EventTracker Upgrade Guide

Upgrade to v7.4
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 v.6.4 to 7.3 who wish to upgrade to v7.4 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 ‘v.6.4 (Build 50)’ and below contact support@eventtracker.com for complete and thorough instructions.
Table of Contents

New Categories available in EventTracker v7.4................................................................. 4
Prerequisites....................................................................................................................... 5
Planning ............................................................................................................................ 5
Upgrade - Quick View....................................................................................................... 6
  Upgrade from v6.4 (Build 50) to v7.4 (Any build)......................................................... 7
  Upgrade from v7.0 (Any build) to v7.4 (Any build)..................................................... 8
  Upgrade from v7.1 (Any build) to v7.4 (Any build)..................................................... 8
  Upgrade from v7.2 (Any build) to v7.4 (Any build)..................................................... 9
  Upgrade from v7.3 (Any build) to v7.4 (Any build)..................................................... 9
  Upgrade from v7.4 (Any build) to v7.4 (Any build)..................................................... 10
Upgrade - Detailed View................................................................................................. 11
  Upgrade from v6.4 (Build 50) to v7.4 (Any build)......................................................... 12
  Upgrade from v7.0 (Any build) to v7.4 (Any build).................................................... 43
  Upgrade from v7.1 (Any build) to v7.4 (Any build).................................................... 46
  Upgrade from v7.2 (Any build) to v7.4 (Any build).................................................... 49
  Upgrade from v7.3 (Any build) to v7.4 (Any build).................................................... 65
  Upgrade from v7.4 (Any build) to v7.4 (Any build).................................................... 69
Post Upgrade- Import New Categories, Alerts, and Reports......................................... 71
Configuring Service Accounts......................................................................................... 73
New Categories available in EventTracker v7.4

The details about new categories available in EventTracker v7.4 is mentioned below.

- ArrayOS forwards the syslog events to EventTracker Enterprise. For detail information, please refer [Array OS Integration Guide](#).

- The Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, In-Band or Out-of-Band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks. For detail information, please refer [Cisco NAC Integration Guide](#).

- MySQL Server can send security General log's to EventTracker. For detail information, please refer [MySQL Integration Guide](#).

- Teradata Database server is used to forward event logs to EventTracker Enterprise. Teradata Database Server Administrators can also forward syslog events to EventTracker Manager. For detail information, please refer [Teradata Integration Guide](#).
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 to v7.4 Enterprise
- Upgrade from v7.0 to v7.4 Enterprise
- Upgrade from v7.1 to v7.4 Enterprise
- Upgrade from v7.2 to v7.4 Enterprise
- Upgrade from v7.3 to v7.4 Enterprise
Upgrade from v6.4 (Build 50) to v7.4 (Any build)

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

NOTE:
Please make sure to install IIS 6 and above before upgrading to v7.4.

Upgrade Procedure

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v7.4 (Build 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 hyperlink, and select Alerts.
   EventTracker displays Alert Management page.
3. Click the alert name to be modified.
4. EventTracker displays Alert Configuration page.
5. Select the threat level from Threat Level dropdown.
6. Click the Finish button.
EventTracker saves the configuration settings.

NOTE:

1. Upgrade process for v6.4 to v7.4 (any build) remains the same.

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

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

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

Upgrade from v7.0 (Any build) to v7.4 (Any build)

Please refer the ‘Detailed view’ section for the upgrade instructions.

NOTE:

As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 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 version 7.4.

Upgrade from v7.1 (Any build) to v7.4 (Any build)

Please refer the ‘Detailed view’ section for the upgrade instructions.

NOTE:

As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 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 version 7.4.
Upgrade from v7.2 (Any build) to v7.4 (Any build)

Before you start with the upgrade process

1. Verify that all the prerequisites have been satisfied.
2. 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.
3. Close/terminate all the EventTracker components like EventTracker Enterprise, EventTracker Control panel, including RDP (Remote Desktop Protocol) sessions.

