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 v8.1 who wish to upgrade to v8.2 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.

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

Before you upgrade:

1. Thoroughly read the ‘EventTracker Architecture’ guide. This guide explains the architecture and sample deployment methods with illustrations.
   Managing Billions of Logs Everyday.
2. Contact support@eventtracker.com for information regarding license keys or license certificates.
3. Make sure that Windows Updates is up-to-date with .NET Framework 4.5.
**IMPORTANT:**

- After upgrade, in a Collection Master, the user might notice inconsistency in Reports/ Log Search/Cab received status (Admin>Collection Master>Archives status), till the database migration is in process.
- After Upgrade, in Collection Point, the user may not be able to view the exact Cab transfer status in (Admin>Collection Point Configuration-> manage archives) till the database migration is in process.
# Table of Contents

Introduction ............................................................................................................................................................. 1

Audience .................................................................................................................................................................. 1

Before you upgrade: ........................................................................................................................................... 1

New Categories/Alerts/Reports available in v8.2 ................................................................................................. 4

Prerequisites .......................................................................................................................................................... 10

Planning.................................................................................................................................................................. 10

Upgrade - Quick View ............................................................................................................................................ 11

Common steps for all upgrades.............................................................................................................................. 11

Upgrade from v6.4.x to v8.2.x ................................................................................................................................ 13

  Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x................................................................................................. 18

  Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x................................................................................................. 18

  Upgrade from v7.6.x to v8.2.x.......................................................................................................................... 18

  Upgrade from v8.0.x/v8.1.x to v8.2.x ............................................................................................................... 18

Upgrade - Detailed View ....................................................................................................................................... 18

Upgrade from v6.4.x to v8.2.x ................................................................................................................................ 19

  Upgrade Procedure ........................................................................................................................................... 27

Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x................................................................................................. 64

Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x................................................................................................. 64

Upgrade from v7.6.x to v8.2.x.......................................................................................................................... 64

  Import the newly added Behavior Rules after upgrade: ................................................................................ 78

Configure Service Accounts .................................................................................................................................. 94

Using the Default Agent Filters in EventTracker version 8.2 ................................................................................. 98

Upgrade from v8.0.x/v8.1.x to v8.2.x..................................................................................................................... 108
New Categories/Alerts/Reports available in v8.2

The details about new categories/alerts/reports available in EventTracker v8.2 is mentioned below.

**New Categories**

- Cisco SourceFire: Correlation events
- Cisco SourceFire: IPS activity
- Cisco SourceFire: Inbound and outbound traffic
- Infoblox: DHCP expire
- Infoblox: DHCP release
- Infoblox: DHCP renew
- Infoblox: Object created
- Infoblox: Object deleted
- Infoblox: Object modified
- Kaspersky Security Centre: All management activity
- Kaspersky Security Centre: Application privilege management
- Kaspersky Security Centre: Malicious object scan status
- Kaspersky Security Centre: Administrative group management
- Kaspersky Security Centre: Group task management
- Kaspersky Security Centre: Policy management
- Kaspersky Security Centre: Report management
- Kaspersky Security Centre: Task management
- Meraki Firewall: Content filtering
- Meraki Firewall: DHCP IP leased
- Meraki Firewall: IDS-alerts detected
- Meraki Firewall: User authentication attempt
- Meraki Firewall: VPN session
- Meraki Firewall: Web traffic
- Meraki Firewall: Peer to Peer VPN connection change
- Meraki Firewall: Traffic flow
- Microsoft Windows DFS: Audit setting changed
- Microsoft Windows DFS: Namespace activity
- Microsoft Windows DFS: Network share object accessed
- Microsoft Windows DFS: Replication activity
- Microsoft Windows DFS: User logon success
- Microsoft Windows DFS: Client desired access
- Trend Micro Deep Security: Active directory activity
• Trend Micro Deep Security: Antimalware activity
• Trend Micro Deep Security: Computer management
• Trend Micro Deep Security: File integrity monitoring
• Trend Micro Deep Security: Firewall activity
• Trend Micro Deep Security: Group management
• Trend Micro Deep Security: Intrusion prevention
• Trend Micro Deep Security: Policy management
• Trend Micro Deep Security: Roles management
• Trend Micro Deep Security: System logs
• Trend Micro Deep Security: User authentication failed
• Trend Micro Deep Security: User logon activity
• Trend Micro Deep Security: User management
• Trend Micro InterScan: HTTP inspection policy added
• Trend Micro InterScan: Trusted URL added
• Trend Micro InterScan: Active digital certificates management
• Trend Micro InterScan: Data loss Prevention
• Trend Micro InterScan: Delete policies
• Trend Micro InterScan: DLP global policy changes
• Trend Micro InterScan: HTTP CPU utilization
• Trend Micro InterScan: HTTP domain tunneling
• Trend Micro InterScan: Policy management
• Trend Micro InterScan: URL access control
• Trend Micro InterScan: URL filter
• Trend Micro InterScan: User logon

