Introduction

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

If you encounter any problems during upgrade process, please contact 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

Audience:

It is incumbent upon all users of EventTracker v6.4 to v7.4 who wish to upgrade to v7.5 Enterprise. Prism strongly recommends that you read the entire document thoroughly before you begin the upgrade process. For the user’s convenience, this document is separated in two parts: 'Upgrade- Quick View' and 'Upgrade- Detailed View'.

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

Upgrade - Detailed View is meant for EventTracker users who upgrade EventTracker for the first time. In this section, upgrade process is explained with the help of GUI.

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.

*IMPORTANT:

Users of versions ‘v6.4 (Build 50)’ and below contact support@eventtracker.com for complete and thorough instructions.
The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems 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 Prism Microsystems, 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.

© 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

New Categories/Alerts available in v7.5 ........................................................................................................................................ 4
Prerequisites .................................................................................................................................................................................. 6
Planning ........................................................................................................................................................................................ 6
Upgrade - Quick View ..................................................................................................................................................................... 7
  Upgrade from v6.4 (Build 50) to v7.5.x ...................................................................................................................................... 8
  Common steps for all upgrades .................................................................................................................................................. 9
    Upgrade from v7.0.x to v7.5.x ........................................................................................................................................... 12
    Upgrade from v7.1.x to v7.5.x ........................................................................................................................................... 13
    Upgrade from v7.2.x to v7.5.x ........................................................................................................................................... 13
    Upgrade from v7.3.x to v7.5.x ........................................................................................................................................... 13
    Upgrade from v7.4.x to v7.5.x ........................................................................................................................................... 13
    Upgrade from v7.5.x to v7.5.x ........................................................................................................................................... 13
Upgrade - Detailed View .................................................................................................................................................................. 14
  Upgrade from v6.4 (Build 50) to v7.5.x .................................................................................................................................. 15
    Upgrade Procedure ............................................................................................................................................................. 23
  Upgrade from v6.4.58 to v7.5.53 ........................................................................................................................................... 45
  Upgrade from v7.0.x to v7.5.x ........................................................................................................................................... 74
  Upgrade from v7.1.x to v7.5.x ........................................................................................................................................... 74
  Upgrade from v7.2.x to v7.5.x ........................................................................................................................................... 74
  Upgrade from v7.3.x to v7.5.x ........................................................................................................................................... 75
  Upgrade from v7.4.x to v7.5.x ........................................................................................................................................... 75
  Upgrade from v7.5.x to v7.5.x ........................................................................................................................................... 89
Configure Service Accounts ......................................................................................................................................................... 90
New Categories/Alerts available in v7.5

The details about new categories/alerts available in EventTracker v7.5 is mentioned below.

**New Categories/Alerts**

- EventTracker: Published reports deleted
- EventTracker: Behavior data reset performed
- Task Scheduler: Task failed to start
- Task Scheduler: Task finished
- Task Scheduler: Task started
- EventTracker: Logbook Email sent.
- Updated category: EventTracker: RSS feed added
- Added new category: EventTracker: Logbook config changes
- Removed category: EventTracker: Change audit access history launched.
- Added new pre-defined behavior rule for ‘Logon Activity’.
- Modified category: EventTracker: Collection master deleted.
- EventTracker: Change audit integrity violation status changed
- EventTracker: Change audit access history launched
- EventTracker: Change audit changed objects authorized
- EventTracker: Behavior rule deleted
- EventTracker: Collection point deleted
- EventTracker: Collection Point cab files deleted
- EventTracker: Collection master port setting changed
- EventTracker: Config assessment policy results deleted
- EventTracker: List entity added
- EventTracker: List entity deleted
- EventTracker: List entity updated
- EventTracker: Correlation rule added
- EventTracker: Correlation rule inactivated
- EventTracker: Correlation rule modified
- EventTracker: EventVault cabs deleted
- EventTracker: EventVault explorer configuration modified
- EventTracker: EventVault flex history database purged
- EventTracker: Incident acknowledged
- EventTracker: Incident unacknowledged
- EventTracker: IP reputation lookup configuration added
• EventTracker: IP reputation lookup configuration deleted
• EventTracker: IP reputation lookup configuration activated-Inactivated
• EventTracker: IP reputation lookup settings modified
• EventTracker: Log book entry added
• EventTracker: Log book entry modified
• EventTracker: Logbook activity Inserted
• EventTracker: Logbook activity modified
• EventTracker: Logbook investigation complete
• EventTracker: Logbook reference deleted
• EventTracker: Logbook reference inserted
• EventTracker: Logbook referenced attachment deleted
• EventTracker: Logbook entry reopened
• EventTracker: Change audit policy schedule added
• EventTracker: Change audit policy schedule modified
• EventTracker: Change audit policy schedule deleted
• EventTracker: RSS feed added
• EventTracker: RSS feed deleted
• EventTracker: RSS feed Modified
• EventTracker: Report sent via Email

New Active Directory Reports

• AD-DisabledUserAccounts
• AD-DomainComputers
• AD-EnabledUserAccounts
• AD-ExpiredUserAccounts
• AD-InactiveUserAccounts
• AD-RecentlyLoggedInUsers
• AD-UserAccountdetails
• AD-UserAccountPasswordNeverExpires
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.

