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.

© 2013 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

About this Guide ........................................................................................................................................ 8
  Purpose of this guide .............................................................................................................................. 8
  Who should read this guide ................................................................................................................... 8
  Intended Audience .............................................................................................................................. 8
Typographical Conventions ........................................................................................................................ 8
Document Revision Control ........................................................................................................................ 9
How to Get In Touch .................................................................................................................................. 10
  Documentation Support ....................................................................................................................... 10
  Customer Support ................................................................................................................................. 10
Getting Started .......................................................................................................................................... 11
  About EventTracker - Change Audit .................................................................................................... 11
  EventTracker - Change Audit Architecture ......................................................................................... 12
  Ports Used by EventTracker - Change Audit ...................................................................................... 13
  EventTracker - Change Audit Events ................................................................................................... 13
  Start Change Browser ........................................................................................................................... 15
    To start Change Browser .................................................................................................................. 15
  Start Results Summary Console .......................................................................................................... 16
    To start Results Summary Console ................................................................................................. 16
  Change Browser User Interface ........................................................................................................... 19
  EventTracker - Change Audit Icons ..................................................................................................... 22
Change Audit Components ....................................................................................................................... 24
  Change Browser .................................................................................................................................... 24
  Configuration Policy Editor ................................................................................................................... 24
  Results Summary Console ................................................................................................................... 26
Results Summary Console ....................................................................................................................... 27
  Change Policy Dashboard ..................................................................................................................... 27
  Set Dashboard Preferences .................................................................................................................. 27
    To set dashboard preferences ........................................................................................................... 27
  Export Change Data .............................................................................................................................. 31
To export Change Data......................................................................................................................31
View Summary of Change Details ..................................................................................................................34
  To view chart view summary of Change Type................................................................................34
  To view statistical data of Change Type..........................................................................................35
  To view chart view summary of Object Type ..................................................................................35
View Change Details – Change Details Console .................................................................................36
  To view change details in the Change Details console ..................................................................36
Authorize Unauthorized Changes.................................................................................................................43
  To authorize unauthorized changes.................................................................................................43
View Access History.................................................................................................................................48
  To view access history .....................................................................................................................48
View Additional Info on Files..................................................................................................................49
View Change Details in the Change Browser......................................................................................49
  To view change details in the Change Browser ..............................................................................49
View Change Report...............................................................................................................................50
  To view change report.....................................................................................................................50
Configuration Policy Dashboard ..............................................................................................................50
Analyze Policy Comparison Results ..................................................................................................55
  To analyze policy comparison results ..........................................................................................55
Compare Policies.................................................................................................................................57
  To compare policies on demand ....................................................................................................57
Schedule Policy Comparison ..............................................................................................................59
  To schedule policy comparison ..................................................................................................59
Access Result Analysis Console ...........................................................................................................60
  To access Result Analysis Console ..........................................................................................60
Change Browser ........................................................................................................................................62
View Groups............................................................................................................................................62
  To switch to Groups view.................................................................................................................62
View System Details..............................................................................................................................67
  To view system details....................................................................................................................67
View File System Changes ......................................................................................................................68
View Registry Changes ..........................................................................................................................70
Full View................................................................................................................................................71
To view Full View of monitored computers ..........................................................................................71
View Compare Details ............................................................................................................................73
To view compare details of File system items .........................................................................................73
Compare Details of Registry Items ..........................................................................................................74
To view compare details of Registry items .............................................................................................74
View Access History ...............................................................................................................................75
Change View .............................................................................................................................................76
Find Changes .............................................................................................................................................76
Search Strings...........................................................................................................................................79
To Search Strings in File System.............................................................................................................79
Search Strings in Registry .......................................................................................................................81
Generate Change Report .........................................................................................................................83
To generate Change report ......................................................................................................................83
Track File Checksum ...............................................................................................................................84
To view file checksum .............................................................................................................................84
To enable file checksum tracking ..........................................................................................................86
View Access History ...............................................................................................................................87
Prerequisites............................................................................................................................................87
Enable O/S Audit on Files & Folders ......................................................................................................87
Enable O/S Audit on Registry Keys ........................................................................................................95
To enable O/S audit on registry keys ......................................................................................................95
Assign Change Type ...............................................................................................................................97
To modify Change Type ..........................................................................................................................97
Snapshots ..................................................................................................................................................99
Take Snapshots On Demand ..................................................................................................................99
To take Snapshots on demand ...............................................................................................................99
Edit Snapshots .......................................................................................................................................102
To edit Snapshot settings ......................................................................................................................102
Reinitialize Snapshots ...........................................................................................................................105
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Change Audit User Guide</td>
<td></td>
</tr>
<tr>
<td>To re-initialize Snapshots</td>
<td>105</td>
</tr>
<tr>
<td>Back up Snapshots</td>
<td>107</td>
</tr>
<tr>
<td>To back up Snapshot</td>
<td>107</td>
</tr>
<tr>
<td>Recover Snapshots</td>
<td>110</td>
</tr>
<tr>
<td>To recover Snapshots</td>
<td>110</td>
</tr>
<tr>
<td>Configuration</td>
<td>113</td>
</tr>
<tr>
<td>Global Configuration</td>
<td>113</td>
</tr>
<tr>
<td>To Set up Global Configuration</td>
<td>113</td>
</tr>
<tr>
<td>To configure Change Type</td>
<td>120</td>
</tr>
<tr>
<td>To add File Change Type</td>
<td>125</td>
</tr>
<tr>
<td>Apply Global Configuration</td>
<td>131</td>
</tr>
<tr>
<td>To apply Global Configuration</td>
<td>131</td>
</tr>
<tr>
<td>System Configuration</td>
<td>132</td>
</tr>
<tr>
<td>To set up System Configuration</td>
<td>133</td>
</tr>
<tr>
<td>Apply System Configuration -- Local System</td>
<td>134</td>
</tr>
<tr>
<td>To apply System Configuration to current system</td>
<td>134</td>
</tr>
<tr>
<td>Apply System Configuration -- Remote Systems</td>
<td>135</td>
</tr>
<tr>
<td>To apply System Configuration to remote systems</td>
<td>135</td>
</tr>
<tr>
<td>Apply System Configuration -- All Systems</td>
<td>137</td>
</tr>
<tr>
<td>To apply System Configuration to all systems</td>
<td>137</td>
</tr>
<tr>
<td>Search the Change Events (EventTracker Search Interface)</td>
<td>139</td>
</tr>
<tr>
<td>Option to Log / Forward Snapshot Results to EventTracker</td>
<td>139</td>
</tr>
<tr>
<td>Generate Reports against Change Audit Category</td>
<td>142</td>
</tr>
<tr>
<td>Filters</td>
<td>144</td>
</tr>
<tr>
<td>Normal Filters</td>
<td>144</td>
</tr>
<tr>
<td>Customized Filters</td>
<td>144</td>
</tr>
<tr>
<td>Difference between Customized Filters and Normal Filters</td>
<td>144</td>
</tr>
<tr>
<td>Demonstration</td>
<td>145</td>
</tr>
<tr>
<td>Customize Filters</td>
<td>156</td>
</tr>
<tr>
<td>To customize filters</td>
<td>156</td>
</tr>
<tr>
<td>Apply Filters -- Local System</td>
<td>158</td>
</tr>
</tbody>
</table>
To apply filters to local system ................................................................. 158
Apply Filters – Remote Systems ................................................................. 159
   To apply filters to remote system .......................................................... 159
Apply Filters – All Systems ........................................................................ 162
   To apply filters to all systems ............................................................... 162
Remove Filters – Local System ................................................................. 165
   To remove filters in local system .......................................................... 165
Remove Filters – Remote Systems ............................................................. 166
   To remove filters in remote systems ....................................................... 166
Remove Filters – All Systems .................................................................... 169
   To remove filters in all systems ............................................................ 169
Restore Registry sub tree ......................................................................... 171
   To restore registry sub tree ................................................................. 171
View Restore Logs .................................................................................. 172
   To view restore logs ........................................................................... 173
Undo Restore ........................................................................................... 173
   To undo restore .................................................................................. 173
Configuration Policy Editor ...................................................................... 175
   Configuration Policy .......................................................................... 175
Create Configuration Policies .................................................................. 175
      To create Configuration Policies ...................................................... 175
To Search a File ....................................................................................... 179
To Search a Folder ................................................................................... 181
To Search a Folder and Sub-folder .......................................................... 185
To Search Registry Key in Hive ................................................................. 186
Edit Policy Description ........................................................................... 189
Edit File/Registry Key Description .......................................................... 190
Add Policy Items ..................................................................................... 191
   To add policy items ............................................................................ 191
Compare Systems .................................................................................... 192
   To compare systems .......................................................................... 192
Schedule Policy Comparison ................................................................. 198
  To schedule Policy comparison ......................................................... 198
Export Configuration Policies ............................................................... 202
  To export configuration Policies ....................................................... 202
Import Configuration Policies ............................................................... 202
  To import configuration Policies ...................................................... 202
Glossary ......................................................................................... 203
About this Guide

Purpose of this guide

This guide will enable you to use every option of EventTracker - Change Audit and provides detailed procedures for the same.

Who should read this guide

Intended Audience

- Administrators who are assigned the task of monitoring and tracking file system changes and registry changes using EventTracker - Change Audit
- Operations personnel who manage day-to-day operations using EventTracker - Change Audit

Typographical Conventions

Before you start, it is important to understand the typographical conventions used in this guide:

<table>
<thead>
<tr>
<th>This</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italics</td>
<td>References to other guides and documents.</td>
</tr>
<tr>
<td>Bold</td>
<td>Input fields, radio button names, check boxes, dropdown lists, links on screens, menus, and menu options.</td>
</tr>
<tr>
<td>CAPS</td>
<td>Keys on the keyboard and buttons on screens.</td>
</tr>
<tr>
<td>{Text_to_customize}</td>
<td>A placeholder for something that you must customize.</td>
</tr>
<tr>
<td>Constant Width</td>
<td>Text that you enter, program code, files and directory names, function names.</td>
</tr>
<tr>
<td>❱</td>
<td>A Note, providing additional information about a certain topic.</td>
</tr>
</tbody>
</table>
Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First three letters – name of the product
- Second two numbers – version of the product
- Third three numbers – build of the product
- Last four letters – document description

The document revision control number for this guide is as given below:

<table>
<thead>
<tr>
<th>File Name</th>
<th>EventTracker Change Audit User Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Updated in accordance with release version 7.x.</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Release Date</td>
<td>Release Date April 30, 2013</td>
</tr>
</tbody>
</table>
How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support

Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@eventtracker.com.

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventTracker - Change Audit, contact us by e-mail at support@eventtracker.com.

While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
- The type of hardware, including the server configuration and network hardware if available
- The version of EventTracker - Change Audit and the operating system
- The exact message that appeared when the problem occurred or any other error messages that appeared on your screen
- A description of how you tried to solve the problem
Getting Started

About EventTracker - Change Audit

EventTracker - Change Audit is a diagnostic tool that targets the broad area of Change Management. Change Management is a concept by which all system changes are tracked periodically, intelligently and reported on demand for the user to analyze, understand and if needed recover from change.

The advantage of change management is that it provides the user information regarding the changes that could be harmful. During the course of a day there are thousands of changes happening on your Windows system, using an effective change management solution you could view the changes with only the critical changes being highlighted, besides having the non-critical folders and registry hives filtered out. In short, change management is a process by which the user can monitor, analyze, understand and recover from change.