New Alerts
• High priority alert generated
• EventTracker: Software installed on EventTracker server
• EventTracker: Abnormal local security authority process
• EventTracker: Out of ordinary process launched
• EventTracker: Software installed on this system
• EventTracker: Software uninstalled from the system
• EventTracker: Browser connecting to non webserver port
• EventTracker: Non browser application connecting to known webserver port
• Windows PowerShell: Command execution failed
• Windows PowerShell: Remote session initiated
- Windows PowerShell: Remote session user authentication failed
- FortiAnalyzer: Device deleted by administrator
- FortiAnalyzer: Removed a disk from RAID array
- Infoblox: Object changed
- Kaspersky Security Centre: Malicious object detected
- Kaspersky Security Centre: Policy changed
- Windows AD Insider Threat: Group policy changes details
- Windows AD Insider Threat: Lmcompatibilitylevel registry changes
- Windows AD Insider Threat: Unauthorized server accessed by user
- Windows AD Insider Threat: User account changes by unauthorized users
- Windows AD Insider Threat: User added in admin group by unauthorised user
- Meraki Firewall: IDS-alert detected
- Meraki Firewall: Suspicious content blocked
- Microsoft Windows DFS-Namespace active directory issues
- Microsoft Windows DFS-Replication stopped
- Suricata IDS: High priority alert generated
- SonicWALL Firewall: Website access denied
- Trend Micro Deep Security: Agent disk space low
- Trend Micro Deep Security: Duplicate computer
- Trend Micro Deep Security: Manager clock changed
- Trend Micro Deep Security: Manager disk space low
- Trend Micro Deep Security: Manager shutdown
- Trend Micro InterScan: Policy created
- Trend Micro InterScan: Policy deleted

New Flex Reports
- EventTracker-Alert details
- EventTracker-Admin activity
- EventTracker-All error events
- EventTracker-All sources log volume
- EventTracker-All warning events
- EventTracker-Software installed
- EventTracker-Software uninstalled
- EventTracker-Unknown and unsafe MD5 hash detected
- EventTracker-Abnormal local security authority process
- EventTracker-New logon pattern found
- Cisco ASA-Traffic details
- Cisco SourceFire-Inbound and outbound traffic
- Cisco SourceFire-IDS and IPS activity
- Cisco SourceFire-Inbound and outbound traffic
- Cisco SourceFire-IDS and IPS activity
- Cisco SourceFire-Correlation events
- Cisco SourceFire-Alert Analysis
- Windows PowerShell-Command execution details
- Windows PowerShell-Script execution details
- Windows PowerShell-Command execution error details
- Windows PowerShell-Remote session creation details
- Windows PowerShell-Remote session authentication failure details
- Windows PowerShell-Remote session authentication success details
- FortiAnalyzer-Network share management
- FortiAnalyzer-Resource monitoring
- FortiAnalyzer-Backup and restore activity
- FortiAnalyzer-IPsec activity
- FortiAnalyzer-Device management
- FortiAnalyzer-System management
- FortiAnalyzer-User management
- FortiAnalyzer-Configuration changes activity
- FortiAnalyzer-Administrator logon activity
- FortiAnalyzer-Administrator logon failed
- Infoblox-Object management details
- Infoblox-DHCP IP assignment details
- Kaspersky Security Centre-Task management
- Kaspersky Security Centre-Policy management
- Kaspersky Security Centre-Group task management
- Kaspersky Security Centre-Administrative group management
- Kaspersky Security Centre-Report management
- Kaspersky Security Centre-All management activity
- Kaspersky Security Centre-Malicious object scan status
- Kaspersky Security Centre-Application privilege management
- Microsoft Windows DFS-Client desired access
- Microsoft Windows DFS-Audit settings changed
• Microsoft Windows DFS-Namespace activity
• Microsoft Windows DFS-Replication activity
• Microsoft Windows DFS-Network share object accessed
• Microsoft Windows DFS-User logon success
• Meraki Firewall-DHCP IP lease details
• Meraki Firewall-Web traffic details
• Meraki Firewall-Blocked content details
• Meraki Firewall-Traffic flow details
• Meraki Firewall-IDS alert details
• Meraki Firewall-User authentication details
• Meraki Firewall-VPN session details
• Sophos Enterprise Console-Virus and adware detected
• Sophos Enterprise Console-Virus removed
• Sophos Enterprise Console-Virus file cleaned up
• Sophos Enterprise Console-Data transfer allowed and blocked
• Sophos Enterprise Console-Policy management
• Sophos Enterprise Console-Configuration change
• Sophos Enterprise Console-Group management
• Sophos Enterprise Console-Update management
• Suricata IDS-Alert analysis
• SonicWALL Firewall-Traffic flow
• SonicWALL Firewall-Website traffic
• Trend Micro Deep Security-User logon activity
• Trend Micro Deep Security-User management
• Trend Micro Deep Security-User authentication failed
• Trend Micro Deep Security-Computer management
• Trend Micro Deep Security-Policy management
• Trend Micro Deep Security-Roles management
• Trend Micro Deep Security-Group management
• Trend Micro Deep Security-Active directory activity
• Trend Micro Deep Security-File integrity monitoring
• Trend Micro Deep Security-Antimalware activity
• Trend Micro Deep Security-Firewall activity
• Trend Micro Deep Security-Intrusion prevention
• Trend Micro Deep Security-System logs
• Trend Micro InterScan-User logon success
- Trend Micro InterScan-Trust URL added
- Trend Micro InterScan-Trust URL added to exception
- Trend Micro InterScan-HTTP inspection policy added
- Trend Micro InterScan-HTTP DLP policy added
- Trend Micro InterScan-URL filter policy added
- Trend Micro InterScan-Digital certificates management
- Trend Micro InterScan-FTP DLP global policy change
- Trend Micro InterScan-HTTP CPU utilization
- Trend Micro InterScan-Delete policies
- Trend Micro InterScan-Policy management
- Trend Micro InterScan-HTTP domain tunneling
- Windows-USB device activity
- Windows-Disk space status
- Windows-Audit log cleared
- Windows-User logon success

