EventTracker Enterprise v7.3

Installation Guide
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

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.
# Table of Contents

**Introduction** ................................................................................................................................................. 3

**System Requirements** .......................................................................................................................... 4

- Hardware Requirements [Min. Configuration]....................................................................................... 4
- Software Requirements.......................................................................................................................... 4
  - EventTracker Manager........................................................................................................................ 4
  - EventTracker Manager........................................................................................................................ 5

**Pre-installation Instructions** ..................................................................................................................... 6

- Creating Local User and Group Accounts............................................................................................ 6
  - Creating EventTracker User Group................................................................................................... 7
  - Creating User ..................................................................................................................................... 10
  - Adding User to EventTracker Group ............................................................................................... 12
- Creating Active Directory User and Group Accounts ................................................................................. 17
  - Creating EventTracker Group ....................................................................................................... 18
  - Creating User ..................................................................................................................................... 22
  - Adding User to EventTracker Group ............................................................................................... 25
  - Adding User to Local Administrators group .................................................................................. 29
- Adding cross-domain users .................................................................................................................. 30
- Adding cross-forest users .................................................................................................................... 31

**EventTracker Manager Installation Procedure** ........................................................................................ 32

- Pre-installation Checklist .................................................................................................................... 32
- Installation Process .............................................................................................................................. 33

**Deploying EventTracker Windows Agent** .................................................................................................. 51

- Pre-installation Instructions .................................................................................................................. 51
- Pre-installation Checklist ..................................................................................................................... 51
- Installation Methods.................................................................................................................................. 52
- Deploying EventTracker Windows Agent Using System Manager ......................................................... 52
- Configuring EventTracker Windows Agent ........................................................................................... 61
- Deploying EventTracker Windows Agent – Vista ..................................................................................... 64
  - Prerequisites....................................................................................................................................... 64
  - Installing / Uninstalling Vista Agent ................................................................................................. 64
Introduction

EventTracker Enterprise provides a unique combination of capabilities, including:

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

This is the good time to familiarize you with the various product features as described on the Web site (http://www.eventtracker.com/products/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 thoroughly read ‘Installing & Customizing Web Server (IIS)” document prior to installing EventTracker 7.3.
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:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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, 7.0, 7.5, 8.0
Web Browsers:
- Internet Explorer 7.0 and above
- Firefox Browser 3.5 and above

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

### 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>
<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>
</tbody>
</table>

**EventTracker Agent for Solaris:** Solaris 9, Solaris10

### Components:
- Microsoft .NET Framework 2.0 and above.

**Note:** Versions other than those specified above are not supported
Pre-installation Instructions

- 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.

Creating 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 ‘Domain Admins’ 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. ETAdmin**.
  ✔ Add ETAdmin user to EventTracker group. Members of this group can log on to EventTracker Enterprise.
  ✔ Add ETAdmin 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 ETAdmin.
Creating EventTracker User Group

1. Click **Start** -> **Settings** -> **Control Panel** -> **Administrative Tools** -> **Computer Management** -> **Local Users and Groups**.
2. Expand the **Local Users and Groups** node

3. Right – click **Groups**, and then select **New Group**
4. Type the name of the group in the **Group name** field.

![Figure 4](image)

5. Click **Create**

6. Click **Close**
Creating User

1. Right-click **Users**, and then select **New User**.

![Computer Management](image)

**Figure 6**

2. Type appropriate user credentials. For example, you can type ‘ETAdmin” as user name.

3. Provide a strong password and confirm the same.
4. Select the **Password never expires** check box.

![New User dialog box](image)

Figure 7

5. Click **Create**

6. Click **Close**

![Computer Management](image)

Figure 8
Adding User to EventTracker Group

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

![Computer Management](image-url)
EventTracker displays EventTracker Properties pop-up window.

![EventTracker Properties](image)

**Figure 10**

2. Click **Add**

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

**Figure 11**
3. Click **Locations**

![Locations](image12.png)

**Figure 12**

4. Select the location, typically the name of the computer.

![Locations](image13.png)

**Figure 13**

5. Click **OK**
6. Type the user name in the **Enter the object names to select** field

7. Click **Check Names**
8. Click **OK**

![EventTracker Properties dialog box](image)

Figure 17

9. Click **Apply** and then Click **OK**
Creating Active Directory User and Group Accounts

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

Summary:

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

b. Create a domain user e.g. ETAdmin**.

Add ETAdmin user to EventTracker group. Members of this group can log on to EventTracker Enterprise.

c. Add ETAdmin 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 ETAdmin.
Creating EventTracker Group


Create a **Global Scope Security Group** in the domain where EventTracker Enterprise is to be installed.
2. Right-click the domain name, point to **New**, and then select **Group**.

![Figure 20](image1)

![Figure 21](image2)
3. Type the name of the group in the **Group name** field.