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.

Planning

This section gives you a rough estimation of time required for upgrade as well as monitoring the successful upgrade. It might 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.
Upgrade - Quick View

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

- Upgrade from v6.4 (Build 50) to v7.5.x Enterprise
- Common steps for all upgrades
- Upgrade from v7.0.x to v7.5.x Enterprise
- Upgrade from v7.1.x to v7.5.x Enterprise
- Upgrade from v7.2.x to v7.5.x Enterprise
- Upgrade from v7.3.x to v7.5.x Enterprise
- Upgrade from v7.4.x to v7.5.x Enterprise
- Upgrade from v7.5.x to v7.5.x Enterprise
Upgrade from v6.4 (Build 50) to v7.5.x

NOTE:

For upgrade from v6.4.58 to v7.5.53, please refer [Upgrade from v6.4.58 to v7.5.53](#) for detail instructions.

Before you start with the upgrade process

1. Verify that all the prerequisites have been satisfied.
2. Backup all custom Categories, Alerts (Please check the ‘Export E-mail Settings’ check box), Filters, Scheduled Reports and RSS Feeds using Export Import Utility.
3. Close/terminate all the EventTracker components like Management console and Reports console, including RDP (Remote Desktop Protocol) sessions.
4. Please note down the custom changes you have made in the ‘Trusted List’ (Agent Configuration -> Network Connection Monitor -> Suspicious Traffic Only (SNAM) -> Trusted List).

Upgrade Procedure

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v7.5.x Enterprise.
4. [Configure the service accounts](#), if the archives/reports are stored in the network path.
5. Using Export Import Utility, import all the custom Categories, Alerts, Filters, Scheduled Reports and RSS Feeds.
6. Verify that the Categories, Alerts, Filters, Legacy Reports and RSS Feeds are intact.
7. Upgrade all agents using the System Manager.
8. Update the Trusted List with the changes you have noted down earlier.

Post Upgrade Process

By default, EventTracker sets the threat level of alerts imported from v6.4 as ‘Undefined’. You need to set the ‘Threat level’ explicitly as per your requirement. To set the Threat Level,
1. Open **EventTracker Enterprise**.

2. Click the **Admin** menu, and then select **Alerts**.
   
   EventTracker displays Alert Management page.

3. Click the alert name to be modified.
   
   EventTracker displays Alert Configuration page.

4. Select the threat level from **Threat Level** dropdown.

5. Click the **Finish** button.
   
   EventTracker saves the configuration settings.

**NOTE:**

- Upgrade process for v6.4 to v7.5 remains the same.

- After upgrading from v6.4 to v7.5, kindly run the executable file ‘**Prism.AlertsMigration.exe**’ available in ‘**\InstallDIR\EventTracker\Prism.AlertsMigration.exe**’ for migrating the incidents.

- For v6.4 to v7.5 upgrade, if ‘Keyword Indexing’ is installed and enabled, then launch the Keyword Indexing migration utility.

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

- For agent upgrade details, please click [here](#).

**Common steps for all upgrades**

**Before you start with the upgrade process**

- Verify that all the **prerequisites** have been satisfied.

- Take a back up of the database. For v7.0 – v7.2, please refer [Back up and Restore Guide](#). For v7.3 onwards you can take a back up of the database from **EventTracker Control Panel** -> **Diagnostics** which is explained in detail in [Upgrade from v7.4.x to v7.5.x](#).
- If you have incorporated your company logo into EventTracker, then take a backup of .jpg file of your company logo before uninstalling the EventTracker. You need to replace the backed up image file after installing EventTracker Enterprise.

- Close/terminate all the EventTracker components like EventTracker Enterprise, EventTracker Control panel, including RDP (Remote Desktop Protocol) sessions.

- If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v7.5. Please make sure to reconfigure it again as mentioned in Securing IIS Web Server with SSL.

- The logged in user who is upgrading to EventTracker v7.5 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

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

- As the menu options have been changed, the User Privileges configuration won't be retained after upgrade to v7.5 for non-admin users. You have to reconfigure it again.

- The dashboard options have been updated and the user has to reconfigure after upgrading to v7.5.

Upgrade from v7.0.x/v7.1.x/v7.2.x/v7.3.x/v7.4.x to v7.5.x

1. Uninstall the existing version by retaining old configuration and data.

2. Restart the EventTracker manager server or system.

3. Install EventTracker v7.5.

4. Configure the service accounts, if the archives/reports are stored in the network path.
5. Verify that the Categories, Alerts, Filters, Scheduled reports and RSS Feeds are intact.