**Updated Knowledge Packs:**

**Updated Alerts:**
- Cisco Sourcefire: High priority alert generated

**Updated Flex Reports:**
- Cisco Sourcefire-Inbound and outbound traffic
- Cisco Sourcefire-Correlation events
- Cisco Sourcefire-Alert analysis
- Cisco SourceFire-IDS and IPS activity
- EventTracker-USB or other removable media insert-remove
- EventTracker-New enterprise activity
- EventTracker-Out of ordinary activity
- EventTracker-Browser connecting to non-standard port
- EventTracker-Non-Browser connecting to port 80 or 443
- Windows-System shutdown-restart
- Windows-User logon failure
- Windows-User logon success
- VMware vCenter-Host added or removed
- VMware vCenter-Virtual machine created or removed
- VMware ESXi-Account created or removed
• Centrify Windows Agent-Run as role failed attempts
• Trend Micro InterScan-Trust URL added to exception
• SonicWALL Firewall-Attacks detection
• SonicWALL Firewall-Intrusion detection
• SonicWALL Firewall-VPN activity
• SonicWALL Firewall-VPN User authentication failed
• Cisco ASA-Connection denied
• Cisco ASA-Attack detection
• Cisco IOS-User logon failure
• Cisco IOS-User logon success
• Cisco IOS-Configuration changed

Updated Categories

• Cisco Sourcefire: Correlation events
• Cisco Sourcefire: IPS activity
• Cisco Sourcefire: Inbound and outbound traffic

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.

• Microsoft .NET Framework 3.5 SP1 and .NET Framework 4 or 4.5.2. Refer: Install .NET Framework.
• IIS or IIS Express. Refer: IIS-Configuration Guide
• Make sure Windows updates with all the latest service packs is installed.

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

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

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

- **Common steps for all upgrades**
- **Upgrade from v6.4 (Build 50) to v8.2.x Enterprise**
- **Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x Enterprise**
- **Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x Enterprise**
- **Upgrade from v7.6.x to v8.2.x Enterprise**
- **Upgrade from v8.0.x/v8.1.x to v8.2.x Enterprise**

**IMPORTANT:**

- For an upgrade from older version to **v8.2**, the earlier configured reports (HTML and DOCX), the reports will be generated in HTML and DOCX export types, until the user edits the reports and saves the changed configuration. The user can also generate the earlier configured report (HTML & DOCX) in the newer version, by importing it from EventTracker Control Panel> Export Import Utility.

- The transferred TLS reports from Collection Point will not display the selected reports, on clicking the information icon in Collection Master, in case the main reports are selected for transferring in Collection Point.

**Common steps for all upgrades**

**Before you start with the upgrade process**

- Verify that all the prerequisites have been satisfied.
- When upgrading from v7.x to v8.2, please verify all prerequisites are installed manually on server machine.
- While uninstalling v7.x, user has to enable the option to retain all the configuration and data. After uninstalling, please check if all prerequisites are installed manually on server machine.
- Take a backup of the database. For v7.0 – v7.2, please refer Backup and Restore Guide. For v7.3 onwards you can take a backup of the database from EventTracker Control Panel -> Diagnostics which is explained in detail in Upgrade from v7.6x to v8.2.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.
For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).

