Abstract

The purpose of this document is to help the existing users of EventTracker to upgrade to a newer version and to verify the expected functionality and performance of all its components.

Audience

It is incumbent upon all users of EventTracker v9.0/v9.1 who wish to upgrade to EventTracker v9.2.
The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion makes no warranties, express or implied, as to the information in this document.

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

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

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

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

1. Introduction .......................................................................................................................... 4  
   1.1 Preparing for upgrading .................................................................................................. 4  
      1.1.1 Software Requirements ......................................................................................... 4  
      1.1.2 Before you upgrade ............................................................................................... 5  
   1.2 Prerequisites .................................................................................................................... 6  
   1.3 Planning .......................................................................................................................... 6  

2. Upgrade - Quick View .......................................................................................................... 7  
   2.1 Common steps for all upgrades ...................................................................................... 7  
      2.1.1 Before you start with the upgrade process ............................................................ 7  
      2.1.2 After the upgrade process .................................................................................... 8  
   2.2 Upgrading to EventTracker v9.2 .................................................................................... 8  

3. Upgrading - Detailed View ................................................................................................ 11  
   3.1 Upgrade from v9.0/v9.1 to v9.2 ................................................................................ 11  
   3.2 Configure Service Accounts .......................................................................................... 38  

4. Source Type Mapping .......................................................................................................... 42
1. Introduction

This guide describes how to upgrade EventTracker. It is strongly recommended that you read the entire document thoroughly before you begin the upgrade process. EventTracker v9.2 upgrade will only support Operating systems Windows Server 2012 R2, Windows 10, Windows Server 2016, and Windows Server 2019.

For the user’s convenience, this guide is separated into two parts: ‘Upgrade- Quick View’ and ‘Upgrade-Detailed View’.

**Upgrade - Quick View** is written for the system administrators and the experts who are familiar with EventTracker and upgrade process. It is presumed that the user of this section has enough knowledge of the system and configuration process.

**Upgrade - Detailed View** is meant for EventTracker users who will upgrade EventTracker for the first time. In this section, the upgrade process is explained with the help of GUI (Graphical User Interface).

**NOTE:**

- It is recommended not to install/upgrade EventTracker in a Domain Controller.
- It is recommended to run the EventTracker Manager Console on a Dedicated Windows Server.

1.1 Preparing for upgrading

1.1.1 Software Requirements

**EventTracker Manager**

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

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

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

**Microsoft Windows 7 Embedded and Microsoft Windows 10 IOT Enterprise**

**Components:**

- Microsoft .NET Framework 3.5 and above.

**NOTE:** Versions other than those specified above are not supported.

**1.1.2 Before you upgrade**

1. Thoroughly read the ‘EventTracker Architecture’ guide. This guide explains the architecture and sample deployment methods with illustrations.
   
   **Managing Billions of Logs Everyday.**

2. Contact support@eventtracker.com for information regarding license keys or license certificates.

3. If you have installed an earlier version of EventTracker using IIS Express, before upgrading please change it to IIS to proceed with the installation.

IMPORTANT:

• Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceType Mapping.exe)

Kindly refer the Source Type Mapping section to install the same.

• After the upgrade, in a Collection Master, the user might notice the inconsistency in Reports/ Log Search/Cab received status (Admin>Collection Master>Archives status), till the database migration is in process.

• After the upgrade, in a Collection Point, the user may not be able to view the exact cab transfer status in (Admin>Collection Point Configuration-> manage archives) till the database migration is in process.

RECOMMENDED

• Any user(s) on EventTracker version below v9.0 needs to upgrade to v9.0/v9.1 first and then upgrade to v9.2.

• Any user(s) on EventTracker version v9.0/v9.1 can upgrade to v9.2

1.2 Prerequisites

Before you begin with the upgrade process, please follow this checklist and make sure that you have all the components in place to perform a successful upgrade.

• Make sure Windows updates with all the latest service packs are installed.

The most effective upgrade method is to first export all the custom settings using Export Import Utility, install the new version, and then import the custom settings. There is no need to export all policy settings since all the categories included in any prior versions have been retained.

The recommended method is to first upgrade the Manager, validate all its functionality, next upgrade the Agents, and lastly verify the performance.

