Introduction

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

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

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

Audience:

It is incumbent upon all users of EventTracker v6.4 to v7.6 who wish to upgrade to v8.0 Enterprise. Prism strongly recommends that you read the entire document thoroughly before you begin the upgrade process. For the user’s convenience, this document is separated in two parts: ‘Upgrade- Quick View’ and ‘Upgrade- Detailed View’.

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

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

Before you upgrade:

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

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

*IMPORTANT:

Users of versions ‘v.6.4 (Build 50)’ and below contact support@eventtracker.com for complete and thorough instructions.
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.

© 2015 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 v8.0............................................................. 4
Prerequisites.................................................................................................................. 25
Planning......................................................................................................................... 25
Upgrade - Quick View................................................................................................. 26
  Upgrade from v6.4.x to v8.0.x.................................................................................. 27
  Common steps for all upgrades ............................................................................ 28
    Upgrade from v7.0.x to v8.0.x............................................................................ 33
    Upgrade from v7.1.x to v8.0.x............................................................................ 34
    Upgrade from v7.2.x to v8.0.x............................................................................ 34
    Upgrade from v7.3.x to v8.0.x............................................................................ 34
    Upgrade from v7.4.x to v8.0.x............................................................................ 34
    Upgrade from v7.5.x to v8.0.x............................................................................ 34
    Upgrade from v7.6.x to v8.0.x............................................................................ 34
Upgrade - Detailed View............................................................................................. 34
  Upgrade from v6.4.x to v8.0.x................................................................................ 35
  Upgrade Procedure ............................................................................................... 44
    Upgrade from v7.0.x to v8.0.x............................................................................ 85
    Upgrade from v7.1.x to v8.0.x............................................................................ 85
    Upgrade from v7.2.x to v8.0.x............................................................................ 85
    Upgrade from v7.3.x to v8.0.x............................................................................ 86
    Upgrade from v7.4.x to v8.0.x............................................................................ 86
    Upgrade from v7.5.x to v8.0.x............................................................................ 87
    Upgrade from v7.6.x to v8.0.x............................................................................ 87
Configure Service Accounts....................................................................................... 105
Using the Default Agent Filters in EventTracker version 8.0................................. 109
New Categories/Alerts/Reports available in v8.0

The details about new categories/alerts/reports available in EventTracker v8.0 is mentioned below.