Preferred: Before upgrading EventTracker, the user has to export the user defined (user created/modified) alerts and categories.

Before upgrading from v7.x to v8.2, make sure that .NET 4.5 is installed. If Microsoft .NET Framework 4.5.2 is not installed, refer the Install Guide v8.2.

NOTE: If .NET 4.0 is already present, the pre-install check will not install .NET 4.5 and the user will have to install it manually.

The logged in user who is upgrading to EventTracker v8.2 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

NOTE: Before upgrading EventTracker from v7.x to v8.2, run the “UpdateBehaviorActivity” utility. The Utility will perform the database related changes.

Why to use the “UpdateBehaviorActivity” utility?

This utility resolves IP addresses as private or public and converts IP address into network order. The same process was being done through upgradation of EventTracker. During this process database log file (.ldf) was growing and installation was not possible in some cases. To avoid the installation failure, this utility should be used.

When to run the “UpdateBehaviorActivity” utility?

1. This utility should be executed only if installation is an upgrade from EventTracker v7.x.

2. In case of v6.4 to v8.2 upgrade, it is not required to run this utility.

How to run “UpdateBehaviorActivity” utility?
1. Before uninstalling EventTracker v7.x, download the utility ‘UpdateBehaviorActivity.exe’ and copy it to a desired location.

2. Run or Execute the utility UpdateBehaviorActivity.exe

3. Check in the log file “UpdateBehaviorActivity.log” from the path where the UpdateBehaviorActivity.exe has been launched.

4. Uninstall the EventTracker version 7.x with retaining configuration and rerun the utility “UpdateBehaviorActivity.exe”.

5. Upgrade to EventTracker version 8.2.

After Upgrade process:

- If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v8.2. Please make sure to reconfigure it again as mentioned in Securing IIS Web Server with SSL.

- As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v8.2 for non-admin users. You have to reconfigure it again.

- After upgrade, if the user wants to import the newly added behavior rules, please refer to: Import newly added Behavior Rules.

- If the user wants to use the default agent filters after upgrading to v8.2, please refer to: Use Default Agent Filters.

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

Upgrade from v6.4.x to v8.2.x

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. 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 v8.2.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. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **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.

- After upgrading from v6.4 to v8.2, kindly run the executable file `Prism.AlertsMigration.exe` available in `\InstallDIR\EventTracker\Prism.AlertsMigration.exe` for migrating the incidents.
- For v6.4 to v8.2 upgrade, if ‘Keyword Indexing’ is installed and enabled, then launch the Keyword Indexing migration utility.
- For agent upgrade details, please click [here](#).

Upgrade from v7.0.x/v7.1.x/v7.2.x/v7.3.x/v7.4.x/v7.5.x/v7.6.x/v8.0.x/v8.1.x to v8.2.x

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v8.2.
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**’.
7. **Preferred**: Import Knowledge Objects after upgrade. Details are explained in [Upgrade from v7.6.x to v8.2.x](#).
8. **Preferred**: Import the parsing rules, token templates and Defined Reports based on the user requirement.
9. **Optional**: To utilize newly added/Modified categories/alerts import the complete alerts /complete categories files from the configuration directory (Install directory). Prior to importing user has to manually delete existing categories and alerts from the application. Then import all categories and all alerts from configuration files.

**NOTE:**

**Behavior**

- From EventTracker v7.6 onwards, the Behavior Dashlets have been renamed. So after upgrading to v8.2, you have to reset the personalization and then configure the dashlets. Please follow the steps given below.
  
  a. Logon to EventTracker Enterprise.
  b. Select the **Behavior** menu, select **Security/Operations** drop down.
  c. Select **Reset Personalization icon**.

![Figure 2](image2.png)

![Figure 3](image3.png)
A message displays.

![Message from webpage](image)

**Figure 4**

d. Select the **OK** button.

e. To customize the required dashlets, select **Security/Operations** drop down, and then select **Customize icon**.

![Available Dashlets](image)

**Figure 5**

Available Dashlets window displays.

f. Select and **Add** the required dashlets.
• After upgrading, if the collection master is v8.2, and if collection point is using any older version of EventTracker, then incidents will not be visible. If you upgrade collection point to v8.2, post upgrade incidents will only be transferred to collection master.

• The keyword dashboard has to be customized after upgrading to v8.2.