- Results Summary Console
- Result Analysis Console
- Policy Comparison Results console
- Search Audit Details
- Track File Checksum
- Change Classification Rules

EventTracker - Change Audit helps you:

- Configure Change Audit to log Snapshot results as Change Audit events locally (Windows Application logs) or directly forward those events as Traps to EventTracker.
- Configure Configuration Policies (Configuration Policy Editor).
- Compare systems based on Configuration Policies. Compare systems can be used generate report if there is a discrepancies between the existing configuration and the actual configuration of systems.
- Export / Import Configuration Policies.
- Schedule Policy comparison.
- Identify and cure your systems of new viruses before your Anti-Virus provider comes up with a cure.
- Capture and store system Snapshots. Snapshots contain detailed information about the file system, registry, and system configuration.
- Track registry changes and restore ‘last known good configuration’ registry settings.
- Schedule or take Snapshots on demand.
- Edit Snapshots.
• Reinitialize Snapshots.
• Compare Snapshots. Unlike first generation products, only differences are stored to maximize speed and minimize disk space usage.
• Configure Filters to filter out non-critical directories and registry hives. You can also turn off the filters anytime you please.
• Create, edit, and delete Logical Computer Groups.
• Create, edit, and delete Configuration Policies.
• Set and apply Global configuration settings.
• Set and apply System configuration settings.

Change Audit provides an organization a strong handle in managing the Windows systems in their enterprise. The key benefits are:

• **Minimize downtime, Increase Availability**: System downtime causes significant losses in customer retention, brand reliability and most importantly ‘revenue.”
• **Reduce fault diagnostic time**.
• **Reduce Total Cost of Ownership (TCO)**: TCO will reduce drastically when system downtime is reduced. Reducing system downtime means higher availability of help desk staff for other tasks, better utilization of technical staff that uses these systems besides enabling higher system availability.
• **Improve control of critical systems / applications**.
• **Enhance security**: Change Audit can provide you with detailed change reports that can help identify breaches in security.
• **Have insurance against change**: With Change Audit installed a user is confident about installing new software or making major configuration changes as he has information available that can help in reverting back to a good configuration in case of any problem.

**EventTracker - Change Audit Architecture**

EventTracker - Change Audit is constituted of two Main Modules, namely the Manager, and the Client. The Manager in turn is constituted of 3 components: Service, Console GUI, and a backend database that stores enterprise change data.

A typical deployment of EventTracker - Change Audit can include one Console and multiple Clients installed on each client machine.

EventTracker - Change Audit architecture is completely centralized and provides you with the control to manage all systems on your network from one console.
## Ports Used by EventTracker - Change Audit

EventTracker - Change Audit uses two TCP port to communicate between EventTracker - Change Audit Client and Server.
Port – 14502 (TCP bi-directional) is used for snapshot transfer between client and Server.
Port – 14508 (TCP bi-directional) is used for real-time comparing any system with golden snapshot located at server.

**NOTE:**
Had you enabled firewall on the EventTracker - Change Audit Manager computer add ports 14502 and 14508 to the firewall exceptions list.

## EventTracker - Change Audit Events

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Cause of Event</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>3400</td>
<td>After taking the system snapshot if Change Audit detects that any new file is added then this event is generated.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3401</td>
<td>After taking the system snapshot if Change Audit detects that any file is modified then this event is generated.</td>
<td>Check if the changes made to file are intentional and then take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3402</td>
<td>After taking the system snapshot if Change Audit detects that any file is deleted then this event is generated</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3403</td>
<td>After taking the system snapshot Change Audit generates this event to summarize all the detected file changes.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3404</td>
<td>After taking the system snapshot if Change Audit detects that any new registry key is added then this event is generated.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3405</td>
<td>After taking the system snapshot if Change Audit detects that any registry key is modified then this event is generated.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3406</td>
<td>After taking the system snapshot if Change Audit detects that any registry key is added then this event is generated.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Description</td>
<td>Action</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>3407</td>
<td>Audit detects that any registry key is deleted then this event is generated.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3408</td>
<td>After taking the system snapshot Change Audit generates this event to summarize all the detected registry changes.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3409</td>
<td>If Change Audit detects any file changes (Addition, modification and deletion) after comparing a configuration policy with the system it generates this event for each file change detected.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3410</td>
<td>If Change Audit detects any registry changes (Addition, modification and deletion) after comparing a configuration policy with the system it generates this event for each registry change detected.</td>
<td>Take appropriate action for the detected change.</td>
</tr>
<tr>
<td>3411</td>
<td>When Change Audit evaluates a category and its result is true then this event is generated.</td>
<td>Take appropriate action.</td>
</tr>
<tr>
<td>3412</td>
<td>When the change type of an object is modified then this event is generated.</td>
<td>Take appropriate action.</td>
</tr>
<tr>
<td>3413</td>
<td>When the Change Audit engine takes a snapshot.</td>
<td>Take appropriate action.</td>
</tr>
<tr>
<td>3414</td>
<td>When the Change Audit engine sends snapshot files to manager.</td>
<td>Take appropriate action.</td>
</tr>
<tr>
<td>3415</td>
<td>When the Change Audit engine performs a scheduled policy comparison.</td>
<td>Take appropriate action.</td>
</tr>
<tr>
<td>3415</td>
<td>When the Change Audit engine performs inventory updation.</td>
<td>Take appropriate action.</td>
</tr>
</tbody>
</table>
When the Change Audit engine executes the policy comparison request from manager.

| 3416 | Take appropriate action. |

Start Change Browser

This option helps you start EventTracker – Change Browser from the Manager and the Client computers.

To start Change Browser

1. Click the Start button, select Programs, and then select Prism Microsystems.
2. Select EventTracker Control Panel, select Change Audit, and then select the Change Browser.
   (OR)
   Double-click Change Audit on the desktop EventTracker Control Panel.
   EventTracker displays the Results Summary Console.
   Click Change Browser on the toolbar.
   EventTracker - Change Audit displays the Change Browser console indicating that the Baseline snapshot is in progress.

   Figure 1

EventTracker - Change Audit displays the Change Browser console indicating that the Automated snapshot is in progress.

   Figure 2
NOTE:

After successful installation, EventTracker - Change Audit takes a baseline Snapshot. EventTracker - Change Audit takes one more Snapshot immediately following the baseline Snapshot after a specific time interval.

If the Baseline and Automated snapshots are over, EventTracker - Change Audit loads the system, compares the two snapshots, and displays the Change View.

Start Results Summary Console

This option helps you start Results Summary Console from the Manager computer.

To start Results Summary Console

1. Double-click Change Audit Results on the desktop Control Panel.
EventTracker - Change Audit displays the Results Summary console with empty panes if the snapshot is in progress. EventTracker - Change Audit displays the graph view of the manager and the EventTracker - Change Audit managed computers.

**Figure 4**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Group</td>
<td>This drop-down list displays all the system groups discovered by the Client Manager.</td>
</tr>
<tr>
<td>View Type</td>
<td>Select an option to view chart or data on the console.</td>
</tr>
<tr>
<td>View By</td>
<td>Change Type</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>Authorized</td>
</tr>
<tr>
<td></td>
<td>Unauthorized</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
</tr>
<tr>
<td></td>
<td>Business Knowledge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object Type</th>
<th>Files Added</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Files Deleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Files Modified</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registry Added</td>
<td>Registry keys added</td>
</tr>
<tr>
<td></td>
<td>Registry Deleted</td>
<td>Registry keys deleted</td>
</tr>
<tr>
<td></td>
<td>Registry Modified</td>
<td>Registry keys modified</td>
</tr>
</tbody>
</table>
Change Browser User Interface

Change Browser is the first component of EventTracker - Change Audit. This section helps you understand the Change Browser user interface. To work with EventTracker - Change Audit effectively, a thorough understanding of its user interface is very important.

Figure 5

**Title Bar**

The strip at the top of the Change Browser is the Title Bar. Title Bar displays the name of the application. You cannot customize, move, or drag the Title Bar.

**Menu Bar**

The strip next to Title Bar is the Menu Bar. Menu Bar contains menus. Each Menu contains a list of commands and shortcut keys to carry out a specific task. You cannot customize, move, or drag the Menu Bar.
System Bar

System pane displays the monitored systems.

Toolbar

The third strip is the Toolbar. Toolbar contains command buttons with images. Frequently used options are provided on the Toolbar. You cannot customize, move, or drag the Toolbar.

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Switch to Groups view.</td>
</tr>
<tr>
<td>Change View</td>
<td>Toggle between Full View and Change View.</td>
</tr>
<tr>
<td>New Snap</td>
<td>Take new Snapshots of the selected system.</td>
</tr>
<tr>
<td></td>
<td>Search strings in File System or Registry.</td>
</tr>
<tr>
<td>Show Next Change</td>
<td>View consecutive changes in File System and Registry.</td>
</tr>
<tr>
<td>Change Report</td>
<td>View change reports based on Snapshots and change reports based on Policies.</td>
</tr>
</tbody>
</table>

Mouse over ToolTip for command buttons help you know the purpose the buttons serve.

Workspace

Workspace consists of left pane and right pane and a strip below the toolbar. The strip contains two drop-down lists that list out Snapshots available for comparison. The right drop-down list contains all the available Snapshots and the left one contains only the latest one.

By default, EventTracker - Change Audit selects the Manager system and displays Drives and Registry trees on the left pane and hardware details on the right pane.
If you expand and select items under Drives or Registry tree, EventTracker – Change Audit compares the Snapshots, typically, Baseline Snapshot with the first Snapshot taken after a specific interval following the Baseline Snapshot and displays the comparison details on the left pane. EventTracker - Change Audit displays the change details that include Addition, deletion, and modification of files, folders, and registry keys in this Change View. EventTracker - Change Audit takes these two Snapshots immediately after installation with no human intervention.

EventTracker - Change Audit displays mouse over ToolTip for all the items on both the panes.

**Status Bar**

EventTracker - Change Audit displays IP address of the selected system in the first section, type and filter status of the item clicked on both the panes in the second section, total count of items modified in the third section, total count of items added in the fourth section, total count of items deleted in the fifth section, and total count of nodes in the sixth section.
### EventTracker - Change Audit Icons

EventTracker - Change Audit Icons represent EventTracker - Change Audit objects.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>▼</td>
<td>Total count of all items added to the File System or Registry.</td>
</tr>
<tr>
<td>▼</td>
<td>Total count of all items modified in the File System or Registry.</td>
</tr>
<tr>
<td>▼</td>
<td>Total count of all items deleted from the File System or Registry.</td>
</tr>
<tr>
<td>📄</td>
<td>An item added to the File System or Registry.</td>
</tr>
<tr>
<td>🔄</td>
<td>An item modified in the File System or Registry.</td>
</tr>
<tr>
<td>✗</td>
<td>An item deleted from the File System or Registry.</td>
</tr>
<tr>
<td>🗑️</td>
<td>Unaltered item.</td>
</tr>
<tr>
<td>🗑️</td>
<td>Items in File System or Registry filtered from tracking.</td>
</tr>
<tr>
<td>🗄️</td>
<td>Folders.</td>
</tr>
<tr>
<td>📖</td>
<td>Files.</td>
</tr>
<tr>
<td>📘</td>
<td>Registry.</td>
</tr>
<tr>
<td>🗄️</td>
<td>File system folders and Registry keys.</td>
</tr>
<tr>
<td>🗄️</td>
<td>Computer Groups.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>🔄</td>
<td>Snapshot in progress.</td>
</tr>
<tr>
<td>🔄</td>
<td>File changes found.</td>
</tr>
<tr>
<td>🔄</td>
<td>Registry changes found.</td>
</tr>
<tr>
<td>🔄</td>
<td>File and registry changes found.</td>
</tr>
<tr>
<td>🔄</td>
<td>No changes found.</td>
</tr>
<tr>
<td>🎯</td>
<td>Fresh item.</td>
</tr>
<tr>
<td>✅</td>
<td>Items accepted.</td>
</tr>
<tr>
<td>⬠</td>
<td>Items ignored.</td>
</tr>
<tr>
<td>✗</td>
<td>Items rejected.</td>
</tr>
</tbody>
</table>
Change Audit Components

Change Browser

The Change Browser is an information rich browser that displays a comparison of current versus previous snapshots.

