel**.
2. Select **Administrative Tools**, and then select **Active Directory Users and Computers**.

Create a **Global Scope Security Group** in the domain where EventTracker Enterprise is to be installed.
3. Right-click the domain name, select **New**, and then select **Group**.
   In this example, domain name is ‘pnplvista.test’.
4. Type the name of the group in the **Group name** field. 
   In this example group name is ‘EventTracker Test’. 
5. Select **Group scope** as **Global**, and **Group type** as **Security**.

6. Click **OK**. 
   ‘EventTracker Test’ group is created. Refer Figure 23.
### Active Directory Users and Computers

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>abc</td>
<td>Organizational</td>
<td></td>
</tr>
<tr>
<td>OUs</td>
<td>Organizational</td>
<td></td>
</tr>
<tr>
<td>Computers</td>
<td>Container</td>
<td>Default container for upgr...</td>
</tr>
<tr>
<td>Domain Controllers</td>
<td>Container</td>
<td>Default container for dom...</td>
</tr>
<tr>
<td>EventTracker Test</td>
<td>Security Group</td>
<td></td>
</tr>
<tr>
<td>ForeignGroupIn principals</td>
<td>Container</td>
<td>Default container for sec...</td>
</tr>
<tr>
<td>OUs testing OU</td>
<td>Organizational</td>
<td></td>
</tr>
<tr>
<td>Testing OU</td>
<td>Organizational</td>
<td></td>
</tr>
<tr>
<td>Testing OU22CH</td>
<td>Container</td>
<td>Default container for upgr...</td>
</tr>
</tbody>
</table>

![Active Directory Users and Computers](image)

**Figure 23**
Create User

1. Right-click Users, point to New, and then User.

New Object – User window displays.
2. Type appropriately in the respective fields.
   In this example, First name is ‘Karen’, Last name is ‘Smith’ and User logon name is ‘ETKaren’.

   ![New Object - User](image)

   Figure 26

3. Select the **Next >** button.

4. Type the password in the **Password** and **Confirm Password** fields.

5. Select the **Password Never Expires** check box.

   ![New Object - User](image)

   Figure 27
NOTE:
It is not mandatory to check **Password never expires** option. In order to avoid password expiry of EventTracker every now and then, we recommend you to check this option.

6. Select the **Next >** button.

![Figure 28](image)

7. Select the **Finish** button.
   Username ‘Karen Smith’ is created. Refer Figure 29.
Figure 29
Add User to EventTracker Group

1. Right-click the **EventTracker Test** group, and then select **Properties**.

![EventTracker Test Group](image)

**Figure 30**

EventTracker Properties window displays.

![EventTracker Properties Window](image)

**Figure 31**
2. Select the **Members** tab.

![EventTracker Properties dialog box](image)

**Figure 32**

3. Select the **Add** button.

![Select Users, Contacts, Computers, or Groups dialog box](image)

**Figure 33**
4. Type the user name in the **Enter the object names to select** field.

![Select Users, Contacts, Computers, or Groups](image)

**Figure 34**

5. Select the **Check Names** button.

![Select Users, Contacts, Computers, or Groups](image)

**Figure 35**

6. Select the **OK** button.

‘Karen Smith’ is a member of ‘EventTracker Test’ group.
7. Select the **Apply** button, and then select the **OK** button.
Add User to Local Administrators group

To add a user to the ‘Administrators’ group on the computer where EventTracker Enterprise is installed follow the steps given below.

1) Right click My Computer, select Manage.
2) Expand Local Users and Groups, select Groups.
3) Right click EventTracker group, select Add to Group.
   EventTracker Properties window displays.
4) Select the Add button.
   Select Users, Contacts, Computers, Service Accounts, or Groups window displays.

![Select Users, Contacts, Computers, Service Accounts, or Groups](Figure 37)

5) In Enter the object names to select box, enter username (i.e. ‘Karen’ in our example), and select the Check Names button.
6) Select the OK button.
Add cross-domain users

Consider Domain A and Domain B exist in Forest 1 and EventTracker Enterprise server is a member of Domain A. If a user in Domain B needs to access and administer EventTracker Enterprise, add that user to EventTracker user group in Domain A. Since these two domains exist in the same forest, Windows creates automatic trust relationship between these two domains.

Figure 38

Windows creates an **automatic trust** relationship (two-way, transitive trust link) between these two domains.