1.3 Planning

This section gives you a rough estimation of the time required for the upgrade as well as monitoring the successful upgrade. It may take 60 – 90 minutes for you to read this document and to complete the upgrade process gracefully. You will also require spending a few minutes the following day after the upgrade, to
verify all your ‘Scheduled Reports’ are being generated. If any reports fail to generate, then please read the Validation section at the end of this document.

2. Upgrade - Quick View

In this section, you can get a quick insight into the upgrade process

- Common steps for all upgrades
- Upgrade from v9.0/v9.1 to v9.2

2.1 Common steps for all upgrades

2.1.1 Before you start with the upgrade process

- Verify that all the prerequisites have been satisfied.

- Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg. Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceTypeMapping.exe)

  Kindly refer the Source Type Mapping section to install the same

- While uninstalling v9.0/v9.1, the user has to enable the option to retain all the configuration and data.

- For v9.0/v9.1, you can take a backup of the database from EventTracker Control Panel -> Diagnostics which is explained in detail in Upgrade from v9.0/v9.1 to v9.2

- If you have incorporated your company logo into EventTracker, then take a backup of the .jpg file of your company logo before uninstalling the EventTracker. You need to replace the backed up image file after installing EventTracker.

- For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).

NOTE: While upgrading from EventTracker v9.0/v9.1 to v9.2, if the environment consists of support SQL server (SQL 2016 or SQL 2017) then the user needs to configure the SQL services to the network services manually

  o To change the configuration from SQL services to the network, open the run command and type in services.msc and then click ok.
In the services page, right click the SQL Server service and click properties, in the properties window click the Log on tab, select This account option and click the Browse button. Select the entire directory option and click okay.

- The logged-in user who is upgrading to EventTracker v9.2 should have SQL sysadmin privilege. If the user does not have enough permission, then an error message is displayed.

![Figure 1]

- Backup all Custom Categories, Alerts (Please check the ‘Export E-mail Settings’ check box), Filters and Reports using Export Import Utility.

- Please note down the custom changes you have made in the ‘Trusted List’ (Agent Configuration -> Network Connection Monitor -> Suspicious Traffic Only (SNAM) -> Trusted List).

2.1.2 After the upgrade process

- If SSL (HTTPS) is configured in the earlier version, then the configuration will not be retained after the upgrade to v9.2. Please make sure to reconfigure it again as mentioned in Securing IIS Web Server with SSL.

- If the user has configured the JSON file in DLA Manager in the older version, after upgrading, the user will have to reconfigure the same.

2.2 Upgrading to EventTracker v9.2

1. Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceTypeMapping.exe)

   Kindly refer the Source Type Mapping section to install the same

2. Uninstall the existing version by retaining old configuration and data.
3. Restart the EventTracker manager server or system.

4. Install EventTracker v9.2. Click on Yes to proceed with upgrade.

5. **Configure the service accounts**, if the archives/reports are stored in the network path.

6. Update the Trusted List with the changes you have noted down earlier.

7. Upgrade all windows agents using ‘System Manager’.

8. **Preferred:** Import the latest knowledge objects (KO) after the upgrade. The newly optimized knowledge objects contain improvements in RegEx matching and source type mapping. Refer to the User Guide for more information on knowledge objects.

Below knowledge objects are optimized to get better performance in elastic indexing.

- Barracuda NG Firewall
- Checkpoint Firewall
- Cisco ASA Firewall
- Cisco Meraki Firewall
- EventTracker
- Fortigate Firewall
- Poliwall Firewall
- Sonicwall Firewall
- Sophos UTM Firewall
- Sophos XG Firewall
- Untangle Firewall
- Watchguard XTM Firewall
- Windows

**Note:**

- Please import EventTracker and Windows KOs on top of existing KO.
- Please delete any other KOs and import the new KOs as per the need.
- If new KOs are not imported, only standard properties will be indexed.
9. **Optional**: To utilize newly added/modified categories/alerts import the complete alerts/complete categories files from the configuration directory (Install directory). Prior to importing user has to manually delete existing categories and alerts from the application. Then import all categories and all alerts from configuration files.

**Compliance Dashboard**

- The Dashlets are preserved after the upgrade and the user can customize the dashlets by selecting the customize icon.

![Figure 3](image1.png)

**My Dashboard**

- The dashlets created under **My Dashboard** are also preserved after the upgrade process and the user can further customize it by selecting the customize icon.

![Figure 4](image2.png)
3. Upgrading - Detailed View

In this section, you will learn the upgrade process in detail.

