EventTracker Upgrade Guide

Upgrade to v7.6
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 v7.5 who wish to upgrade to v7.6 Enterprise.
Prism strongly recommends that you read the entire document thoroughly before you begin the upgrade process. For the user’s convenience, this document is separated in two parts: 'Upgrade- Quick View' and 'Upgrade- Detailed View'.

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

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

Before you upgrade:

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

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

*IMPORTANT:

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

New Categories/Alerts/Reports available in v7.6 ................................................................. 4
Prerequisites ................................................................................................................................. 18
Planning ..................................................................................................................................... 18
Upgrade - Quick View ............................................................................................................... 19
  Upgrade from v6.4.x to v7.6.x .................................................................................................. 20
  Common steps for all upgrades ............................................................................................. 21
    Upgrade from v7.0.x to v7.6.x .............................................................................................. 25
    Upgrade from v7.1.x to v7.6.x .............................................................................................. 25
    Upgrade from v7.2.x to v7.6.x .............................................................................................. 25
    Upgrade from v7.3.x to v7.6.x .............................................................................................. 25
    Upgrade from v7.4.x to v7.6.x .............................................................................................. 26
    Upgrade from v7.5.x to v7.6.x .............................................................................................. 26
    Upgrade from v7.6.x to v7.6.x .............................................................................................. 26
Upgrade - Detailed View ......................................................................................................... 27
  Upgrade from v6.4.x to v7.6.x .............................................................................................. 28
  Upgrade Procedure ................................................................................................................ 36
  Upgrade from v7.0.x to v7.6.x .............................................................................................. 84
  Upgrade from v7.1.x to v7.6.x .............................................................................................. 84
  Upgrade from v7.2.x to v7.6.x .............................................................................................. 84
  Upgrade from v7.3.x to v7.6.x .............................................................................................. 85
  Upgrade from v7.4.x to v7.6.x .............................................................................................. 85
  Upgrade from v7.5.x to v7.6.x .............................................................................................. 86
  Upgrade from v7.6.x to v7.6.x .............................................................................................. 101
Configure Service Accounts ..................................................................................................... 102
New Categories/Alerts/Reports available in v7.6

The details about new categories/alerts/reports available in EventTracker v7.6 is mentioned below.

