EventTracker Upgrade Guide
Upgrade to v8.1
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 v8.0 who wish to upgrade to v8.1 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.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

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

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

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

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

New Categories/Alerts/Reports available in v8.1................................................................. 4
Prerequisites.......................................................................................................................... 12
Planning............................................................................................................................... 12
Upgrade - Quick View.......................................................................................................... 13
  Common steps for all upgrades ....................................................................................... 13
  Upgrade from v6.4.x to v8.1.x......................................................................................... 15
    Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.1.x................................................................. 20
    Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.1.x................................................................. 20
    Upgrade from v7.6.x to v8.1.x..................................................................................... 20
    Upgrade from v8.0.x to v8.1.x..................................................................................... 20
Upgrade - Detailed View..................................................................................................... 20
  Upgrade from v6.4.x to v8.1.x......................................................................................... 20
    Upgrade Procedure ....................................................................................................... 29
    Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.1.x................................................................. 69
    Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.1.x................................................................. 69
    Upgrade from v7.6.x to v8.1.x..................................................................................... 70
      Import the newly added Behavior Rules after upgrade: ......................................... 89
Configure Service Accounts............................................................................................... 105
Using the Default Agent Filters in EventTracker version 8.1............................................. 109
  Upgrade from v8.0.x to v8.1.x......................................................................................... 120
New Categories/Alerts/Reports available in v8.1

The details about new categories/alerts/reports available in EventTracker v8.1 is mentioned below.

**NOTE:** For Fortigate, the user will have to delete the old (Categories, Alerts, Flex Reports, Parsing Rules (.istoken) and Knowledge Objects), and will have to Import the new configuration files.

**New Categories**

- Barracuda Spam Firewall: Configuration changes
- Barracuda Spam Firewall: Firewall received messages
- Barracuda Spam Firewall: Firewall scan messages
- Barracuda Spam Firewall: Firewall sending messages
- Barracuda Spam Firewall: Login and logout activity
- EZproxy: Audit log purged
- EZproxy: System startup/shutdown
- FortiGate(4.0): Activex script removed
- FortiGate(4.0): Admin account locked
- FortiGate(4.0): Admin account timed out
- FortiGate(4.0): Admin Logon Fail
- FortiGate(4.0): Admin Logon Success
- FortiGate(4.0): Anomaly attack detected
- FortiGate(4.0): App control log message
- FortiGate(4.0): Content type blocked
- FortiGate(4.0): CPU usage is high
- FortiGate(4.0): Daily quota status
- FortiGate(4.0): Data leak detected
- FortiGate(4.0): DHCP statistics
- FortiGate(4.0): Endpoint filter detected
- FortiGate(4.0): Firewall traffic accepted
- FortiGate(4.0): Firewall traffic deny
- FortiGate(4.0): Firewall traffic time out
- FortiGate(4.0): FortiGuard service inactive
- FortiGate(4.0): HA group deleted
- FortiGate(4.0): Infected file found
- FortiGate(4.0): Infection detected
- FortiGate(4.0): IPsec connection failure
- FortiGate(4.0): IPsec connection status changed
- FortiGate(4.0): IPsec DPD failure
- FortiGate(4.0): IPsec ESP transform success
- FortiGate(4.0): IPsec phase 1 SA delete
- FortiGate(4.0): IPsec phase 2 SA delete
- FortiGate(4.0): IPsec SA install
- FortiGate(4.0): L2tp client connection finished
- FortiGate(4.0): L2tp settings changed
- FortiGate(4.0): Memory Log is full
- FortiGate(4.0): Negotiate IPsec phase 1 error
- FortiGate(4.0): Negotiate IPsec phase 2 error
- FortiGate(4.0): Oversized content detected
- FortiGate(4.0): Performance statistics
- FortiGate(4.0): POP3 spam detected
- FortiGate(4.0): PPPD authentication failed
- FortiGate(4.0): Quota counting
- FortiGate(4.0): Scan error detected
- FortiGate(4.0): SCCP call end
- FortiGate(4.0): SCCP call failed
- FortiGate(4.0): SCCP call info
- FortiGate(4.0): SCCP call timeout
- FortiGate(4.0): SCCP register
- FortiGate(4.0): SCCP unregister
- FortiGate(4.0): Signature attack detected
- FortiGate(4.0): SMTP spam detected
- FortiGate(4.0): Spam IMAP detected
- FortiGate(4.0): Spam MM1 duplicate detected
- FortiGate(4.0): SSL-VPN session discarded
- FortiGate(4.0): SSL timeout
- FortiGate(4.0): SSL tunnel established
- FortiGate(4.0): SSL tunnel shutdown
- FortiGate(4.0): SSL VPN user login failed
- FortiGate(4.0): SSL Web app activated
- FortiGate(4.0): SSL web app blocked
- FortiGate(4.0): SSL web app closed
- FortiGate(4.0): Switching protocols
- FortiGate(4.0): System configuration is changed
- FortiGate(4.0): System entered conserve mode
- FortiGate(4.0): Url filter block
- FortiGate(4.0): Virtual cluster deleted
- FortiGate(4.0): Virtual cluster member dead
- FortiGate(4.0): WAN optimization traffic
- FortiGate(4.0): Web script filter
- FortiGate(4.0): Webfilter category allow
- FortiGate(4.0): Webfilter category block
- FortiGate(4.0): Webfilter error
- FortiGate(5.0): AntiVirus
• FortiGate(5.0): Application control
• FortiGate(5.0): DLP
• FortiGate(5.0): Email Filter
• FortiGate(5.0): EndPoint Control
• FortiGate(5.0): GTP
• FortiGate(5.0): High Availability
• FortiGate(5.0): IPS
• FortiGate(5.0): Router
• FortiGate(5.0): System
• FortiGate(5.0): User
• FortiGate(5.0): VPN
• FortiGate(5.0): WAN
• FortiGate(5.0): Web Filter
• FortiGate(5.0): Wireless
• FortiGate: All events
• FortiGate(5.0): Traffic Allowed or Denied
• FortiGate(4.0): PPTP maximum connection reached
• FairWarning: All alerts
• HP ProCurve: Console session established
• HP ProCurve: Security violation detected
• HP ProCurve: System authentication failed
• HP ProCurve: System configuration changed
• HP ProCurve: User logon failed
• PhoneFactor: Authentication failure
• PhoneFactor: Authentication success
• PhoneFactor: User configuration
• SonicWALL Firewall: VPN client activity
• SonicWALL Firewall: VPN IPSec tunnel status changed
• SonicWALL Firewall: VPN PKI error
• SonicWALL Firewall: VPN IKE activity
• SonicWALL Firewall: VPN IPsec activity
• Terminal Services: Connection broker
• Terminal Services: Desktop session host
• Terminal Services: Gateway

