EventTracker Enterprise v8.1

Install 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 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.

Target Audience

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

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

Known Issues for v8.1 ................................................................................................. 5

System Requirements ................................................................................................. 13
  - Hardware Requirements [Min. Configuration] ......................................................... 13
  - Software Requirements ......................................................................................... 13

Pre-install instructions for Local Account and Active Directory authentication .......... 15
  - Create Local User and Group Accounts ................................................................. 15
    - Create EventTracker User Group ...................................................................... 17
    - Create User ........................................................................................................ 19
  - Create Active Directory User and Group Accounts .............................................. 26
    - Create EventTracker Group ............................................................................. 27
    - Create User ........................................................................................................ 29
      - Add User to EventTracker Group ................................................................. 32
  - Add cross-domain users ......................................................................................... 36
  - Add cross-forest users ........................................................................................... 38

Install EventTracker Manager ..................................................................................... 39
  - Pre-install Checklist for EventTracker Manager .................................................. 39
    - IIS Settings ......................................................................................................... 40
    - User Permission on SQL Server ....................................................................... 42

Procedure to install EventTracker Manager - Custom .............................................. 54

Procedure to install EventTracker Manager - Standard / Collection Point Evaluation Version ................................................................. 107

Deploy EventTracker Windows Agent ........................................................................ 121
  - Pre-install Instructions for Windows Agent ......................................................... 121
  - Pre-install Checklist for Windows Agent ............................................................. 121
  - Different methods to install EventTracker Agents ............................................... 122

Deploy EventTracker Windows Agent via System Manager for Agent Based (full featured) ................................................................. 122

Configure EventTracker Windows Agent ................................................................... 133

Configuring Agent-less collection via System Manager (limited features) ............... 137
  - Adding Systems for Agent-less monitoring ....................................................... 138
  - To add systems for Agent-less monitoring ......................................................... 138
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 8.1.
Known Issues for v8.1

The below mentioned issues are related to v8.1 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:

       http://download.microsoft.com/download/1/6/3/163BBBDE-5523-416D-A293-EA0492020E4A/iisexpress_8_1_RTM_x86_en-US.msi

   c. Install IIS Express 8.1.
   d. To run EventTracker Configuration, click Start, click Programs, and then click Prism Microsystems.
   e. Select EventTracker, and then select EventTracker Configuration.
   f. 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 privilege 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.

(OR)

What should I do if the message ‘A reboot is still pending’ occurs?
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.

Q5. Setup gives weird errors about not being able to access a folder/file.

(OR)
Please make sure that you give a gap of ten seconds between launching the setup. It takes some time for the Operating system to clean up the temporary files/folders created during installation.

Q6. If I get an error message ‘You need to format the disk in the drive before you use it. Do you want to format it? ’, what should I do?
If the setup ends up using an unformatted drive for archive folder, either format the drive for use, or please use a drive that is formatted and is ready for use.

Q7. If IIS Express fails to start, then what should I do?
1. To launch Services Manager, click the Start button.

2. In Search Programs and Files box, type Services.msc and then press Enter. Services Window displays.

3. Start the service 'IISExpress' manually.

Q8. If IIS Express failed to install, then what should I do?

Please run the EventTracker Configuration again.

1. To run EventTracker Configuration, click Start, click Programs, and then click Prism Microsystems.

2. Select EventTracker, and then select EventTracker Configuration.

3. Enter valid User Credentials, and then select the OK button.

Q9. How can I use MS SQL Server Enterprise Edition for EventTracker?
MS SQL Server Enterprise Edition can be used for **Custom** option only. The user can use either SQL Express or Enterprise Edition for Custom installation.

SQL Express Edition will be used for Standard and Collection Point Install/Setup Type. The user will be forced to install SQL Express for Standard and Collection Point even if SQL Enterprise Edition is already present on the machine.

Q10. What shall I do if the Collection Master/Collection Point console service is stopped after installation?

Make sure that the certificate contains collection point feature.
(The install wizard will allow the user to proceed even if the license doesn’t contain the Collection Point feature).

Q11. What should I do if I get the following error message “PkgMgr.exe has been deprecated.”
If you are using **IIS Express** click **OK** and proceed with the installation.