- Upgrade from v9.0/v9.1 to v9.2

3.1 Upgrade from v9.0/v9.1 to v9.2

1. Please refer to the Common steps for all upgrades for more details.

2. Before upgrading, please take a backup of the database and details are given below.
   b. Click the Backup Configuration button.
      Backup & Restore window displays.
      
      ![Backup & Restore window]

      Figure 5

   c. Browse and select the folder you wish to back up.
   d. Click the Backup now button.
      After the backup has been taken, go to the folder for which the backup has been taken. A file with the extension .bkp will be used to restore later.

Step 1: Close/terminate all the EventTracker Components

Before you start the upgrade process, please ensure to install EventTracker Update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1) and run Source Type Mapping Utility available in install path (Eg.Installpath\PrismMicrosystems\EventTracker\AdvancedReports\EventTracker.Update.SourceTypeMapping.exe)
Before you start with the upgrade, it is very crucial to close/terminate all the EventTracker components present in the system, like EventTracker, EventTracker Control Panel, and even RDP (Remote Desktop Protocol) session.

During uninstall, if any of the previous EventTracker components is open then EventTracker asks you to close the program.

Close the open component, and then click the Retry button. EventTracker resumes the uninstall process.

**Step 2: Uninstall v9.0/v9.1**

1. Select the Start button, select Settings, and then select Control Panel.
2. Select Add or Remove Programs, select EventTracker, and then select the Remove button.

(OR)
Select the Start button, select Programs, and then select Prism Microsystems. Select EventTracker, and then select Uninstall EventTracker. EventTracker will display the confirmation message.

3. If you have installed EventTracker agents on different systems then a message box will appear to confirm the uninstall process.

4. Click the Yes button to continue the installation process. EventTracker starts the uninstall process, and displays ‘Uninstall EventTracker’ dialog box.
Uninstall EventTracker™ dialog box for EventTracker v9.0

![Uninstall EventTracker Enterprise dialog box](image)

Please select the files which you wish to retain and click “Ok.”

- **Configuration**: Retains all the related configuration files
- **Configuration, Reports and Data**: Retains Archives, Elasticsearch Data, published reports and all the related configuration files
- **Keep Snapshots**: Snapshots collected in Change Audit

![Figure 8](image)

Uninstall EventTracker™ dialog box for EventTracker v9.1

![Uninstall EventTracker dialog box](image)

Please select the files which you wish to retain and click “Clean.”

- **Configuration**: Retains all the related configuration files
- **Reports and Data**: Retains Archives, Elasticsearch Data and published reports
- **Keep Snapshots**: Snapshots collected in Change Audit

![Figure 9](image)
By default, all the file options are selected. Keep the default selection to retain the data and configurations.

5. Click the Ok button.

Step 3: Restart the EventTracker Manager Server or System

1. Close all the open applications on the desktop.
2. Click the Start button and then click Shut Down dropdown.
3. Select the Restart option, and then click the OK button.

Step 4: Install EventTracker v9.2

Kindly follow the steps mentioned below for the upgrade process.

1. Double-click the executable file.

NOTE: .NET 4.8. is enabled by default for Microsoft Windows 2012 R2/2016/10/2019. If it is not available, EventTracker pre-install check will install .NET 4.8.

![Figure 10](image)

**IMPORTANT:** In Internet Explorer->Browser Settings->Security->Custom Level-> In the downloads->File Download-> Please make sure “enable” option is selected.
2. Once the .net framework 4.8 is installed a message pop’s up, click ok and reboot manually.

3. After the reboot relaunch the EventTracker setup.

EventTracker Pre-Install Check window displays.
4. Click the **Next >** button. License page displays.

5. 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.
6. Click the **Next >** button.
Prerequisite page displays.

![Prerequisite page](image)

**Figure 16**

**NOTE:**

- If the prerequisites are not installed, then a message **`Not-Installed`** displays against the respective prerequisite.

- If the Elasticsearch (7.2.1) is not installed the following message pop’s up.

![Elasticsearch not installed](image)

**Figure 17**
“During upgrade to v9.2, EventTracker old Elasticsearch index data will be deleted”.

7. Click **OK** to proceed.
8. Click Next and the summary page displays. In Summary page, verify all the data entered, and then click the Install button.

9. Click the Install button to proceed with the installation.

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

10. Click Next >.
   Select a Certificate File page displays.
• To locate the path of the certificate file, click the Browse button. Select File window displays.