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

NOTE:

- From EventTracker v7.5 onwards, the Behavior Dashlets have been renamed. So after upgrading from v7.x to v7.5, you have to reset the personalization and then configure the dashlets (except for upgrade from v7.5 to v7.5). Please follow the steps given below.

1. Logon on to EventTracker Enterprise.

2. Select the Behavior menu, select Security/Operations drop down.

3. Select Reset Personalization.

4. A message displays.

5. To customize the required dashlets, select Security/Operations drop down, and then select Customize.
Available Dashlets window displays.

6. Select and **Add** the required dashlets.

- After upgrading, if the collection master is v7.5 and above versions, and if collection point is using any older version of EventTracker, then incidents will not be visible. If you upgrade collection point to v7.5, post upgrade incidents will only be transferred to collection master.

**Upgrade from v7.0.x to v7.5.x**

The procedure to upgrade from v7.0.x to v7.5.x is same like [upgrade from v7.4.x to v7.5.x](#).

After upgrading from v7.0 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in “\InstallDIR\EventTracker\Prism.AlertsMigration.exe” for migrating the incidents.
Upgrade from v7.1.x to v7.5.x

The procedure to upgrade from v7.1.x to v7.5.x is same like upgrade from v7.4.x to v7.5.x.

After upgrading from v7.1 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in "\InstallDIR\EventTracker\Prism.AlertsMigration.exe" for migrating the incidents.

Upgrade from v7.2.x to v7.5.x

The procedure to upgrade from v7.2.x to v7.5.x is same like upgrade from v7.4.x to v7.5.x.

After upgrading from v7.2 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in "\InstallDIR\EventTracker\Prism.AlertsMigration.exe" for migrating the incidents.

Upgrade from v7.3.x to v7.5.x

The procedure to upgrade from v7.3.x to v7.5.x is same like upgrade from v7.4.x to v7.5.x.

Upgrade from v7.4.x to v7.5.x

The procedure to upgrade from v7.4.x to v7.5.x is mentioned in the detail section.

Upgrade from v7.5.x to v7.5.x

The procedure to upgrade from v7.5.x to v7.5.x is same like upgrade from v7.4.x to v7.5.x.
Upgrade - Detailed View

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

- Upgrade from v6.4 (Build 50) to v7.5.x Enterprise
- Upgrade from v6.4.58 to v7.5.53 Enterprise
- Upgrade from v7.0.x to v7.5.x Enterprise
- Upgrade from v7.1.x to v7.5.x Enterprise
- Upgrade from v7.2.x to v7.5.x Enterprise
- Upgrade from v7.3.x to v7.5.x Enterprise
- Upgrade from v7.4.x to v7.5.x Enterprise
- Upgrade from v7.5.x to v7.5.x Enterprise
Upgrade from v6.4 (Build 50) to v7.5.x

Before you start with the upgrade process, create Backup of the Configuration Data and Reports.

In order to retain the configuration data and report of existing version, you need to create backup for all custom Categories, Alerts, Filters, Scheduled reports, and RSS Feeds.

This section will help you in creating backup files.

1. Open the EventTracker Management Console.

2. Click the Tools menu, and click Import and Export Utility.

EventTracker displays Export-Import Utility window.

3. Select the Category option, if not selected by default.

4. From the Categories field, select the EventTracker categories to be exported, and click the Add button. (Example: My Category).
Click **Add All** button to select all the categories.

5. Click the **Export** button.

EventTracker displays **Select Export File** window.

The file extension should be `.iscat`
6. Click **Save** in dropdown to select the file location, enter the **File name**, and click the **Save** button.

EventTracker displays confirmation message box.

![Export Import Utility](image)

**Figure 9**

7. Click the **OK** button.

8. Select **Filters** option, and then click the **Export** button.

![Export Import Utility](image)

**Figure 10**

EventTracker displays **Select Export File** window.

9. Select the file location, enter file name, and click the **Save** button.

EventTracker displays confirmation message box.

10. Click **Alerts** option, and then click **Export E-mail Settings** checkbox.

11. From the **Alerts** field, select the alerts to be exported, and click the **Add** button.
Example: My Alerts

12. Click the **Export** button.

   EventTracker displays **Select Export File** window.

13. Click **Save in** dropdown to select the file location, enter the file name, and click the **Save** button.

   EventTracker displays confirmation message box.

14. Click the **OK** button.

15. Click the **Scheduled Reports**, click the **Export without System names** box, and then click the **Export** button.
EventTracker displays **Select Export File** window.

16. Click **Save in** dropdown to select the file location, enter the file name, and click the **Save** button.

Example: My Reports

EventTracker displays confirmation message box.

17. Click the **OK** button.

If there are no scheduled reports present in the database then EventTracker will display the information message.