New Alerts

• Barracuda Spam Firewall: Configuration changes
• Barracuda Spam Firewall: Mail contains virus
• Barracuda Spam Firewall: Spam mails
• Cyberoam UTM: Admin operations
• Cyberoam UTM: User authentication failed
• EventTracker: New process MD5 hash activity
• EventTracker: Unknown MD5 hash detected
• EventTracker: Unsafe MD5 hash detected
• EventTracker: Product license expired
• EventTracker: Non reporting system with high asset value from last 24 hours
• EventTracker: Non reporting system with low asset value from last 24 hours
• FortiGate: Attack detected
• FortiGate: Configuration changed
• FortiGate: Virus detected
• HP ProCurve: System authentication failed
• HP ProCurve: User logon failed
• Infoblox: High CPU usage detected
• Infoblox: High disk usage detected
• Infoblox: High memory usage detected
• MSSQL: Sysadmin role assigned
• MSSQL: User created
• MSSQL: User deleted
• MSSQL: User modified
• MSSQL: User role changed
• PhoneFactor: Authentication fails
• PhoneFactor: User configuration changes
• SonicWALL Firewall: VPN User authentication failed
• Terminal Services: Licensing error
• Terminal Services: Remote desktop service start failed
• Terminal Services: TS gateway service is shutting down
• Terminal Services: failed to load TS profile path
• Juniper Netscreen: VPN service down
• Juniper Netscreen: IP address conflict
• Linux: Action taken by user with admin privileges
• Linux: Audit configuration changes
• Linux: Audit log stop
• Linux: Creation and deletion of system level objects
• Linux: Elevation of privileges