Upgrade from v7.2 to v7.4

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v7.4.
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 the ‘System Manager’.
7. After upgrading from v7.2 to v7.4, to view the incidents generated in the EventTracker v7.2, the user has to use the Prism.AlertsMigration.exe to view the incidents.

NOTE:

1. For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).
2. The custom image files like .jpg or .png in the ‘EventTrackerWeb’ folder will not be retained after the upgrade. You need to take a backup of those files.
3. As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 for non-admin users. You have to reconfigure it again.
4. The dashboard options have been updated and the user has to reconfigure after upgrading to v7.4.

Upgrade from v7.3 (Any build) to v7.4 (Any build)

Before you start with the upgrade process

1. Verify that all the prerequisites have been satisfied.
2. 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.

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

Upgrade from 7.3 to v 7.4

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v7.4.
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 the ‘System Manager’.
7. After upgrading from 7.3 to 7.4, to view the incidents generated in the EventTracker v7.3, the user has to use the Prism.AlertsMigration.exe to view the incidents.

NOTE:

1. For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).
2. The custom image files like .jpg or .png in the ‘EventTrackerWeb’ folder will not be retained after the upgrade. You need to take a backup of those files.
3. As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.3 for non-admin users. You have to reconfigure it again.
4. The dashboard options have been updated and the user has to reconfigure after upgrading to version 7.3.

Upgrade from v7.4 (Any build) to v7.4 (Any build)

The procedure to upgrade from v7.4 to v7.4 (any build) is same like upgrade from v7.3 to v7.4.
Upgrade - Detailed View

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

- Upgrade from v6.4 to v7.4 Enterprise
- Upgrade from v7.0 to v7.4 Enterprise
- Upgrade from v7.1 to v7.4 Enterprise
- Upgrade from v7.2 to v7.4 Enterprise
- Upgrade from v7.3 to v7.4 Enterprise
Upgrade from v6.4 (Build 50) to v7.4 (Any build)

Before you start with the upgrade process:

Creating 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).
5. Click the **Export** button.

EventTracker displays **Select Export File** window.

OR

Click **Add All** button to select all the categories.
6. Click **Save in** dropdown to select the file location, enter the **File name**, and click the **Save** button.

   EventTracker displays confirmation message box.

   ![Figure 4](image)

7. Click the **OK** button.

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

   ![Figure 5](image)

   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 the **Alerts** option,

11. Click the **Export E-mail Settings** checkbox.

12. From the **Alerts** field, select the alerts to be exported, and click the **Add** button.

   (Example: My Alerts)
OR
Click Add All button to select all the Alerts.

13. Click the Export button.

EventTracker displays Select Export File window.

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

EventTracker displays confirmation message box.

15. Click the OK button.

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

17. 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.

18. Click the **OK** button.

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

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

20. 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.

21. Click the **OK** button.

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

22. 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**.

![Figure 11](image)

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.
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.

![Figure 14](image)

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. Click 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.

   ![Figure 15: Add or Remove Programs](image)

   OR

   Click the **Start** button, select **Programs**, select **Prism Microsystems**.
   Select **EventTracker**, and then select **Uninstall EventTracker**.
   EventTracker displays the confirmation message.

   ![Figure 16: Windows Installer](image)

3. Click the **Yes** button.
   EventTracker starts the uninstall process.
4. Click the **No** button.

EventTracker displays ‘**Uninstall EventTracker**’ dialog box.

![Uninstall EventTracker dialog box](image)

- 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 v7.4 Enterprise

For details about Installation process, please refer ‘EventTracker v7.4 Install Guide’.

NOTE:

For v6.4, EventTracker uses MS Access database, and uses SQL database for v7.4. Before upgrade, you need to migrate the database from MS Access to SQL database. For this purpose, a Migration Utility will appear while installing v7.4 (See figure 20). This utility will migrate 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 [here](#) to read ‘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. Click the **Start button**, select **Programs**, select **Prism Microsystems**.
2. Select **EventTracker**, and then select **EventTracker Control Panel**.