18. Click the **RSS Feeds** option, and click the **Export** button.
EventTracker displays **Select Export File** window.

19. Click **Save in** dropdown to select the file location, enter the file name, and click the **Save** button. (Example: RSS Feed)

   EventTracker displays confirmation message box.

20. Click the **OK** button.

   If there are no RSS feeds present in the database then EventTracker displays an information message.

21. Click the **Close** button, to close the **Export Import Utility** window.
Note down the list of Trusted Connections

Note down the custom changes you have made in the ‘Trusted List’. This option will help you to get the ‘Trusted list’ details.

1. Click the Start button, select All Programs, and then select Prism Microsystems.

2. Select EventTracker, and then select EventTracker Control Panel.

EventTracker displays EventTracker Control Panel.

3. Click Agent Configuration icon.
By default, EventTracker displays **Managers** tab.

4. Click **Network Connection Monitor** tab, select **Suspicious Traffic Only (SNAM)** option, and click the **Trusted List** button.

EventTracker displays **Trusted Connections List** pop-up window.

![Trusted Connections List](image)

**Figure 18**

5. Note down the custom changes you have done in the list.

**Close/terminate all the EventTracker Components**

Before you start with upgrade, it is very crucial to close/terminate all the EventTracker components present in the system, like Management Console, Report Console, and even **RDP** (Remote Desktop Protocol) session.

During uninstall, if any of the EventTracker components is open then EventTracker asks you to close the program.
Close the open components, and then click the **Retry** button. EventTracker resumes uninstall process.

**Upgrade Procedure**

**Step 1: Uninstall the version 6.4 b50 by retaining old configuration and data.**

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.

Control Panel displays the confirmation message.

(OR)

Click the **Start button**, select **Programs**, select **Prism Microsystems**.

Select **EventTracker**, and then select **Uninstall EventTracker**.
EventTracker displays the confirmation message.

![Figure 21](image)

3. Click the **Yes** button.

EventTracker starts the uninstall process.

![Figure 22](image)

EventTracker displays, ‘**Uninstall EventTracker**’ confirmation message.

![Figure 23](image)

4. Click the **No** button.
EventTracker displays ‘Uninstall EventTracker’ dialog box.

By default, the checkboxes are selected. Keep the default selection to retain the data, reports, and configurations.

5. Click the OK button.

Step 2: 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.
3. Select the Restart option from the dropdown, and then click the OK button.

Step 3: Install EventTracker v7.5 Enterprise

For the details about Installation process, please refer ‘EventTracker v7.5 Enterprise Installation Guide’.

NOTE:

For v6.4, EventTracker uses MS Access database, and for v7.5 EventTracker uses SQL database. Before upgrade, you need to migrate the database from MS Access to SQL database. For this purpose, a Migration Utility will appear while installing v7.5 (Refer Figure above). This utility migrates EventVault path, Install path, SMTP port, VCP port details etc. to new SQL database.
If you have more than one SQL database instances, then you can select the required instance from the **Server** dropdown, and then click the **Next>>** button to proceed migration.

After a successful migration process, EventTracker displays a **Status: Migration Success** message. Click the **Finish** button go back to the EventTracker installation process.
Step 4: Configure the service accounts, if the archives/reports are stored in the network path.

Click ‘Configure the service accounts’ section.

Step 5: Import all the custom Categories, Alerts, Filters, Scheduled reports and RSS Feeds

After successful EventTracker Enterprise installation, you need to import the custom categories, Alerts, Filters, Scheduled reports and RSS Feeds, which you have exported from EventTracker v6.4.

1. Select the Start button, select Programs, and then select Prism Microsystems. Select EventTracker, and then select EventTracker Control Panel.

   EventTracker displays EventTracker Control Panel.

   ![EventTracker Control Panel](image)

   Figure 27

2. Click Export Import Utility icon.

   EventTracker displays Export Import Utility window.

3. Click Export Import Utility icon.

   EventTracker displays Export Import Utility window.

4. Click Import tab.
5. Click **Category** (If not selected).

6. Click the **browse** button, select the location of the file, and click the **Open** button.

7. Click the **Import** button.

   EventTracker displays **Export Import Utility** success message box.

8. Click the **OK** button.

9. Select **Filters** option.

10. Click the **browse** button, select the location of the file, and click the **Open** button.

11. Click the **Import** button.
EventTracker displays **Export Import Utility** success message box.

![Figure 30](image)

12. Click the **OK** button.

13. Click **Alerts** option.

![Figure 31](image)

14. Select **Import E-mail settings** checkbox, if not selected.

15. In the **Set Active** pane, select the appropriate option.

16. Click the **browse** button, select the location of the file, and click the **Open** button.

17. Click the **Import** button.

EventTracker displays **Export Import Utility** success message box.
18. Click the **OK** button.