New Categories

- *Security: User account unlocked
- Centrify: Adclient agent started
- Centrify: Adclient agent stopped
- Centrify: Auditing enabled
- Centrify: Configuration settings reloaded
- Centrify: Create desktop failed
- Centrify: Desktop created successfully
- Centrify: DirectAuthorize Agent started
- Centrify: DirectAuthorize agent stopped
- Centrify: Dzdo execution denied
- Centrify: Dzdo execution granted
- Centrify: Join to zone success.
- Centrify: Leave from zone failed
- Centrify: Local cache flushed
- Centrify: Network access successful
- Centrify: PAM Account management granted
- Centrify: PAM Authentication failed
- Centrify: PAM Authentication successful
- Centrify: PAM Session closed
- Centrify: PAM Session opened
- Centrify: Remote login failed
- Centrify: Remote login successful
- Centrify: Run as role attempt failed
- Centrify: Run as role attempt successful
- Centrify: SSHD denied
- Centrify: SSHD granted
- Centrify: Switch to desktop successful
- Cisco IronPort ESA: Email bounced
- Cisco IronPort ESA: Email delivery delayed
- Cisco IronPort ESA: User authentication failed
- Cisco IronPort ESA: User authentication success
- Cisco IronPort WSA: User authentication failed
- Cisco IronPort WSA: Web access allowed
- Cisco IronPort WSA: Web access blocked
- Cisco ISE: Administrator authentication failed
- Cisco ISE: Administrator authentication success
- Cisco ISE: Administrator session rejected
- Cisco ISE: Configuration changed
- Cisco ISE: Configuration deleted
- Cisco ISE: User password change failed
- Cisco ISE: User password changed
- Cisco PIX: User account locked out
- Cisco PIX: User login failed
- Cisco Switch: User login failed
- Clavister: Admin login failed
- Clavister: Admin login success
- Clavister: Admin logout
- Clavister: Application content allowed
- Clavister: Application content denied
- Clavister: Application control disabled
- Clavister: AV signatures missing
- Clavister: AV Update Denied
- Clavister: AV Update Failed
- Clavister: Bad interface status
- Clavister: Blacklisted mail id detected
- Clavister: Blacklisted url blocked
- Clavister: Block0net dropped
- Clavister: Block127net dropped
- Clavister: Blocked filetype
- Clavister: Both peers are active
- Clavister: Both peers are inactive
- Clavister: Compressed data received
- Clavister: Compression ratio violation
- Clavister: Configuration changed
- Clavister: Content filtering disabled
- Clavister: Decompression error
- Clavister: DHCP lease acquired
- Clavister: DHCP lease expired
- Clavister: DHCP lease renewed
- Clavister: DNS resolution failed
- Clavister: Exited reduced functionality
- Clavister: Failed create new ALG session
- Clavister: Failed to add OSPF route
- Clavister: Failed to add route
- Clavister: Failed to bind port
- Clavister: Fan RPM alarm
- Clavister: GPIO alarm
- Clavister: HASync connection failed
- Clavister: IDP DB update failure
• Clavister: IDP evasion
• Clavister: IDP out of memory
• Clavister: IDP virus detected
• Clavister: Intrusion detected
• Clavister: Intrusion Prevented
• Clavister: IP collision
• Clavister: IPsec initialization failed
• Clavister: IPsec Remote Peer is dead
• Clavister: IPsec started successfully
• Clavister: IPsec tunnel disabled
• Clavister: IPsec tunnels limit reached
• Clavister: L2TP client resolve failed
• Clavister: L2TP client resolve successful
• Clavister: L2TP client tunnel up
• Clavister: L2TP connection disallowed
• Clavister: L2TP session closed
• Clavister: L2TP Session up
• Clavister: L2TP tunnel closed
• Clavister: LDAP Authentication failed
• Clavister: LDAP Authentication successful
• Clavister: Malformed packet received
• Clavister: Maximum download size reached
• Clavister: Maximum protocol sessions reached
• Clavister: Memory low
• Clavister: OSPF Authentication mismatch
• Clavister: OSPF Neighbour Connectivity lost
• Clavister: Out of memory
• Clavister: Peer firewall disappeared.
• Clavister: Peer synchronization failed
• Clavister: placed in local lockdown mode
• Clavister: Placed in reduced functionality
• Clavister: PPP authentication failed
• Clavister: PPP tunnel limit exceeded
• Clavister: PPPOE tunnel closed
• Clavister: PPPOE tunnel up
• Clavister: PPTP client connected
• Clavister: PPTP connection disallowed
• Clavister: PPTP session closed
• Clavister: PPTP session up
• Clavister: PPTP tunnel closed
• Clavister: PPTP tunnel up
• Clavister: PPTP user disconnected
• Clavister: RADIUS user authenticated
• Clavister: Received HA heartbeat
• Clavister: Received OSPF data mismatch
- Clavister: Registration hijack detected
- Clavister: Restricted site notice
- Clavister: Route added
- Clavister: Route removed
- Clavister: Ruleset drop packet
- Clavister: Ruleset reject packet
- Clavister: Sender email id mismatched
- Clavister: Shutdown
- Clavister: SLB server offline
- Clavister: SLB server online
- Clavister: SSLVPN connection disallowed
- Clavister: SSLVPN maximum sessions reached
- Clavister: SSLVPN session closed
- Clavister: SSLVPN session created
- Clavister: SSLVPN user disconnected
- Clavister: SSLVPN user logged in
- Clavister: Startup normal
- Clavister: Suspicious data received
- Clavister: temperature alarm
- Clavister: Unable to export route
- Clavister: Unknown vlan id
- Clavister: User authentication failed
- Clavister: User authentication rejected
- Clavister: User authentication successful
- Clavister: User logged out
- Clavister: Virus found
- Clavister: Virus scan failure
- Clavister: Virus url detected
- Clavister: Voltage alarm
- Clavister: WCF server authentication failed
- Clavister: WCF server unreachable
- LOGbinder SQL: Alter command issued
- LOGbinder SQL: Assembly command issued
- LOGbinder SQL: Audit change command issued
- LOGbinder SQL: Audit failure
- LOGbinder SQL: Audit session changed
- LOGbinder SQL: Backup command issued
- LOGbinder SQL: Bulk administration command issued
- LOGbinder SQL: Change command issued
- LOGbinder SQL: Create command issued
- LOGbinder SQL: Database restore command issued
- LOGbinder SQL: Database role member addition failed