New Categories

- AWS CloudWatch: Alarm action disabled
- AWS CloudWatch: Alarm action enabled
- AWS CloudWatch: Alarm history described
- AWS CloudWatch: Alarm state set
- AWS CloudWatch: Alarms deleted
- AWS CloudWatch: Alarm described
- AWS CloudWatch: Metric alarm described
- AWS CloudWatch: Put metric alarm
- AWS EC2: Account attribute described
- AWS EC2: Availability zone described
- AWS EC2: Bundle task cancelled
- AWS EC2: Bundle task described
- AWS EC2: Conversion task cancelled
- AWS EC2: Conversion task described
- AWS EC2: Customer gateway created
- AWS EC2: Customer gateway deleted
- AWS EC2: Customer gateway described
- AWS EC2: DHCP option associated
- AWS EC2: DHCP option created
- AWS EC2: DHCP option deleted
- AWS EC2: DHCP option described
- AWS EC2: Image attribute described
- AWS EC2: Image attribute modified
- AWS EC2: Image attribute reset
- AWS EC2: Image copied
- AWS EC2: Image created
- AWS EC2: Image deregistered
- AWS EC2: Image described
- AWS EC2: Image registered
- AWS EC2: Instance attribute described
- AWS EC2: Instance attribute modified
- AWS EC2: Instance attribute reset
- AWS EC2: Instance bundled
- AWS EC2: Instance described
• AWS EC2: Instance imported
• AWS EC2: Instance monitored
• AWS EC2: Instance rebooted
• AWS EC2: Instance started
• AWS EC2: Instance status
• AWS EC2: Instance stopped
• AWS EC2: Instance terminated
• AWS EC2: Instance unmonitored
• AWS EC2: Internet gateway attached
• AWS EC2: Internet gateway created
• AWS EC2: Internet gateway deleted
• AWS EC2: Internet gateway described
• AWS EC2: Internet gateway detached
• AWS EC2: IP address allocated
• AWS EC2: IP address associated
• AWS EC2: IP address described
• AWS EC2: IP address disassociated
• AWS EC2: IP address released
• AWS EC2: Key pair created
• AWS EC2: Key pair deleted
• AWS EC2: Key pair described
• AWS EC2: Key pair imported
• AWS EC2: Network ACLs activity
• AWS EC2: Network interface attached
• AWS EC2: Network interface attribute described
• AWS EC2: Network interface attribute modified
• AWS EC2: Network interface attribute reset
• AWS EC2: Network interface created
• AWS EC2: Network interface deleted
• AWS EC2: Network interface described
• AWS EC2: Network interface detached
• AWS EC2: Placement group created
• AWS EC2: Placement group deleted
• AWS EC2: Placement group described
• AWS EC2: Private IP address assigned
• AWS EC2: Private IP address unassigned
• AWS EC2: Product instance confirmed
• AWS EC2: Reserved instance described
• AWS EC2: Reserved instances listing cancelled
• AWS EC2: Reserved instances listing created
• AWS EC2: Reserved instances listing described
• AWS EC2: Reserved instances modified
• AWS EC2: Reserved instances offering purchased
• AWS EC2: Route created
• AWS EC2: Route deleted
• AWS EC2: Route replaced
• AWS EC2: Route table associated
• AWS EC2: Route table association replaced
• AWS EC2: Route table created
• AWS EC2: Route table deleted
• AWS EC2: Route table described
• AWS EC2: Route table disassociated
• AWS EC2: Security group activities
• AWS EC2: Security group created
• AWS EC2: Security group deleted
• AWS EC2: Security group described
• AWS EC2: Snapshot attribute described
• AWS EC2: Snapshot attribute modified
• AWS EC2: Snapshot attribute reset
• AWS EC2: Snapshot copied
• AWS EC2: Snapshot created
• AWS EC2: Snapshot deleted
• AWS EC2: Snapshot described
• AWS EC2: Spot datafeed subscription created
• AWS EC2: Spot datafeed subscription deleted
• AWS EC2: Spot datafeed subscription described
• AWS EC2: Spot instance request cancelled
• AWS EC2: Spot instance request described
• AWS EC2: Spot instances requested
• AWS EC2: Spot price history described
• AWS EC2: Subnet attribute modified
• AWS EC2: Subnet created
• AWS EC2: Subnet deleted
• AWS EC2: Subnet described
• AWS EC2: Tags created
• AWS EC2: Tags deleted
• AWS EC2: Tags described
• AWS EC2: Virtual machine export instance created
• AWS EC2: Virtual machine export task cancelled
• AWS EC2: Virtual machine export task described
• AWS EC2: Virtual private cloud attribute described
• AWS EC2: Virtual private cloud attribute modified
• AWS EC2: Virtual private cloud created
• AWS EC2: Virtual private cloud deleted
• AWS EC2: Virtual private cloud described
• AWS EC2: Virtual private cloud peer connection accepted
• AWS EC2: Virtual private cloud peer connection created
• AWS EC2: Virtual private cloud peer connection deleted
• AWS EC2: Virtual private cloud peer connection described
• AWS EC2: Virtual private cloud peer connection rejected
- AWS EC2: Virtual private gateway route propagation disabled
- AWS EC2: Virtual private gateway route propagation enabled
- AWS EC2: Volume attached
- AWS EC2: Volume attribute described
- AWS EC2: Volume attribute modified
- AWS EC2: Volume created
- AWS EC2: Volume deleted
- AWS EC2: Volume described
- AWS EC2: Volume detached
- AWS EC2: Volume imported
- AWS EC2: Volume status described
- AWS EC2: VPN connection created
- AWS EC2: VPN connection deleted
- AWS EC2: VPN connection described
- AWS EC2: VPN gateway attached
- AWS EC2: VPN gateway created
- AWS EC2: VPN gateway deleted
- AWS EC2: VPN gateway described
- AWS EC2: VPN gateway detached
- AWS EC2: VPN route connection created
- AWS EC2: VPN route connection deleted
- Apache Web Server: Attribute breaking injections
- Apache Web Server: Bad client request
- Apache Web Server: Bad gateway
- Apache Web Server: Base href injections detected
- Apache Web Server: Binding and behaviour injections
- Apache Web Server: Client request method not allowed
- Apache Web Server: Client request timeout
- Apache Web Server: Code injections
- Apache Web Server: Common comment types detected
- Apache Web Server: Common DB attacks
- Apache Web Server: Cross Site Scripting attacks
- Apache Web Server: etc/passwd inclusion attempt
- Apache Web Server: Format string attacks
- Apache Web Server: Gateway timeout
- Apache Web Server: HTTP request forbidden
- Apache Web Server: HTTP version not supported
- Apache Web Server: IE entities detected
- Apache Web Server: Internal server error
- Apache Web Server: JavaScript injections
- Apache Web Server: Mail header injections
- Apache Web Server: MySQL injections
- Apache Web Server: Page request success
- Apache Web Server: Path traversal attacks
- Apache Web Server: Payload attacks
- Apache Web Server: Perl shellcode injections
- Apache Web Server: Possibly malicious HTML elements
- Apache Web Server: PostgreSQL injections
- Apache Web Server: Precondition failed
- Apache Web Server: Proxy authentication required
- Apache Web Server: Request entity too large
- Apache Web Server: Request expectation failed
- Apache Web Server: Requested range not satisfiable
- Apache Web Server: Request-URI too long
- Apache Web Server: Resource created
- Apache Web Server: Resource down permanently
- Apache Web Server: Resource not found