19. Select the **RSS Feeds** option.

20. Click the **browse** button, select the location of the file, and click the **Open** button.

21. Click the **Import** button.

EventTracker displays **Export Import Utility** success message box.
22. Click the **OK** button.

23. Select **Scheduled Reports** option.

24. Click the **browse** button, select the location of the file, and click the **Open** button.

25. Click the **Import** button.

EventTracker displays **Export Import Utility** success message box.
26. Click **OK**, and then click the **Close** button.

**Step 6: Verify that the imported Categories, Alerts, Filters, Legacy reports and RSS Feeds are intact.**

**Verify Category:**

1. Log on to **EventTracker Enterprise**.
2. Click the **Admin** hyperlink, and click **Category**.
   
   EventTracker displays ‘Category Management’ Page.
3. Search for the imported custom category under **Category Tree** tab.

   In addition, you can find the custom category on the right side of the page, in **Last 10 modified categories** list.

   Example: My Category.

   ![Figure 37](image)

   (OR)

   Click the **Search** tab, enter the category name in the **Search** field, and then click the **Go** button.
Verify Alerts:

1. Click the Admin menu, and then click Alerts.

   EventTracker displays Alert Management page.

2. Enter the alert name in Search Field, and click the Go button.

   ![Figure 38](image1)
   ![Figure 39](image2)
   ![Figure 40](image3)
In addition, you can make use of scroll bar to find alerts and the page numbers provided at the top and bottom of Alert Management page.

**Verify Filters:**

1. Click the **Admin** menu, and then click **Event Filters**.

   EventTracker displays **Event Filters** page. The newly imported filters are listed in this page.

   ![Figure 41](image)

2. Click the filter name to see the imported filter details.

   EventTracker displays **Event Filter configuration** page.

   ![Figure 42](image)

**Verify Generated Reports:**

Upon upgrade to version 7.x, the successfully generated reports from version 6.4 can be viewed in **'Legacy Reports'** present under the **Tools** menu. Using **'Export Import Utility'** you can import the report configurations (of version 6.4) to continue the report generation process in the
scheduled time. The report configurations can be seen under the respective reports/analysis tab.

1. Click the **Tools** menu, and click **Legacy Reports**.

   EventTracker displays **Legacy Reports** dialog box.

   ![Legacy Reports dialog box](image)
   
   **Figure 43**

2. Expand **Legacy Reports** folder, and click **Scheduled**.

   Here you will get to see the list of successfully generated reports from version 6.4.

   ![Scheduled reports](image)
   
   **Figure 44**

**Verify RSS Feeds:**

1. Click the **Admin** menu, and then click the **RSS**.

   EventTracker displays **RSS Feeds** page. The newly imported RSS feeds are listed in this page.
Step 7: Upgrade all agents using the System Manager.

EventTracker agent upgrade is necessary to keep the agents up to date with the manager system.
1. Log on to EventTracker Enterprise.
2. Select the Admin menu, and then select Systems.
   EventTracker displays ‘System Manager’ page.
3. Right click the desired domain/group name, and then select Upgrade agent.

EventTracker displays Upgrade Remote Agent(s) pop-up window.
(OR)

Move the cursor on the remote systems name (where the agent is installed), click the dropdown arrow, and select **Upgrade Agent**.

EventTracker displays **Upgrade Remote Agent(s)** pop-up window.
4. Choose the agent(s) to be upgraded by selecting checkbox, and click the **Next** button.

5. Select **Windows Domain Network** option, and enter user credentials,
(OR)

Select the **Upgrade over IP (Non-Windows Domain)** option.

![Figure 52](image)

6. Select **Install default Remedial Action EXEs on this system** checkbox.

EventTracker displays confirmation message.

![Figure 53](image)

7. Click **OK**, and then click the **Upgrade** button.

EventTracker displays information message.
8. Click the **OK** button.

   EventTracker displays **System Status** screen.

9. Click the refresh button, to see the latest status.

   **NOTE:** It may take some time to load the status.
Step 8: Update Trusted list

In v6.4, if you have made any changes in ‘Trusted Connection List’ then you need to update the same in v7.1 ‘Trusted connection List’. This option will help you to update the trusted connection list.

1. Log on to EventTracker Enterprise.

2. Select the Admin menu, select Windows Agent Config, and then select Network Connection Monitor tab.

3. Select Suspicious Traffic Only (SNAM) option, and then select the Trusted List button.

EventTracker displays ‘Trusted Connections List’ pop-up window.

4. Click the New button, fill in the appropriate credentials, and then click the Ok button.

The updated details will appear in ‘Trusted Connection List’.
NOTE:

- You can also find the 'Trusted Connection List' details in spmConfig.ini file. The file is saved under:

  ...Program Files\Prism Microsystems\EventTracker\Agent\spmConfig.ini

- If Keyword indexing is installed and enabled, launch the keyword indexing file migration utility. The keyword Indexer folder is restructured. To put the old indexed files into the new structure, KeywordMigration.exe utility file has been provided along with build 7.5.