• If On Demand/Scheduled/Queued reports are getting failed irrespective of the export type chosen (pdf, xml, word) in windows 2003 environment, kindly reinstall crystal reports. To clean up crystal reports, please refer Fix for Crystal Report Error. After the clean-up, download and install the executable file 32bit.msi for Support Pack 10 (v. 13.0.10.1385) from the location http://scn.sap.com/docs/DOC-7824.

Dashboard

• The Dashlets in Security/Operations are preserved after the upgrade and the user can customize the dashlets by selecting the customize icon 📐.

![Figure 7](image)

My EventTracker

• The dashlets created under My EventTracker> Dashboard are also preserved after the upgrade process and the user can further customize it by selecting the customize icon 📐.
Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x

The procedure to upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x is same like upgrade from v7.6.x to v8.2.x.

After upgrading from v7.0.x/v7.1.x/v7.2.x to v8.2.x, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x

The procedure to upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x is same like upgrade from v7.6.x to v8.2.x.

Upgrade from v7.6.x to v8.2.x

The procedure to upgrade from v7.6.x to v8.2.x is mentioned in the detail section.

Upgrade from v8.0.x/v8.1.x to v8.2.x

The procedure to upgrade from v8.0.x/v8.1.x to v8.2.x is same like upgrade from v7.6.x to v8.2.x.

Upgrade - Detailed View

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

- Upgrade from v6.4.x to v8.2.x Enterprise
- Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x Enterprise
- Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x Enterprise
- Upgrade from v7.6.x to v8.2.x Enterprise
- Upgrade from v8.0.x/v8.1.x to v8.2.x Enterprise
Upgrade from v6.4.x to v8.2.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.
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 12](image)

7. Click the **OK** button.

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

   ![Figure 13](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 **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.

   ![Figure 19](image1.png)

   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 21**

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.

![Closing EventTracker Components](image)

**Figure 22**
Close the open components, and then click the **Retry** button.

EventTracker resumes uninstall process.

**Upgrade Procedure**

**Step 1: Uninstall the version 6.4.x 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.

   ![Add or Remove Programs](image)

   **Figure 23**

   (OR)

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

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

   EventTracker displays the confirmation message.

   ![Windows Installer](image)

   **Figure 24**

3. Click the **Yes** button.

   EventTracker starts the uninstall process.
EventTracker displays, ‘Uninstall EventTracker’ confirmation message.

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 v8.2 Enterprise**

Kindly follow the steps mentioned below for upgrade process.

1. To install v8.2, launch **EventTrackerSetup.exe**.

EventTracker will Extract the files

![Extracting files](attachment:image.png)

**NOTE:** For Windows 2008, 2008R2 (32bit/64bit), Windows 7 (32bit/64bit), Microsoft.NET Framework 4.5.2 will be installed.

And for Windows 2008, 2008R2 (32bit/64bit), Windows 7 (32bit/64bit), Windows 8.1 and Windows 2012, PowerShell 3.0 will be installed.

Microsoft.NET Framework 4.5.2 Installation page displays.
After the .NET Framework 4.5.2 is installed, EventTracker Pre-Install Check message displays.

2. Click on Yes.

The Pre-Installer welcome window displays. For the detailed Pre-Installation Check process, please refer to Install Guide v 8.2 (Figure 68- Figure 106).

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

---

Figure 30

Figure 31
3. Click **Next >**.

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

4. 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.](image)

**Figure 32**

Select a Certificate File page displays.
5. To locate the path of the certificate file, click the **Browse** button.

   InstallShield Wizard displays the **Select File** window.

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

   InstallShield Wizard updates the folder path.
7. Click **Next >**.

   InstallShield[R] Wizard displays the **Select Components** screen.
8. Click the **Next >** button.

Select EventTracker Console Type page displays.
9. Select a console type (Standard/Collection Point/Collection Master).

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

   b. Enter Collection Master 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 Audit SnapShot** dialog box.
NOTE: Do not change the install path.

10. Select the Next > button.

11. Ready to Install the Program page displays. Click the Install button.
InstallShield Wizard installs the selected components. Migration Utility displays.
12. Click the **Next >** button.

![Migration Utility window](image)

**Figure 42**

13. Click the **Finish** button.

Basic Configuration window displays.
14. Select appropriate options, and then select the **OK** button.

InstallShield Wizard displays the last screen.
15. Click **Finish** to conclude the installation process.

   InstallShield Wizard displays the **EventTracker Configuration** screen.
16. 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.

17. Click the **OK** button.

**NOTE:**

If the password is changed for the above configured user, it is mandatory to re-run the EventTracker Configuration (Figure: 46) with the updated password.
i. To find ‘**EventTracker Configuration**’, select the **Start** button, select All **Programs**.

ii. Select **Prism Microsystems**, select **EventTracker**, and then select **EventTracker Configuration**.

iii. Enter appropriate credentials and then select the **OK** button.