The Change Browser is very similar to Microsoft Windows Explorer which is the most used utility to diagnose problems. The color-coded presentation of useful information about system changes helps you resolve the problem quickly.

Configuration Policy Editor

Configuration Policy Editor helps you set Configuration Policies for your enterprise environment. Policies are grouping together of registry hives and directories of a specific application. Once a Policy is created, then changes to any file or registry item belonging to that particular Policy will be indicated as change to the Policy. It is easy to monitor changes through Policies rather than run through the entire file system and registry.
Figure 6

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add Policy</td>
<td>Create a new Policy.</td>
</tr>
<tr>
<td>Edit Description</td>
<td>Edit description of the Policy.</td>
</tr>
<tr>
<td>Remove Policy</td>
<td>Delete the selected Policy.</td>
</tr>
<tr>
<td>Compare Systems</td>
<td>Compare the monitored computers against the selected policy.</td>
</tr>
</tbody>
</table>

File Details pane

| Remove                  | Remove the selected item from the Policy. |
| Add Item                | Add an item to the Policy.                |
| Edit Description        | Edit description of the selected item.    |
| Select All              | Select this check box to select all files. |
### Registry Details pane

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove</td>
<td>Remove the selected item from the Policy.</td>
</tr>
<tr>
<td>Add Item</td>
<td>Add an item to the Policy.</td>
</tr>
<tr>
<td>Edit Description</td>
<td>Edit description of the selected item.</td>
</tr>
<tr>
<td>Select All</td>
<td>Select this check box to select all keys.</td>
</tr>
</tbody>
</table>

**Policies pane:** Displays the list of configuration policies configured.

**File Details pane:** Displays the list of files and folders associated with the policy selected in the policies pane.

**Registry Details pane:** Displays the list of registry keys associated with the policy selected in the policies pane.

---

### Results Summary Console

**Change Policy Dashboard** displays the summary of snapshot results.

**Configuration Policy Dashboard** displays the most recent results of on demand policy comparison done through Compare Systems console and scheduled policy comparison done through Policy Comparison Scheduler.
Results Summary Console

**NOTE:** You can access Results Summary Console from the EventTracker - Change Audit manager computer alone and not from the EventTracker - Change Audit managed computers.

Change Policy Dashboard

*Change Policy Dashboard* displays the summary of snapshot results.

Set Dashboard Preferences

This option helps you set preferences to view change details. Preferences you set are reflected on the desktop Results Summary Console and the Web interface (Change Audit -> Change Policy Dashboard) as well.

To set dashboard preferences

1. Click the **Tools** menu and then select the **Dashboard Preferences** option.

   Reports Summary Console displays the Dashboard Preferences window.
Field | Description
--- | ---
Enable Auto Refresh | Select this check box if you prefer EventTracker – Change Audit to refresh the Results Summary Console automatically. EventTracker - Change Audit enables the “Auto Refresh Interval [in seconds]” drop-down list. Set the interval for EventTracker - Change Audit to refresh the console.

Change Summary Dashboard

Make “View by Change Type” as the default option | EventTracker – Change Audit selects this check box by default. Clear this check box if you prefer to view Object Type as default view.

Select the segments to view in graph for | EventTracker – Change Audit selects the ‘View By Change Type” option by default and displays the related segments with respective color codes. You can select or clear the check boxes against the respective segments.
2. Set the preferences and then click **OK**.
3. To change the color of the preferred segment, click the color strip.
   EventTracker - Change Audit displays the browse button.
4. Click the browse button.
EventTracker - Change Audit displays the color palette.
5. Select the color and then click **OK**.

Export Change Data

This option helps you to export the details about the files that are present on your system. The exported data can be further utilized to monitor the files/processes as discussed in EventTracker Enterprise User Guide -> **List Management**. Later this list can be generated to track irrelevant files/processes.

To export Change Data

1. Click the **Tools** menu and then select **Export Change Data**.

   Change Data Export Utility window displays.
2. Select the required **Output Columns** or the **Select All** option.
3. In **System(s)** pane, select the required systems.
4. In **File Type(s)** pane, select **All Files** option or enter the required file extensions separated by comma.
5. In **Output Settings** pane, browse the **CSV File Path**.
6. If required select **File Header, Write Log File, Create separate file for each system** options.
7. Select the **Export** button.  
A successful message displays.
You can view the data regarding the files in the respective CSV file. You can import this list as discussed in List Management.

View Summary of Change Details

To view chart view summary of Change Type

By default, EventTracker displays chart view summary of Authorized, Unauthorized, Configuration, and Business Knowledge Change Types for all managed systems irrespective of the system groups.

Figure 13
To view statistical data of Change Type

1. Select the **Data** option from the **View Type** drop-down list.
   (OR)
   Double-click the pie chart to view data.
   EventTracker displays the statistical data of Change Type.

![Figure 14](image)

To view chart view summary of Object Type

1. Select the **Object Type** option from the **View By** drop-down list.
   EventTracker displays the chart view summary of Object Type.
View Change Details – Change Details Console

To view change details in the Change Details console

1. Click the hyperlink under the System Name column to view change details of that particular system in the Change browser.
2. Click the hyperlink under the respective columns of Change Type/Object Type entities.
Figure 16

Results Summary Console displays the Change Details console.
NOTE:

Results Summary Console enables the "Authorize" button when changes to "Unauthorized" items (*.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, and *.vxd) are detected. Results Summary Console enables the "More Info" button when new/modified/deleted DLLs and EXEs are detected.

3. Select an item and then click Filter to add new filter to System or Global Configuration. Results Summary Console displays the Add Filters console.
4. Select an appropriate option under 'Filter the objects by using the filter string to match'.
5. Select 'All systems' option under 'Apply this filter on' to add this filter to Global Configuration. Click OK on the Change Details console.
   Results Summary Console displays the confirmation message box.

6. Click Yes.
   Results Summary Console displays the Applying Configuration dialog box with appropriate message.
7. Click **View Details**.
   Results Summary Console displays the Apply configuration results window.

8. Click **Finish** on the Applying Configuration dialog box.
9. Open the **Change Browser**.
10. Click the **Options** menu and select the **Global Configuration** option.
11. Click the **Filters** tab.
   EventTracker - Change Audit displays the newly added Global Filter.
12. Select ‘This system’ option under ‘Apply this filter on’ to add this filter to System Configuration.
13. Open the Change Browser.
14. Load the system that you want to view the newly added filter.
15. Click the Options menu and select the System Configuration option.
16. Click the Filters tab.
Check and click ‘Remove’ to UnFilter checked nodes.
To filter right click on a folder or registry key in the change browser and select the option.

Figure 23
Authorize Unauthorized Changes
To authorize unauthorized changes

1. Click the hyperlink in the Unauthorized column.

Results Summary Console displays the Change Details console.
Select the **Select / Unselect All unauthorized items** check box to select all unauthorized items if not selected. You can also select / unselect individual items by selecting or clearing the respective check box.

(OR)

Click **Group by Path** to view all unauthorized changes based on location. Results Summary Console displays the Group by Path window.
3. Select the items and then click **Authorize**.
   Results Summary Console displays the Authorization Comment window.
   Note that each path selected, Results Summary Console displays a separate Authorization Comment window.
4. Type an appropriate comment.
5. Select the **Apply same comment for all items** check box if you wish to apply the comment for all items.
6. Click **OK**.
   If you leave the comment field empty, Results Summary Console displays the confirmation message box.

7. Click **Close** on the Group by Path window.
8. Click **OK** on the Change Details window.
   Results Summary Console displays the confirmation message box.
9. Click **Yes** to save the changes.
   EventTracker - Change Audit authorizes the unauthorized changes.
View Access History

To view access history

NOTE:

It is mandatory to enable Windows Object Access auditing on the target system prior to using this feature. For further details, refer Prerequisites under “Viewing Access History” section.

1. Select an item and then click **Access History**.
   EventTracker - Change Audit displays the progress bar.
   EventTracker - Change Audit displays the access history of the selected item.

2. Click **Export** to export the report into Excel format.
   EventTracker - Change Audit displays the Save As window.

3. Select destination folder, type an appropriate name in the File name field, and then click **Save**.
   EventTracker - Change Audit displays the message box.
4. Click OK. 
EventTracker - Change Audit displays the exported report.

View Additional Info on Files

**NOTE:**

You can view more info only on Authorized and Unauthorized items.

1. Select an item and then click More Info.


View Change Details in the Change Browser

To view change details in the Change Browser

1. Click a hyperlink under **System Name** column.

   EventTracker - Change Audit loads the system in the Change Browser and displays the changes.

   (OR)

   Click the **Change Policy** menu and select the **Change Browser** option.

   EventTracker - Change Audit displays the Change Browser.

   Double-click the system that you want to view change details.

   (OR)

   Press **M** holding **CTRL** on your keyboard.

   EventTracker - Change Audit displays the Change Browser.

   Double-click the system that you want to view change details.
View Change Report

To view change report

1. Select a system.
2. Click the Change Policy menu and select the View Report option.

Results Summary Console displays the report in the Notepad.

Configuration Policy Dashboard

Configuration Policy Dashboard displays the most recent results of on demand policy comparison done through Compare Systems console and scheduled policy comparison done through Policy Comparison Scheduler.
<table>
<thead>
<tr>
<th>Icon</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Snapshot in progress.</td>
</tr>
<tr>
<td>🎨</td>
<td>No changes found.</td>
</tr>
<tr>
<td>📞</td>
<td>File changes found.</td>
</tr>
<tr>
<td>🤑</td>
<td>Registry changes found.</td>
</tr>
<tr>
<td>📝📅</td>
<td>File and registry changes found.</td>
</tr>
</tbody>
</table>

1. Click the name of the policy in the **Policy Name** column to view and edit policy details in the Configuration Policy Editor.  
   (OR)  
   Click the **Analyze** drop-down button.  
   EventTracker - Change Audit displays the shortcut menu.  
   From the shortcut menu, choose **Edit Policy**.  
   (OR)  
   Right-click a record.  
   EventTracker - Change Audit displays the shortcut menu.  
   From the shortcut menu, choose **Edit Policy**.
2. Click the name of the system in the **System Name** column to view compare system details. You can also compare policies on systems on demand.

   (OR)

   Click the **Analyze** drop-down button.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose **Run**.

   (OR)

   Right-click a record.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose **Run**.
3. Click the frequency of the schedule in the **Schedule Frequency** column to view and schedule policy comparison.
   (OR)
   Click the **Analyze** drop-down button.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose **Schedule**.
   (OR)
   Right-click a record.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose **Schedule**.
### Figure 35

<table>
<thead>
<tr>
<th>Title</th>
<th>Policy Name</th>
<th>Frequency</th>
<th>Scheduled At</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Schedule for Sample Critical File</td>
<td>Sample Critical File Policy</td>
<td>Daily</td>
<td>8/6/2010 2:00:00 AM</td>
</tr>
</tbody>
</table>

**Policy Comparison Scheduler**

- New Schedule
- Edit
- Delete
- Close
Analyze Policy Comparison Results

To analyze policy comparison results

1. Click an item in the **Integrity Violations** column.

   (OR)

   Select an item.