This error message appears if ASP.NET is not installed with IIS. If IIS is already installed, the DISM will enable ASP.NET.

Please make sure that if IIS is installed, then ASP.NET is also installed in the machine. For detail instructions, please refer [How To Install and Customize Web Server (IIS)](#).
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, 32-bit (x86) Xeon ® Dual Core or equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>HDD</td>
<td>80 GB Free Hard disk space for the application</td>
</tr>
</tbody>
</table>

Table 1

64-bit Installation:

<table>
<thead>
<tr>
<th>CPU</th>
<th>2.80 GHz, 64-bit (x64) Xeon ® Dual Core or equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>4 GB</td>
</tr>
<tr>
<td>HDD</td>
<td>80 GB Free Hard disk space for the application</td>
</tr>
</tbody>
</table>

Table 2

NOTE: The recommended RAM is 8 GB.

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 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 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8.1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</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/upgrade 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 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 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 7</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows XP</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 8, 8.1</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Vista</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Windows 10</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 manually, please refer Create Local User and Group Accounts or Create Active Directory User and Group Accounts as per the requirement.

- 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.
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 13](image)

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

5. Select **Create**, and then select **Close**.
EventTracker group is created.

Create User

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

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.

![New User dialog box](image18.png)

**Figure 18**

**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**.

![Computer Management](image19.png)

**Figure 19**
ETKaren user is created.

Add User to EventTracker Group

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

![Figure 20](image)

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

3. Select the **Locations** button. Locations window displays.
4. Select the location, typically the name of the computer. In this example, name of the computer is SPIDER-II.

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.

Figure 29
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**.

![Figure 30](image)

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'.

![Figure 31](image)

New Object – Group displays.
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.

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’.

3. Select the Next > button.

4. Type the password in the Password and Confirm Password fields.
5. Select the **Password Never Expires** check box.

![Figure 38](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.

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

![Figure 39](image)

7. Select the **Finish** button.

Username 'Karen Smith' is created.
Add User to EventTracker Group

1. Right-click the **EventTracker Test** group, and then select **Properties**.
2. Select the **Members** tab.

3. Select the **Add** button.
4. Type the user name in the **Enter the object names to select** field.

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

'Karen Smith' is a member of 'EventTracker Test' group.

7. Select **Apply**, and then select the **OK** button.

Add User to Local Administrators group

To add a user in 'Administrators' group on the computer where EventTracker Enterprise is installed please 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.

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

Figure 49
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.

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

![Diagram](image_url)
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.

<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>

Table 5
IIS Settings

Please ensure that IIS Settings under Application Pools are as follows in Windows 2008/2008 R2/2012/2012 R2.

![Advanced Settings](image)

**Figure 51 – 64 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$SQLEXPRESS**’ to ‘**Network Service**’.

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

For this,

- Go to **services.msc**.
- Double click on the **SQL server** and click on **properties**.

To stop the SQL Server,

**Step 1:** In the **Startup type** option, select **Disabled** and click **OK**.

![Image of SQL Server Properties](image-url)
Step 2: Now, double click the SQL server and click on the Log On tab. If it is MSSQL Server, then change it to Network Services.

![Figure 54](image)

Step 3: For this, click the browse button, enter “Network Services” in the Enter the object name to select field and click OK, as shown in the figure below:

![Figure 55](image)
**Step 4:** Enter the user credentials and click **OK**.

![Figure 56](image)

Refer the above steps and then start the SQL Server.

**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 / 2012 R2 / 2014)** 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.
F) 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 60**.

**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**.

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.
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 60.

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 data base 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 64](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 - 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:


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:

![Image of error message]

Figure 67
EventTracker Pre-Install Check window displays.

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

Figure 68

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 74](image)

**Figure 74**

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

![Figure 75](image)

**Figure 75**

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

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:
6. Select Appropriate Instance to proceed with the installation process.

7. If MSSQL Server – Express Edition 2005/2008/2008 R2/2012 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 >.
The pre-installer prompts to download SQL Server Express Edition.
Figure 80

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)

9. Select the browse button 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** 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 84](image)

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, click **Configuration Guide** link for detail instructions to install IIS.

If IIS Express is already installed, on clicking **Next >**, **Disk Usage** page displays.