- Apache Web Server: Service unavailable
- Apache Web Server: SQL injections
- Apache Web Server: Unauthorized client request
- Apache Web Server: Unspecified content length
- Apache Web Server: Unsupported media type
- Apache Web Server: URL injection/cache poisoning/LFI attacks
- Apache Web Server: URL/VBS injection/common URL schemes
- Apache Web Server: VBScript injections
- A10 ADC: Configuration Change
- A10 ADC: HA Events
- A10 ADC: Management Service Status
- A10 ADC: Port Status Change
- A10 ADC: Radius Server Error
- A10 ADC: SLB Server Status
- Barracuda SSL VPN: User logoff
- Barracuda SSL VPN: User logon failure
- Barracuda SSL VPN: User logon success
- Barracuda MA - Configuration changes
- Barracuda MA - Mail entities count
- Barracuda MA - New mails storage
- Barracuda MA: User login activities
- Barracuda MA: User login success
- Barracuda MA: User login failed
- Dell FORCE 10 Switch: Authentication failure
- Dell FORCE 10 Switch: Authentication success
- Dell FORCE 10 Switch: Interface status
- Dell FORCE 10 Switch: Port channel details
- Dell FORCE 10 Switch: User logoff
- Dell FORCE 10 Switch: User logon success
- eDirectory: Access token created
- eDirectory: Account created
- eDirectory: Account deleted
• eDirectory: Account disabled
• eDirectory: Account enabled
• eDirectory: Account modified
• eDirectory: Account security token modified
• eDirectory: Authentication failed
• eDirectory: Data item association created
• eDirectory: Data item association modified
• eDirectory: Data item association terminated
• eDirectory: Data item attribute modified
• eDirectory: Data item created
• eDirectory: Data item deleted
• eDirectory: Peer association created
• eDirectory: Peer association destroyed
• eDirectory: Process context modified
• eDirectory: Role created
• eDirectory: Role deleted
• eDirectory: Role modified
• eDirectory: Service disabled
• eDirectory: Service enabled
• eDirectory: Service terminated
• eDirectory: Session authenticated
• eDirectory: Session created
• eDirectory: Session management
• eDirectory: Session terminated
• eDirectory: Session unauthenticated
• eDirectory: System shutdown
• eDirectory: System started
• LDAP: Directory Object Added
• LDAP: Directory Object Deleted
• LDAP: Directory Object Modified
• NetScreen: Web Filtering
• OpenDNS: All activities
• OpenDNS: Allowed and blocked activities
• OpenDNS: Security activities
• PaloAlto Firewall: Logon Success
• RRAS: All events
• RRAS: Broadcast enabling failure
• RRAS: Certificate config failure
• RRAS: Certificate not found
• RRAS: Client auto disconnected
• RRAS: Client called back
• RRAS: Client connected to RAS automatically
• RRAS: Client disconnected to RAS automatically
• RRAS: Client exceeded license limit
• RRAS: Communication device failure
- RRAS: ConfigStore open failure
- RRAS: Configured accounting provider load failed
- RRAS: Configured authentication provider load failed
- RRAS: Connection attempt failed
- RRAS: Connection manager initialize failed
- RRAS: Critical section initialization failed
- RRAS: Demand-dial connection initiation failed
- RRAS: Demand-dial interface not loaded
- RRAS: Demand-dial interface not registered
- RRAS: DHCP RELAY FORWARD packet relay failure
- RRAS: DHCP REPLY packet relay failure
- RRAS: DHCP server contact error
- RRAS: DHCPV6 relay agent configuration failure
- RRAS: DHCPv6 relay agent incoming msg receive failure
- RRAS: DHCPV6 relay agent multicast enable failure
- RRAS: DHCPv6 relay agent packet discarded
- RRAS: DHCPV6 relay agent socket creation failed
- RRAS: DHCPv6 relay event registration failed
- RRAS: DHCPV6R called to start but running already
- RRAS: DHCPV6R critical section initialize failure
- RRAS: DHCPV6R event creation failed
- RRAS: DHCPV6R event notification failure
- RRAS: DHCPV6R memory allocation failure
- RRAS: DHCPV6R semaphore creation failed
- RRAS: DHCPV6R started successfully
- RRAS: DHCPV6R stopped
- RRAS: DHCPV6R synchronization object creation failed
- RRAS: DHCPV6R timer queue creation failed
- RRAS: DHCPV6R windows socket initialize failure
- RRAS: DLL component load failed
- RRAS: EAP-TLS certificate not configured
- RRAS: EAP-TLS certificate not found
- RRAS: Error detected
- RRAS: Event notification request failure
- RRAS: Forward info hold table creation failed
- RRAS: Host DLL registry key open failed
- RRAS: HTTP layer initialize failure
- RRAS: IGMP event creation failure
- RRAS: IGMP memory allocation failure
- RRAS: IGMP multicast group join failure
- RRAS: IGMP packet discarded
- RRAS: IGMP proxy failed to register with MGM
- RRAS: IGMP RAS client configuration failure
- RRAS: IGMP router failed to register with MGM
- RRAS: IGMP socket operation failure
- RRAS: IGMP task scheduling failure
- RRAS: IGMPv2 network event enumeration failure
- RRAS: IGMPv2 packet receive error
- RRAS: Impersonation revert error occurs
- RRAS: Incoming message receive failure
- RRAS: Interface add error
- RRAS: Interface info hold table creation failed
- RRAS: Interface loading error
- RRAS: Interface remove error
- RRAS: Interface unreachable
- RRAS: IP address assigned to connected user
- RRAS: IP address obtain error
- RRAS: IP address unavailable
- RRAS: IP address user disconnected
- RRAS: IP packet filter configure error
- RRAS: IP security apply failure
- RRAS: IPBOOTP configuration failure
- RRAS: IPBOOTP started successfully
- RRAS: IPBOOTP stopped
- RRAS: IPMGM memory allocation failure
- RRAS: IPMGM protocol component find failure
- RRAS: IPMGM protocol component register failed
- RRAS: IPMGM semaphore creation failed
- RRAS: IPMGM started successfully
- RRAS: IPRIPv2 bind to IP address failed
- RRAS: IPRIPv2 enabling failure
- RRAS: IPRIPv2 started successfully
- RRAS: IPRIPv2 stopped
- RRAS: Leaky multicast local scope detected
- RRAS: Line disconnected
- RRAS: Link disconnected
- RRAS: Media access control handle failed
- RRAS: Memory allocation failure
- RRAS: MGM interface ownership failed
- RRAS: MGM register with RTM failure
- RRAS: Multicast enable on interface failed
- RRAS: Multicast scope mismatch error occurs
- RRAS: NAP enforcement client registration failed
- RRAS: NAP received invalid request
- RRAS: NapAgent request failure
- RRAS: Network address obtain failure
- RRAS: Network event enumeration failed
- RRAS: Network events enumeration failure
- RRAS: Next-hop route changed by IPRIPv2
• RRAS: Packet discarded
• RRAS: Packet filter disable error
• RRAS: Packet filter disabled
• RRAS: Packet filter enable error
• RRAS: Packet receiving error
• RRAS: Peer receive RIP messages failure
• RRAS: Port opening failure
• RRAS: PPP engine load failure
• RRAS: PPP key information obtain failed
• RRAS: PPP module error occurred
• RRAS: PPP module initialize error
• RRAS: PPP Session timeout
• RRAS: Protocol component enabled
• RRAS: Protocol component invalid
• RRAS: RAS authentication attribute invalid