New Flex Reports
• Barracuda Spam Firewall-Login and logout activity
• Barracuda Spam Firewall-Login failed activity
• Barracuda Spam Firewall-Configuration changes
• Barracuda Spam Firewall-Blocked messages
• Barracuda Spam Firewall-Allowed messages
• Barracuda Spam Firewall-Message contains virus
- Barracuda Spam Firewall-Spam mails
- Barracuda Spam Firewall-Quarantined message
- Cyberoam UTM-User authentication success
- Cyberoam UTM-User authentication failed
- Cyberoam UTM-Firewall traffic allowed and denied
- Cyberoam UTM-Application and web filtering
- Cyberoam UTM-Antivirus activity
- Cyberoam UTM-Antispam activity
- Cyberoam UTM-User account management
- Cyberoam UTM-Admin operations
- Centrify Unix Agent-Adclient agent started and stopped
- Centrify Unix Agent-PAM authentication status
- Centrify Unix Agent-Session status
- Check Point-User VPN logon failure
- Check Point-User VPN logon success
- Check Point-Management station logon success
- Check Point-Management station logout
- Check Point-Management station logon failed
- Check Point-Object creation deletion or modification
- Check Point-Firewall policy changed
- Check Point-All IPS event details
- Check Point-Firewall traffic accepted
- Check Point-Firewall traffic denied
- Check Point-User VPN session details
- Check Point-SMTP traffic accept and drop
- Check Point-FTP traffic accept and drop
- Check Point-Web activity[HTTP and HTTPS]
- Check Point-Network activity
- Check Point-Firewall activity
- Check Point-Peer to Peer activity
- Cisco ASA-Connection denied
- Cisco ASA-Outbound traffic denied
- Cisco IOS-Port status change
- Cisco IOS-Access denied
- Cisco IOS-Configuration changed
- Cisco IOS-User logon failure
- Cisco IOS-User logon success
- BIG-IP LTM-User account management details
- BIG-IP LTM-System configuration changed
- BIG-IP LTM-User logon success details
- BIG-IP LTM-User logon failure details
- EventTracker-Bad IP Reputation network activity
- Linux-Account operation
- Linux-Audit configuration changes
- Paloalto firewall-VPN login activity
• Paloalto firewall-VPN logoff activity
• Paloalto firewall-VPN authentication
• Paloalto firewall-VPN configuration succeed
• EventTracker-Unsigned exe launched
• EventTracker-New unique hash process activity
• EventTracker-New windows software install activity
• EventTracker-New windows applications activity
• EventTracker-New USB started activity
• EventTracker-New windows runaway process activity
• EventTracker-New windows network activity
• EventTracker-New windows process activity
• EventTracker-New windows network processes activity
• EventTracker-New windows user location affinity activity
• EventTracker-New windows logon activity
• EventTracker-New windows interactive logon activity
• EventTracker-New windows logon failure activity
• EventTracker-New windows network connections activity
• EventTracker-New windows audit policy and account management
• FortiGate (For FortiOS 4.0)-Attack detected
• FortiGate (For FortiOS 4.0)-Traffic denied
• FortiGate (For FortiOS 4.0)-Virus detected
• FortiGate (For FortiOS 4.0)-Suspicious email content detected
• FortiGate (For FortiOS 4.0)-Administrator logon details
• FortiGate (For FortiOS 4.0)-Configuration change details
• FortiGate (For FortiOS 4.0)-VPN logon details
• FortiGate (For FortiOS 4.0)-Data leak detected
• FortiGate (For FortiOS 4.0)-Traffic allowed
• FortiGate (For FortiOS 4.0)-Suspicious web content detected
• FortiGate (For FortiOS 5.0 or later)-Traffic denied
• FortiGate (For FortiOS 5.0 or later)-Traffic allowed
• FortiGate (For FortiOS 5.0 or later)-Virus detected
• FortiGate (For FortiOS 5.0 or later)-Data leak detected
• FortiGate (For FortiOS 5.0 or later)-Suspicious email content detected
• FortiGate (For FortiOS 5.0 or later)-Suspicious web content detected
• FortiGate (For FortiOS 5.0 or later)-Attack detected
• FortiGate (For FortiOS 5.0 or later)-Configuration change details
• FortiGate (For FortiOS 5.0 or later)-Administrator logon details
• FortiGate (For FortiOS 5.0 or later)-VPN logon details
• FortiGate (For FortiOS 5.0 or later)-User authentication details
• FortiGate (For FortiOS 4.0)-User authentication details
• MSSQL-User created
• MSSQL-User deleted
• MSSQL-User role changed
• MSSQL-User modified
• SonicWALL Firewall-VPN user authentication success
- SonicWALL Firewall-VPN activity
- SonicWALL Firewall-VPN IPSec tunnel status changed
- SonicWALL Firewall-VPN User authentication failed
- Terminal Services-Gateway server configuration success
- Terminal Services-Gateway server configuration failure
- Terminal Services-Gateway server connections success
- Terminal Services-Gateway server connections failure
- Terminal Services-Web access configuration
- Terminal Services-Desktop session host activity
- Terminal Services-Load balancing
- Terminal Services-IP virtualization
- Terminal Services-Connection and session manager activity
- Terminal Services-User activity
- Terminal Services-Logon activity
- EZproxy-Allowed traffic details
- EZproxy-Denied traffic details
- EZproxy-User logon success details
- EZproxy-Intrusion details
- EZproxy-User logon failure details
- FairWarning-HIPAA category based alerts
- FairWarning-Policy compliance category based alerts
- FairWarning-FTC category based alerts
- FairWarning-Identity theft
- FairWarning-All alert report
- HP ProCurve-Port status change details
- HP ProCurve-Security violation details
- HP ProCurve-User logon details
- Infoblox-User logon success details
- Infoblox-Blacklist ruleset management details
- Infoblox-Administrative user management details
- Infoblox-User logon failure details
- PhoneFactor-Authentication failed
- PhoneFactor-Authentication succeeded
- PhoneFactor-User configuration changes