   Click the **Analyze** button.

   Results Summary Console displays the shortcut menu.

   From the shortcut menu, choose **Analyze**.

   Results Summary Console displays the Policy Comparison Results window.

---

**Figure 36**

---
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Top pane</strong></td>
<td></td>
</tr>
<tr>
<td>System Name</td>
<td>Name of the target system where the policy is compared.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>Name of the policy compared on the target system.</td>
</tr>
<tr>
<td>Total Violations</td>
<td>Total no. of violations detected.</td>
</tr>
<tr>
<td>Compared on</td>
<td>Date and time when the policy was compared.</td>
</tr>
<tr>
<td>Policy Description</td>
<td>Description of the policy.</td>
</tr>
<tr>
<td><strong>Left pane</strong></td>
<td></td>
</tr>
<tr>
<td>Item Name</td>
<td>Name of the policy item.</td>
</tr>
<tr>
<td><strong>Right pane</strong></td>
<td></td>
</tr>
<tr>
<td>Policy Values</td>
<td>Values of the policy item selected in the left pane when the policy was</td>
</tr>
<tr>
<td></td>
<td>configured.</td>
</tr>
<tr>
<td>Actual Values</td>
<td>Actual Values of the policy item selected in the left pane after the policy</td>
</tr>
<tr>
<td></td>
<td>comparison is done. This reflects any change in the value of the policy</td>
</tr>
<tr>
<td></td>
<td>item.</td>
</tr>
<tr>
<td>Item Description</td>
<td>Description of the item selected in the left pane is displayed at the</td>
</tr>
<tr>
<td></td>
<td>bottom of the right pane.</td>
</tr>
</tbody>
</table>

**Field** | **Description**
--- | ---
Tool tips are provided to understand the purpose of buttons. Move the mouse cursor on the buttons.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next</td>
<td>Move to the next item.</td>
</tr>
<tr>
<td>Previous</td>
<td>Move to the previous item.</td>
</tr>
<tr>
<td>Accept</td>
<td>If changes are found for the selected item, you can update the master policy with the new value.</td>
</tr>
<tr>
<td>Reject</td>
<td>If you find an item to be irrelevant to the present context, you can select and remove that item from the master policy.</td>
</tr>
<tr>
<td>Ignore</td>
<td>When you generate a report, ignored items will not be considered for report generation. Note that these items are not removed from the master policy.</td>
</tr>
<tr>
<td>Save</td>
<td>Save the policy with the same name.</td>
</tr>
<tr>
<td>Save As</td>
<td>Save the policy with a different name.</td>
</tr>
<tr>
<td>Run</td>
<td>Manually run the policy again on the same system. This will open the Compare Systems window. The result will be displayed as Manual Comparison in the Results Summary Console -&gt; Configuration Policy Dashboard.</td>
</tr>
<tr>
<td>Report</td>
<td>Generate report. Note that ignored items are not included in the report.</td>
</tr>
<tr>
<td>More Info</td>
<td>Click to view additional information on the selected process.</td>
</tr>
<tr>
<td>Finish</td>
<td>To close the Policy Comparison Results window.</td>
</tr>
</tbody>
</table>
EventTracker Change Audit User Guide

## Compare Policies

This option helps you compare policies on demand against managed systems.

### To compare policies on demand

1. Select a record.
2. Click the **Configuration Policy** menu and select the **Compare Systems** option. Results Summary Console displays the Compare Systems window.

![Compare Systems Window](image)

**Figure 37**
3. Select the policy that you want to compare and then click **Next**.
4. Select the domains/systems and then click **OK**.

Results Summary Console displays the result in the Policy Comparison Results window.
Schedule Policy Comparison

To schedule policy comparison

1. Right-click a record.

   Results Summary Console displays the shortcut menu.

   From the shortcut menu, choose **Schedule**.

   (OR)

   Click the **Analyze** button.

   Results Summary Console displays the shortcut menu.

   From the shortcut menu, choose **Schedule**.

   (OR)

   Click the **Configuration Policy** menu and select the **Schedule Policy Comparison** option.

   Results Summary Console displays the Policy Comparison Scheduler.

---

![Policy Comparison Scheduler](image)

**Figure 39**
2. Set the schedule and then click **Close**.

   A red icon indicates policies that are scheduled for comparison.

   **NOTE:**

   A red icon precedes the policy that is scheduled for comparison. The red icon appears only when the policy is scheduled for the first time. For the second and the consecutive executions only the recent changes found are displayed with appropriate icons.

   For example, three computers namely WEBDOC1, BALOO, and ALICE-II are compared against Sample Critical File Policy. A red icon is displayed against computers BALOO and ALICE-II, which means Sample Critical File Policy is executed for the first time against these computers and a File changes found icon is displayed against WEBDOC1, which means Sample Critical File Policy was executed earlier against this computer.

**Access Result Analysis Console**

**To access Result Analysis Console**

1. Select a record.
2. Click the **Configuration Policy** menu and then select the **Result Analysis Console** option.

   (OR)

   Double-click anywhere inside the Configuration Policy Dashboard. EventTracker - Change Audit displays the Result Analysis Console.
Figure 40

Policies that are scheduled and run on demand are displayed on the left pane. Details of the item selected in the left pane are displayed on the right pane.
Change Browser

View Groups

This option helps you switch to Groups view.

To switch to Groups view

1. Open the Change Browser.

   **Note:**

   When you open the Change Browser for the first time after installation, EventTracker - Change Audit displays the File System, Registry, and Hardware details of monitored computers. However, when you open the Change Browser after installing clients in remote computers, EventTracker - Change Audit displays the Groups view.

2. Click the **View** menu and select the **Groups** option.

   (OR)

   Press **G** holding **Ctrl** key on your keyboard.

   EventTracker - Change Audit displays the Groups view.

   (OR)

   Click **Groups** on the toolbar.
3. To view Groups, expand the **Computers** node on the left pane.
4. Click a Group.

EventTracker - Change Audit displays the members of that Group alone on the Right pane.

A tick mark appears before the Groups command in the **View** menu, when EventTracker - Change Audit displays the Groups view.
If you try to clear the tick mark, EventTracker - Change Audit displays the Change Browser message box.

5. To access the System Bar, click the **View** menu and select the **System Bar** option.

   (OR)

   Press **S** holding **Ctrl** key on your keyboard.

   EventTracker - Change Audit displays the System Bar.
6. Double-click a system on the System Bar or on the right pane to view change details.

EventTracker - Change Audit loads the system and displays the change details.
Figure 45
View System Details

This option helps you view Hardware Information, Operating System Information and Memory Status of the selected system.

To view system details

1. Select a system on the System Bar.
2. Click the File menu and select the **System Details** option.

   (OR)

   Right-click a system on the System Bar.

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose **Details**.

   EventTracker - Change Audit displays the System Details window.
3. If there is no Snapshot for the selected system, then EventTracker - Change Audit displays the error message.

View File System Changes

This option helps you to view File System change details alone of the selected system.

1. Select a system on the System Bar.

2. Click the File menu and select the File System option.

   (OR)

   Right-click a system on the System Bar.
EventTracker - Change Audit displays the shortcut menu.

From the shortcut menu, choose **File System**.

EventTracker - Change Audit loads and displays the File System details of the selected computer.

![Image of EventTracker - Change Browser with details of a computer's file system]
View Registry Changes

This option helps you view Registry change details alone of the selected system.

1. Select a system on the System Bar.

2. Click the File menu and select the Registry option.

   (OR)

   Right-click a system on the System Bar.

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose Registry.

   EventTracker - Change Audit loads and displays the registry details of the selected computer.

Figure 48
Full View

This option helps you view Full View of monitored computers. In Full View, EventTracker - Change Audit compares two latest Snapshots and displays the difference in Snapshots that includes Addition, Deletion or Modification of files, folders and registry keys, filtered items and all other unaltered items. You can also select Snapshots for comparison from the drop-down lists.

To view Full View of monitored computers

1. Double-click a system on the System Bar.

   **NOTE:**

   If you click the toggle button when EventTracker - Change Audit displays the Groups view, then EventTracker - Change Audit displays the EventTracker - Change Audit message box to load the system as shown in the following figure.

   ![EventTracker - Change Browser](image)

   **Figure 49**

2. Click the **View** menu and select the **Full View** option.

   (OR)

   Click the toggle button on the toolbar.

   EventTracker - Change Audit displays the shortcut menu.

   ![Change View](image)

   **Figure 50**

   From the shortcut menu, choose **Full View**.

3. Expand the Drives or Registry trees and click an item.
EventTracker - Change Audit displays the Full View.

4. Move the mouse pointer over the items on the left and right panes.

   EventTracker - Change Audit displays the mouse over tool tip about the status of the item.
View Compare Details
This option helps you view Compare Details of folders and files.

To view compare details of File system items

1. Expand the File system tree.

2. Click a folder on the left pane.
   EventTracker - Change Audit displays the immediate sub-folder or files on the right pane.
   If EventTracker - Change Audit displays the folder on the right pane, double-click it to traverse down the tree. You can also traverse down by double-clicking the folder on the right pane.
   If EventTracker - Change Audit displays the file on the right pane, double-click it to view Compare Details.

3. Double-click a file on the right pane.
   (OR)
   Right-click a folder on the left pane or a folder/file on the right pane.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose Compare details.
   EventTracker - Change Audit displays the comparison details.
Compare Details of Registry Items

This option helps you view Compare Details of Registry items.

To view compare details of Registry items

1. Expand the Registry tree.

2. Double-click a hive on the left pane to traverse down the tree.

3. Double-click an item on the right pane.

   (OR)

   Right-click an item on the right pane.
EventTracker - Change Audit displays the shortcut menu.
From the shortcut menu, choose **Compare details**.
EventTracker - Change Audit displays the comparison details.

**Figure 53**

View Access History

1. Right-click an item on the left or right pane.

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose **Access History**.

   EventTracker - Change Audit displays the access history of the selected item.
Change View

In Change View, EventTracker - Change Audit compares two latest Snapshots and displays the difference in Snapshots that includes Addition, Deletion or Modification of files, folders and registry keys. You can also select Snapshots for comparison from the drop-down lists.

Find Changes

This option helps you find Addition, deletion and modification of folders, files, registry keys and values both in Full and Change Views.

1. Click the Edit menu and select the Find Change option.

   (OR)

   Press **N** holding **Ctrl** key on your keyboard.

   EventTracker - Change Audit displays the Next (From Selected Node) dialog box.

   ![Figure 54](image)

   **Table: Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Next Changed</td>
<td>EventTracker - Change Audit selects this check box by default. This option enables you to view modified items. Clear this check box if you do not want to view the modified items.</td>
</tr>
<tr>
<td>Next Added</td>
<td>EventTracker - Change Audit selects this check box by default. This option enables you to view Added items. Clear this check box if you do not want to view the Added items.</td>
</tr>
<tr>
<td>Next Deleted</td>
<td>EventTracker - Change Audit selects this check box by default. This option enables you to view Deleted items. Clear this check box if you do not want to view the Deleted items.</td>
</tr>
</tbody>
</table>
2. Select the option appropriately and then click **Find**.

EventTracker - Change Audit displays the Change Browser with the change details.