• RRAS: RAS connected to client automatically
• RRAS: RAS IP address acquired
• RRAS: RAS IP address changed
• RRAS: RAS server certificate retrieve failed
• RRAS: RAS server not accept calls
• RRAS: RAS unable to renew IP address
• RRAS: RASMAN Service port enumeration failed
• RRAS: RASMAN service start failed
• RRAS: Registry key access failure
• RRAS: Registry key enumeration failure
• RRAS: Registry key value access failure
• RRAS: Registry key value enumeration failure
• RRAS: Registry parameter section open failure
• RRAS: Registry value overridden
• RRAS: Remote access connection manager service start failed
• RRAS: Remote access security host registry key open failure
• RRAS: RRAS DHCP relay agent packet discarding
• RRAS: RRAS DHCP relay agent protocol initialized
• RRAS: RRAS DHCP relay failure
• RRAS: RRAS IGMP audits
• RRAS: RRAS IGMP configuration error
• RRAS: RRAS RIP protocol initialization
• RRAS: RRAS RIP socket operation
• RRAS: RRAS route ignoring
• RRAS: RRAS RTM route addition
• RRAS: RRAS start failed
• RRAS: Security host module component load failure
• RRAS: Semaphore creation failed
• RRAS: Socket creation failed
• RRAS: SSTP incoming connection failure
- RRAS: SSTP memory allocation failure
- RRAS: SSTP negotiation failed
- RRAS: SSTP protocol request send failure
- RRAS: SSTP request send failure
- RRAS: SSTP response receive failure
- RRAS: SSTP SHA1 certificate hash read failure
- RRAS: SSTP SHA256 certificate hash read failure
- RRAS: SSTP-based VPN connection terminated
- RRAS: Task schedule failure
- RRAS: Timer set failed for forwarding entry
- RRAS: URL secure failure
- RRAS: User authentication success
- RRAS: User authentication success encrypted
- RRAS: User authentication success strongly encrypted
- RRAS: User callback failed
- RRAS: User connected and disconnected again
- RRAS: User connection failure
- RRAS: User device connection established
- RRAS: User device disconnection occurred
- RRAS: User disconnected
- RRAS: VPN connection failure
- RRAS: VPN server route configuration failure
- RRAS: Windows socket start failure
- RRAS: ConfigStore open failure
- Sophos UTM: Node changed
- Sophos UTM: Object changed
- Sophos UTM: Object created
- Sophos UTM: Object deleted
- Sophos UTM: Packet accepted
- Sophos UTM: Packet dropped
- Sophos UTM: User authentication failure
- Sophos UTM: User authentication success
- Sophos EC: Adware detected
- Sophos EC: Controlled application detected
- Sophos EC: Controlled device detected
- Sophos EC: Data transfer allowed
- Sophos EC: Data transfer blocked
- Sophos EC: Device blocked
- Sophos EC: File access denied
- Sophos EC: Virus detected
- Sophos EC: Virus file cleaned
- Sophos EC: Virus removed
- Sophos EC: Write attempt to device failed
- WatchGuard XTM: Authentication failure
- WatchGuard XTM: Authentication success
- WatchGuard XTM: Configuration changed
- WatchGuard XTM: DHCP activity
- Watchguard XTM: Firewall allowed traffic
- Watchguard XTM: Firewall denied traffic
- WatchGuard XTM: Interface status
- WatchGuard XTM: IPS attack detected
- WatchGuard XTM: PPPoE session details
- WatchGuard XTM: Proxy policy allowed traffic
- WatchGuard XTM: Proxy policy denied traffic
- WatchGuard XTM: Security services error
- WatchGuard XTM: VPN session details
- Windows Audit Log Clear
- ZoneDirector: Access point join attempt failed
- ZoneDirector: Additional management interface created
- ZoneDirector: Additional management interface removed
- ZoneDirector: Additional management interface updated
- ZoneDirector: Admin locked out
- ZoneDirector: Admin logged out
- ZoneDirector: Admin login failed
- ZoneDirector: Admin login success
- ZoneDirector: Admin password changed
- ZoneDirector: AP configuration update request failed
- ZoneDirector: AP contact lost with ZD
- ZoneDirector: AP limit exceeded
- ZoneDirector: AP management VLAN setting disabled
- ZoneDirector: AP management VLAN setting enabled
- ZoneDirector: Bonjour service disabled
- ZoneDirector: Bonjour service enabled
- ZoneDirector: Cable Modem interface down
- ZoneDirector: Client disconnected by admin
- ZoneDirector: DHCP server disabled
- ZoneDirector: DHCP server enabled
- ZoneDirector: eMesh AP connected to Mesh AP
- ZoneDirector: eMesh AP disconnected from Mesh AP
- ZoneDirector: eMesh AP disconnected from uplink
- ZoneDirector: File retrieve failure
- ZoneDirector: FlexMaster management disabled
- ZoneDirector: FlexMaster management enabled
- ZoneDirector: FM user login failed
- ZoneDirector: FM user login success
- ZoneDirector: Global client isolation disabled
- ZoneDirector: Global client isolation enabled
- ZoneDirector: Location service disabled
- ZoneDirector: Location service enabled
- ZoneDirector: Mesh AP connected to eMesh AP
• ZoneDirector: Mesh AP disconnected from eMesh AP
• ZoneDirector: Mesh AP disconnected from uplink
• ZoneDirector: Mesh name changed by admin
• ZoneDirector: Mesh packet forwarding filter disabled
• ZoneDirector: Mesh packet forwarding filter enabled
• ZoneDirector: Mesh packet forwarding filter modified
• ZoneDirector: Mesh passphrase changed by admin
• ZoneDirector: Peer ZD configuration restored
• ZoneDirector: Peer ZD connected
• ZoneDirector: Peer ZD disconnected
• ZoneDirector: Peer ZD firmware version mismatched
• ZoneDirector: Peer ZD license mismatched
• ZoneDirector: Peer ZD model mismatched
• ZoneDirector: Peer ZD upgrade failure
• ZoneDirector: Peer ZD upgrade pending
• ZoneDirector: Remote syslog disabled
• ZoneDirector: Remote syslog enabled
• ZoneDirector: Rogue AP detected
• ZoneDirector: Rogue DHCP server detected
• ZoneDirector: Rogue DHCP server detector process disabled
• ZoneDirector: Rogue DHCP server detector process enabled
• ZoneDirector: SNMP authentication failed
• ZoneDirector: System configuration restored by administrator
• ZoneDirector: System name changed
• ZoneDirector: System received failover command
• ZoneDirector: System restarted by administrator
• ZoneDirector: System restore command received
• ZoneDirector: System state changed
• ZoneDirector: System upgrade command received
• ZoneDirector: System warm restarted
• ZoneDirector: Telnet service disabled
• ZoneDirector: Telnet service enabled
• ZoneDirector: Temp license expired
• ZoneDirector: Unrecognized command received
• ZoneDirector: ZD authentication to location server failed
• ZoneDirector: ZD auto-recovery failed
• ZoneDirector: ZD auto-recovery successful
• ZoneDirector: ZD connection to location server dropped
• ZoneDirector: ZD dhcp pool full
• ZoneDirector: ZD image upgrade failed
• ZoneDirector: ZD image upgrade success
• ZoneDirector: ZD/AP high entropy certificate install failed
• ZoneDirector: ZD/AP high entropy certificate install success
• ZoneDirector: ZoneDirector management VLAN disabled
• ZoneDirector: ZoneDirector management VLAN enabled
• ZoneDirector: ZD authentication to location server failed