• Go to the appropriate folder, select the file and then click Open. The folder path is updated.
11. Click Next >. Select Components screen displays.
### EventTracker 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 the manager console on target the computer.</td>
</tr>
<tr>
<td>Change Audit</td>
<td>Optional component. Installing this component enables you to monitor and manage change over the enterprise. The agent component will also be installed along with the Manager Console. You can also deploy the agent to the monitored computers using System Manager after installing the Manager Console.</td>
</tr>
<tr>
<td>Trap Tracker</td>
<td>Optional component. Installing this component enables you to monitor and manage traps sent by SNMP compliant devices.</td>
</tr>
</tbody>
</table>
12. Click **Next >**.

InstallShield Wizard displays the **Select EventTracker Console Type** screen. And displays previously selected option in version 9.0 or 9.1 by default.

13. Select the Next > button.

   The **Ready to Install the Program screen** displays the summary of the installation path, console type, and the selected features.
14. Click the **Install** button.
   InstallShield Wizard installs the selected components.
   InstallShield Wizard displays the last screen.
15. Click **Finish** to conclude the installation process.

InstallShield Wizard displays the **EventTracker Configuration** screen.
• Type valid user credentials in the **User Name** and **Password** fields respectively and then click the **OK** button.
  After successfully validating the user credentials, InstallShield[R] Wizard displays the **EventTracker Configuration** message box.

![EventTracker Configuration](image)

Figure 30

16. Click the **OK** button.

**Step 5: Configure the service accounts, if the archives/reports are stored in the network path.**

Click ‟**Configure the service accounts**’ section.

**Step 6: Verify that the Categories, Alerts, Filters, are intact**

**Step 7: Upgrade all Windows agents using the System manager**

EventTracker agent upgrade is necessary to keep the agents up to date with the manager system.

1. Logon to **EventTracker**.
2. Select the **Admin** menu and select **Systems**.

   EventTracker displays **System** manager page.

3. Click the desired domain/group name and then select the **Upgrade agent**.
EventTracker displays **Upgrade Remote Agent(s)** dialog box.

Figure 31

Figure 32
<table>
<thead>
<tr>
<th>Option</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>All systems in the selected group</td>
<td>Click this option to upgrade all the agents in the selected group.</td>
</tr>
<tr>
<td>Take systems from the text file</td>
<td>Create a text file containing agent system names for which the upgrade has to be done. The text file should contain one system name per line. If you select this option, then browse the text file to select the agent system names.</td>
</tr>
<tr>
<td>Agent type</td>
<td>Select the agent to upgrade.</td>
</tr>
<tr>
<td>Specific systems in the selected group</td>
<td>Out of all the agent systems present in the group, select a specific agent system(s) to upgrade.</td>
</tr>
</tbody>
</table>

(OR)

Select the icon corresponding to the remote system’s name (where the agent is to be upgraded), and then click Upgrade Agent from the dropdown list.

Figure 33
EventTracker displays **Upgrade Remote agent(s)** pop-up window.

### Figure 34

4. Check the agent type option which you wish to upgrade, and then click the **Next** button.

### Figure 35
5. Select the **Windows Domain Network** option, and fill in the user credentials.

(OR)

If the remote agent is in some other non-trusted domain or the remote system is not accessible using Windows file sharing, then select the **Upgrade over IP (Non-Windows Domain)** option.
6. Check **Install default Remedial Action EXEs on this system** option to install remedial action scripts.

   EventTracker displays a message box.

   ![Message from webpage](image)

   **Figure 38**

   **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.

7. Click **OK** to install remedial action EXEs

   (OR)

   Click **Cancel** to not to install remedial action EXEs.

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

8. Click the **Advanced** button to set a more specific configuration while agent upgrade.
The **Default** option is selected by default to apply the 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.

9. Click the **Upgrade** button.

EventTracker displays an information message.
10. Click the **OK** button.

EventTracker displays **System Status** screen.

11. Click the **↻** button, to see the latest status.
NOTE: It may take some time to load the status.

Step 8:
As the menu options have been changed, the User Privileges configuration won’t be retained after the upgrade to v9.2 for non-admin users. You have to reconfigure it again.

- a) To configure the privileges, go to Admin hyperlink, select Users. EventTracker displays the User Management window.
  b) Select the user(s) and click the Assign Privileges icon.

EventTracker displays the Add Privileges window.