![EventTracker - Change Browser](image)

**Figure 55**

(OR)

Click **Show Next Change** on the toolbar. This option is equivalent to selecting all the check boxes in the Next (From Selected Node) dialog box.

3. To view next change, click the **Edit** menu and select the **Next Change** option.

(OR)

Press **F3** holding **Shift** key on your keyboard.

EventTracker - Change Audit displays the next change.
4. If there is no change in File System to display, the EventTracker – Change Audit displays the dialog box with appropriate message.

![EventTracker - Change Browser](image)

Figure 56

5. If there is no change in Registry to display, then EventTracker - Change Audit displays the dialog box with appropriate message.

![EventTracker - Change Browser](image)

Figure 57
Search Strings

This option helps you search strings both in Full and Change Views.

To Search Strings in File System

1. Open the Change Browser.

2. Click the Edit menu and select the Find option.

   (OR)

   Press F holding Ctrl key on your keyboard.

   (OR)

   Click on the toolbar.

   EventTracker - Change Audit displays the Find (From Selected Node) dialog box.

3. Enter the string in Find What field.

   Example: Windows.

4. Click Find Next.

   EventTracker - Change Audit displays the search result.
5. If there are no matches found, then EventTracker - Change Audit displays the message box with appropriate message.

![EventTracker - Change Browser](image)

Figure 60

6. To find the consecutive occurrence of the string searched for, click the Edit menu and select the Find Next option.

(OR)
Press **F3** on your keyboard.

### Search Strings in Registry

1. Open the Change Browser.

2. Click the **Edit** menu and select the **Find** option.

   (OR)

   Press **F** holding **Ctrl** key on your keyboard.

   (OR)

   Click on the toolbar.

   EventTracker - Change Audit displays the Find (From Selected Node) dialog box.

3. Select the **Registry** option.

4. Type the string in **Find What** field.

   Example: Prism.

5. Click **Find Next**.

   EventTracker - Change Audit displays the search result.
6. To find the consecutive occurrence of the string searched for, click the **Edit** menu and select the **Find Next** option.

(OR)

Press **F3** on your keyboard.
Generate Change Report

This option helps you view reports generated by EventTracker - Change Audit based on Snapshots and Policies. You can view reports based on Snapshots either in text file or in Excel file.

To generate Change report

1. Open the Change Browser.
2. On the System Bar, double-click the system for which you want to generate change report.
3. Select the Snapshots from the drop-down lists.
4. Click the Reports menu and select the View Reports option.
   (OR)
   Click on the toolbar.
   EventTracker - Change Audit displays the Select Format window.

   ![Select Format Window](image)

5. Select the Notepad (Text) option to view the report in text format.
   (OR)
   Select the Excel (Tab delimited) option to view the report in Excel format.
6. Click OK.
   EventTracker - Change Audit generates and displays the change report.
Track File Checksum

This feature helps to check if the files are tampered. By default, Track File Checksum is enabled for SYSTEM32 (C:\WINDOWS\system32) folder for all monitored systems. When you enable this feature, EventTracker - Change Audit tracks file checksum for all files and sub-folders associated with chosen folder, in this case for system32 folder.

To view file checksum

1. Open the Change Browser.
2. Double-click a system to load.
3. Select Full View or Change View.
4. Expand the **Drives** tree and click **system32**.

EventTracker - Change Audit displays the sub-folders and the files associated with the selected folder.

![Figure 65](image)

5. Double-click an item in the right pane.

EventTracker - Change Audit displays the Compare Details window with checksum details.
To enable file checksum tracking

1. Open the Change Browser.

2. Double-click a system to load.

3. Select Full View or Change View.

4. Expand the Drives tree and right-click a folder.

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose Track File Checksum to track file checksum for the local system.

   (OR)
Choose **Track File Checksum (All Systems)** to track file checksum for all monitored systems.

**View Access History**

**Prerequisites**

This option helps to monitor Audit Success / Audit Failure events emitted by the monitored computers.

Prerequisites to search audit details

1. Enable O/S auditing for the folder, file, or registry keys that you are interested in.
2. EventTracker Manager must be up and running on the EventTracker - Change Audit server.
3. Remote systems monitored by EventTracker - Change Audit Manager should also forward events to the EventTracker Manager that is running on the EventTracker - Change Audit server.

**Enable O/S Audit on Files & Folders**

1. Right-click the folder that you want to enable auditing.
   Example: `\<systemname>\Program Files\Prism Microsystems\EventTracker\Cache`

2. From the shortcut menu, choose **Properties**.

3. Click the **Security** tab on the Properties window.
4. Click **Advanced**.

5. Click the **Auditing** tab on the Advanced Security Settings window.
6. Click **Add**.
   
   Select User, Computer, or Group window is displayed.

---

**Advanced Security Settings for Cache**

To view more information about special auditing entries, select an auditing entry, and then click **Edit**.

**Auditing entries:**

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Access</th>
<th>Inherited From</th>
<th>Apply To</th>
</tr>
</thead>
</table>

- **Add...**
- **Edit...**
- **Remove**

- **Allow inheritable auditing entries from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.**

- **Replace auditing entries on all child objects with entries shown here that apply to child objects.**

Learn more about **auditing**.

---

**Select User, Computer, or Group**

Select this object type:

- **User, Group, or Built-in security principal**

From this location:

- **Toons.local**

Enter the object name to select (examples):

**Advanced...**

---

Figure 68

Figure 69
7. Click **Locations**, to select the location from where you want to pick users.

![Locations window](image)

8. Select the **Location** from the Locations window and then click **OK**.

9. Enter the user name in the **Enter the object name to select** field.

   Example: ETAdmin

10. Click **Check Names**.

    If the user name is valid, the user name is displayed in the **Enter the object name to select** field. Otherwise an error message is displayed.
11. Click **OK**.

Auditing Entry for... window is displayed.
12. Select **Full Control** under **Successful** and **Failed**.

All other check boxes are also selected automatically when you select **Full Control** check box.
NOTE:

It’s not mandatory that you should select Full Control check box. You select the options as per your requirement.

13. Click **OK**.

Advanced Security Settings window is displayed with the newly added user.
14. Click **Apply** and then click **OK**.

15. Click **OK** on the Properties window.

**NOTE:**

Similarly you can enable auditing for file or registry keys.
Enable O/S Audit on Registry Keys

To enable O/S audit on registry keys

1. Open the Registry Editor.
2. Right-click the key that you want to audit.
3. From the shortcut menu, choose Permissions.
4. Click Advanced.
5. Click the Auditing tab on the Advanced Security Settings window.
6. Add users as explained in the previous section.
Assign Change Type

This option helps you modify the Change Type a folder / file / registry key.

To modify Change Type

1. Open the Change Browser.

2. Select Full View or Change View.

3. Expand the File System node or Registry node.

4. Right-click an item (folder / file / registry key) on the left or right pane.

   EventTracker - Change Audit displays the shortcut menu.

5. From the shortcut menu, select Assign Change Type.

   EventTracker - Change Audit displays the Assign Change Type window.

   ![Assign Change Type Window](image)

6. Select a Change Type from the drop-down list.

7. Select the Apply on all systems check box if you wish to apply the settings to all monitored computers.

8. Click Assign.
EventTracker - Change Audit refreshes the Change Browser.

9. Right-click the key that you have modified the Change Type.

10. Load a monitored system.

11. Right-click a key and choose **Assign Change Type** from the shortcut menu.

   EventTracker - Change Audit displays the confirmation message box.
Snapshots

Snapshot is a read-only copy of File System structure, Registry structure and System configuration. Snapshot helps you to track registry changes and restore 'last known good configuration' registry settings.

After successful installation, EventTracker - Change Audit takes a baseline Snapshot. EventTracker - Change Audit takes one more Snapshot immediately following the baseline Snapshot after a specific time interval. By default, EventTracker - Change Audit automatically takes Snapshots Daily at 2 A.M. EventTracker - Change Audit preserves up to 64 Snapshots for comparison. When the maximum limit exceeds, EventTracker - Change Audit deletes the earliest one and adds the newest one to the Snapshot pool.

You can modify the Snapshot schedule and the maximum number to preserve through System Configuration settings. By default, EventTracker - Change Audit preserves the baseline and the latest Snapshots forever. You can also modify these settings through Edit Snapshot settings.

Suppose you have configured maximum number as 30 and have chosen to retain all the 30 Snapshots and trying to take a new Snapshot, in this scenario, EventTracker - Change Audit will not delete any of the earlier Snapshots as well as will not attempt to take the new Snapshot.

Take Snapshots On Demand

This option helps you take new Snapshots of the selected system.

To take Snapshots on demand

1. Open the Change Browser.
2. On the System Bar, double-click the computer for which you want to take Snapshot.

   If you try to take Snapshots in Groups view, EventTracker - Change Audit displays the message box asking you to load the system prior to taking the Snapshots.
EventTracker - Change Audit loads the details of the selected system.

3. Click the **Options** menu and select the **Take Snapshot** option.

(OR)

Click **New Snap** on the toolbar.

EventTracker - Change Audit displays the Snapshot progress.

After completion of taking the Snapshot, EventTracker - Change Audit displays the Snapshot Details dialog box.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of snap</td>
<td>Display box displays the date and time when the Snapshot was taken.</td>
</tr>
<tr>
<td>Snap label</td>
<td>Text box displays the EventTracker - Change Audit name of the Snapshot. You can edit and rename the Snapshot.</td>
</tr>
<tr>
<td>Keep Snap Forever</td>
<td>Select this check box, if you want to preserve the Snapshot forever.</td>
</tr>
<tr>
<td>Start Compare</td>
<td>Click this button for the EventTracker - Change Audit to start comparing with the immediate previous Snapshot.</td>
</tr>
</tbody>
</table>

4. Type an appropriate name for the new Snapshot in Snap label field.

5. Select Keep Snap Forever check box, if you want to preserve the Snapshot for future comparison.

6. Click Start Compare.

EventTracker - Change Audit compares the new Snapshot with the immediate previous Snapshot and displays the changes in the Change Browser.
Edit Snapshots

This option helps you edit Snapshot settings.

To edit Snapshot settings

1. Open the Change Browser.

2. Double-click a computer on the System Bar.

3. Click the Options menu and select the Edit Snapshots option.

EventTracker - Change Audit displays the Snap Editor.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of snapshots for current system</td>
<td>Displays the list of Snapshots taken for the selected Computer.</td>
</tr>
<tr>
<td>Time of snap</td>
<td>Display box displays the date and time when the Snapshot was taken.</td>
</tr>
<tr>
<td>Snap label</td>
<td>Displays the name of the selected Snapshot.</td>
</tr>
<tr>
<td>Keep Snap Forever</td>
<td>EventTracker - Change Audit selects this check box for the Snapshots that are configured not to be deleted. The names of the Snapshots that are marked to keep forever are preceded by an asterisk mark. You select and clear for all the Snapshots, whenever you please.</td>
</tr>
<tr>
<td>Update</td>
<td>After making appropriate changes, click this button for the EventTracker - Change Audit to update the changes.</td>
</tr>
<tr>
<td>Close</td>
<td>Click this button to close Snap Editor.</td>
</tr>
</tbody>
</table>

4. Make appropriate changes and then click **Update**.

EventTracker - Change Audit displays the message box.

![EventTracker - Change Browser](image)

**Figure 85**

5. Click **OK**, and then Click **Close** on Snap Editor.
EventTracker - Change Audit displays the message box, if the update is done for remote system.

![EventTracker - Change Browser](image)

**Figure 86**

6. Click **OK**.

EventTracker - Change Audit displays the message box.