New Alerts

• A10 ADC: Configuration Change
• A10 ADC: User Authentication Failed
• Barracuda SSL VPN: User logon success
• Barracuda SSL VPN: User logon failure
• Barracuda MA: User login failed
• Barracuda MA: Configuration changes
• Dell FORCE 10 Switch: Authentication failure
• Dell FORCE 10 Switch: User logoff
• Dell FORCE 10 Switch: User logon success
• eDirectory: Account created
• eDirectory: Authentication failed
• eDirectory: Role created
• eDirectory: Role deleted
• eDirectory: Service disabled
• eDirectory: System shutdown
• EventTracker: Behavior Lagging
• EventTracker: New Event ID Activity
• EventTracker: New IP Address Activity
• EventTracker: New System Activity
• EventTracker: New Unique Process Hash Activity
• EventTracker: New USB Activity
• EventTracker: New Windows Applications Activity
• EventTracker: New Windows Audit Policy and Account Management Activity
• EventTracker: New Windows Interactive Logon Activity
• EventTracker: New Windows Logon Activity
• EventTracker: New Windows Logon Failure Activity
• EventTracker: New Windows Network Activity
• EventTracker: New Windows Process Activity
• EventTracker: New Windows Runaway Process Activity
• EventTracker: New Windows Software Install Activity
• EventTracker: New Windows User Location Affinity Activity
• EventTracker: Out of Ordinary Event ID Activity
• EventTracker: Out of Ordinary IP Address Activity
• EventTracker: Out of Ordinary System Activity
• EventTracker: Out of Ordinary Unique Process Hash Activity
• EventTracker: Out of Ordinary USB Activity
• EventTracker: Out of Ordinary Windows Applications Activity
• EventTracker: Out of Ordinary Windows Audit Policy and Account Management Activity
• EventTracker: Out of Ordinary Windows Interactive Logon Activity
• EventTracker: Out of Ordinary Windows Logon Activity
• EventTracker: Out of Ordinary Windows Logon Failure Activity
• EventTracker: Out of Ordinary Windows Network Activity
• EventTracker: Out of Ordinary Windows Process Activity
• EventTracker: Out of Ordinary Windows Runaway Process Activity
• EventTracker: Out of Ordinary Windows Software Install Activity
• EventTracker: Out of Ordinary Windows User Location Affinity Activity
• Disk space critically low
• LDAP: Directory Object Deleted
• Linux: User authentication failure Maximum tries limit reached
• Linux: CD/DVD insertion detected
• Linux: USB device insertion detected
• OpenDNS: Blocked activities
• OpenDNS: Security Activities
• RRAS: Broadcast enabling failure
• RRAS: Certificate config failure
• RRAS: Client auto disconnected
• RRAS: Client disconnected to RAS automatically
• RRAS: Client exceeded license limit
• RRAS: Communication device failure
• RRAS: Connection attempt failed
• RRAS: Critical section initialization failed
• RRAS: Demand-dial connection initiation failed
• RRAS: DHCP REPLY packet relay failure
• RRAS: DHCP RELAY FORWARD packet relay failure
• RRAS: DHCPV6 relay agent configuration failure
• RRAS: DHCPV6 relay agent incoming msg receive failure
• RRAS: DHCPV6 relay agent multicast enable failure
• RRAS: DHCPv6 relay agent packet discarded
• RRAS: DHCPv6 relay event registration failed
• RRAS: DHCPV6R critical section initialize failure
• RRAS: DHCPV6R event creation failed
• RRAS: DHCPV6R event notification failure
• RRAS: DHCPV6R memory allocation failure
• RRAS: DHCPV6R semaphore creation failed
• RRAS: DHCPV6R stopped
• RRAS: DHCPV6R synchronization object creation failed
• RRAS: DHCPV6R timer queue creation failed
• RRAS: DHCPV6R windows socket initialize failure
• Sophos UTM: Node changed
• Sophos UTM: Object changed
• Sophos UTM: Object deleted
• Sophos UTM: Shell terminal password changed
• Sophos UTM: User authentication failure
• Sophos EC: Adware detected
- Sophos EC: Data transfer blocked
- Sophos EC: Device blocked
- Sophos EC: File access denied
- Sophos EC: Virus detected
- Sophos EC: Write attempt to device failed
- VMware ESXi: Account deleted
- VMware ESXi: High resource usage alarm
- VMware ESXi: Host added
- VMware ESXi: Task failed
- VMware ESXi: User authentication failed
- VMware ESXi: User authentication success
- VMware ESXi: Virtual machine created
- VMware ESXi: Virtual machine reconfigured
- VMware vCenter: Lockdown mode enabled
- VMware vCenter: SSH access enabled
- VMware vCenter: User permission removed
- VMware vCenter: User role deleted
- VMware vCenter: User role modified
- VMware vCenter: Virtual disk download
- VMware vCenter: Virtual machine created
- VMware vCenter: Virtual machine removed
- VMware vCentre: Bypass Attemp
- VMware: Firewall configuration changed
- VMware: SCSI error
- VMware: SCSI high IO latency
- VMware: SSO authentication failure
- WatchGuard XTM: Authentication failure
- WatchGuard XTM: Configuration changed
- WatchGuard XTM: IPS attack detected
- WatchGuard XTM: Security services error
- ZoneDirector: Access point join attempt failed
- ZoneDirector: AP configuration update request failed
- ZoneDirector: AP contact lost with ZD
- ZoneDirector: AP limit exceeded
- ZoneDirector: Cable Modem interface down
- ZoneDirector: eMesh AP connected to Mesh AP
- ZoneDirector: eMesh AP disconnected from Mesh AP
- ZoneDirector: eMesh AP disconnected from uplink
- ZoneDirector: Mesh AP connected to eMesh AP
- ZoneDirector: Mesh AP disconnected from eMesh AP
- ZoneDirector: Mesh AP disconnected from uplink
- ZoneDirector: Peer ZD disconnected
- ZoneDirector: Peer ZD firmware version mismatched
- ZoneDirector: Peer ZD license mismatched
- ZoneDirector: Peer ZD model mismatched
• ZoneDirector: Peer ZD upgrade failure
• ZoneDirector: Rogue AP detected
• ZoneDirector: System ready to sync
• ZoneDirector: System received failover command
• ZoneDirector: System state changed
• ZoneDirector: Temp license expire
• ZoneDirector: Unrecognized command received