- LOGbinder SQL: Database role member addition success
- LOGbinder SQL: Delete command issued
- LOGbinder SQL: Login command issued
- LOGbinder SQL: Member deletion from database role failed
- LOGbinder SQL: Member deletion from database role successful
- LOGbinder SQL: Member deletion from server role failed
- LOGbinder SQL: Member deletion from server role successful
- LOGbinder SQL: Privileges change command issued
- LOGbinder SQL: Privileges change failed
- LOGbinder SQL: Privileges change successful
- LOGbinder SQL: Scope command issued
- LOGbinder SQL: Server principal disable command issued
- LOGbinder SQL: Server principal enable command issued
- LOGbinder SQL: Server role member addition failed
- LOGbinder SQL: Server role member addition failed
- LOGbinder SQL: Server state command issued
- LOGbinder SQL: Transport security command issued
- LOGbinder SQL: User account unlocked
- LOGbinder SQL: User login failed
- LOGbinder SQL: User login successful
- LOGbinder SQL: User logout successful
- LOGbinder SQL: User password change failed
- LOGbinder SQL: User password change successful
- LOGbinder SQL: User password expired
- SEP: Administrator account locked
- SEP: Administrator log on failed
- SEP: Administrator log on success
- SEP: Administrator password changed
- SEP: Administrator property changed
- SEP: Administrator renamed
- SEP: Auto protect disabled
- SEP: Auto protect enabled
- SEP: Backup restore error
- SEP: Client connectivity
- SEP: Computer created
- SEP: Computer deleted
- SEP: Configuration error
- SEP: Content package downloaded
- SEP: Definition unprotected
- SEP: Domain added
- SEP: Domain deleted
- SEP: Domain disabled
- SEP: Domain enabled
- SEP: Domain property changed
- SEP: Domain renamed
- SEP: Group added
- SEP: Group deleted
- SEP: Intrusion prevention disabled
• SEP: Intrusion prevention enabled
• SEP: LDAP user imported
• SEP: Live update started
• SEP: No update found
• SEP: Package exported
• SEP: RDP allowed
• SEP: Scan completed
• SEP: Scan warning
• SEP: Security risk found
• SEP: User created
• SEP: User deleted
• SEP: Web attack blocked
• SEP: Whitelist failure
• Sonicwall: Application control detection
• Sonicwall: Application control prevention
• Sonicwall: Application filter blocked
• Sonicwall: Application filter detection
• Sonicwall: Back orifice attack dropped
• Sonicwall: Backup firewall has transitioned to Active
• Sonicwall: Backup firewall has transitioned to Idle
• Sonicwall: Bad CRL format
• Sonicwall: Connection timed out
• Sonicwall: CRL missing - Issuer requires CRL checking
• Sonicwall: DHCP Server IP conflict detected
• Sonicwall: DHCP Server Received DHCP decline from client
• Sonicwall: DHCP Server sanity check failed
• Sonicwall: DHCP Server sanity check passed
• Sonicwall: DNS rebind attack detected
• Sonicwall: DOS protection on WAN
• Sonicwall: DSL device down
• Sonicwall: DSL device up
• Sonicwall: DSL WAN connected
• Sonicwall: DSL WAN initialized
• Sonicwall: Failed to find certificate
• Sonicwall: FIN-Flooding machine blacklisted
• Sonicwall: Forbidden email attachment disabled
• Sonicwall: FTP port bounce attack dropped
• Sonicwall: ICMP flood attack detected
• Sonicwall: Ini Killer attack dropped
• Sonicwall: Initiator from country blocked
• Sonicwall: Interface link down
• Sonicwall: Interface link up
• Sonicwall: Issuer match failed
• Sonicwall: Issuer path validation failed
• Sonicwall: Land attack dropped
- Sonicwall: MAC IP anti spoof check enforced for hosts
- Sonicwall: Machine removed from FINflood blacklist
- Sonicwall: Machine removed from RSTflood blacklist
- Sonicwall: Machine removed from SYNflood blacklist
- Sonicwall: Malformed DNS packet detected
- Sonicwall: Malformed or unhandled IP packet dropped
- Sonicwall: Maximum events per second threshold exceeded
- Sonicwall: Maximum syslog data per second threshold exceeded
- Sonicwall: NetBus attack dropped
- Sonicwall: NetSpy attack dropped
- Sonicwall: Network security appliance activated
- Sonicwall: Network security appliance activated
- Sonicwall: No firewall rule associated with VPN policy
- Sonicwall: PC card device not detected
- Sonicwall: PC card inserted
- Sonicwall: PC card removed
- Sonicwall: Ping of death dropped
- Sonicwall: Port scan detected
- Sonicwall: Primary firewall transitioned to Active
- Sonicwall: Primary firewall transitioned to Idle
- Sonicwall: Probing failure
- Sonicwall: Remote WAN acceleration device started
- Sonicwall: Responder from country blocked
- Sonicwall: SIM detection failure
- Sonicwall: SSO agent down
- Sonicwall: Suspected botnet initiator blocked
- Sonicwall: SYN flood detected on WAN
- Sonicwall: System fan failure
- Sonicwall: TCP Syn packet dropped
- Sonicwall: Terminal services agent down
- Sonicwall: UDP Flood attack detected
- Sonicwall: Unhandled multicast IPv6 packet dropped
- Syslog: Object access failed
- Syslog: Object creation failed
- Syslog: Object deletion failure
- Syslog: Object modification failure
- Trend Micro: Administrator password changed
- Trend Micro: Firewall policy added
- Trend Micro: Firewall policy deleted
- Trend Micro: Firewall policy modified
- Trend Micro: Grayware/Spyware detection
- Trend Micro: User account created
- Trend Micro: User account deleted
- Trend Micro: User account modified
- Trend Micro: User authentication success
• Trend Micro: User roles created
• Trend Micro: User roles deleted
• Trend Micro: Virus detection
• Trend Micro: Virus quarantine
• Trend Micro: Web security violation
• Websense WSG: Bandwidth web category access blocked
• Websense WSG: Bandwidth web category access permitted
• Websense WSG: Baseline web category access blocked
• Websense WSG: Baseline web category access permitted
• Websense WSG: Productivity web category access blocked
• Websense WSG: Productivity web category access permitted
• Websense WSG: Security web category access blocked
• Websense WSG: Security web category access permitted
• Websense WSG: Social networking web category access blocked
• Websense WSG: Social networking web category access permitted