EventTracker displays **EventTracker Control Panel**.
3. Click **Export Import Utility** icon.
   EventTracker displays Export Import Utility window.

4. Click the **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.

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

   ![Figure 24](image)

9. Click the **OK** button.

10. Select the **Filters** option.

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

12. Click the **Import** button.


   ![Figure 25](image)

14. Click the **OK** button.

15. Click the **Alerts** option.
16. Select **Import E-mail settings** checkbox, if not selected.
17. In the **Set Active** pane, select the appropriate option.
18. Click the **browse** button, select the location of the file, and click the **Open** button.
19. Click the **Import** button.

21. Click the **OK** button.
22. Select the **RSS Feeds** option.
23. Click the **browse** button, select the location of the file, and click the **Open** button.
24. Click the **Import** button. EventTracker displays **Export Import Utility** success message box.

25. Click the **OK** button.
26. Select the **Scheduled Reports** option.
27. Click the **browse** button, select the location of the file, and click the **Open** button.

28. Click the **Import** button.

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

30. Click the **OK** button.

31. Click the **Close** button.

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

**Verify Category:**

32. Log on to **EventTracker Enterprise**.
33. Click the Admin hyperlink, and click Category. EventTracker displays 'Category Management' Page.

34. 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

OR

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

Verify Alerts:

35. Click the Admin hyperlink, and click Alerts.
EventTracker displays Alert Management page.
36. Enter the alert name in **Search** Field, and click the **Go** button.

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:**

37. Click the **Admin** hyperlink, and click **Event Filters**.

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

![Event Filter configuration page](image)

**Figure 36**

**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.

39. Click the **Tools** dropdown, and click **Legacy Reports**. EventTracker displays **Legacy Reports** dialog box.
40. Expand **Legacy Reports** folder, and click **Scheduled**. Here you will get to see the list of successfully generated reports from version 6.4.

Verify RSS Feeds:

41. Click the **Admin** hyperlink, 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.
42. Log on to **EventTracker Enterprise**.
43. Click the **Admin** hyperlink, and select **Systems**.
   EventTracker displays ‘System Manager’ page.

44. Right click the desired domain/group name, and 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.

45. Choose the agent(s) to be upgraded by selecting checkbox, and click the Next button.

46. Select Windows Domain Network option, and fill in the user credentials,
OR

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

47. Select **Install default Remedial Action EXEs on this system** checkbox. EventTracker displays confirmation message.
48. Click the OK button, and click the **Upgrade** button.

EventTracker displays information message.

49. Click the OK button.

EventTracker displays **System Status** screen.

50. 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 v7.4 ‘Trusted connection List’. This option will help you to update the trusted connection list.

51. Log on to EventTracker Enterprise.
52. Click the Admin hyperlink, select Windows Agent Config, and select the Network Connection Monitor tab.
53. Click Suspicious Traffic Only (SNAM) option, and click the Trusted List button.
   EventTracker displays ‘Trusted Connections List’ pop-up window.
54. 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 7.4
- 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.

![Figure 55](image)

You need to explicitly set the threat level as per your requirement. To set the threat level,
55. Open EventTracker Enterprise.
56. Click the Admin hyperlink, and select Alerts.
   EventTracker displays Alert Management page. (Refer Figure 56)
57. Click the alert name to be modified.
   EventTracker displays Alert Configuration page. (Refer Figure 57)

58. Select the threat level from Threat Level dropdown.
59. Click the Finish button.
   EventTracker saves the configuration settings.
Upgrade from v7.0 (Any build) to v7.4 (Any build)

NOTE:

- Close/terminate all the EventTracker components like EventTracker Enterprise, EventTracker Control panel, including RDP (Remote Desktop Protocol) sessions.
- The menu options have been altered for v7.4.
- The dashboard has been updated and the user has to configure while upgrading version 7.4

Earlier version menu options:

![Figure 58](image-url)
Menu options for v7.4:

- If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v7.4. Please make sure to reconfigure it again as mentioned in **How to - Secure IIS Web Server with SSL**.