EventTracker User Group in Domain A

User in Domain B
Add cross-forest users

Consider Domain A and Domain B exist in Forest 1 and Domain C and Domain D exist in Forest 2. EventTracker Enterprise server is a member of Domain A. If a user in Domain C needs to access and administer EventTracker Enterprise, add that user to EventTracker user group in Domain A. Since these two domains exist in different forests, you need to create trust prior to adding users.

**Figure 39**

**Windows Server 2003 forests**: Create a forest trust. A forest trust lets you create a trust relationship between two separate Active Directory forests.
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 etwrel74.exe. 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.

<table>
<thead>
<tr>
<th>ENSURE</th>
<th>User is a member of ‘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>

<table>
<thead>
<tr>
<th>VERIFY</th>
<th>User has permission on ‘Application install directory’ (Folders and sub folders).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User must have create service permission on the target system(SCM- service control manager)</td>
</tr>
<tr>
<td></td>
<td>User has Read/Write permission on windows registry.</td>
</tr>
</tbody>
</table>
User Permission on SQL Server

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

NOTE:

In SQL 2008 / 2008 R2 / 2012, please make sure that sysadmin privilege has been granted to NT AUTHORITY\SYSTEM.

Scenario 1:

If NT AUTHORITY\SYSTEM is not available under Security -> Logins then it has to be created. The steps are mentioned below

A) Select the Start button, select Microsoft SQL Server (2008 / 2008 R2 / 2012) and then select Microsoft SQL Server Management Studio.
B) Expand Security node, right click Logins node and then select New Login.
   Login – New window displays.
C) Select the **Search**.. button.

Select User or Group window displays. The location should be your local system.
D) In **Enter the object name to select** box, type **system** and then select **Check Names**.

E) Select the **OK** button.

NT AUTHORITY\SYSTEM displays in Login window.
In **Select a page** pane, select **Server Roles** and then select **sysadmin** option.
G) Select the **OK** button.

**Scenario 2:**

If NT AUTHORITY\SYSTEM is already available under Security -> Logins then please follow the steps mentioned below to grant sysadmin permission.

a) Expand **Security** node, expand **Logins** node.

b) Right click **NT AUTHORITY\SYSTEM** and then select **Properties**.
c) Select **Server Roles** and then select **sysadmin**, if not selected. Refer Figure 43.

**Scenario 3:**

To grant sysadmin privilege to an individual user or an administrators group, please follow the steps given below.

A) Expand **Security** node, right click **Logins** node and then select **New Login**.
   Refer Figure 40.

B) Click the **Search** button.
   Select User or Group window displays.
C) Select the **Object Types** button, select **Groups**, and then select the **OK** button.

![Object Types](image)

**Figure 45**

D) In **Enter the object name to select box**, enter ‘administrators/username’ and then click **Check Names**.
E) Click OK.

F) Select Server Roles and then select sysadmin.
   
   Refer Figure 43.

G) Click OK.

NOTE:

If the SQL service is running on a different account apart from system and network account, then the user account on which SQL service is running should have full permission to the reports folder. In order to use persist flex data, EventVault Explorer search and Correl reports, sysadmin permissions is required since SQL database is created for these reports.
1. To grant full permission on **Reports** folder, browse the path where EventTracker is installed i.e. `\<INSTALLDIR>\EventTracker`.
2. Right click **Reports** folder, and then select **Properties**.
3. Select **Sharing** tab, and then select **Share this folder**.

![Figure 47](image)

4. Select **Permissions**, and then select **Add...**
   Select Users, Computers, or Groups displays.
5. In **Enter the object names to select** box, add the relevant users and then select **Check Names**.
6. Click **OK** and assign the relevant permissions.
7. Click **Apply** and then click **OK**.
8. Select **Security** tab, and then select **Add...**
9. In **Enter the object names to select**, add the relevant users and then select **Check Names**. Assign full permission to appropriate users.
Procedure to install EventTracker Manager

If you are using EventTracker for the first time, launch the executable program etwrel74.exe and then 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.


2. Click the OK to proceed with installation.

3. 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.

4. Click **Yes** to continue
   (OR)
   Click **No** to abort the installation process, and then click the **Finish** button.

   If the mandatory components are found to be installed, InstallShield[R] Wizard displays the EventTracker dialog box.