If IIS Express is not installed, please refer Figure 87 and 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.
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.

If Active Directory is selected earlier, You have selected Active Directory domain: page displays.

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

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’.

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 95.

**NOTE:**

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

![Figure 101](image)

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.

![Figure 105](image)

- Click the **Yes** button.

18. In **Summary** page, verify all the data entered, and then click the **Install** button.
19. Click the **Yes** button.
   EventTracker – Install Shield Wizard displays.
EventTracker 8.1 Enterprise Install Guide

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

---

**Figure 108**

**Figure 109**
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.

![Select SQL Instance](image)

**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.

![EventTracker 8.1](image)
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.

![Select Certificate File Window](Figure 112)

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.
26. Click Next >.

Select Components screen displays.

![Select Components Screen](image)

**Figure 115**

<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 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>
</tbody>
</table>
### Status Tracker

Optional component. Installing this component enables you to monitor and manage TCP/IP networks, Web sites, applications, and ports in mission critical environments.

**Click**

Select different destination folder to install EventTracker.

<table>
<thead>
<tr>
<th>Look in:</th>
<th>Change...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prism Microsystems</td>
<td>EventTracker</td>
</tr>
</tbody>
</table>

Folder name: `C:\Program Files (x86)\Prism Microsystems\`
View **Select Component** conventions.

Check the disk space available in the target computer.
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.

![Figure 116](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.

c) Enter **Collection Master**: name or IP Address, and then select the **Next >** button.
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.
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. Select the Install Remedial Action EXEs on this machine option.

Remedial Action EXEs are copied to `<InstallDir>\EventTracker\Agent\Script` folder.
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 Wizard displays the **Basic configuration** dialog box.

![Basic configuration dialog box](image)

EventTracker includes several important features. You can customize EventTracker by enabling/disabling the above list of available features.

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

InstallShield Wizard displays the **Alert and Report generation settings** dialog box.
33. 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 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.

![Windows Security Alert](image)

*Figure 130*
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.

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

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

![EventTracker Configuration Screen](image)

**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.

35. 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.

36. 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.

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

38. Click **OK**.

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

![EventTracker Configuration](image)

39. 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.
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.

1. Double-click the executable file.

2. Click the **Yes** button.

   EventTracker Pre-Install Check window displays.
3. Click the **Next >** button.

Hardware Summary pane displays.
4. Select **Standard/Collection Point** option, and then select the **Next >** button.
Prerequisites page displays.
If prerequisites are not installed, please refer Figure 71 and Figure 73 onwards—Installing Windows Installer and Powershell to install all the prerequisites mentioned.

5. Click the **Next >** button.

If all the prerequisites are installed, then Database page displays.
If MS SQL Server Express is not installed, please refer Figure 75 – Figure 78 for detail instructions.

6. Click the **Next >** button.

IIS Web Server page displays.
If IIS Express is installed, then Define User page displays if EventTrackerAdmin user is not created otherwise Summary page displays.

If IIS Express is not installed, please refer Figure 81–83 for detail instructions.

7. Enter EventTrackerAdmin credentials, and then click the Next > button.

**NOTE:**

It will be displayed only if there are two instances of SQL running or some pre-requisites are missing.
The Summary page displays.

Figure 140

Figure 141
NOTE: If you still wish to change the path of EventTracker Archive Drive, EventTracker Program Drive, click the **Browse** button and proceed to do required changes.

8. Click the **Install** button.

Welcome page displays.

![Welcome page](image)

**Figure 142**

9. Click the **Next >** button.

License Agreement page displays.

10. Select I **accept the terms in the license agreement** option, and then select the **Next >** button.
If **Standard** option is selected earlier, then Install Default Remedial action displays. Please refer Figure-142.

If **Collection Point** option is selected earlier, then Configure Collection Point site page displays.

11. Enter the **Collection Point** name and then click the **Next >** button.
Configure Collection Master page displays.

12. Enter **Collection Master**: name or IP address, and then click the **Next >** button.
Ready to install the program page displays.

13. Select **Install default Remedial Action EXEs on this machine** option, and then select the **Install** button.
A successful message displays.
14. Select respective options, and then select the Finish button.

EventTracker: Configuration window displays.