- The logged in user who is upgrading to EventTracker v7.4 should have SQL sysadmin privilege.

- As the menu options have been changed, the **User Privileges** configuration won't be retained after upgrade to v7.4 for non-admin users. You have to reconfigure it again.
  
  a) To configure the privileges, go to **Admin** hyperlink, select **Users**.

  b) Click login name dropdown, select **Assign Privileges**.
Figure 60
Upgrade from v7.1 (Any build) to v7.4 (Any build)

NOTE:

- Close/terminate all the EventTracker components like EventTracker Enterprise, EventTracker Control panel, including RDP (Remote Desktop Protocol) sessions.
- The menu options have been changed for v7.4.
- The dashboard has been updated and the user has to configure while upgrading version 7.4.

Earlier version menu options:

Figure 61
Menu options for v7.4:

- If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v7.4. Please make sure to reconfigure it again as mentioned in How to - Secure IIS Web Server with SSL.
- The logged in user who is upgrading to EventTracker v7.4 should have SQL sysadmin privilege.
- Before upgrading, take a back up of the database and follow the instructions mentioned in Backup and Restore Guide.
- As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 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.
EventTracker displays the Add Privileges window.

c) Select required field and click **OK**.
Upgrade from v7.2 (Any build) to v7.4 (Any build)

Before you start with the upgrade process

- 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 v7.4. Please make sure to reconfigure it again as mentioned in How to - Secure IIS Web Server with SSL.
- The logged in user who is upgrading to EventTracker v7.4 should have SQL sysadmin privilege.

Upgrade Procedure

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.

Figure 65
Close the open component, and then click the **Retry** button. EventTracker resumes uninstall process.

**Step 2: Uninstall version 7.2**

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

![Add or Remove Programs](image)

**Figure 66**

**OR**

Click the **Start** button, select **Programs**, and select **Prism Microsystems**. Select **EventTracker**, and select **Uninstall EventTracker**. EventTracker will display the confirmation message.

![Windows Installer](image)

**Figure 67**

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

![EventTracker](image)

**Figure 68**
4. Click the **Yes** button to continue the installation process. EventTracker starts uninstall process, and displays 'Uninstall EventTracker' dialog box.

![Uninstall EventTracker](image)

**Figure 69**

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 **Start** > click **Shut Down**.
3. Select the **Restart** option from the dropdown, and then click the **OK** button.

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

For details regarding installation process, please refer ‘EventTracker v7.4 Install Guide’.

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

Click [here](#) to read ‘Configure the service accounts’ section.
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 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: New Category

![Figure 70](image)

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

Verify Alerts:
1. Click the Admin hyperlink, and click Alerts.
   EventTracker displays Alert Management page.
2. Enter the alert name in **Search** Field, and click the **Go** button.

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** hyperlink, 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 hyperlink, and click the 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. Click the Admin hyperlink, and select Systems.
   EventTracker displays System manager page.
3. Right click the desired domain/group name, and select Upgrade agent.
   EventTracker displays Upgrade Remote Agent(s) dialog box.
Table of Upgrade Options:

<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 upgrade all the agents 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 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><strong>Agent type</strong></td>
<td>Select the agent to upgrade.</td>
</tr>
<tr>
<td><strong>Specific systems in the selected group</strong></td>
<td>Out of all the agent systems present in the group, select specific agent system(s) to upgrade.</td>
</tr>
</tbody>
</table>

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

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.

![Figure 80](image)

**OR**

If you wish to deploy agent(s) to Linux or other BSD systems then select the **Upgrade over IP (Non Windows Domain)** option.

![Figure 81](image)
6. Check **Install default Remedial Action EXEs on this system** option 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 83**

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

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 KeywordMigration.exe utility file has been provided along with build 7.4. This utility migrates the existing keyword files to the new structure.