NOTE:
If another user who does not have SQL sysadmin privilege has logged in to the system and tries to install EventTracker, then an error message is displayed.
5. Click **Yes** to continue, had you created Local / Active Directory user group and added users to that group prior to this installation attempt. InstallShield[R] Wizard displays the **Welcome** screen.

(OR)

Click **No** to abort the installation process, and then click the **Finish** button.

**NOTE:**
If the required components are not installed or found to be missing, InstallShield[R] Wizard displays the EventTracker Prerequisites dialog box with appropriate message.
Click the **Cancel** button, and then click the **Finish** button.

InstallShield[R] Wizard safely exits the installation process.

After installing the mandatory components, start installing EventTracker Enterprise afresh.

**(OR)**

Keep the installation wizard open, install the prerequisites, and then click the **Refresh** button.

Click the **OK** button to continue with the installation process.

6. **Click Next>**.

   InstallShield[R] Wizard displays the **License Agreement** screen.
7. Read the license agreement, and then click 'I accept the terms in the license agreement' option to accept the terms and condition.

8. Select the Next > button. 
   InstallShield[R] Wizard prompts to provide the path of the certificate file.
9. Click the **Browse** button. InstallShield[R] Wizard displays the **Select File** window.

10. Go to the appropriate folder, and then select the file.

11. Click **Open**. InstallShield[R] Wizard updates the folder path.
12. Click **Next >**. InstallShield[R] Wizard displays the **Select Components** screen.
<table>
<thead>
<tr>
<th>EventTracker Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EventTracker Console</strong></td>
<td>Select this option to install manager console on the target computer.</td>
</tr>
<tr>
<td><strong>Change Audit</strong></td>
<td>Optional component.</td>
</tr>
<tr>
<td></td>
<td>Installing this component enables you to monitor and manage change over the enterprise.</td>
</tr>
<tr>
<td></td>
<td>Agent component will also be installed along with the Manager Console.</td>
</tr>
<tr>
<td></td>
<td>You can also deploy agent to the monitored computers using System Manager after installing the Manager Console.</td>
</tr>
<tr>
<td><strong>Trap Tracker</strong></td>
<td>Optional component.</td>
</tr>
<tr>
<td></td>
<td>Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.</td>
</tr>
<tr>
<td><strong>Status Tracker</strong></td>
<td>Optional component.</td>
</tr>
<tr>
<td></td>
<td>Installing this component enable you to monitor and manage TCP/IP networks, Web sites, applications, and ports in mission critical environment.</td>
</tr>
<tr>
<td>Click</td>
<td>To</td>
</tr>
<tr>
<td>-------</td>
<td>----</td>
</tr>
<tr>
<td><strong>Change...</strong></td>
<td>Select different destination folder to install EventTracker.</td>
</tr>
</tbody>
</table>

**View Select Component conventions**

- The icon next to the feature name indicates the install state of the feature. Click the icon to drop down the install state menu for each feature.

- This install state means the feature...
  - ✅ - Will be completely installed to the local hard drive.
  - ✅ - Will have some subfeatures installed to the local hard drive. (Available only if the feature has subfeatures.)
  - ✗ - Will not be installed.
  - ✖️ - Will be useful for some build to some build upgrade. (Available only if the feature supports this option.)

- InstallShield

---

EventTracker: Install Guide

---

EventTracker


53
13. Click **Next >**
   InstallShield[R] 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.

Figure 60
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[R] Wizard displays Site or group name screen.
b) Type an appropriate group/site name for the **Collection Point**, and then click **Next >**.

**NOTE:**
Some special characters are not allowed while providing site/group name. InstallShield[R] Wizard will display a pop-up window if site or group name is provided with such special characters.
Collection Master:

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

14. Select a console type, and then click **Next >**.

If you have selected **Change Audit** component, then InstallShield[R] Wizard displays **Change Audit SnapShot** dialog box.
15. Click the **Next >** button to keep the default store location.
(OR)
Click the **Change** button to change the snapshot store location.
16. 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 uninstallation, 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.
17. Select the **Install Remedial Action EXEs on this machine** option. Remedial Action EXEs are copied to `<InstallDir>\EventTracker\Agent\Script` folder.

18. Click the **Install** button. InstallShield[R] Wizard installs the selected components.
InstallShield [R] 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.