New Alerts
• Security: User account unlocked
• Centrify: Adclient agent stopped
• Centrify: Configuration settings reloaded
• Centrify: Create desktop failed
• Centrify: DirectAuthorize agent stopped
• Centrify: Dzdo execution denied
• Centrify: Dzdo execution granted
• Centrify: Join to zone success.
• Centrify: PAM Authentication failed
• Centrify: Remote login failed
• Centrify: Run as role attempt failed
• Centrify: SSHD denied
• Cisco ASA: System password changed
• Cisco ASA: User account locked out
• Cisco ASA: User login failed
• Cisco IronPort ESA: Email bounced
• Cisco IronPort ESA: Email delivery delayed
• Cisco IronPort ESA: User authentication failed
• Cisco IronPort WSA: User authentication failed
• Cisco ISE: Administrator authentication failed
• Cisco ISE: Configuration added
• Cisco ISE: Configuration changed
• Cisco ISE: Configuration deleted
- Cisco ISE: User password change failed
- Cisco PIX: User account locked out
- Cisco PIX: User login failed
- Cisco Switch: User login failed
- Clavister: Admin login failed
- Clavister: Admin login success
- Clavister: Application content denied
- Clavister: Application control disabled
- Clavister: AV signatures missing
- Clavister: AV update denied
- Clavister: AV update failed
- Clavister: Bad interface status
- Clavister: Blacklisted mail id detected
- Clavister: Blacklisted URL blocked
- Clavister: BlockOnet dropped
- Clavister: Block127net dropped
- Clavister: Both peers are active
- Clavister: Both peers inactive
- Clavister: Compressed data received
- Clavister: Compression ratio violation
- Clavister: Content filtering disabled
- Clavister: DHCP lease acquired
- Clavister: Fan RPM alarm
- Clavister: GPIO alarm
- Clavister: IDP DB update failure
- Clavister: IDP evasion
- Clavister: IDP out of memory
- Clavister: Intrusion detected
- Clavister: IP collision
- Clavister: IPsec initialization failed
- Clavister: IPsec Remote Peer is dead
- Clavister: IPsec tunnel disabled
- Clavister: IPsec tunnels limit reached
- Clavister: L2TP client resolve failed
- Clavister: L2TP connection disallowed
- Clavister: L2TP tunnel closed
- Clavister: LDAP Authentication failed
- Clavister: Malformed packet received
- Clavister: Maximum download size reached
- Clavister: Maximum protocol sessions reached
- Clavister: Memory low
- Clavister: OSPF neighbor connectivity lost
- Clavister: Peer firewall disappeared
- Clavister: Peer synchronization failed
- Clavister: placed in local lockdown mode
- Clavister: Placed in reduced functionality
- Clavister: PPP authentication failed
- Clavister: PPP tunnel limit exceeded
- Clavister: PPTP connection disallowed
- Clavister: PPTP tunnel closed
- Clavister: Registration hijack detected
- Clavister: Restricted site notice
- Clavister: Route removed
- Clavister: Sender email id mismatched
- Clavister: SLB server offline
- Clavister: SSLVPN connection disallowed
- Clavister: SSLVPN maximum sessions reached
- Clavister: SSLVPN user logged in
- Clavister: Suspicious data received
- Clavister: Suspicious file type blocked
- Clavister: Temperature alarm
- Clavister: User authentication failed
- Clavister: User authentication rejected
- Clavister: Virus detected
- Clavister: Virus found
- Clavister: Virus URL detected
- Clavister: Voltage alarm
- Clavister: WCF server authentication failed
- Clavister: WCF server unreachable
- LOGbinder SQL: Audit change command issued
- LOGbinder SQL: Audit failure
- LOGbinder SQL: Change command issued
- LOGbinder SQL: Delete command issued
- LOGbinder SQL: Member added to database role
- LOGbinder SQL: Member added to server role
- LOGbinder SQL: Member deleted from database role
- LOGbinder SQL: Member deleted from server role
- LOGbinder SQL: Privileges change command issued
- LOGbinder SQL: Privileges change successful
- LOGbinder SQL: User login failed
• LOGbinder SQL: User password expired
• SEP: Administrator account locked
• SEP: Administrator log on failed
• SEP: Administrator password changed
• SEP: Administrator property changed
• SEP: Auto protect disabled
• SEP: Domain disabled
• SEP: Intrusion prevention disabled
• SEP: Live update started
• SEP: No update found
• SEP: Remediation action failed
• SEP: Remediation action pending
• SEP: Scan error
• SEP: Scan stopped
• SEP: Security risk found
• SEP: Service shutdown
• SEP: Virus detected
• SEP: Web attack blocked
• SEP: Whitelist failure
• Sonicwall: Antispam service disabled
• Sonicwall: Antispam service expired
• Sonicwall: Application control detection
• Sonicwall: Application control prevention
• Sonicwall: Application filter blocked
• Sonicwall: Back orifice attack dropped
• Sonicwall: Backup firewall transitioned to active
• Sonicwall: Bad CRL format
• Sonicwall: Certificate import failed
• Sonicwall: CRL validation failure
• Sonicwall: DHCP lease expired
• Sonicwall: DHCP Server IP conflict detected
• Sonicwall: DHCP Server sanity check failed
• Sonicwall: DNS rebind attack detected
• Sonicwall: DSL device down
• Sonicwall: DSL WAN connected
• Sonicwall: DSL WAN initialized
• Sonicwall: Failed to get CRL
• Sonicwall: Failed to process CRL
• Sonicwall: Firewall access rule added
• Sonicwall: Firewall access rule deleted
• Sonicwall: Firewall access rule modified
• Sonicwall: FTP connection dropped
• Sonicwall: FTP logon failure
• Sonicwall: Interface link down
• Sonicwall: Issuer match failed
• Sonicwall: L2TP error
• Sonicwall: Multicast policy list deleted
• Sonicwall: NetBus attack dropped
• Sonicwall: NetSpy attack dropped
• Sonicwall: Outbound access blocked
• Sonicwall: Ping of death dropped
• Sonicwall: PPP Dial-Up dialing failed
• Sonicwall: SIM detection failure
• Sonicwall: SSO agent down
• Sonicwall: System fan failure
• Sonicwall: VPN authentication failed
• Sonicwall: Website access denied
• Syslog: Object access failed
• Syslog: Object creation failed
• Syslog: Object deletion failure
• Syslog: Object modification failure
• Trend Micro: Administrator password changed
• Trend Micro: Grayware/Spyware detected
• Trend Micro: Virus detected
• Trend Micro: Virus quarantine
• Trend Micro: Web security violation detected
• Websense WSG: Bandwidth web category access blocked
• Websense WSG: Baseline web category access blocked
• Websense WSG: Productivity web category access blocked
• Websense WSG: Security web category access blocked
• Websense WSG: Social networking web category access blocked