New Flex Reports

• Apache Web Server-SQL Injection Attacks Reports
• Apache Web Server-Cross Site Scripting Attacks Report
• Apache Web Server-Payload Attack Report
• Apache Web Server-Format String Attacks Report
• Apache Web Server-Common DB attack Report
• Apache Web Server-JavaScript Injection Attacks Reports
• Apache Web Server-Possible Malicious HTML Elements Report
• Apache Web Server-Etc or Passwd Inclusion Attempt
• Apache Web Server-Path Traversal Attacks Report
• Apache Web Server-Code Injections
• Apache Web Server-All Events
• A10 ADC - Application Delivery Traffic Details
• A10 ADC - Console Logon Success Details
• A10 ADC - User Authentication Failure Details
• AWS EC2-Addresses described
• AWS EC2-Instance status described
• AWS VPC: Customer Gateway
• AWS VPC: DHCP Options
• AWS VPC: Elastic IP Address
• AWS VPC: Flow
• AWS VPC: Internet Gateway
• AWS VPC: Network ACLs
• AWS VPC: Route Tables
• AWS VPC: Security Groups
• AWS VPC: Subnet
• AWS VPC: Virtual Private Cloud
• AWS VPC: Virtual Private Gateway
• Barracuda SSL VPN-User Logon Failure
• Barracuda SSL VPN-User Logon Success
• Barracuda SSL VPN-User Logoff
• Barracuda MA- Configuration Change
• Barracuda MA- Mail Entity Count Change
• Barracuda MA- New Email Storage
• Barracuda MA- User Login failed
- Barracuda MA- User Login Success
- Dell FORCE 10 Switch-Authentication Success
- Dell Force 10 Switch-User Login Success
- Dell Force 10 Switch-User Logoff
- eDirectory-Authentication Failure Report
- eDirectory-Account Creation and Deletion Report
- eDirectory-Account Modification Report
- eDirectory-Role Creation and Deletion Report
- eDirectory-Role Modification Report
- EventTracker-New IP Pair Activity Report
- F5 BIG IP ASM-Violations
- JunOS - User Authentication Success
- JunOS - User Authentication Failure
- JunOS - User Logon Failure
- JunOS - Dynamic ARP Inspection Failure
- JunOS - Untrusted DHCP Server Detection
- JunOS - User Logon Success
- Junos-Webfilter Details
- Junos-Flow Session Details
- Junos-Screen Attack Details
- Junos-VPN Session Details
- Juniper NetScreen-User Logoff Report
- Juniper NetScreen-User Logon Success Report
- Juniper NetScreen-User Authentication Success
- Juniper NetScreen-User Authentication Failed
- Juniper NetScreen-Web filtering
- Juniper NetScreen-URL allowed or blocked
- Juniper NetScreen-USB storage device attached or detached
- Juniper NetScreen-Firewall policy change
- Juniper NetScreen-System authentication
- Juniper NetScreen-Intrusion detection system
- Juniper NetScreen-Account management
- Juniper NetScreen-Traffic allowed or blocked
- Linux-User authentication failed
- Linux-User authentication success
- Linux-USB device insertion
- Linux-CD DVD insertion
- NetScreen Administration Report
- NetScreen-Login and logout
- Office 365 - Exchange License Usage Details
- Office 365 - Exchange Browser Usage Details
- Office 365 - Exchange OS Usage Details
- Office 365 - Exchange Client Usage Details
- Office 365 - Exchange Mailbox Audit Details
- Office 365 - Exchange Mailbox Usage Details
• Office 365 - Exchange Mailbox DLP Policy Details
• Office 365 - Exchange Mail Traffic Details
• Office 365 - Exchange Mail Policy Traffic Details
• Office 365 - Exchange Message Trace Details
• Office 365 - Exchange Spam Mail Traffic Details
• Office 365 - Exchange Top Mail User Details
• Office 365 - Exchange Top Inactive Mail User Details
• Office 365 - Exchange Top Mail Traffic Details
• Office 365 - Exchange Group Activity Details
• Office 365 - Exchange Admin Audit Details
• Office 365 - Exchange Mailbox Activity Details
• Office 365 - Exchange Top Outbound Mail Traffic Details
• Office 365 - Exchange Top Inbound Mail Traffic Details
• Office 365 - SharePoint Deployment Details
• Office 365 - SharePoint Storage Details
• Office 365 - SharePoint Tenant Storage Details
• Office 365 - SharePoint License Usage Details
• Office 365 - Lync Active User Details
• Office 365 - Lync Device Usage Details
• Office 365 - Lync Conference Duration Details
• Office 365 - Lync P2P Session Duration Details
• Office 365 - Lync P2P Session Details
• Office 365 - Lync Conference Details
• OpenDNS-Allowed activities
• OpenDNS-Blocked activities
• OpenDNS-Security activities
• Palo Alto Firewall User Logon Failed Report
• Palo Alto Firewall Configuration Failed or Success Report
• Palo Alto Firewall Vulnerability Detected Report
• Palo Alto Firewall Virus Detected Report
• Palo Alto Firewall URL Filtered Report
• RRAS-Access Request
• RRAS-Access Success
• RRAS-Accounting Request
• RRAS-Authentication Type
• RRAS-Access Failure
• Sophos EC-Write Attempt to Devices Failed Report
• Sophos EC-Controlled Application Detection Report
• Sophos EC-File Access Denied Report
• Sophos EC-File Transfer Blocked Report
• Sophos EC-Blocked Devices Report
• Sophos UTM-User Authentication Failure
• Sophos UTM-Node Changed
• Sophos UTM-Object Deleted
• Sophos UTM-Object Changed
- Sophos UTM-Object Created
- Sophos UTM-Packet Accepted
- Sophos UTM-Packet Dropped
- Sophos UTM-Shell Terminal Password Changed
- Sophos UTM-User Authentication Success
- SonicWALL Firewall-Network Access Report
- SonicWALL Interface Link UP or Down Report
- SonicWALL Connection Closed Dropped or Terminated Report
- SonicWALL Connection Opened or Established Report
- SonicWALL: Terminal Services or SSO Agent down Report
- SonicWALL: Multicast address Added or Deleted
- SonicWALL Website Access Denied Report
- SonicWALL Intrusion Detection Report
- SonicWALL AntiSpam Service Enabled or Disabled Report
- SonicWALL System Shutdown by Administrator Report
- SonicWALL: Attacks detection
- SonicWALL-Configuration change details
- Syslog-User Password Changed
- Syslog-System Shutdown and Reset
- Snort-Intrusion Detected Report
- Trend Micro User Authentication Success
- Trend Micro User Account Management Report
- Trend Micro Firewall Policy Management Report
- VMware ESXi-Account created
- VMware-SSO user deleted
- VMware-SSO user created
- VMware ESXi-Account deleted
- VMware vcCenter-Host removed from datacenter
- VMware vcCenter-Successful logins
- VMware ESXi-Failed login attempts
- VMware ESXi-Host added to datacenter
- VMware ESXi-Failed login attempts by source and user
- VMware vcCenter-Virtual machine created
- VMware ESXi-Successful logins
- VMware vcCenter-Virtual machine removed
- VMware ESXi-Firewall configuration change
- VMware vSphere-Task detail report
- VMware vSphere-Alarm detail report
- WatchGuard XTM Proxy Policy Traffic Details
- WatchGuard XTM Firewall User Logon Details
- WatchGuard XTM Configuration Change Details
- WatchGuard XTM Firewall Attack Details
- WatchGuard XTM Firewall Authentication Failure
- WatchGuard XTM Firewall Authentication Success
- WatchGuard XTM Firewall Traffic Details
• Windows-User Account Locked
• Windows-System Time Change
• Windows-Patches and Hot Fixes

Updated Knowledge Packs:

Updated Alerts:

• BIG-IP LTM: ARP entry deleted
• BIG-IP LTM: Authentication failed
• BIG-IP LTM: Authentication success
• BIG-IP LTM: Connection error
• BIG-IP LTM: Monitor removed
• BIG-IP LTM: Packet filtering disabled
• BIG-IP LTM: Packet filtering rule modified
• BIG-IP LTM: Pool member status down
• BIG-IP LTM: Root login failure
• BIG-IP LTM: User account deleted
• Windows: Audit log cleared
• NCM-Browser Connecting to Non Webserver Port
• NCM-Non Browser EXE Connecting to Known Webserver Port
• Disk space is Critically Low on EventTracker Server
• High CPU Utilization on EventTracker Server
• EventTracker Service down
• EventTracker: New IP Activity Reputation Lookup
• Critical Potential Breach: A New Process Connecting to Low Reputation IP Address
• Critical Potential Breach: Unknown Process Connected to a Bad Reputed Remote Site Across Firewall
• EventTracker: Connection to Bad IP Reputation Process Lookup

Updated Categories:

• BIG-IP LTM: ARP entry deleted
• BIG-IP LTM: ARP static entry
• BIG-IP LTM: Authentication failed
• BIG-IP LTM: Authentication success
• BIG-IP LTM: Configuration failed
• BIG-IP LTM: Connection error
• BIG-IP LTM: Member unavailable for pool
• BIG-IP LTM: Monitor created
• BIG-IP LTM: Monitor removed
• BIG-IP LTM: New node added
• BIG-IP LTM: New route addition failed
• BIG-IP LTM: New route addition success
• BIG-IP LTM: New SNAT added
• BIG-IP LTM: NTP server configured
• BIG-IP LTM: Packet filtering disabled
• BIG-IP LTM: Packet filtering enabled
• BIG-IP LTM: Packet filtering rule modified
• BIG-IP LTM: Pool member creation failed
• BIG-IP LTM: Pool member creation success
• BIG-IP LTM: Pool member deleted
• BIG-IP LTM: Pool member status down
• BIG-IP LTM: Pool member status up
• BIG-IP LTM: Remote server added
• BIG-IP LTM: Root login failure
• BIG-IP LTM: SNMP agent configured
• BIG-IP LTM: System shutdown
• BIG-IP LTM: User account deleted
• BIG-IP LTM: User account modified
• BIG-IP LTM: Virtual server created
• EventTracker: Network Connections
• Watchguard XTM: Firewall allowed traffic
• Watchguard XTM: Firewall denied traffic