**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, 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**.

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

EventTracker displays EventTracker Control Panel.

![EventTracker Control Panel](image-url)
3. Click **Export Import Utility** icon.
   
   EventTracker displays Export Import Utility window.

4. Click **Import** tab.

   ![Figure 49](image)

   **Figure 49**

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.

   ![Figure 50](image)

   **Figure 50**
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.

12. Click the OK button.

13. Click Alerts option.
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.

![Image of Export Import Utility window with RSS Feeds option selected]

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.

![Image of Export Import Utility success message box]

22. Click the **OK** button.

23. Select **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. Logon 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: My Category.

![Figure 58](image)

(OR)

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

![Figure 59](image)

Verify Alerts:

1. Click the **Admin** menu, and then click **Alerts**.
EventTracker displays **Alert Management** page.

![Alert Management Page](image)

Figure 60

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

![Alert Management Search](image)

Figure 61

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 62](image1)

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

EventTracker displays Event Filter configuration page.

![Figure 63](image2)

Verify Generated Reports:

Upon upgrade to version 8.x, the successfully generated reports from version 6.4 can be viewed in ‘Reports dashboard’ present under the Reports 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 dashboard tab.

1. Click the Reports tab, and click Dashboard.

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

![Figure 64](image)

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.

![Figure 67](image1.png)

**Figure 67**

(OR)

Select the ![icon](image2.png) icon corresponding to the remote systems name (where the agent is installed), and select **Upgrade Agent** from the dropdown list.

![Figure 68](image3.png)

**Figure 68**
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.

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

EventTracker displays confirmation message.
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 v8.2 ‘Trusted connection List’. This option will help you to update the trusted connection list.

1. Logon 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.

![Figure 78](image1)

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

![Figure 79](image2)

**NOTE:**

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

  ```plaintext
  ...Program Files\Prism Microsystems\EventTracker\Agent\spmConfig.ini
  ```
• 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.

  I. Click the Advanced button.

  EventTracker displays Upgrade Remote Agent(s) dialog box.

  ![Upgrade Remote Agent(s) dialog box](image)

  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. Logon to 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.

### Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.2.x

The upgrade procedure from v7.0/v7.1/v7.2 to v8.2 is the same as v7.6 to v8.2. The detail procedure is described in [Upgrade from v7.6.x to v8.2.x](#).

**NOTE:**

- Before upgrading, take a backup 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 v7.0/v7.1/v7.2 to v8.2, kindly run the executable file `Prism.AlertsMigration.exe` available in `\InstallDIR\EventTracker\Prism.AlertsMigration.exe`, for migrating the incidents.

### Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.2.x

The upgrade procedure from v7.3/v7.4/v7.5 to v8.2 is the same as v7.6 to v8.2. The detail procedure is described in [Upgrade from v7.6.x to v8.2.x](#).

**NOTE:**

- Before upgrading, please take a backup of the database and follow the instructions mentioned in [Upgrade from v7.6.x to v8.2.x](#).

  This is an alternate method to take a backup 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 v7.6.x to v8.2.x

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

- Before upgrading, please take a backup 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.

![Backup & Restore window](image)

Figure 83

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 v7.6**

1. Select the **Start** button, select **Settings**, and then select **Control Panel**.

2. Select **Add or Remove Programs**, select **EventTracker**, and then select the **Remove** button.
(OR)

Select the Start button, select Programs, and then select Prism Microsystems.

Select EventTracker, and then select Uninstall EventTracker.

EventTracker will display the confirmation message.

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

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

   EventTracker starts 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 v8.2 Enterprise**

For the details regarding installation process, please refer ‘**EventTracker v8.2 Enterprise Installation Guide**’.

**Step 3: Install EventTracker v8.2 Enterprise**

Kindly follow the steps mentioned below for upgrade process.

1. To install v8.2, launch **EventTrackerSetup.exe**.

   EventTracker Pre-Install Check displays below message.
NOTE:

- For Windows 2008, 2008R2 (32bit/64bit), Windows 7 (32bit/64bit), Microsoft.NET Framework 4.5.2 will be installed.
- And for Windows 2008, 2008R2 (32bit/64bit), Windows 7 (32bit/64bit), Windows 8.1 and Windows 2012, PowerShell 3.0 will be installed.

If Microsoft .NET Framework 4.5.2 is not installed, refer the Install Guide v8.2.

NOTE: If .NET 4.0 is already present, the pre-install check will not install .NET 4.5 and the user will have to manually install it.