New Reports
• Centrify Unix Agent-dzdo command execution failure report
• Centrify Unix Agent-Failed user login report
• Centrify Unix Agent-Successful dzdo command execution report
• Centrify Unix Agent-successful user login report
• Centrify Windows Agent-Remote login failure report
• Centrify Windows Agent-Report of successfully accessed network resources
- Centrify Windows Agent-Run as role failed attempts report
- Centrify Windows Agent-Run as role successful attempt report
- Cisco IronPort ESA-Email bounced
- Cisco IronPort ESA-Email delayed
- Cisco IronPort ESA-User authentication failed
- Cisco IronPort ESA-User authentication success
- Cisco IronPort WSA-User authentication failed
- Cisco IronPort WSA-Web access allowed
- Cisco IronPort WSA-Web access blocked
- Clavister-Admin login failed
- Clavister-Application content allowed
- Clavister-Application content denied report
- Clavister-Blacklisted URL blocked report
- Clavister-Blocked file types access
- Clavister-DHCP lease acquired report
- Clavister-IDP evasion report
- Clavister-IDP virus detected report
- Clavister-Intrusion detection
- Clavister-Intrusion prevention
- Clavister-Maximum download size reached
- Clavister-Restricted site access report
- Clavister-Rule set packet dropped
- Clavister-SSL vpn user login report
- Clavister-user authentication failed
- Clavister-Virus detection
- Clavister-Virus url detected
- EventTracker-New enterprise activity report
- EventTracker-Out of ordinary activity report
- LOGbinder SQL-Account Unlocked Report
- LOGbinder SQL-Authentication failed report
- LOGbinder SQL-Authentication Successful Report
- LOGbinder SQL-Database Delete Command Issued Report
- LOGbinder SQL-Database privilege change failed report
- LOGbinder SQL-Database Privileges Change Successful Report
- LOGbinder SQL-Privileges change command issued report
- LOGbinder SQL-SQL Server audit trail integrity report
- Sonicwall-Admin login failed
- Sonicwall-Anti-Spyware detected
- Sonicwall-Application control detection
- Sonicwall-Application control prevention
• Sonicwall-Attacks detection
• Sonicwall-Authentication failed
• Sonicwall-Authentication success
• Sonicwall-DSL activity
• Sonicwall-Firewall access rule change
• Sonicwall-FTP logon details
• Sonicwall-User activity
• Sonicwall-Website access allowed
• Sonicwall-WLAN IDS report
• Symantec Endpoint Protection - At Risk Computers
• Symantec Endpoint Protection - Confirmed Risks
• Symantec Endpoint Protection - Detected Risks Not Confirmed
• Symantec Endpoint Protection - New Risks Detected in the Network
• Symantec Endpoint Protection - Permitted Applications
• Symantec Endpoint Protection - TruScan Proactive Threat Detection Over Time
• Symantec Endpoint Protection - TruScan Proactive Threat Distribution
• Symantec Endpoint Protection - Virus deletion failed
• Symantec Endpoint Protection - Virus found report
• Trend Micro-Administrator password changed report
• Trend Micro-Spyware detected report
• Trend Micro-Virus detected report
• Trend Micro-Virus quarantine report
• Trend Micro-Web reputation report
• Windows-AD object access detail report
Prerequisites