- This utility migrates the existing keyword files to new structure. The path for utility file is:

  <Install folder>\EventTrackerWeb\bin\KeywordMigration.exe

- In EventTracker Control Panel -> EventTracker Agent Configuration -> Event Filters tab, ‘Information’ and ‘Audit Success’ event types are unchecked by default. Select the ‘Information’ and ‘Audit Success’ checkboxes in order to filter large number of ‘Information’ and ‘Audit Success’ events.

- Agent upgrade: While performing remote agent upgrade, make sure to select the appropriate configuration file containing the port that was previously configured in v6.4.
  
  1. Click the Advanced button.

    EventTracker displays Upgrade Remote Agent(s) dialog box.
II. Select **Custom Config** option.

III. Select the required .ini file from the **File** dropdown.

IV. Click the **Upgrade** button.

Example: In v6.4, if the agent is deployed in a port (Ex. 14575) then during upgrade, select `etaconfig_14575.ini` file from the file dropdown.

- For further configuration changes, please contact support@eventtracker.com.

**Post Upgrade Process:**

By default, EventTracker sets the Threat level of alerts imported from v6.4 as Undefined.

You need to explicitly set the threat level as per your requirement. To set the threat level,
1. Open EventTracker Enterprise.
2. Click the Admin menu, and then select Alerts.
   EventTracker displays Alert Management page.
3. Click the alert name to be modified.
   EventTracker displays Alert Configuration page.
   ![Alert Configuration](image)
   
   **Figure 62: Alert Configuration**
4. Select the threat level from Threat Level dropdown.
5. Click the Finish button.
   EventTracker saves the configuration settings.
Upgrade from v6.4.58 to v7.5.53

Kindly follow the steps mentioned below for upgrade process.

1. Uninstall the existing version of EventTracker, by retaining all configuration, data and Reports.

2. Reboot the machine.

3. To install v7.5.53, launch EventTrackerSetup.exe.

   EventTracker Pre-Install Check displays below message.

   ![EventTracker Pre-Install Check](Figure 63)

4. Click the Yes button.

   Welcome to EventTracker Pre-Install check displays.
5. Click the **Next >** button.

Hardware Summary pane displays.
6. Select the **Next >** button.

   Install Type page displays.

7. Select **Custom** option, and then select the **Next >** button.
Figure 66

Prerequisite page displays.
If prerequisites are not installed, then appropriate message displays. For details please refer EventTracker v7.5 Install Guide for v7.5.53.

8. Click the Next > button.

Database page displays.
9. If MS SQL Server Express Edition is not installed, then click **Next >**.
10. Click **Download**.

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

SQL Express starts downloading and is installed in the background.
Web Server page displays.
12. If IIS Express (Not Installed) option is selected, then click the Next > button.

**NOTE:** IIS Express is not supported in 2003 R2/2003 64 bit machines.

13. Click the Install button.
Disk Usage page displays.
14. Click the **Next >** button.

Installation Summary page displays.
Figure 75

Define User Group page displays.
15. Select **Active Directory** option.

   **NOTE:** In case you wish to configure EventTracker on local machine, then select Local Machine. For detail instructions, please refer [EventTracker v7.5 Install Guide](#) – section ‘Procedure to install EventTracker Manager v7.5.53 Custom’.

16. Click the **Next >** button.

   Define User Group page displays.

17. Select **Select existing User Group** option, and then select the **Next >** button.
18. Click the **Next >** button.

Define User page displays.

19. Click **Select existing User** option, and then select appropriate user.
If user is not EventTracker Administrator then, EventTracker Pre-Install Check displays the below message.

20. Click the Yes button.

Summary page displays.
21. Cross verify all the data entered, and then click the **Install** button.

InstallShield Wizard displays the **Welcome** screen.
22. Click **Next >**.

   InstallShield Wizard displays the **License Agreement** screen.

23. Read the license agreement, click 'I accept the terms in the license agreement' option and then click the **Next >** button.
Select a Certificate File page displays.

24. To locate the path of the certificate file, click the **Browse** button.
InstallShield Wizard displays the Select File window.

25. Locate the file from the appropriate folder, and then select Open.

InstallShield Wizard updates the folder path.

![Figure 84](image)

26. Click Next >.

InstallShield(R) Wizard displays the Select Components screen.

![Figure 85](image)
27. Click the **Next >** button.

Select EventTracker Console Type page displays.

![Select EventTracker Console Type](image)

**Figure 86**

28. Select a console type.

   a. If **Collection Point** Console Type is selected, click **Next >**.

   b. Enter **Collection Point** details, click **Next >**.
c. Enter **Collection Master** details, enable **Skip** option, and then click **Next >**.

(OR)

a. If **Collection Master** option is selected, and then click **Next >**.