**Updated Knowledge Packs:**

**Updated Alerts:**

- Cyberoam UTM: Attack Detected
- Cyberoam UTM: Spam Detected
- Cyberoam UTM: Virus Detected
- FortiGate: Administrator Logon Failed
Updated Categories:

- Windows Audit Log Clear

Updated Flex Reports:

- Clavister-User Authentication Failed
- MySQL-Authentication Failed
- MySQL-Authentication Success
- MySQL-Database Management
- MySQL-Database Query Log Detail
- MySQL-Privileges Change
- MySQL-Table Management
- Windows-Application Crash Analysis
- Windows-User Account Locked
- EventTracker-Bad IP Reputation network activity
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 v8.1.x Enterprise
• Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.1.x Enterprise
• Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.1.x Enterprise
• Upgrade from v7.6.x to v8.1.x Enterprise
• Upgrade from v8.0.x to v8.1.x Enterprise

NOTE:

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 v8.1, 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 v8.1.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 v8.1, make sure that .NET 4.5 is installed. If Microsoft .NET Framework 4.5.2 is not installed, refer the Install Guide v8.1.

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 v8.1 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

Select SQL Instance

Currently logged in user and the system's administrator group do not have necessary permissions on SQL Instance 'EVENTTRACKER'.

Please make sure the logged in user is having sysadmin permission on the SQL Instance '\EVENTTRACKER' before continuing the installation.

Do you want to continue?

Yes No

Figure 1

After Upgrade process:

If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v8.1. 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 v8.1 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 v8.1, 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 v8.1.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 v8.1.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 v8.1, kindly run the executable file ‘**Prism.AlertsMigration.exe**’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.
   - For v6.4 to v8.1 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 to v8.1.x

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

   ![EventTracker Pre-Install Check](image)

   **Figure 2**

2. Restart the EventTracker manager server or system.

3. Install EventTracker v8.1.

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 v8.1.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 v8.1, 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 3](image)

A message displays.

![Figure 4](image)

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

![Available Dashlets window displays.](image)

f. Select and Add the required dashlets.

![Figure 6](image)

- After upgrading, if the collection master is v8.1, and if collection point is using any older version of EventTracker, then incidents will not be visible. If you upgrade collection point to v8.1, post upgrade incidents will only be transferred to collection master.

- The keyword dashboard has to be customized after upgrading to v8.1.

- 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](http://scn.sap.com/docs/DOC-7824).
On upgrade from 7.x to 8.1 the user has to export the alerts and category and he/she has to import the complete alerts and category from configuration files. Later the user has to import the alerts and category which he/she has exported on previous version.

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.

![Figure 8](image)
Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.1.x

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

After upgrading from v7.0.x/v7.1.x/v7.2.x to v8.1.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 v8.1.x

The procedure to upgrade from v7.3.x/v7.4.x/v7.5.x to v8.1.x is same like upgrade from v7.6.x to v8.1.x.

Upgrade from v7.6.x to v8.1.x

The procedure to upgrade from v7.6.x to v8.1.x is mentioned in the detail section.