2. Click the Yes button.

InstallShield Wizard displays the **Welcome** screen.
3. Click **Next >**.
   
   InstallShield Wizard displays the **License Agreement** screen.

4. 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.

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

6. Locate the file from the appropriate folder, and then select **Open**.
   
   InstallShield Wizard updates the folder path.
7. Click **Next >**.

InstallShield[R] Wizard displays the **Select Components** screen.

![Figure 93](image)

**Figure 93**

![Figure 94](image)

**Figure 94**
8. Click the **Next >** button.

Select EventTracker Console Type page displays.

![Figure 95](image)

9. Select a console type (**Standard/**Collection Point/**Collection Master**).

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

   e. Enter **Collection Master** details, click **Next >**.
f. Enter **Collection Master**: details, enable **Skip** option, and then click **Next >**.
(OR)

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

If you have selected **Change Audit** component, then InstallShield Wizard displays **Change Audit SnapShot** dialog box.

![Figure 98](image_url)

**NOTE:** Do not change the install path.

10. Select the **Next >** button.

11. **Ready to Install the Program** page displays. Select the **Install** button.
12. The installation process will start, with a message displaying “Please wait, Migration in Progress....”
Basic Configuration window displays.

![Basic configuration window](image)

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

InstallShield Wizard displays the last screen.
13. Click **Finish** to conclude the installation process.

InstallShield Wizard displays the **EventTracker Configuration** screen.
14. 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.

Figure 105

15. Click the OK button.

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

Click ‘Configure the service accounts’ section.

Import the newly added Behavior Rules after upgrade:

(This is common for all the upgrades from older versions to v8.2)

- After upgrading to v8.2, the user has to import the newly added behavior rules using the Export Import Utility. The newly added behavior rules are kept in the Install directory, i.e. <Install folder>\EventTracker\Configuration Files...

- To import the newly added Behavior rule, go to Export Import Utility>Select Import> click the Behavior Rule option> browse the behavior rule file (.isrule) from the configuration files folder.

Figure 116
Step 6: Import the Safe List

- Go to Admin > Active Watch List.
- Click the Safe List under Processes.
- Click the Import icon.

Browse the .csv file from <Install folder>\EventTracker\Configuration Files\KnownProcess_MD5_details.csv
• The list will be retained after importing.
Step 7: Verify that the Categories, Alerts, Filters, and RSS Feeds are intact

**Verify Category:**

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

![Alert Management](image1)

Figure 122

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.

![Event Filters](image2)

Figure 123

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 8: Upgrade all Windows agents using the System manager

**NOTE:** After upgrading from the earlier versions, if the user wants the newly added agent filter settings available in EventTracker 8.2 (Build 14), please refer to the section “Using the Default Agent Filters in EventTracker version 8.2” to upgrade the remote agents. If not, please follow the below mentioned steps:

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

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

(OR)

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

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.
If the remote agent is in some other non trusted domain or the remote system is not accessible using Windows file sharing, then select the **Upgrade over IP (Non Windows Domain)** option.

6. Check **Install default Remedial Action EXEs on this system** option to install remedial action scripts.

   EventTracker displays a message box.
Remedial Actions are scripts or executable files that can be launched at either the agent or the manager side, in response to events. If this option is enabled, predefined scripts will be placed in the EventTracker\Agent\Script folder at the manager side. These may be installed at the agent side also, during deployment via the System manager.

7. Click OK to install remedial action EXEs

(OR)

Click Cancel to not to install remedial action EXEs.

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

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

Figure 135

10. Click the OK button.

EventTracker displays System Status screen.

Figure 136
11. Click the button, to see the latest status.

![Figure 137](image)

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

**Step 10:**

As the menu options have been changed, the **User Privileges** configuration won’t be retained after upgrade to v8.2 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) Select **Assign Privileges** from the dropdown list by clicking the icon.

![Figure 138](image)

EventTracker displays the Add Privileges window.

c) Select required field and click **OK**.
Step 11: Import Knowledge Objects after upgrade

1. Logon to EventTracker Enterprise.

2. To import Knowledge Objects, select the Admin menu, and then select Knowledge Objects.

3. Select the Import icon.

   EventTracker Knowledge Objects Import/Export window displays.

4. Select the Browse… button and then select the file from desired location.

   **NOTE:** The file extension should be ‘.etko’ only. The default knowledge object is available in \InstallDIR\EventTracker\Configuration Files\DefaultKnowledgeObject.etko. And individual knowledge Object files are also available and the user can import them as per requirement.
5. Select the **Open** button.

6. Select the **Upload** button.

7. To upload knowledge objects, select the **Object name** option.
8. Select the **Merge/OverWrite** button as per the requirement.