If you have selected **Change Audit** component, then InstallShield Wizard displays **Change**
29. Select the **Next >** button.

Ready to install the Program page displays.

30. Select **Install Remedial Action EXEs on this machine** option, and then select the **Install** button.
InstallShield Wizard installs the selected components. Migration Utility displays.

31. Click the **Next >** button.

Figure 91

Migration process completed.

Status: Migration Success

Database migrated successfully

Figure 92
32. Click the **Finish** button.

Basic Configuration window displays.

![Basic Configuration Window](image)

33. Select appropriate options, and then select the **OK** button.

EventTracker Agent Configuration window displays.
NOTE: Ignore the above message. Close the window and proceed with the installation.

InstallShield Wizard displays the Alert and Report generation settings dialog box.
34. Select/enter appropriate data in the relevant fields, and then select the **Add** button.

InstallShield Wizard displays the last screen.

![InstallShield Wizard Last Screen](image)

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

InstallShield Wizard displays the **EventTracker Configuration** screen.
36. 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.

37. Click the **OK** button.

If there are any Collection Points (CP) reporting to the Collection Master (CM), then following change has to be done in the CM. Please follow the steps given below.

38. Login to EventTracker Enterprise.
39. Select the **Admin** menu, select **Collection Master**, and then select **Collection Point Details** tab.

![Collection Master](image)

**Figure 99**

40. Select the respective Collection Point site, and then select **Edit**.

![Collection Master](image)

**Figure 100**

41. Click **Update** and save the changes.
Upgrade from v7.0.x to v7.5.x

The upgrade procedure from v7.0 to v7.5 is the same as v7.4 to v7.5. The detail procedure is described in Upgrade from v7.4.x to v7.5.x.

NOTE:

- Before upgrading, take a back up of the database and follow the instructions mentioned in Backup and Restore Guide.
- Please refer Common steps for all upgrades for more details.
- After upgrading from v7.2 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in “\InstallDIR\EventTracker\Prism.AlertsMigration.exe” for migrating the incidents.

Upgrade from v7.1.x to v7.5.x

The upgrade procedure from v7.1 to v7.5 is the same as v7.4 to v7.5. The detail procedure is described in Upgrade from v7.4.x to v7.5.x.

NOTE:

- Before upgrading, take a back up of the database and follow the instructions mentioned in Backup and Restore Guide.
- Please refer Common steps for all upgrades for more details.
- After upgrading from v7.2 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in “\InstallDIR\EventTracker\Prism.AlertsMigration.exe” for migrating the incidents.

Upgrade from v7.2.x to v7.5.x

The upgrade procedure from v7.2 to v7.5 is the same as v7.4 to v7.5. The detail procedure is described in Upgrade from v7.4.x to v7.5.x.

NOTE:

- Before upgrading, take a back up of the database and follow the instructions mentioned in Backup and Restore Guide.
• Please refer [Common steps for all upgrades](#) for more details.

• After upgrading from v7.2 to v7.5, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in "\InstallDIR\EventTracker\Prism.AlertsMigration.exe" for migrating the incidents.

---

## Upgrade from v7.3.x to v7.5.x

The upgrade procedure from v7.3 to v7.5 is the same as v7.4 to v7.5. The detail procedure is described in [Upgrade from v7.4.x to v7.5.x](#).

**NOTE:**

• Before upgrading, please take a back up of the database and follow the instructions mentioned in [Upgrade from v7.4.x to v7.5.x](#).

This is an alternate method to take a back up of the database from v7.3 Build 59 onwards via EventTracker Control Panel -> Diagnostics otherwise please refer [Backup and Restore Guide](#).

• Please refer [Common steps for all upgrades](#) for more details.

---

## Upgrade from v7.4.x to v7.5.x

• Please refer [Common steps for all upgrades](#) for more details.

• Before upgrading, please take a back up of the database and details are given below.

  a) Double-click EventTracker Control Panel, double-click Diagnostics.

  b) Click the Backup Configuration button.

     Backup & Restore window displays.
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 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 with upgrade, it is very crucial to close/terminate all the EventTracker components present in the system, like EventTracker Enterprise, EventTracker Control Panel, and even **RDP** (Remote Desktop Protocol) session.

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

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

**Step 2: Uninstall v7.5**

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.

![Add or Remove Programs](image)

**Figure 102**

(OR)

Click the **Start** button, select **Programs**, and then select **Prism Microsystems**.

Select **EventTracker**, and then select **Uninstall EventTracker**.

EventTracker will display the confirmation message.

![Windows Installer](image)

**Figure 103**

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

![EventTracker](image)

**Figure 104**

4. Click the **Yes** button to continue the installation process.

EventTracker starts uninstall process, and displays **‘Uninstall EventTracker’** dialog box.
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** drop down.
3. Select **Restart** option, and then click the **OK** button.