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

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

Upgrade - Detailed View

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

- Upgrade from v6.4.x to v8.1.x Enterprise
- Upgrade from v7.0.x/v7.1.x/v7.2.x to v8.1.x Enterprise
- Upgrade from v7.3.x/v7.4.x/v7.5.x to v8.1.x Enterprise
- Upgrade from v7.6.x to v8.1.x Enterprise
- Upgrade from v8.0.x to v8.1.x Enterprise

Upgrade from v6.4.x to v8.1.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).
Figure 10

(OR)

Click **Add All** button to select all the categories.

5. Click the **Export** button.

EventTracker displays **Select Export File** window.

Figure 11

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

EventTracker displays confirmation message box.

![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**

   ![Figure 14](image)

   (OR)

   Click **Add All >>** button to select all the Alerts.

12. Click the **Export** button.

   EventTracker displays the **Select Export File** window.

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

   EventTracker displays confirmation message box.

14. Click the **OK** button.

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

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

Example: My Reports

EventTracker displays confirmation message box.

17. Click the **OK** button.

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

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

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

   EventTracker displays confirmation message box.

20. Click the **OK** button.

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

21. Click the **Close** button, to close the Export Import Utility window.

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

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

   EventTracker displays EventTracker Control Panel.

3. Click **Agent Configuration** icon.

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

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

![Figure 21](image)

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

**Close/terminate all the EventTracker Components**

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

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

EventTracker resumes uninstall process.

Upgrade Procedure

**Step 1: Uninstall the version 6.4.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.

   (OR)

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

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

   EventTracker displays the confirmation message.
3. Click the **Yes** button.

EventTracker starts the uninstall process.

![Windows Installer dialog box](image)

**Figure 24**

EventTracker displays the 'Uninstall EventTracker' confirmation message.

![EventTracker uninstall confirmation message](image)

**Figure 25**

4. Click the **No** button.

EventTracker displays the 'Uninstall EventTracker' dialog box.
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 Sh**ut Down**.
3. Select the **Restart** option from the dropdown, and then click the **OK** button.

**Step 3: Install EventTracker v8.1 Enterprise**

Kindly follow the steps mentioned below for upgrade process.

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

   EventTracker will Extract the files

   ![Extracting files](image)

   **Figure 28**

   **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.

![Installation Progress](image)

**Figure 29**

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

![EventTracker Pre-Install Check](image)

**Figure 29**

2. Click on Yes.
The Pre-Installer welcome window displays. For the detailed Pre-Installation Check process, please refer to Install Guide v 8.1 (Figure 68- Figure 106).

EventTracker - Install Shield Wizard displays.

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.

Figure 32
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.
10. Select the **Next >** button.

   Ready to install the Program page displays.

11. Select **Install Remedial Action EXEs on this machine** option, and then select the **Install** button.
InstallShield Wizard installs the selected components. Migration Utility displays.
12. Click the **Next >** button.
13. Click the **Finish** button.

Basic Configuration window displays.

![Basic configuration dialog box](image)

**Figure 43**

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

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

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

   InstallShield Wizard displays the **EventTracker Configuration** screen.
17. 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.

18. Click 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)

   **Figure 48**

3. Click Export Import Utility icon.

   EventTracker displays Export Import Utility window.
4. Click **Import** tab.

5. Click **Category** (If not selected).

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

7. Click the **Import** button.

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

8. Click the **OK** button.

9. Select **Filters** option.
10. Click the browse button, select the location of the file, and click the Open button.

11. Click the Import button.

EventTracker displays Export Import Utility success message box.

![Figure 51](image-url)

12. Click the OK button.

13. Click Alerts option.

![Figure 52](image-url)

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

15. In the Set Active pane, select the appropriate option.
16. Click the **browse** button, select the location of the file, and click the **Open** button.

17. Click the **Import** button.

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

18. Click the **OK** button.

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

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

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

![Figure 55](image)

22. Click the **OK** button.

23. Select **Scheduled Reports** option.

![Figure 56](image)

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.

   ![Category Management](Figure 58)

(OR)

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

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

   EventTracker displays **Alert Management** page.

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

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

EventTracker displays Event Filter configuration page.
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.
Verify RSS Feeds:

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

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

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

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

Select the icon corresponding to the remote systems name (where the agent is installed), and select **Upgrade Agent** from the dropdown list.
EventTracker displays **Upgrade Remote Agent(s)** pop-up window.

![Image of Upgrade Remote Agent(s) pop-up window]

**Figure 69**

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

![Image of upgraded agent(s) with selected agent]

**Figure 70**

5. Select **Windows Domain Network** option, and enter user credentials,
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.
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 v8.1 ‘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.