![Basic configuration dialog box](image)

19. Select appropriate options, and then click OK.

InstallShield [R] Wizard displays the Alert and Report generation settings dialog box.
20. Select/enter appropriate data in the relevant fields, and then click **Add**.

   (OR)

   Click **Skip** if you do not wish to add the basic settings.

   InstallShield[R] Wizard displays the last screen.
21. Click **Import existing event log entries** option to import event logs of EventTracker. Windows Security Alert message will be displayed if Firewall is on.

![Windows Security Alert](image)

Figure 73

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

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

23. 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.
24. Click **Finish** to conclude the installation process.
   InstallShield[R] Wizard displays the **EventTracker Configuration** screen.

![EventTracker Configuration Screen](image.png)

**Figure 74**

**NOTE:**
Make sure that you select/enter the correct **User Credentials, User Authentication and EventTracker Group** in order to login successfully.

25. 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 ‘Event Tracker Administrator’ role and can login to EventTracker.

26. Select a **User Authentication** option.

   **Local Account:** Authentication is done locally on the computer where EventTracker is being installed. For more information see: Creating Local User and Group Accounts

   **Active Directory:** Authentication is done in the Active Directory.
   For more information please refer “Create Active Directory User and Group Accounts”.

27. Type the EventTracker group name in the **EventTracker Group** field.
28. Click **OK**.
   After successfully validating the user credentials, InstallShield[R] Wizard displays the
EventTracker Configuration message box.

![EventTracker Configuration Message Box](image)

Figure 75

29. Click OK.

**NOTE:**
If you change the system logon password, EventTracker logon password has to be updated. In order to synchronize the password, please update the same in **EventTracker Configuration**.

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.
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>Access this computer from network</td>
</tr>
<tr>
<td></td>
<td>User has permission on ‘Application install directory’ (Folders and sub folders).</td>
</tr>
</tbody>
</table>
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

Installation procedure is identical for Windows XP/Vista/7/2003/2008/2008R2/2012/8 systems.

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 76](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'.

5. Right-click the system group on the right-pane in which the target systems exist. EventTracker displays the shortcut menu.

6. From the shortcut menu, click the **Install agent/Start poll** option. EventTracker displays the **Install agent/Start poll** dialog box.
There are various options to Select systems and agent type. They are

- All Systems in 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>

7. Click Next.

8. To install EventTracker /Change Audit Agent on all the system present in the domain, select the checkbox against EventTracker/Change Audit (OR)
Select the respective check box against the systems where you wish to deploy the EventTracker/Change Audit agent.

(OR)

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.

9. Click **Next**.

10. Select **EventTracker Agent Type**.

   ![Figure 82](image-url)
11. 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]

   **Figure 83**

   **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.

**Figure 84**

12. 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.

13. Check the **Create “Program Menu” shortcuts** option to create shortcuts.

14. Enter valid **Account** name and **Password**.

15. Reenter the password in **Confirm Password**.

16. 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.

![Message from webpage](image)

17. Click OK.

EventTracker displays Installation Status screen.
### EventTracker: Install Guide

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

18. Click Refresh 🔄 to see the current status (OR) reopen the **Installation Status** dialog box to see the updated status.

19. Click **Close**.

20. 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. Click the Admin drop-down list at the upper-right corner.
2. Click the Windows Agent Config.

(OR)

1. Open EventTracker Control Panel.
2. Double-click EventTracker Agent Configuration.
EventTracker Agent Configuration window displays.
3. Click appropriate tabs and configure the agent as you wish.
Deploy EventTracker Windows Agent – Vista and Above

Prerequisites for Windows Agent – Vista and Above

Following are the mandatory settings you ought to do on Vista 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 Vista and above Agent

Install and uninstall procedure for Vista 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.

![Windows Installer](image)

Figure 92

3. Select the **Yes** button.

EventTracker window displays.

4. Select **Yes/No** as per the requirement.

![EventTracker](image)

Figure 93

**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.

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

1. Select the **Start** button, select **All Programs**, and then select **Prism Microsystems**.
2. Select **EventTracker**, and then select **Uninstall EventTracker**.

![Windows Installer window appears displays.](image1)

Figure 97

Windows Installer window appears displays.

![Windows Installer window](image2)

Figure 98

3. Select the **Yes** button.
EventTracker window displays.
4. Select the OK button. Uninstall EventTracker Enterprise window displays.

![Uninstall EventTracker Enterprise](image)

Figure 100

**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.