![EventTracker - Change Browser](image)

**Figure 87**
Reinitialize Snapshots
This option helps you delete all the previous Snapshots for the selected Computer. After deleting all the Snapshots, EventTracker - Change Audit takes a new baseline Snapshot.

To re-initialize Snapshots

1. Open the Change Browser.

2. Double-click a computer on the System Bar.

3. Click the Options menu and select the Re-initialize Snaps option.

EventTracker - Change Audit displays the confirmation message box.

4. Click Yes to proceed.

EventTracker - Change Audit displays the re-initialization process progress.

After successfully re-initializing the Snapshots, EventTracker - Change Audit displays the message box.
5. Click **OK**.

EventTracker - Change Audit displays the Change Browser.

![EventTracker - Change Browser](image)

**Figure 90**

**NOTE:**

EventTracker - Change Audit has deleted all the previous Snapshots including baseline and has created a new baseline Snapshot. Since no other Snapshots exist, EventTracker - Change Audit compares the **Baseline Snapshot** with the **Baseline Snapshot**.
Back up Snapshots
This option helps you back up Snapshots.

To back up Snapshot

1. Open the Change Browser.

2. Click the **Options** menu and select the **Backup / Recovery (Snapshots)** option.

   Have you loaded a computer, EventTracker - Change Audit displays the confirmation message box.

3. Click **Yes** to proceed.

   EventTracker - Change Audit displays the Backup / Recovery Tool.

   ![Backup / Recovery Tool for Snapshot Files](image)

   **Figure 92**
Click | To
--- | ---
Backup | Back up the Snapshots of the current system.
Recover | Select the back up file from the list and then click to recover the Snapshots.
Remove | Select the back up file from the list and then click to delete the file
Exit | Exit Backup / Recovery Tool.

4. Click **Backup**.

EventTracker - Change Audit displays the Browse for Folder window.

![Figure 93](image)

5. Select the appropriate folder and then click **OK**.
EventTracker - Change Audit displays the Label window.

![Label Window](image)

**Figure 94**

6. Type a unique label in the text box and then click **OK**.

After successfully backing up the Snapshots, EventTracker - Change Audit displays the Success message box.

![Success Message](image)

**Figure 95**

7. Click **OK**.

EventTracker - Change Audit displays the Backup / Recovery Tool with the backup.
8. Click Exit.

Recover Snapshots

This option helps you recover Snapshots.

To recover Snapshots

1. Open the Change Browser.
2. Click the Options menu and select the Backup / Recovery (Snapshots) option.

Have you loaded a computer, EventTracker - Change Audit displays the confirmation message box.
3. Click **Yes** to proceed.

   EventTracker - Change Audit displays the Backup / Recovery Tool.

   ![Backup / Recovery Tool for Snapshot Files](image)

   Figure 98

4. Select the file from the list and then click **Recover**.

   EventTracker - Change Audit displays the Confirm restore message box.

   ![Confirm restore](image)

   Figure 99

5. Click **Yes** to proceed.

   After successful recovery, EventTracker - Change Audit displays the Restore Status.
6. Click **OK**.

7. Click **Exit** on Backup / Recovery Tool.

   If the recovery is partially successful, then EventTracker - Change Audit displays the Restore Status dialog with appropriate message.
Configuration

The administrator can configure any Client through Change Audit Manager console. This configuration can be customized for each system or can be global for all systems on the network. The idea is to create a configuration setting on the server and apply it to any or all Clients.

The following can be configured:

- Time and frequency of the automated Snapshot.
- Filter Drives and Registry Hives. This feature enables the user to filter out track of drives and directories that are not critical.
- File Types to Track. This feature enables the tracking of only specific file types. This feature is aimed at performance and efficiency enhancement.

Global Configuration

Global Configuration option helps you apply configuration settings to all monitored computers from a centralized location.

To Set up Global Configuration

This option helps you set Global Configuration.

1. Open the Change Browser.

2. Click the Options menu and select the Global Configuration option.

   Change Audit displays the Global Configuration window.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>General Change Audit selects this tab by default and displays information about the Working Directory path, Data Store directory path, name of the Server and the Port on which the server listens for incoming traffic.</td>
</tr>
<tr>
<td>Snapshot Results:</td>
<td>EventTracker - Change Audit client will log Snapshot Results as events with source set to ‘Change Audit’ to local log (Windows Application logs) or forward Snapshot Results as Traps to EventTracker with source set to ‘Change Audit’.</td>
</tr>
</tbody>
</table>
| Log into local event log | Select this option if  
1. EventTracker Manager and Change Audit are installed on different systems. EventTracker Manager can fetch those events through Agent-less monitoring available in EventTracker System Manager  
2. EventTracker Agent and Change Audit are installed on same system.  
3. You need guaranteed delivery of events. The transport mode can be set to TCP via EventTracker Agent.  
4. You need permanent entries in event log.  
5. You wish to make Change Audit events available to third party tools. |
Send directly to EventTracker as Traps

Select this option if Change Audit and EventTracker Manager are installed on same system. Delivery of Traps is not guaranteed since the transport mode is UDP.

![Global Configuration](image)

Type the IP address of the EventTracker Server. Type the port number if you wish to send Traps through a different port.

3. Click the **File Types** tab.

   EventTracker - Change Audit displays the File Types tab.
Field Types

Click this tab to view the File Types being tracked by EventTracker - Change Audit.

By default, EventTracker - Change Audit tracks the file types listed in File Types list. You can add or remove file types for tracking of your choice from the list.

EventTracker - Change Audit selects the Track Only Files Of the Above Types check box by default. Clear this check box, if you want to track all file types.

Track Only Files Of The Above Types

Clear this check box if you wish to track all file types.

Do Not consider a file changed if only file attributes are changed

Clear this check box to exclude files if only the attributes of those files are changed.

For files with checksum tracking enabled,

Clear this check box to exclude checksum
Do Not consider a file changed if its checksum has not changed  tracking enabled files, if the checksum has not changed.

4. Click **Add** to add a new file type.

EventTracker - Change Audit displays the Include New File Type window.

![Figure 104](image)

5. Type the filename extension and then click **OK**.

![Figure 105](image)

EventTracker - Change Audit includes the file type and displays the File Types tab.
6. To delete a certain file type, select it from the list and then click **Delete**.

   EventTracker - Change Audit removes the selected file type from tracking.

7. Click the **Filters** tab.

   EventTracker - Change Audit displays the Filters tab with the preset filter items.
8. Select the check box against the item that you wish to remove from the filter list and then click **Remove**.

   EventTracker - Change Audit removes the selected item from the filter list.

9. Click the **Change Type** tab.

   EventTracker - Change Audit displays the Change Type tab.
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Change Type**       | **Authorized**: Detected changes that can be matched with an approved change request.  
                        | **Unauthorized**: Detected changes that cannot be matched to an approved change request.  
                        | **Configuration**: Configuration audit helps to track all changes that have been made to a computer configuration or to be able to restore the configuration of that computer back to a known valid restore point.  
                        | **Business Knowledge**: It is the concept in which an enterprise consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills. |

### To configure Change Type

1. Right-click a folder, file, registry hive, or registry key.

   EventTracker - Change Audit displays the shortcut menu.
2. From the shortcut menu, choose **Assign Change Type**.

EventTracker – Change Audit displays the Assign Change Type window.
Field | Description
--- | ---
**Change Type** | But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type.

- **Configuration** - *.ini, *.cfg, *.inf, *.nt

Select an appropriate change type from this drop-down list.

- **Replace change type on all child objects**

Select this check box to apply the change type on all child objects.

- **Apply on all systems**

Select this check box to set it as global. i.e. apply the same settings on all monitored computers.

3. Select appropriate options and then click **Assign**.
Had you selected Apply on all systems check box, EventTracker - Change Audit displays the confirmation message box.

4. Click **OK** to continue.

EventTracker - Change Audit applies the change on the local system alone. To apply globally to all monitored computers, do as advised on the message box.

5. Open the Global Configuration window and then click the Change Type tab.

EventTracker - Change Audit displays the objects that have modified Change Type.

6. Select an object and then click **Remove**.
EventTracker - Change Audit removes the selected object and propagates the changes to all systems.

7. Click the **File Change Type** tab.

EventTracker - Change Audit displays the File change Type tab with the preconfigured FileName strings.

![Global Configuration](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **File Change Type** | But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type.  

- **Configuration** - *.ini, *.cfg, *.inf, *.nt  

Figure 113
8. Select an item and then click **Remove**.

EventTracker - Change Audit removes the selected item.

**To add File Change Type**

1. Click **Add** to add a new FileName String.

EventTracker - Change Audit displays the File Change Type window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for matching file path</td>
<td>Select this check box. EventTracker - Change Audit enables File Path String and File Path Operator fields.</td>
</tr>
<tr>
<td>File Path String</td>
<td>Type the location of the file.</td>
</tr>
<tr>
<td>File Path Operator</td>
<td>Select an operator from this drop-down list.</td>
</tr>
<tr>
<td>Search for matching file name</td>
<td>Select this check box. EventTracker - Change Audit enables File Name String and File Name Operator fields.</td>
</tr>
</tbody>
</table>
2. Enter/select appropriate options.

3. Click **Save** to save changes.

   EventTracker - Change Audit displays the message box.

   ![Figure 115](image)

4. Click **OK** and do as advised on the message box to propagate the changes to all monitored computers.

5. Click the **Registry Change Type** tab.

   EventTracker - Change Audit displays the Registry Change Type tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Registry Change Type</strong></td>
<td>But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type.</td>
</tr>
<tr>
<td></td>
<td><strong>Configuration</strong> - <code>*.ini</code>, <code>*.cfg</code>, <code>*.inf</code>, <code>*.nt</code></td>
</tr>
</tbody>
</table>

6. Click **Add** to add new registry keys.

EventTracker - Change Audit displays the Registry Change Type window.
### Field Tracker Change Audit User Guide

- **Table**
  - **Field**
  - **Description**
    - **Search for matching registry key path**
      - Select this check box. EventTracker - Change Audit enables Registry Key Path String and Registry Key Path Operator fields.
    - **Registry Key Path String**
      - Select an operator from this drop-down list.
    - **Search for matching registry value name**
      - Select this check box. EventTracker - Change Audit enables Value Name String and Value Name Operator fields.
    - **Value Name String**
      - Type the key value.

---

**Figure 117**
<table>
<thead>
<tr>
<th>Value Name Operator</th>
<th>Select an operator from this drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search for matching registry data</td>
<td>Select this check box. EventTracker - Change Audit enables Data String and Data Operator fields.</td>
</tr>
<tr>
<td>Data String</td>
<td>Type the data string.</td>
</tr>
<tr>
<td>Data Operator</td>
<td>Select an operator from this drop-down list.</td>
</tr>
<tr>
<td>Change Type</td>
<td>Select a change type from this drop-down list.</td>
</tr>
</tbody>
</table>

7. Enter/select appropriate options.

8. Click **Save** to save changes.

   EventTracker - Change Audit displays the message box.

9. Click **OK** and do as advised on the message box to propagate the changes to all monitored systems.

10. Click **OK** on the Global Configuration window.

    EventTracker - Change Audit displays the confirmation message box.
11. Click **Yes** to apply to all the systems.

EventTracker - Change Audit applies the settings and displays the Configuration Status window.

12. Click **OK**.

If the application of Global Configuration is partially successful, then EventTracker - Change Audit displays the Configuration Status window with appropriate message.
Apply Global Configuration

This option helps you apply the Global Configuration to all the monitored systems.