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

- 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.
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 v8.1.x

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

The upgrade procedure from v7.3/v7.4/v7.5 to v8.1 is the same as v7.6 to v8.1. The detail procedure is described in [Upgrade from v7.6.x to v8.1.x](#).

**NOTE:**

- Before upgrading, please take a backup of the database and follow the instructions mentioned in [Upgrade from v7.6.x to v8.1.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 v8.1.x

- Please refer to 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)

  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.

   ![Add or Remove Programs](image1)
   
   **Figure 84**

   (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.

   ![Windows Installer](image2)
   
   **Figure 85**

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.

   ![Uninstall EventTracker Dialog Box](image)

   **Figure 87**

   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 v8.1 Enterprise**

For the details regarding installation process, please refer [EventTracker v8.1 Enterprise Installation Guide](#).
Step 3: Install EventTracker v8.1 Enterprise

Kindly follow the steps mentioned below for upgrade process.

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

EventTracker Pre-Install Check displays below message.

![EventTracker Pre-Install Check](image)

**Figure 88**

**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 v8.1.

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

Select EventTracker Console Type page displays.
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 >**.
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.
10. Select the Next > button.

Ready to install the Program page displays.

11. Select Install Remedial Action EXEs on this machine option, and then select the Install button.
12. The installation process will start, with a message displaying ‘Please wait, Migration in Progress.....’
Basic Configuration window displays.

Figure 100
12. Select appropriate options, and then select the **OK** button.

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

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

InstallShield Wizard displays the *EventTracker Configuration* screen.
15. 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.

16. Click the **OK** button.

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

Import the newly added Behavior Rules after upgrade:

(This is common for all the upgrades from older versions to v8.1)

- After upgrading to v8.1, 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.

![Image showing the Export Import Utility and ISRULE files](image.png)

**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`
Step 7: Configure the service accounts, if the archives/reports are stored in the network path

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

Step 8: 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

   ![Category Management Page](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 menu, and then 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** menu, and click **Event Filters**.

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

EventTracker displays **Event Filter configuration** page.

Verify RSS Feeds:

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

EventTracker displays **RSS Feeds** page. The newly imported RSS Feeds are listed in this page.
Step 9: 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 8.1 (Build __), please refer to the section “Using the Default Agent Filters in EventTracker version 8.1” 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.
### Option

<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 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.

(OR)

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

EventTracker displays a message box.

![Message from webpage](image)

This feature permits the execution of scripts on agent systems. Carefully review the risks and benefits before enabling this feature. Are you sure?

**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.

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

**Figure 134**

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.

![Figure 135](image)

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

![Figure 136](image)

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

![Figure 137](image)

**Step 10:**

- As the menu options have been changed, the **User Privileges** configuration won’t be retained after upgrade to v8.1 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**

EventTracker displays the Add Privileges window.

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

---

**Figure 139**
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.

![Figure 141](image)

8. Select the **Merge/OverWrite** button as per the requirement.

**NOTE:**

- After upgrading from v7.5/ v7.6 /v8.0 to v8.1, 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’.

![Figure 142](image)

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

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

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

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

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

![Services Window](image)

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.

![Service Configuration](image)

Figure 152

### Using the Default Agent Filters in EventTracker version 8.1

In the EventTracker version 8.1 (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.

![EventTracker Agent Configuration](image)

*Figure 147*

Step 3: Select the `etaconfig.ini` file from `install DIR\Program Files\Prism MicroSystems\EventTracker\Configuration Files` and click **Open**.
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.

![Figure 153](image)

**Step 7:** Go to File-> License Server, add the License Server name as Manager Name, which is already added in the agent configuration.

![Figure 154](image)

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

![Figure 155](image)
Step 8: Now, go to the **File** option and click **Save** option from the dropdown list for saving the configuration changes.

![EventTracker Agent Configuration](image)

**Figure 156**

**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.

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**.
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.
The Upgrade Remote Agent(s) window displays.

3. Check the Agent type option that you wish to upgrade.
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 to v8.1.x

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

**NOTE:**

- For upgrading from **v8.0.x to v8.1.x**, the user will not have to follow the section “**Using the Default Agent Filters in EventTracker version 8.1**” as the default agent filters will already be available in v8.0.
• For upgrading from v8.0 to v8.1, 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 v8.1.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.