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

NOTE:
- As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 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 version 7.4.
Earlier version menu options:

![Figure 88]
Menu options for v7.4:

![Figure 89](image)

d) As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.4 for non-admin users. You have to reconfigure it again.

e) To configure the privileges, go to Admin hyperlink, select Users.

f) Click login name dropdown, select Assign Privileges.
Figure 90
Upgrade from v7.3 (Any build) to v7.4 (Any build)

NOTE:

- 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 v7.4. Please make sure to reconfigure it again as mentioned in How to - Secure IIS Web Server with SSL.

- The logged in user who is upgrading to EventTracker v7.4 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

![Select SQL Instance](image)

Figure 91

- Before upgrading, please take a back up of the database and follow the instructions mentioned in upgrade from v7.4 (Any Build) to v7.4 (Any Build).

This is an alternate method to take a back up of the database from v7.3 Build 59 onwards via EventTracker Control Panel -> Diagnostics.
Menu options for v7.3

Figure 92
The user interface of Incidents Dashboard, Reports menu and Tools menu has been changed.

Menu options for v7.4

![Image of Incidents Dashboard with menu options](image)

**Figure 93**

Menu options for reports

![Image of menu options for reports](image)

**Figure 94**
Menu options for Tools

As the menu options have been changed, the User Privileges configuration won't be retained after upgrade to v7.4 for non-admin users. You have to reconfigure it again.

1. To configure the privileges, go to Admin hyperlink, select Users.
2. Click login name dropdown, select Assign Privileges.
Upgrade from v7.4 (Any build) to v7.4 (Any build)

The upgrade from v7.4 (Any Build) to v7.4 (Any Build) is the same as the Upgrade from v7.3 to v7.4.

- 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 v7.4. Please make sure to reconfigure it again as mentioned in How to - Secure IIS Web Server with SSL.

- The logged in user who is upgrading to EventTracker v7.4 should have SQL sysadmin privilege.
  
  If the user does not have sufficient permission then an error message is displayed.

- 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.
Post Upgrade - Import New Categories, Alerts, and Reports

After upgrade to v7.4, the newly added categories have to be imported from <install dir>\EventTracker\Configuration Files. Please refer the below list of newly added categories, alerts and flex reports.

New Categories

- All RSA SecurID group of categories.iscat
- All CheckPoint group categories.iscat
- All Ms Forefront TMG group of categories.iscat
- All Forefront UAG group of categories.iscat
- All McAfee IntruShield group categories.iscat
- All McAfee IntruShield alerts.iscat
- All Palo Alto group of categories.iscat
- All Aventail SSL VPN group of categories.iscat
- All ArubaOS group of categories.iscat
- All Raritan group of categories.iscat
- All Windows Time Service categories.iscat
- All F5 BIG-IP LTM Categories.iscat
- VMware ESX failed user login.iscat (Modification of existing category)
- EventTracker Admin audit event.iscat (Modification of existing category)
- EventTracker resource scheduled discovery.iscat
- No events received in last 24 hour.iscat

New Alerts

- All RSA SecurID group of alerts.isalt
- All CheckPoint group alerts.isalt
- All LOGbinder SP group alerts.isalt
- All MS Forefront TMG group of alerts.isalt
- All Forefront UAG group of alerts.isalt
- All Palo Alto group of alerts.isalt
- All Aventail SSL VPN group of alerts.isalt
- All ArubaOS group of Alerts.isalt
- All Raritan group of alerts.isalt
• All Windows Time Service alerts
• All F5 BIG-IP LTM Alerts
• VMware ESX user authentication failed
• No events received in last 24 hour
• StatusTracker new resource discovered

New Flex Reports
• All LOGbinder SP Flex reports
• McAfee IntruShield reports
• VMware vSphere Alarm reports
• VMware vSphere Tasks reports
Configuring 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 & 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. Click the **Start** button, and select **Run**.

2. Type **services.msc**, and click the **OK** button.

![Figure 99](image1.png)

3. In the **Services** window, search for EventTracker services.

![Figure 100](image2.png)
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 101](image1.png)

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

   ![Figure 102](image2.png)
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.

   ![Figure 103](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.

   ![Figure 104](image)