To apply Global Configuration

1. Open the Change Browser.

2. Click the Options menu and select the Apply Configuration option.

   If the selected Computer is a local system, then EventTracker - Change Audit displays the Select Configuration window with option to apply global configuration alone.

   If the selected Computer is a remote system, then EventTracker - Change Audit displays the Select Configuration window with an additional option.
3. Select the **Apply global configuration to all systems** option and then click **OK**. If you select the **Apply system configuration to current system** option, then EventTracker - Change Audit will apply the system configuration to the current system.

EventTracker - Change Audit applies the global configuration to all the monitored systems and displays the Configuration Status window.

4. Click **OK**.

EventTracker - Change Audit displays the Configuration Status window if it could not apply the changes to all the monitored systems.

**System Configuration**

System Configuration is exclusive to the selected system. You can configure automated Snapshot time, Snapshot limit and Filters through system configuration. You can also apply the Snapshot time and Snapshot limit for a specific system to all the monitored systems. A word of
caution, once the Filter is set either through System Configuration or Global Configuration, EventTracker - Change Audit will not consider the filtered items for Snapshots.

To set up System Configuration
This option helps you set System Configuration.

1. Open the Browser Console.

2. On the System Bar, double-click the computer for which you want to set configuration.
   EventTracker - Change Audit loads the system details.

3. Click the Options menu and select the System Configuration option.
   EventTracker - Change Audit displays the System Configuration window.

![System Configuration Window](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Configuration</td>
<td>By default, EventTracker - Change Audit selects 2 A.M.</td>
</tr>
<tr>
<td>Start Time</td>
<td>By default, EventTracker - Change Audit selects 2 A.M.</td>
</tr>
</tbody>
</table>

Figure 125
You can modify the time by selecting from the drop-down list.

**Frequency**

By default, EventTracker - Change Audit selects Daily as the frequency. You can modify the frequency by selecting from the drop-down list.

**Snapshot Limit**

By default, EventTracker - Change Audit select the maximum limit as 30. You can modify this limit by selecting from the drop-down list.

**Apply configuration to all systems**

Select this check box and then click OK to propagate the Snapshot automation settings to all the systems in your enterprise.

---

4. To set Filters, refer Filters.

---

**Apply System Configuration – Local System**

This option helps you apply Snapshot and Filter settings to the current system.

**To apply System Configuration to current system**

1. Open the Change Browser.

2. On the System Bar, double-click the local computer.

3. Click the **Options** menu and select the **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.

4. Make appropriate changes under relevant tabs, for example, modify the Snapshot Automation settings and then click **OK**.

   EventTracker - Change Audit applies the changes and displays the EventTracker - Change Audit message box.
5. Click OK.

**Apply System Configuration – Remote Systems**

This option helps you apply Snapshot and Filter settings to remote systems.

To apply System Configuration to remote systems

1. Open the Change Browser.

2. On the System Bar, double-click the remote computer for which you want to apply configuration.

3. Click the **Options** menu and select the **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.
4. Modify the Snapshot Automation settings and then click OK.
EventTracker - Change Audit displays the EventTracker - Change Audit message box.

5. Click **Yes** to proceed.

EventTracker - Change Audit applies changes to the selected computer. If the changes are applied successfully on the remote systems, EventTracker - Change Audit applies the changes and displays the message box.

6. Click **OK**.

If the changes are not applied successfully on the remote systems, EventTracker - Change Audit displays the error message.

**Apply System Configuration – All Systems**

This option helps you apply Snapshot settings to all systems.

To apply System Configuration to all systems

1. Open the Change Browser.

2. Double-click a computer on the System Bar.
3. Click the **Options** menu and select the **System Configuration** option.
   
   EventTracker - Change Audit displays the System Configuration window.


5. Select the **Apply configuration to all systems** check box.
   
   EventTracker - Change Audit displays the EventTracker - Change Audit message box.

   ![EventTracker - Change Browser](image)

   **Figure 131**

6. Click **OK**.

7. Click **OK** on the System Configuration window.
   
   EventTracker - Change Audit displays the Configuration Status window.

   ![Configuration Status](image)

   **Figure 132**

8. Click **OK**.
Search the Change Events (EventTracker Search Interface)

Option to Log / Forward Snapshot Results to EventTracker

You can configure EventTracker - Change Audit Manager to automatically log Snapshot results as EventTracker - Change Audit events locally (Windows Application logs) or directly forward those events as Traps to EventTracker.

1. Open the Change Browser.

2. Click the **Options** menu and select the **Global Configuration** option.

EventTracker - Change Audit displays the Global Configuration window.

![Global Configuration Window](image)

**Figure 133**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Results:</td>
<td>Change Audit client will log Snapshot Results as events with source set to</td>
</tr>
<tr>
<td></td>
<td><code>Change Audit</code> to local log (Windows Application logs) or forward Snapshot</td>
</tr>
<tr>
<td></td>
<td>Results as Traps to EventTracker with source set to <code>Change Audit</code>.</td>
</tr>
</tbody>
</table>
| Log into local event log | Select this option if  
1. EventTracker Manager and Change Audit are installed on different systems. EventTracker Manager can fetch those events through Agent-less monitoring available in EventTracker System Manager.  
2. EventTracker Agent and Change Audit are installed on same system.  
3. You need guaranteed delivery of events. The transport mode can be set to TCP via EventTracker Agent.  
4. You need permanent entries in event log.  
5. You wish to make Change Audit events available to third party tools. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Send directly to EventTracker as Traps</td>
<td>Select this option if Change Audit and EventTracker Manager are installed on same system. Delivery of Traps is not guaranteed since the transport mode is UDP.</td>
</tr>
</tbody>
</table>

3. Select the **Log into local event log** option to log snapshot results into the Application log.

4. Open the Event Viewer to view Change Audit events.
5. Double-click an event in the right pane to view event properties.
6. Select the **Send directly to EventTracker as Traps** option and take new snapshots of the monitored computers.

   EventTracker - Change Audit forwards the snapshot results to EventTracker.

---

**Generate Reports against Change Audit Category**

1. Log on to EventTracker.

2. Click the **Tools** drop-down list at the right-upper corner and select the **Alphabetical Reports** option.

3. Click ‘C’ in the **Alphabetical** list.

4. Select a Change Audit Category.
Example: Change Audit: Summary of registry changes.

5. Select a Report Type, for example, On Demand.

6. Click Next.

   EventTracker displays the Reports Wizard.

7. Select the systems.

8. Select the report generation interval.

9. Select the report options.

10. Set Refine and Filter criteria.

11. Type the Title, Description, Header, and Footer.


Filters
Filters are configured to avoid EventTracker - Change Audit taking snapshots of frequently changing non-critical directories (such as the browser cache, temp directories) or registry entries. By default, EventTracker - Change Audit uses its own knowledge base to filter out non-critical directories and registry entries. You can modify and customize these default filters. In addition to global filters you can add and remove local filters.

Normal Filters
Adding a normal filter does not remove the filtered node from the snapshots i.e. the changes detected so far will be retained; it only stops monitoring any changes in the object from the time it is filtered. When we declare a normal filter, it means we do not want to monitor any future changes to the filtered object, until we un-filter it again. Adding a normal filter does not delete the change history of the filtered object, it only stops monitoring any new changes to the filtered object. When the filtered object is unfiltered again, then the change list of this object will contain the changes that were detected before it was filtered and the changes detected since it has been unfiltered.

Customized Filters
When we declare a customized filter, it means we do not want to monitor any changes to the object and we do not want to retain any previous changes detected to the object also.

Difference between Customized Filters and Normal Filters

<table>
<thead>
<tr>
<th>Normal Filter</th>
<th>Customized Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>can be applied at both the levels system level as well as global level.</td>
<td>can only be added at the global level.</td>
</tr>
<tr>
<td>can only be added when the complete path of a file or registry system object is known.</td>
<td>can be added even if a substring within the path of file or registry system is known.</td>
</tr>
</tbody>
</table>
Adding a normal filter does not remove the filtered node from the snapshots i.e. the changes detected so far will be retained; it only stops monitoring any changes in the object from the time it is filtered.

When we declare a customized filter, it means we do not want to monitor any changes to the object and we do not want to retain any previous changes detected to the object also.

Change history of the filtered object is retained.

Change history of the filtered object is NOT retained.

When the object is unfiltered again, because change history is retained, the object is reported as modified.

When the object is unfiltered again, because change history is not available, the object is reported as added.

Adding a normal filter does not decrease size of the snapshot file.

Adding a customized filter may decrease size of the snapshot file.

**Demonstration**

1. Add a normal filter to filter the file ‘E:\WCWDB\ESXWIN2k832VM4\wcw.ini’.

2. Add a customized filter to filter the file ‘E:\WCWDB\PNPLDEV6\wcw.ini’.

   Note that both the files are currently being monitored.

   The following screenshots display the properties of 2 files ‘E:\WCWDB\PNPLDEV6\wcw.ini’ and ‘E:\WCWDB\ESXWIN2k832VM4\wcw.ini’ before adding the filters.

   Current Snapshot: 2010-01-06T02:01:48

   Previous Snapshot: 2010-01-05T02:02:20
### Figure 136

**Comparison of Two Snapshots**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>AS: Wed Jan 06 02:01:48 2010</th>
<th>AS: Tue Jan 05 02:02:20 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Label</td>
<td>E:\WCDB\PNPLDEV\wow.ini</td>
<td>E:\WCDB\PNPLDEV\wow.ini</td>
</tr>
<tr>
<td>Snapshot Time</td>
<td>Wed Jan 06 02:01:48 2010</td>
<td>Tue Jan 05 02:02:20 2010</td>
</tr>
<tr>
<td>Size</td>
<td>2 KB (1195 Bytes)</td>
<td>2 KB (1195 Bytes)</td>
</tr>
<tr>
<td>Version</td>
<td>-none-</td>
<td>-none-</td>
</tr>
<tr>
<td>Checksum</td>
<td>-not tracked-</td>
<td>-not tracked-</td>
</tr>
<tr>
<td>Attributes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Archive</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Compressed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hidden</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offline</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read Only</td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Temporary</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**OK**
The following screenshots display the properties (with respect to baseline snapshot) of 2 files E:\WCWDB\PNPLDEV6\wcw.ini and E:\WCWDB\ESXWIN2k832VM4\wcw.ini before adding the filters.

Current Snapshot: 2010-01-06T02:01:48

Baseline Snapshot: 2009-12-24T02:04:42
Figure 138
3. Add a customized filter to filter the folder `wcwd\pnpldev6`.

![Image of compare details of PNPLDEV6 Drives](image)

Figure 139
4. Add a Normal filter to filter the folder ‘E:\WCWDB\ESXWIN2k832VM4\’. 
5. Make changes to the two files and take a new snapshot after adding the two filters.

Neither of the file will be reported as changed.

Note that the folder ‘E:\WCWDB\ESXWIN2K832VM4’ is displayed as filtered, while the folder ‘E:\WCWDB\PNPLDEV6’ is not at all displayed because it has been completely removed from snapshots.
6. Remove both the filters and take a new snapshot.

The following screenshots display the properties of both the files after taking the snapshot without the filters.

Note that the file ‘E:\WCWDB\PNPLDEV6\wcw.ini’ is displayed in green color which means it is reported as a new file added to snapshot because no change history for this file is available.

The file ‘E:\WCWDB\ESXWIN2k832VM4\wcw.ini’ is reported in blue color that means it is modified.