Updated Flex Reports:

• Snort-Alert Analysis
• Windows-Administrative Activities
• Windows-AD Object Access Detail Report
• NCM - All New Network Connection Report
• NCM-Browser Connecting to Non Webserver Port
• NCM-Non Browser EXE Connecting to Known Webserver Port
• Palo Alto Firewall - Threat Details
• Palo Alto Firewall - Traffic Details
• SonicWALL - AntiSpam Service Enabled or Disabled
• SonicWALL - Multicast Policy Added or Deleted
• SonicWALL - System Shutdown by Administrator
• SonicWALL - Terminal Service and SSO Agent Down
Prerequisites

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

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

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

Planning

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

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

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

NOTE: 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 v8.0.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. Close/terminate all the EventTracker components like Management console and Reports console, including RDP (Remote Desktop Protocol) sessions.

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

Upgrade Procedure

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

2. Restart the EventTracker Manager server or system.

3. Install EventTracker v8.0.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.

**NOTE:**
- Upgrade process for v6.4 to v8.0 remains the same.
- After upgrading from v6.4 to v8.0, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.
- For v6.4 to v8.0 upgrade, if ‘Keyword Indexing’ is installed and enabled, then launch the Keyword Indexing migration utility.
- For CM and CP set up, please upgrade CM (Collection Master) first, and then upgrade CP (Collection point).
- For agent upgrade details, please click [here](#).

**Common steps for all upgrades**

**Before you start with the upgrade process**

- Verify that all the prerequisites have been satisfied.
- When upgrading from v7.x to v8.0, please verify all prerequisites are installed manually on server machine.
  
  **NOTE:** 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 v8.0.x](#).
If you have incorporated your company logo into EventTracker, then take a backup of .jpg file of your company logo before uninstalling the EventTracker. You need to replace the backed up image file after installing EventTracker Enterprise.

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

If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v8.0. Please make sure to reconfigure it again as mentioned in Securing IIS Web Server with SSL.

The logged in user who is upgrading to EventTracker v8.0 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

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

As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v8.0 for non-admin users. You have to reconfigure it again.

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

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

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.
3. Install EventTracker v8.0.
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 v8.0.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 from v7.x to v8.0, 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](image3.png)

A message displays.

![Figure 4](image4.png)

d. Select the **OK** button.

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

![Figure 5](image5.png)

Available Dashlets window displays.

f. Select and **Add** the required dashlets.
After upgrading, if the collection master is v8.0, and if collection point is using any older version of EventTracker, then incidents will not be visible. If you upgrade collection point to v8.0, post upgrade incidents will only be transferred to collection master.

The keyword dashboard has to be customized after upgrading to v8.0.

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.

On upgrade from 7.x to 8.0 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 

![Available Dashlets](image-url)
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 to v8.0.x

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

After upgrading from v7.0 to v8.0, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.
Upgrade from v7.1.x to v8.0.x
The procedure to upgrade from v7.1.x to v8.0.x is same like upgrade from v7.6.x to v8.0.x.

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

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

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

Upgrade from v7.3.x to v8.0.x
The procedure to upgrade from v7.3.x to v8.0.x is same like upgrade from v7.6.x to v8.0.x.

Upgrade from v7.4.x to v8.0.x
The procedure to upgrade from v7.4.x to v8.0.x is same like upgrade from v7.6.x to v8.0.x.

Upgrade from v7.5.x to v8.0.x
The procedure to upgrade from v7.5.x to v8.0.x is same like upgrade from v7.6.x to v8.0.x.

Upgrade from v7.6.x to v8.0.x
The procedure to upgrade from v7.6.x to v8.0.x is mentioned in the detail section.

Upgrade - Detailed View
In this section, you will learn upgrade process in detail.

- Upgrade from v6.4.x to v8.0.x Enterprise
- Upgrade from v7.0.x to v8.0.x Enterprise
- Upgrade from v7.1.x to v8.0.x Enterprise
Upgrade from v7.2.x to v8.0.x Enterprise

Upgrade from v7.3.x to v8.0.x Enterprise

Upgrade from v7.4.x to v8.0.x Enterprise

Upgrade from v7.5.x to v8.0.x Enterprise

Upgrade from v7.6.x to v8.0.x Enterprise

Upgrade from v6.4.x to v8.0.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](image)

(OR)

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.

7. Click the **OK** button.

8. Select **Filters** option, and then click the **Export** button.
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
Click **Add All >>** button to select all the 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.

   ![Export Import Utility](image)

   **Figure 18**

   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.

   ![EventTracker Control Panel](image19.png)

   **Figure 19**

3. Click **Agent Configuration** icon.

   ![Agent Configuration](image20.png)

   **Figure 20**

   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.

   ![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.
3. Click the **Yes** button.

EventTracker starts the uninstall process.

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 v8.0 Enterprise**

Kindly follow the steps mentioned below for upgrade process.

1. To install v8.0, launch EventTrackerSetup.exe.

   EventTracker Pre-Install Check displays below message.

   ![EventTracker Pre-Install Check](image)

   **Figure 28**

   Previous installation configuration has been detected, would you like to upgrade?

   Yes  No

   **NOTE:** For Windows 2008, 2008R2 (32bit/64bit), Windows 7 (32bit/64bit), Microsoft.NET Framework 4.5 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.
2. Click the **Yes** button.

Microsoft .NET Framework 4.5 Installation page displays.

![Installation Progress](image)

3. The PowerShell download page will display.

4. Click the **Download** button.
PowerShell download starts.

5. Once the download is completed, it will search for windows updates.

6. After the search completes, it will ask to install the Windows software updates.

The below message box displays.
7. Click **OK** to install the updates.

The Download and Install Updates page displays.

8. Click **I Accept** button.

The updates installation starts.
9. Once the installation is complete, click the **Restart Now** button.
10. Once it is restarted, run the EventTracker.exe setup.

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

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

12. Read the license agreement, click ‘**I accept the terms in the license agreement**’ option and then click the **Next >** button.

   ![Figure 39](image)

   **PRISM MICROSYSTEMS, INC. SOFTWARE LICENSE AGREEMENT**

   PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING, COPYING, OR USING THE SOFTWARE.