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

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

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

Planning

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

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

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

- After upgrading from v6.4 to v7.6, kindly run the executable file `Prism.AlertsMigration.exe` available in `\InstallDIR\EventTracker\Prism.AlertsMigration.exe` for migrating the incidents.

- For v6.4 to v7.6 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 v7.6, 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.

- Before upgrading EventTracker, user has to export the custom created alerts and categories. After upgrading user has to import the custom created alerts and categories.
After upgrading EventTracker successfully, prior to importing all categories and all alerts from configuration files user has to manually delete existing categories and alerts from application. Then import all categories and all alerts from configuration files.

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 v7.5.x to v7.6.x.

If you have incorporated your company logo into EventTracker, then take a backup of .jpg file of your company logo before uninstalling the EventTracker. You need to replace the backed up image file after installing EventTracker Enterprise.

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

If SSL (HTTPS) is configured in earlier version, then the configuration will not be retained after upgrade to v7.6. 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 v 7.6 should have SQL sysadmin privilege. If the user does not have sufficient permission then an error message is displayed.

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

As the menu options have been changed, the User Privileges configuration won’t be retained after upgrade to v7.6 for non-admin users. You have to reconfigure it again.

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

1. Uninstall the existing version by retaining old configuration and data.
2. Restart the EventTracker manager server or system.

3. Install EventTracker v7.6.

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. To utilize newly added categories/alerts/reports, export and import them.

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

8. Import Knowledge Objects after upgrade. Details are explained in [Upgrade from v7.5.x to v7.6.x](#).

**NOTE:**

- From EventTracker v7.6 onwards, the Behavior Dashlets have been renamed. So after upgrading from v7.x to v7.6, you have to reset the personalization and then configure the dashlets (except for upgrade from v7.6 to v7.6). 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**.
A message displays.

![Message from webpage](image)

Figure 4

d. Select the **OK** button.

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

![Available Dashlets window displays](image)

Figure 5

Available Dashlets window displays.

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

![Available Dashlets](image)

Figure 6

- After upgrading, if the collection master is v7.6 and above versions, and if collection point is using any older version of EventTracker, then incidents will not be visible. If you upgrade collection point to v7.6, post upgrade incidents will only be transferred to collection master.

- The keyword dashboard has to be customized after upgrading to v7.6.
- 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 7.6 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.

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

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

After upgrading from v7.0 to v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

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

The procedure to upgrade from v7.1.x to v7.6.x is same like upgrade from v7.5.x to v7.6.x.

After upgrading from v7.1 to v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

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

The procedure to upgrade from v7.2.x to v7.6.x is same like upgrade from v7.5.x to v7.6.x.

After upgrading from v7.2 to v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

Upgrade from v7.3.x to v7.6.x

The procedure to upgrade from v7.3.x to v7.6.x is same like upgrade from v7.5.x to v7.6.x.
Upgrade from v7.4.x to v7.6.x

The procedure to upgrade from v7.3.x to v7.6.x is same like [upgrade from v7.5.x to v7.6.x](#).

Upgrade from v7.5.x to v7.6.x

The procedure to [upgrade from v7.5.x to v7.6.x](#) is mentioned in the detail section.

Upgrade from v7.6.x to v7.6.x

The procedure to upgrade from v7.6.x to v7.6.x is same like [upgrade from v7.5.x to v7.6.x](#).
Upgrade - Detailed View

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

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

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

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

This section will help you in creating backup files.

1. Open the EventTracker Management Console.
2. Click the Tools menu, and click Import and Export Utility.

EventTracker displays Export-Import Utility window.