**Step 4: Install EventTracker v7.5 Enterprise**

For the details regarding installation process, please refer to ‘EventTracker v7.5 Enterprise Installation Guide’.

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

Click **Configure the service accounts** for more details.

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

**Verify Category:**
1. Log on to EventTracker Enterprise.

2. Click the Admin menu, and then click Category.

   EventTracker displays Category Management Page.

3. Search for the imported custom category under Category Tree tab.

   In addition, you can find the custom category on the right side of the page, in Last 10 modified categories list. Example: New Category

   Figure 106

   (OR)

   Click the Search tab, enter the category name in Search field, and then click the Go button.

Verify Alerts:

1. Click the Admin menu, and then click Alerts.

   EventTracker displays Alert Management page.
Figure 107

2. Enter the alert name in **Search Field**, and click the **Go** button.

Figure 108

To find alert(s) in the list, you can make use of scroll bar and the page numbers provided at the bottom of **Alert Management page**.

**Verify Filters:**

1. Click the **Admin** menu, and click **Event Filters**.

EventTracker displays **Event Filters** page. The newly imported filters are listed in this page.
2. Click the filter name to see the imported filter details.

EventTracker displays *Event Filter configuration* page.

**Verify RSS Feeds:**

1. Click the **Admin** menu, and then click **RSS**.

EventTracker displays **RSS Feeds** page. The newly imported RSS Feeds are listed in this page.
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. Log on to EventTracker Enterprise.
2. Select the Admin menu, and select Systems.

   EventTracker displays System manager page.

3. Right-click the desired domain/group name, and then select Upgrade agent.

   EventTracker displays Upgrade Remote Agent(s) dialog box.
All systems in the selected group

Click this option to upgrade all the agents in the selected group.

Take systems from the text file

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.

Agent type

Select the agent to upgrade.

Specific systems in the selected group

Out of all the agent systems present in the group, select specific agent system(s) to upgrade.

(OR)

Move the cursor on the remote system's name (where the agent is to be upgraded), click the dropdown arrow, and then click Upgrade Agent.
Figure 114

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

Figure 115

4. Check the agent type option which you wish to upgrade, and then click the **Next** button.
5. Select **Windows Domain Network** option, and fill in the user credentials.

(OR)

If you wish to deploy agent(s) to Linux or other BSD systems 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.

**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.

![Advance Agent/Start poll](image)

After events are collected, they are processed at the Manager. To apply a predefined configuration, select ‘Custom’ and specify the file.

You can also select ‘Default’ and configure later.

- **Default**
- **Custom config**

Select ‘Install’ to proceed.

![Select Install to proceed](image)

**Figure 120**

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

(OR)

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

The custom configuration will provide you the templates which you have created in Agent configuration and two more predefined templates.

You can select the template of your choice.

- **etaconfig_Servers.ini**: This predefined template contains the ideal server configurations which can be applied to the selected agent system.

- **etaconfig_Workstations.ini**: This predefined template contains the ideal workstation configurations which can be applied to the selected agent system. This option disables the ‘Offline event sending’ option.

9. Click the **Upgrade** button.

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

EventTracker displays **System Status** screen.

![System Status Screen](image)

**Figure 122**

11. Click the refresh button, to see the latest status.

![Status Update Screen](image)

**Figure 123**

**NOTE:** It may take some time to load the status.

**Step 8: Run KeywordMigration.exe file**

The Keyword Indexer folder is restructured. To put the old indexed files into the new structure, the **KeywordMigration.exe** utility file has been provided along with build 7.5. This utility migrates the existing keyword files to the new structure.

The path for utility file is `<Install folder>\EventTrackerWeb\bin\KeywordMigration.exe`

- As the menu options have been changed, the **User Privileges** configuration won’t be retained after upgrade to v7.5 for non-admin users. You have to reconfigure it again.

  a) To configure the privileges, go to **Admin** hyperlink, select **Users**.
EventTracker displays User Management window.

b) From the login name dropdown, select **Assign Privileges**.

![Figure 124](image1.png)

EventTracker displays the Add Privileges window.

c) Select required field and click **OK**.

![Figure 125](image2.png)

**Upgrade from v7.5.x to v7.5.x**

The upgrade from v7.5.x to v7.5.x is the same as the Upgrade from v7.4.x to v7.5.x.
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. 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.

![Image of Services window with EventTracker services highlighted]
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.

![Figure 128](image)

5. Click **Log On** tab, and select **This account** option.

![Figure 129](image)
6. Enter the user credentials and correct password.  
   The user name should be in 'domain name\user name' format.
7. Click the **Apply** button.  
   Warning message will be displayed on the desktop.

![Services](image)

![Figure 130](image)

8. Click the **OK** button.
9. To run the service with new logon name, stop and start the service.
10. Likewise, for 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.

![Services](image)

![Figure 131](image)