   BY CLICKING ON THE "ACCEPT" (OR EQUIVALENT) BUTTON OR SIGNING BELOW, OPENING THE PACKAGE, DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU ARE CONSENTING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE "DECLINE" (OR EQUIVALENT) BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. IF YOU CLICK "DECLINE", YOU MUST RETURN THE SOFTWARE LICENSE KEY(S) TO THE

   - [ ] I accept the terms in the license agreement
   - [ ] I do not accept the terms in the license agreement

   ![InstallShield Wizard](image)

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

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

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

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

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

Select EventTracker Console Type page displays.
17. 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 >**.
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.

![Change Audit SnapShot dialog box](image)

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

18. Select the **Next >** button.

Ready to install the Program page displays.

19. Select **Install Remedial Action EXEs on this machine** option, and then select the **Install** button.
Figure 47
InstallShield Wizard installs the selected components. Migration Utility displays.

Figure 48
20. Click the **Next >** button.

![Migration Utility](image)

Figure 49

21. Click the **Finish** button.

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

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

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

   InstallShield Wizard displays the **EventTracker Configuration** screen.
25. 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.

26. 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 55

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.

   ![Export Import Utility](image)

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.

![Figure 60](image)

18. Click the **OK** button.

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

![Figure 61](image)

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.

![Export Import Utility](image)

**Figure 62**

22. Click the **OK** button.

23. Select **Scheduled Reports** option.

![Export Import Utility Window](image)

**Figure 63**

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 65](image)

   (OR)

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

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

   EventTracker displays **Alert Management** page.

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

   ![Figure 73](image)

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

Figure 74

Figure 75
EventTracker displays **Upgrade Remote Agent(s)** pop-up window.

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

**Figure 76**

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

![Selected agent](image)

**Figure 77**

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 v8.0 ‘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`

- **If Keyword indexing is installed and enabled, launch the keyword indexing file migration utility.** The keyword Indexer folder is restructured. To put the old indexed files into the new structure, `KeywordMigration.exe` utility file has been provided along with build 7.6.

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

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

- In **EventTracker Control Panel -> EventTracker Agent Configuration -> Event Filters** tab, ‘Information’ and ‘Audit Success’ event types are unchecked by default. Select the ‘Information’ and ‘Audit Success’ checkboxes in order to filter large number of ‘Information’ and ‘Audit Success’ events.
• **Agent upgrade:** While performing remote agent upgrade, make sure to select the appropriate configuration file containing the port that was previously configured in v6.4.

  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](mailto: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 to v8.0.x

The upgrade procedure from v7.0 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in [Upgrade from v7.6.x to v8.0.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 to v8.0, kindly run the executable file `Prism.AlertsMigration.exe` available in `"\InstallDIR\EventTracker\Prism.AlertsMigration.exe"` for migrating the incidents.

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

The upgrade procedure from v7.1 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in [Upgrade from v7.6.x to v8.0.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 v7.1 to v8.0, kindly run the executable file `Prism.AlertsMigration.exe` available in `"\InstallDIR\EventTracker\Prism.AlertsMigration.exe"` for migrating the incidents.

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

The upgrade procedure from v7.2 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in [Upgrade from v7.6.x to v8.0.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 v7.2 to v8.0, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

Upgrade from v7.3.x to v8.0.x

The upgrade procedure from v7.3 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in Upgrade from v7.6.x to v8.0.x.

NOTE:

- Before upgrading, please take a backup of the database and follow the instructions mentioned in Upgrade from v7.6.x to v8.0.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 v7.4.x to v8.0.x

The upgrade procedure from v7.4 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in Upgrade from v7.6.x to v8.0.x.

NOTE:

- Before upgrading, please take a backup of the database and follow the instructions mentioned in Upgrade from v7.6.x to v8.0.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 v7.5.x to v8.0.x

The upgrade procedure from v7.5 to v8.0 is the same as v7.6 to v8.0. The detail procedure is described in Upgrade from v7.6.x to v8.0.x.

**NOTE:**

- Before upgrading, please take a backup of the database and follow the instructions mentioned in Upgrade from v7.6.x to v8.0.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 v8.0.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.
Figure 90

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 v8.0 Enterprise

For the details regarding installation process, please refer 'EventTracker v8.0 Enterprise Installation Guide'.

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

Click Configure the service accounts for more details.

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

Verify Category:
1. 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](Figure%2095.png)

   (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.

![Event Filter Configuration](image)

**Figure 99**

**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.

![RSS Feeds](image)

**Figure 100**
Step 7: 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 8.0 (Build 29), please refer to the section “Using the Default Agent Filters in EventTracker version 8.0” 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</td>
</tr>
<tr>
<td></td>
<td>upgrade has to be done. The text file should contain one system</td>
</tr>
<tr>
<td></td>
<td>name per line.</td>
</tr>
<tr>
<td></td>
<td>If you select this option then browse the text file to select the</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>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.

![Figure 105](image)

(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.

![Figure 106](image)
6. Check **Install default Remedial Action EXEs on this system** option to install remedial action scripts.

   EventTracker displays a message box.

   ![Message from webpage]

   **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.
10. Click the **OK** button.

   EventTracker displays **System Status** screen.

   ![System Status Screen](image)

   **Figure 111**

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

   ![Status Refresh Screen](image)

   **Figure 112**

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

### Step 8: Run KeywordMigration.exe file

The Keyword Indexer folder is restructured. To put the old indexed files into the new structure, the `KeywordMigration.exe` utility file has been provided along with build 8.0. This utility migrates the existing keyword files to the new structure.

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

- As the menu options have been changed, the **User Privileges** configuration won’t be retained after upgrade to v8.0 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.

EventTracker displays the Add Privileges window.

c) Select required field and click OK.
Step 9: 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 to v8.0, 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.
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]

Figure 123

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 account change](image)

   Figure 124

**Using the Default Agent Filters in EventTracker version 8.0**

In the EventTracker version 8.0 (Build 29), 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 window](image)

**Figure 125**

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

![EventTracker Agent Configuration](image)

*Figure 127*

**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**.

![DLA Manager Window](image)

**Figure 131**

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

![License Server Configuration Window](image)

**Figure 132**

Here we have taken *MCLOON-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.

![EventTracker Agent Configuration](image)

**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\RemotInstaller 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 directory `Program Files\Prism MicroSystems\EventTracker\RemoteInstaller`. 

---

**Figure 134**

**Figure 135**
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)

**Select the Method of Upgrade.**

- **Windows Domain Network**
  - Account: `toons\Karen` (ex. `mydomain\administrator`)
  - Password: `**********`
  - Confirm Password: `**********`
- **Upgrade over IP (Non Windows Domain)**
  - Choose `Upgrade Over IP` option to upgrade the agent which is outside the domain.
  - Deploy SCAP
  - Deploy WinSCP
  - Install default Remedial Action EXEs on this system

EventTracker:
- `ESWINVM001`

Select `Upgrade` to proceed.

![Figure 139](image)

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.