3. Select the Category option, if not selected by default.
4. From the Categories field, select the EventTracker categories to be exported, and click the Add button. (Example: My Category).
Click **Add All** button to select all the categories.

5. Click the **Export** button.

EventTracker displays **Select Export File** window.
6. Click **Save** in dropdown to select the file location, enter the **File name**, and click the **Save** button.

EventTracker displays confirmation message box.

![Export Import Utility](image)

**Figure 10**

7. Click the **OK** button.

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

![Export Import Utility](image)

**Figure 11**

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

(OR)

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.
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.
Figure 15

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.

Figure 16

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

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

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

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

   EventTracker displays EventTracker Control Panel.

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

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

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

![Figure 19](image)

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

**Close/terminate all the EventTracker Components**

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

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

EventTracker resumes uninstall process.

**Upgrade Procedure**

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

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

   Control Panel displays the confirmation message.

   (OR)

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

EventTracker displays the confirmation message.

![Figure 22](image)

3. Click the **Yes** button.

EventTracker starts the uninstall process.

![Figure 23](image)

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

![Figure 24](image)
4. Click the No button.
   EventTracker displays ‘Uninstall EventTracker’ dialog box.
   ![Uninstall EventTracker dialog box](image)

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

5. Click the OK button.

**Step 2: Restart the EventTracker manager server or System.**

1. Close all the open applications on the desktop.
2. Click the Start button, and then click Shut Down.
3. Select the Restart option from the dropdown, and then click the OK button.

**Step 3: Install EventTracker v7.6 Enterprise**

Kindly follow the steps mentioned below for upgrade process.

1. To install v7.6, launch EventTrackerSetup.exe.
   EventTracker Pre-Install Check displays below message.
   ![EventTracker Pre-Install Check](image)

2. Click the Yes button.
Welcome to EventTracker Pre-Install check displays.

Figure 27

3. Click the Next > button.

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

   Install Type page displays.

5. Select **Custom** option, and then select the **Next >** button.
Prerequisite page displays.
If prerequisites are not installed, then appropriate message displays. For details please refer EventTracker v7.6 Install Guide.

6. Click the Next > button.

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

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

SQL Express starts downloading and is installed in the background.

Web Server page displays.
10. If IIS Express (Not Installed) option is selected, then click the Next > button.

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

11. Click the Install button.
Disk Usage page displays.
12. Click the **Next >** button.

   Installation Summary page displays.
Define User Group page displays.
13. Select **Active Directory** option.

   **NOTE:** In case you wish to configure EventTracker on local machine, then select Local Machine. For detail instructions, please refer **EventTracker v7.6 Install Guide** – section ‘Procedure to install EventTracker Manager - Custom’.

14. Click the **Next >** button.

   Define User Group page displays.

15. Select **Select existing User Group** option, and then select the **Next >** button.

![Figure 40](image)

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

   Define User page displays.

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

18. Click the Yes button.

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

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

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

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

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

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

InstallShield Wizard updates the folder path.

![Select File Window](image)

**Figure 47**

24. Click **Next >**.

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

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

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

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

(OR)

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

If you have selected **Change Audit** component, then InstallShield Wizard displays **Change Audit SnapShot** dialog box.
**NOTE:** Do not change the install path.

27. Select the **Next >** button.

Ready to install the Program page displays.

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

29. Click the **Next >** button.
30. Click the **Finish** button.

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

InstallShield Wizard displays the **Alert and Report generation settings** dialog box.
32. Select/enter appropriate data in the relevant fields, and then select the **Add** button. InstallShield Wizard displays the last screen.
33. Click **Finish** to conclude the installation process.

   InstallShield Wizard displays the **EventTracker Configuration** screen.
34. 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.

35. 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, Scheduled reports and RSS Feeds

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

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

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

   EventTracker displays EventTracker Control Panel.

   ![EventTracker Control Panel](image)

   Figure 61

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.

![Image of Export Import Utility success message box](image)

**Figure 64**

12. Click the **OK** button.

13. Click **Alerts** option.

![Image of Export Import Utility with Alerts option selected](image)

**Figure 65**

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

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

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

17. Click the **Import** button.

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

19. Select the RSS Feeds option.

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

21. Click the Import button.

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

23. Select Scheduled Reports option.

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

25. Click the Import button.

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

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

**Verify Category:**

1. Logon to **EventTracker Enterprise**.

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

   EventTracker displays ‘Category Management’ Page.

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

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

   Example: My Category.

   ![Category Management](image)

   *(Figure 71)*

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

EventTracker displays **Legacy Reports** dialog box.

![Figure 77](image)

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

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

![Figure 78](image)

**Verify RSS Feeds:**

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

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

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

EventTracker displays Upgrade Remote Agent(s) pop-up window.
Move the cursor on the remote systems name (where the agent is installed), click the dropdown arrow, and select **Upgrade Agent**.