15. Enter valid user credentials and then select the OK button.
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 149](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 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><strong>All systems in the selected group</strong></td>
<td>Click this option to install agents on all the systems present in the selected group.</td>
</tr>
<tr>
<td><strong>Take systems from the text file</strong></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><strong>Agent type</strong></td>
<td>Select the agent type to be Installed</td>
</tr>
<tr>
<td><strong>Specific systems in the selected group</strong></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

7. Click **Next**.

8. 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.

(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**.

![Figure 153](image)

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 i.e. Agent based (Full Featured) / Agent-less (limited feature) option.
Table 8

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]

   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 156

   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.

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

**Figure 157**

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.
17. Click **OK**.

EventTracker displays **Installation Status** screen.

<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 Date application was installed / on which System it is installed / Type of activity performed / Status of the application.</td>
</tr>
</tbody>
</table>
18. Click **Refresh** to view 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.
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**.

![Figure 165](image)

EventTracker displays the **Install Agent/Start poll** dialog box.
Figure 166

- 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.
Agent less (limited feature)

Select this option to add the system with limited EventTracker Agent features.

In the Agent-less type, the following features are not available:

- Log file Monitoring
- System Monitoring
- Network Connection Monitoring
- Software Install / Uninstall
- Guaranteed Event Delivery
- Process Monitoring
- Application Monitoring
- Service Monitoring

Poll Every

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

**NOTE:** The poll frequency is applicable for windows 2003 and below and not for Vistas and above.


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 168**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling frequency</td>
<td><strong>Poll Every</strong> Select the time frequency for which you want to get the events</td>
</tr>
<tr>
<td>Domain Admin account</td>
<td>Type valid user name and password in Account, Password and Confirm Password fields respectively.</td>
</tr>
<tr>
<td>Selected Systems</td>
<td>This field displays the selected system list.</td>
</tr>
</tbody>
</table>

f) Click **Install**.

The agent 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.

g) 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)

*Install in progress. Check the Installation status screen for updates.*

**Figure 170**

h) Click **OK**.

EventTracker displays **Installation Status** screen.

![Installation Status](image)

**Figure 171**

<table>
<thead>
<tr>
<th>Application</th>
<th>Group/System</th>
<th>By</th>
<th>Agent</th>
<th>Type</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EDWIN090211VM3</td>
<td>commands</td>
<td>EventTracker</td>
<td>Start poll</td>
<td>Success</td>
<td>Installed successfully</td>
</tr>
<tr>
<td></td>
<td>EDWIN090211VM3</td>
<td>commands</td>
<td>EventTracker</td>
<td>Start poll</td>
<td>Success</td>
<td>Search was successful.</td>
</tr>
<tr>
<td></td>
<td>EDWIN090211VM3</td>
<td>commands</td>
<td>N/A</td>
<td>Search computers</td>
<td>Success</td>
<td>Search was successful.</td>
</tr>
<tr>
<td></td>
<td>EDWIN090211VM3</td>
<td>commands</td>
<td>N/A</td>
<td>Search computers</td>
<td>Success</td>
<td>Search was successful.</td>
</tr>
</tbody>
</table>

**Select**

<table>
<thead>
<tr>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort the <strong>Installation Status</strong> results by the application installed. Available options are EventTracker &amp; Change Audit.</td>
</tr>
</tbody>
</table>
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:
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.
Figure 173
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.

   ![Image](image1.png)

   **Figure 174**

3. Select the **Yes** button.

   EventTracker window displays.

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

   ![Image](image2.png)

   **Figure 175**

**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.

![Uninstall EventTracker Windows Agent via System Manager](image)

Figure 176

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.

3. Select the **Yes** button.

EventTracker window displays.
4. Select the **Ok** button.

Uninstall EventTracker Enterprise window displays.

![Uninstall EventTracker Enterprise](image)

**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.
Frequently Asked Questions

1. How to change webserver port used by EventTracker?

   If the EventTracker installation is using IISXRPESS 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.

   ![EventTrackerWeb Properties](Figure 183)
f. Modify **URL**: as shown below.

![EventTracker Web Properties](image)

**Figure 184**

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 185](image)

![Figure 186](image)

![Figure 186](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 187]

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

![Figure 188]

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