4. Select **Group scope** as **Global**, if not selected.

5. Select **Group type** as **Security**, if not selected.

![New Object - Group](image)

Figure 22

6. Click **OK**
Figure 23
Creating User

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

![Figure 24](image-url)

![Figure 25](image-url)
2. Type appropriately in the respective fields. For example, you can type ‘ETAdmin’ as user name.

![Image of User Object Creation]

3. Click **Next >**.

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

5. Select the **Password Never Expires** check box.
6. Click **Next >**

7. Click **Finish**
Adding User to EventTracker Group

1. Right-click the EventTracker group, and then select Properties.
Figure 31
2. Click the **Members** tab.

![Figure 32](image)

3. Click **Add**.

![Figure 33](image)
4. Type the user name in the **Enter the object names to select** field.

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

**Figure 34**

5. Click **Check Names**.

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

**Figure 35**

6. Click **OK**.
7. Click **Apply**.
8. Click **OK**.

**Adding User to Local Administrators group**

Add user to the ‘Administrators’ group on the computer where EventTracker Enterprise is to be installed.
Adding 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.
Adding cross-forest users

Consider Domain A and Domain B exist in Forest 1 and Domain C and Domain D exists 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.
EventTracker Manager Installation Procedure

Prism recommends you read “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. Use the CD to execute etwrel73.exe.
2. Launch the downloaded self-extracting, 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.


Pre-installation Checklist

The pre-installation 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>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>User has ‘Logon As Batch job’ rights</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>Network Discovery is enabled</td>
<td>System cryptography: Use FIPS 140 compliant cryptographic algorithms, with encryption, hashing and signing algorithms disabled.</td>
</tr>
<tr>
<td>User is assigned the role of sysadmin in SQL server.</td>
<td></td>
</tr>
</tbody>
</table>
Installation Process

1. Uninstall fully if any previous version of EventTracker exists on the computer.
2. Insert the CD in the CD-ROM, and the installation wizard should start automatically. If it does not, click Start -> Run, and type G:\etwrel73.exe (assuming your CDROM is drive G).

   Setup prepares the InstallShield[R] Wizard for installation.
3. EventTracker checks for all the prerequisites.

![EventTracker Prerequisites](image)

   Figure 40: EventTracker Prerequisites

4. Click the OK to proceed with installation.

   In case of multiple SQL instances, select the appropriate instance name from Instance name dropdown, and then click the OK button.

![Select SQL Instance](image)

   Figure 41: Select SQL Instance
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.

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

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

6. 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.
Click **No** to abort the installation process, and then click the **Finish** button.

**PLEASE NOTE:**

If the required components are not installed or found to be missing, InstallShield® Wizard displays the EventTracker Prerequisites dialog box with appropriate message.

Click the **Cancel** button, and then click the **Finish** button.
InstallShield® 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.

7. Click Next>.

InstallShield® Wizard displays the License Agreement screen.

8. Read the license agreement, and then click 'I accept the terms in the license agreement' option to accept the terms and condition.

9. Click Next >.

InstallShield® Wizard prompts to provide the path of the certificate file.
10. Click the **Browse** button.

   InstallShield[R] Wizard displays the **Select File** window.

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

12. Click **Open**.

   InstallShield[R] Wizard updates the folder path.

13. Click **Next >**.
InstallShield® Wizard displays the **Select Components** screen.

![Select Components](image)

**Figure 49: Select Components**

<table>
<thead>
<tr>
<th>EventTracker Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Console</td>
<td>Select this option to install manager console on the target computer.</td>
</tr>
<tr>
<td>Change Audit</td>
<td>Optional component. Installing this component enables you to monitor and manage change over the enterprise. Agent component will also be installed along with the Manager Console. You can also deploy agent to the monitored computers using Client 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.

View Select Component conventions

<table>
<thead>
<tr>
<th>EventTracker 7.3</th>
<th>EventTracker 7.3</th>
</tr>
</thead>
</table>
| **Select Components Tips** | Custom Setup allows you to selectively install program features.

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.

The install state means the feature...

- ** prosperous ** Will be completely installed to the local hard drive.
- ** prosperous ** Will have some subfeatures installed to the local hard drive. (Available only if the feature has subfeatures.)
- ** prosperous ** Will not be installed.
- ** prosperous ** Will be useful for same build to same build upgrade. (Available only if the feature supports this option.)

InstallShield | OK | Cancel
14. 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 (See Figure 50).
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. (See Figure 51).

Select the console type as Collection Point, and then click Next >. InstallShield[R] Wizard displays Site or group name screen. (See Figure 52).
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.