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

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

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

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.

![System Status Screen](image)

Figure 89

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

![System Status Screen](image)

Figure 90

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

**Step 8: Update Trusted list**

In v6.4, if you have made any changes in ‘Trusted Connection List’ then you need to update the same in v7.6 ‘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.

![Figure 91: Trusted Connection List](image)

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

![Figure 92](image)

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.

  1. Click the **Advanced** button.

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

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

IV. Click the **Upgrade** button.

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

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

**Post Upgrade Process:**

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

You need to explicitly set the threat level as per your requirement. To set the threat level,
1. 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 v7.6.x

The upgrade procedure from v7.0 to v7.6 is the same as v7.5 to v7.6. The detail procedure is described in Upgrade from v7.5.x to v7.6.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 v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

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

The upgrade procedure from v7.1 to v7.6 is the same as v7.5 to v7.6. The detail procedure is described in Upgrade from v7.5.x to v7.6.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 v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

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

The upgrade procedure from v7.2 to v7.6 is the same as v7.5 to v7.6. The detail procedure is described in Upgrade from v7.5.x to v7.6.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 v7.6, kindly run the executable file ‘Prism.AlertsMigration.exe’ available in ‘\InstallDIR\EventTracker\Prism.AlertsMigration.exe’ for migrating the incidents.

### Upgrade from v7.3.x to v7.6.x

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

**NOTE:**

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

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

**NOTE:**

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

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

- After upgrading from V7.5 Build 53 to V7.6 Build 21 the OS win 8 and 2012 will be shown as XP Pro and XP respectively on system manager. Either user has to change the system type manually or he can remove those systems and perform auto discover. The upgraded agent systems type will be shown correctly.

- Before upgrading, please take a backup of the database and details are given below.
  a) Double-click [EventTracker Control Panel](#), double-click [Diagnostics](#).
  b) Click the [Backup Configuration](#) button.

    Backup & Restore window displays.

    ![Backup & Restore window](#)

    Figure 97

  c) Browse and select the folder you wish to back up.
  d) Click the [Backup now](#) button.

    After the backup has been taken, go to folder for which the backup has been taken. A file with the extension .bkp will be used to restore later.
Step 1: Close/terminate all the EventTracker Components

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

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

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

Step 2: Uninstall v7.5

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

   ![Add or Remove Programs](image)

   (OR)

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

   Select EventTracker, and then select Uninstall EventTracker.

   EventTracker will display the confirmation message.

   ![Windows Installer](image)

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.

![Figure 100](image)

By default all the file options are selected. Keep the default selection to retain the data and configurations.

5. Click the **Ok** button.

**Step 3: Restart the EventTracker Manager Server or System**

1. Close all the open applications on the desktop.
2. Click the **Start** button and then click **Shut Down** drop down.
3. Select **Restart** option, and then click the **OK** button.

**Step 4: Install EventTracker v7.6 Enterprise**
For the details regarding installation process, please refer ‘EventTracker v7.6 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

(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.

   ![Alert Management Page](image1)

   Figure 103

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

   ![Alert Management Page](image2)

   Figure 104

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

**Verify Filters:**

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

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

EventTracker displays Event Filter configuration page.

Verify RSS Feeds:

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

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

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

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

(OR)

Move the cursor on the remote system's name (where the agent is to be upgraded), click the dropdown arrow, and then click **Upgrade Agent**.
EventTracker displays **Upgrade Remote agent(s) pop-up window.**

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

(OR)

If you wish to deploy agent(s) to Linux or other BSD systems then select the **Upgrade over IP (Non Windows Domain)** option.
6. Check **Install default Remedial Action EXEs on this system** option to install remedial action scripts.

   EventTracker displays a message box.

   ![Message from webpage](image)

   **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.

![Install Agent/Start poll window](image)

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](image1.png)

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

![Latest Status Screen](image2.png)

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

### Step 8: Run KeywordMigration.exe file

The Keyword Indexer folder is restructured. To put the old indexed files into the new structure, the **KeywordMigration.exe** utility file has been provided along with build 7.6. This utility migrates the existing keyword files to the new structure.

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

- As the menu options have been changed, the **User Privileges** configuration won’t be retained after upgrade to v7.6 for non-admin users. You have to reconfigure it again.
  
  a) To configure the privileges, go to **Admin** hyperlink, select **Users**.
EventTracker displays User Management window.

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

![Figure 120](image)

EventTracker displays the Add Privileges window.

c) Select required field and click OK.

![Figure 121](image)

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`.

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.

**Upgrade from v7.6.x to v7.6.x**

The upgrade from v7.6.x to v7.6.x is the same as the Upgrade from v7.5.x to v7.6.x.
Configure Service Accounts

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

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

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

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

![Warning Message]

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 Log On As]

---

EventTracker Enterprise v7.6 Upgrade Guide