**NOTE:**

- After upgrading from v7.5/v7.6/v8.0 to v8.2, the user will first have to import the new Token templates (with the extension .ettd) from the.. install DIR\Program Files\Prism Microsystems\EventTracker\Configuration Files and then import the newly available Defined Reports (with the extension .issch) from the same path.

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

**Configure Service Accounts**

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

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

2. Configure the same with a user who has full permissions to access the shared archives folder.
** "Karen" has full permissions to access the archives UNC path.

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

1. Select the **Start** button, and then select **Run**.

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

![Figure 142](image)

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

![Figure 143](image)

4. Right click the service name, and click **Properties**.

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

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 146

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 147

Using the Default Agent Filters in EventTracker version 8.2

In the EventTracker version 8.2 (Build 9), we have added some default agent filters. Now if the user has multiple Virtual Collection Points (VCPs) and wants to use the default agent filters, follow the steps mentioned below:

NOTE: Before making the agent configuration changes, please note down the manager name and also the port number.

Step 1: Go to Event Tracker Control Panel and select the EventTracker Agent Configuration.

Step 2: Go to File option and select Load a Template from the dropdown list.
Step 3: Select the `etaconfig.ini` file from `install DIR\Program Files\Prism Microsystems\EventTracker\Configuration Files` and click **Open**.
Figure 148

The below message gets displayed:

Figure 149

Step 4: Click Yes to continue.

Step 5: Now, in the Manager tab, click the Add button to add the manager name with the default port, i.e. 14505.
The Add Destination window displays. Add the Manager name and click **OK**.
Step 6: Now, in the **File Transfer** tab, add the manager name and port by clicking the **Add** button.

In the DLA Manager window, add the manager name and then click **OK**.
Step 7: Go to File-> License Server, add the License Server name as Manager Name, which is already added in the agent configuration.

Here we have taken “MCLOUD-II” as the Manager Name.

Step 8: Now, go to the File option and click Save option from the dropdown list for saving the configuration changes.
NOTE: The previous etaconfig.ini file will not be retained after replacing it with the new custom configuration file. So make sure you have a copy of the existing configuration file, if you have made changes in the agent configuration.

Step 9: Now, make sure that the new etaconfig.ini file is copied both in the Remote Installer folder and the Agent Folder in the installation path.

For example: install DIR\Program Files\Prism MicroSystems\EventTracker\RemoteInstaller folder.

And install DIR\Program Files\Prism MicroSystems\EventTracker\Agent

In case, the user wants to use multiple VCPs for deploying agents with a different port number. (For e.g.: Port Number 14515)

1. Go to the EventTracker Agent Configuration window.
2. Go to the File option and select Load a template option from the dropdown list.
3. In the Manager tab, click the edit button to add the port number: 14515.
1. Click the **File Transfer** tab and change the port number to 14515.

![Figure 158](image)

**Figure 158**

4. Now for saving the changes made, go to **File** option and click **Save As**.

5. Enter a custom configuration name for the file and save it in the install DIR \Program Files\Prism MicroSystems\EventTracker\RemoteInstaller.

![Figure 159](image)

**Figure 159**
6. Click the **Save** button.

Now, to upgrade the agent, login to the EventTracker web.

1. Click on **Admin** Dropdown and select **Systems**.
2. Search the system and select Upgrade Agent from the dropdown list.

![Figure 160](image1.png)

The Upgrade Remote Agent(s) window displays.

3. Check the Agent type option that you wish to upgrade.

![Figure 161](image2.png)
4. Click the **Next** button.

5. Select the Windows Domain Network option and enter the user credentials.

![Upgrade Remote agent(s)](image)

**Figure 162**

6. Click the **Advanced** button.

In the Apply Configuration page, select the **custom config** option and select the custom configuration file from the dropdown list.
7. Click the Upgrade button.

**NOTE:** If you follow the above steps mentioned, the default configuration settings will be overwritten by the custom configuration settings selected.

**Upgrade from v8.0.x/v8.1.x to v8.2.x**

The upgrade procedure from v8.0/v8.1 to v8.2 is the same as v7.6 to v8.2. The detail procedure is described in [Upgrade from v7.6.x to v8.2.x](#).

**NOTE:**

- For upgrading from **v8.0.x/v8.1.x to v8.2.x**, the user will not have to follow the section “Using the Default Agent Filters in EventTracker version 8.2” as the default agent filters will already be available in v8.0/v8.1.
- For upgrading from **v8.0/v8.1 to v8.2**, the user need not import any of the Behavior Rules.
• Before upgrading, please take a backup of the database and follow the instructions mentioned in Upgrade from v7.6.x to v8.2.x.

This is an alternate method to take a backup 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.