- c) Select the required field and click OK.
Step 9: Import Knowledge Objects after the upgrade

Import the latest knowledge objects (KO) after the upgrade. The newly optimized knowledge objects contain improvements in RegEx matching and source type mapping. Refer to the User Guide for more information on knowledge objects.

Below knowledge objects are optimized to get better performance in elastic indexing.

- Barracuda NG Firewall
- Checkpoint Firewall
- Cisco ASA Firewall
- Cisco Meraki Firewall
- EventTracker
- Fortigate Firewall
- Poliwall Firewall
- Sonicwall Firewall
- Sophos UTM Firewall
- Sophos XG Firewall
- Untangle Firewall
- Watchguard XTM Firewall
- Windows
Note:

- Please import EventTracker and Windows KOs on top of existing KO.
- Please delete any other KOs and import the new KOs as per the need.
- If new KOs are not imported, only standard properties will be indexed.

1. Logon to EventTracker.
2. To import Knowledge Objects, select the Admin menu, and then select Knowledge Objects.
3. Select the Import icon.
   EventTracker Knowledge Objects Import/Export window displays.
4. Select the Browse… button and then select the file from the desired location.

   NOTE: The file extension should be ‘.etko’ only. The knowledge objects are segmented into folders. Based on the devices the user(s) is having, they can import them which is available in ...
   InstallDIR\EventTracker\Knowledge Packs

5. Select the Open button.
6. Select the Upload button.
7. To upload knowledge objects, select the Object name option.
8. Click on **Import**.

NOTE:

- After upgrading from v9.0/v9.1 to v9.2, the user will first have to import the new Token templates (with the extension `.ettd`) from the install `DIR\Program Files\Prism MicroSystems\EventTracker\Configuration Files` and then import the newly available Defined Reports (with the extension `.issch`) from the same path.

- While importing the newly added defined reports from the **EventTracker Control Panel**, the user has to select the Old Type option with extension `.issch`.

### 3.2 Configure Service Accounts

If the user is setting UNC path (Uniform Naming Convention) for storing Archives/Reports, then service account of EventTracker Scheduler, EventTracker EventVault, EventTracker Reporter, EventTracker Indexer, and Event Correlator (if available) services should be made to run on the user account which will have full permission on the set UNC path.

1. Open the “**EventTracker Configuration**” from the **Start** button, and “**Run as administrator**”.

---

**Figure 46**

[Import dialog box with selected object]
2. Configure the same with a user who has full permissions to access the shared archives folder.

**"Karen"** has full permissions to access the archives UNC path.

**NOTE:** Please ignore the above steps, if it is already configured with the required user.

1. Select the **Start** button, and then select **Run**.
2. Type **services.msc** and click the **OK** button.
3. In the **Services** window, search for EventTracker services.

![Services Window](image)

**Figure 50**

4. Right-click the service name and click **Properties**.
   - For example, Right click **EventTracker EventVault** service.
   - ‘EventTracker EventVault Properties (Local Computer)’ dialog box will appear on the screen.
5. Click the Log On tab and select This account option.

6. Enter the user credentials and correct password. The user name should be in the ‘domain name\user name’ format.

7. Click the Apply button. A warning message will be displayed on the desktop.
8. Click the OK button.
9. To run the service with the new logon name, stop and start the service.
10. Likewise, for the rest of the services, repeat step 4 to step 10 to change the service account. The Log On As column will display the changed service account name.

![Figure 53](image)

4. Source Type Mapping

1. After applying the update ET90U19-074 (on v9.0) and ET91U19-050 (on v9.1), user has to navigate to the following install path “Prism Microsystems\EventTracker\AdvancedReports”.

2. Right click on the “EventTracker.Update.SourceTypeMapping.exe” file and choose “Run as Administrator”.

3. The Source Type Mapping window appears, click on the “Scan indexed data for syslog sources” button
4. The following message appears and click ok.
   This message confirms that the source type temp database is created successfully

![Source type mapping](image)

Figure 56

5. Open EventTracker Database.
6. Find and edit the `dbo.TempSourceTypeMapping` table and confirm if all the data is available.

If you encounter any problems during the upgrade process, please contact the support team to get quick and thorough instructions.

**Technical Support Contact Details:**
Toll-Free: 877-333-1433 ext. 2
Phone: +1-410-953-6776 ext. 2
Fax: +1-410-953-6780
Email: support@eventtracker.com