![Figure 53](image)

**Collection Master:**

Used in hierarchical network topologies where collection points replicate their event log archives to a Collection Master. (See Figure 54)

![Figure 54: Collection Master Console](image)

15. Select a console type, and then click **Next >**.
16. If you have selected **Change Audit** component, then InstallShield[R] Wizard displays **Change Audit SnapShot** dialog box.
Click the Next > button to keep the default store location.
(OR)
Click the Change button to change the snapshot store location.

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 installation, if the change audit snapshots are retained during product uninstallation, then the snapshot store location path cannot be changed. (See Figure 57).

17. If you have not selected to install Change Audit then InstallShield[R] Wizard displays the Ready to Install the Program screen.
18. Select the **Install Remedial Action EXEs on this machine** option, and then click **Install**.

Remedial Action EXEs are copied to `<InstallDir>\EventTracker\Agent\Script` folder.

19. Click **Install**.

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](image)

**Figure 60: Basic Configuration**

20. Select appropriate options, and then click **OK**.

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

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

22. InstallShield[R] Wizard displays the last screen.

    Figure 61: Alert and Report generation settings

    Figure 62
Click **Import existing event log entries** option to import event logs into EventTracker. **Windows Security Alert** message will be displayed if **Firewall** is on.

![Figure 63: Windows Security Alert](image)

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.

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

![EventTracker Configuration Screen](image)

24. 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 ‘Administrator’ role to manage users.

25. 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 see: Creating Active Directory User and Group Accounts.

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

27. Click **OK**.

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

![EventTracker Configuration Message Box](image)

28. Click **OK**.
NOTE

Whenever you change the EventTracker logon password, please update the same in EventTracker Configuration. You can find 'EventTracker configuration' in

Start > Programs > Prism Microsystems > EventTracker > EventTracker Configuration
Deploying EventTracker Windows Agent

Pre-installation Instructions

- You MUST have Local Admin privileges on the remote systems where you want to remotely install the Agents.
- You can also install Agents with Domain 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-installation Checklist

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>
Installation Methods

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.

Deploying EventTracker Windows Agent Using System Manager


1. Click Start -> Programs -> Prism Microsystems -> EventTracker -> EventTracker Enterprise.
   EventTracker displays the login page.

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

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

Figure 66
This console displays the list of systems that are members of all trusted domains. 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'.

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

From the shortcut menu, click the Install agent/Start poll option. EventTracker displays the Install agent/Start poll dialog box.
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, and then click the dropdown. EventTracker displays the drop-down list.

Click **Install agent/ Start poll**.

![Figure 70](image)

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

![Figure 71](image)
Check the **EventTracker** option to install EventTracker agent. Check the **Change Audit** option to install Change Audit agent.

5. Click **Next**.
6. Select **EventTracker Agent Type**.

![Figure 72](image)

**Agent based (Full featured)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Install default Remedial Action EXEs on this system</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Deploy SCAP</strong></td>
<td>Provides an option to install SCAP components to remote machines while deploying agent(s).</td>
</tr>
<tr>
<td><strong>Deploy WinSCP</strong></td>
<td>Provides an option to install WinSCP components to remote machines while deploying agent(s).</td>
</tr>
</tbody>
</table>

**Agentless (limited feature)**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Poll Every</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
7. If agent type is selected as 'Agent based (Full Featured)', then remedial actions EXEs can be installed on the system.

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

EventTracker displays a message box.

![Message from webpage]

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

[OK] [Cancel]

**Figure 73: Caution**

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

8. Click **OK** to install remedial action EXEs (OR) **Cancel** to not to install remedial action EXEs.
9. Click **Next**.

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

![Install Agent/Start poll]

**Figure 74**

10. 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.

11. Check the **Create "Program Menu" shortcuts** option to create shortcuts.
12. Enter valid **Account** name and **Password**.

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

14. Click **Install**.

   The agent will be installed on the selected machine with the default `etaconfig.ini` configuration.

   (OR)

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

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

(OR)

- Select the **Custom config** option to select a custom configuration file.

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.
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]

**Message from webpage**

Instal in progress. Check the Installation status screen for updates.

15. Click OK

EventTracker displays **Installation Status** screen.
16. Click refresh to see the current status (OR) reopen the Installation Status dialog box to see the updated status.

17. Click Close

18. Refresh the System manager
Configuring 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 Control Panel

EventVault  Diagnostics  License Manager  Export Import Utility  Append Archives

EventTracker Agent Configuration  Traffic Analyzer  Agent Management  SCAP Profile Editor  TrapTracker

Change Audit  About EventTracker

E-mail: support@prismmicrosys.com

Figure 80
Click appropriate tabs and configure the agent as you wish.
Deploying EventTracker Windows Agent – Vista

Prerequisites

Following are the mandatory settings you ought to do on Vista systems before you deploy Vista 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 Vista agent remotely, on Vista system 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 the Vista system where the agent has to be deployed.

Installing / Uninstalling Vista Agent

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