Current Snapshot: 2010-01-06T16:56:12

Previous Snapshot: 2010-01-06T15:40:48
Figure 143
The following screenshots display the properties (with respect to baseline snapshot) of 2 files ‘E:\WCWDB\PNPLDEV6\wcw.ini’ and ‘E:\WCWDB\ESXWIN2k832VM4\wcw.ini’ after removing both the filters.

Note that there is no information available for file ‘E:\WCWDB\PNPLDEV6\wcw.ini’ in the baseline snapshot.

Current Snapshot: 2010-01-06T16:56:12
Baseline Snapshot: 2009-12-24T02:04:42
Figure 145
Customize Filters

This option helps you customize filters.

To customize filters

1. Open the Change Browser.
2. Double-click any system on the System Bar.
3. Click the Options menu and select the Customize Filter option.

   (OR)

   Expand the Drives or Registry trees.

   Right-click any item.

   EventTracker - Change Audit displays the shortcut menu.
From the shortcut menu, choose **Customize Filter**.

EventTracker - Change Audit displays the Customizing filters for files window.

![Customizing filters for files](image)

EventTracker - Change Audit displays the files and folders that are filtered by default in the Filter Name list.

4. Select the check box against the filter name that you want to include in the Snapshot and then click **Remove**.

   EventTracker - Change Audit removes the selected file.

5. Click **OK**.

6. To add file or folder to the filter, type the name of the file or folder in the **Add File or Folder to Filter** field.
7. Click **Add**.

   EventTracker - Change Audit adds the file to the Filter.

8. Click **OK**.

### Apply Filters – Local System

This option helps you apply filters to local system.

**To apply filters to local system**

1. Open the Change Browser.

2. Double-click the local computer on the System Bar.

3. Right-click any item under Drives or Registry trees, for example, C:

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose **Filter**.

   EventTracker - Change Audit filters the selected drive.

4. Click the **Options** menu and select the **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.

5. Click the **Filters** tab.

   EventTracker - Change Audit displays the Filters tab with the newly added filter.
Apply Filters – Remote Systems

This option helps you apply filters to remote system.

To apply filters to remote system

1. Open the Change Browser.

2. On the System Bar, double-click the remote computer for which you want to apply filters.

3. Right-click any item under Drives or Registry trees.

   For example, C:

   EventTracker - Change Audit displays the shortcut menu.

   From the shortcut menu, choose Filter.

   EventTracker - Change Audit displays the EventTracker - Change Audit confirmation window.
4. Click Yes.

EventTracker - Change Audit filters the selected drive.

5. Click the Options menu and select the Apply Configuration option.

EventTracker - Change Audit displays the Select Configuration window.

6. Select the Apply system configuration to current system option and then click OK.

EventTracker - Change Audit displays the EventTracker - Change Audit message box.

7. Click OK.

8. Click the Options menu and select the System Configuration option.

EventTracker - Change Audit displays the System Configuration window.
9. Click the **Filters** tab.

EventTracker - Change Audit displays the Filters tab with the newly added filter.

![Figure 152](image-url)

Check and click ‘Remove’ to UnFilter checked nodes.
To filter right click on a folder or registry key in the change browser and select the option.
Apply Filters – All Systems

This option helps you apply filters to all systems.

To apply filters to all systems

1. Open the Change Browser.
2. Double-click any Computer on the System Bar.
3. Right-click any item under Drives or Registry trees, for example, C:
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose Filter (All Systems).
   EventTracker - Change Audit displays the EventTracker - Change Audit confirmation message box.

4. Click Yes to proceed.
5. Click the Options menu and select the Global Configuration option.
   EventTracker - Change Audit displays the Global Configuration window.
6. Click the Filters tab.
   EventTracker - Change Audit displays the Filters tab with the filtered drive.
7. Click the **Options** menu and select the **Apply Configuration** option.

If the selected system is a local system, then EventTracker - Change Audit displays the Select Configuration window.

![Select Configuration Window](image)

If the selected system is a remote system, then EventTracker - Change Audit displays the Select Configuration window.

![Select Configuration Window](image)
8. Select the **Apply global configuration to all systems** options and then click **OK**.

EventTracker - Change Audit applies the global configuration settings and displays the Configuration Status window.

9. Click **OK**.

If the application of global configuration fails, then EventTracker - Change Audit displays the Configuration Status window with appropriate message.

10. Double-click the remote system on the System Bar.
Remove Filters – Local System
This option helps you remove filters from local system.

To remove filters in local system
1. Open the Change Browser.
2. Double-click the local computer on the System Bar.
3. Right-click the drive example C: in the Drives tree which was filtered earlier.

   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose Filter and clear the tick mark.
   EventTracker - Change Audit un-filters the selected drive.
   (OR)
   Click the Options menu and select the System Configuration option.
   EventTracker - Change Audit displays the System Configuration window.
   Click the Filters tab.
   EventTracker - Change Audit displays the Filters tab with the filtered drive.
   Select the check box against the drive and then click Remove.
   Click OK.
   EventTracker - Change Audit un-filters and displays the success message box.

   ![Figure 159](image)
   Click OK.
Remove Filters – Remote Systems

This option helps you remove filters from remote systems.

To remove filters in remote systems

1. Open the Change Browser.
2. Double-click the remote computer on the System Bar for which you want to remove filters.
3. Right-click the drive.
   
   Example C: in the Drives tree, which was filtered earlier.

   EventTracker - Change Audit displays the shortcut menu.
   
   From the shortcut menu, choose Filter and clear the tick mark.

   EventTracker - Change Audit displays the confirmation message box.

   ![EventTracker - Change Browser](image)

   **Figure 160**

4. Click Yes.
5. Click the Options menu and select the Apply Configuration option.

   EventTracker - Change Audit displays the Select Configuration window.
6. Select the **Apply system configuration to current system** option and then click **OK**.

   EventTracker - Change Audit displays the message box.

7. Click **OK**.

   EventTracker - Change Audit un-filters the selected drive.

   (OR)

   Click the **Options** menu and select the **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.

8. Click the **Filters** tab.

   EventTracker - Change Audit displays the Filters tab with the filtered drive.
9. Select the check box against the drive and then click **Remove**.

10. Click **OK**.

   EventTracker - Change Audit displays the confirmation message box.

11. Click **Yes**.

   EventTracker - Change Audit displays the message box.
12. Click **OK**.

EventTracker - Change Audit un-filters the selected drive.

**Remove Filters – All Systems**

This option helps you remove filters in all systems.

To remove filters in all systems

1. Open the Change Browser.

2. Double-click any computer on the System Bar.

3. Right-click the drive

   Example C: in the Drives tree, which was filtered earlier.

EventTracker - Change Audit displays the shortcut menu.

From the shortcut menu, choose **Filter (All Systems)** and then clear the tick mark.

EventTracker - Change Audit displays the confirmation message box.
4. Click Yes.

EventTracker - Change Audit un-filters the selected drive in all the local and remote computers.
Restore Registry sub tree

This feature helps you select a previously taken Snapshot of your system and return your system to that (registry) configuration. You can restore a selected registry key from previous Snapshot. The key value is restored to its previous contents. Only users with Admin privileges may perform this operation. This feature should be used with care since it may potentially damage a working system. You can also Undo registry restore.

To restore registry sub tree

1. Open the Change Browser.

2. On the System Bar, double-click the computer for which you want to restore the registry sub tree.

3. Select the Snapshots from the drop-down lists.

   EventTracker - Change Audit displays the EventTracker - Change Audit message box, had you selected system name or the drives and tried to restore the registry keys.

   ![Figure 167](image)

4. Select the appropriate sub tree from the Registry tree.
5. Click the **Options** menu and select the **Restore Registry sub tree** option.

EventTracker - Change Audit displays the Restore confirmation message box.

![Figure 169](image1.jpg)

6. Click **Restore**.

EventTracker - Change Audit displays the EventTracker - Change Audit confirmation message box.

![Figure 170](image2.jpg)

7. Click **Yes** to continue.

EventTracker - Change Audit displays the Restore status.

After successful restore operation, EventTracker - Change Audit displays the success message box.

**View Restore Logs**

This option helps you view the restore logs.
To view restore logs
1. Open the Change Browser.
2. Double-click the system on the System Bar.
3. Click the View menu and select the Restore Log option.
   - EventTracker - Change Audit displays the restore log file in the Notepad.
   - EventTracker - Change Audit displays appropriate message if no log exists.

Undo Restore
This option helps you undo registry key restore.

To undo restore

1. Open the Change Browser.
2. Double-click the system for which you want to undo restore.
3. Select appropriate Snapshots from the drop-down lists.
4. Click the Options menu and select the Undo Restore option.
   - EventTracker - Change Audit displays the confirmation message box.

   ![Confirmation Message Box]

   EventTracker - Change Audit displays the information message box if you are on the File system tree and trying to undo restore.
5. **Click Yes to continue.**

   EventTracker - Change Audit displays the success message box after successfully undoing the previous restore.
Configuration Policy Editor

Configuration Policy

Configuration Policies facilitate you compare files, folders, registry items and registry keys in hives among monitored systems. The advantage of configuring Configuration Policies is that, instantly you will get to know the differences between the comparing and compared systems without initiating Snapshots. You are permitted to elect only one Policy and any number of computers for comparison. Generating ad-hoc reports like this saves you resource, cost and time.

As an administrator of your enterprise network the onus is on you to secure the network from the vagaries of Internet and internal threats as well. Suppose you have applied Microsoft DST updates and want to check if you have applied to all monitored systems. You can do it without moving from your work desk. All you have to do is to configure a Configuration Policy and compare the systems. The report generated by

EventTracker - Change Audit helps you easily figure out whether it is applied or not to the monitored systems.

Create Configuration Policies

To create Configuration Policies

1. Open the Change Browser.

   Click the Tools menu and select the Configuration Policy Editor option.

   EventTracker - Change Audit displays Configuration Policy Editor.
2. Click **Add Policy**.

EventTracker - Change Audit displays the Policy Name tab.
3. Type the name and description of the Policy in the **Policy Name** and **Policy Description** fields respectively.
   Example: ET, EventTracker.

4. Click **Next**.
   EventTracker - Change Audit displays the Policy Item Type tab.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add file</strong></td>
<td>This option allows you to select any file from the local system into policy. Policy captures the file name, file create date, file version, file modify and checksum for the selected file name.</td>
</tr>
<tr>
<td><strong>Add particular folder</strong></td>
<td>This option allows you to select all the files within a particular folder. Policy captures details of all the files such as file name, file size, file create date, file version, file modify date and checksum that reside in that folder.</td>
</tr>
<tr>
<td><strong>Select folder and subfolder</strong></td>
<td>This option allows you to select all the files within a particular folder and sub-folder. Policy captures details of</td>
</tr>
</tbody>
</table>
all the files such as file name, file size, file create date, file version, file modify date and checksum that reside in folder and sub-folders.

| Search for Registry key in Hive | This option allows you to add any key into the policy. Policy captures all the sub-level keys, values and data. |

To Search a File

EventTracker - Change Audit selects the **Add File** option by default.

1. Click **Next**.

   EventTracker - Change Audit displays the Select the file name window.

   ![EventTracker - Select the file name](image_url)

   **Figure 176**

2. Go to the appropriate folder and select the file.
Example: etagent.exe

3. Select the **Open as read only** check box, if you want to restrict the permission on the file and then click **Open**.

EventTracker - Change Audit displays the File/Folder Search tab.

![Figure 177](image)

**NOTE:**

You have an option to keep the file name same along with the existing drive letter and folders associated with it. When you compare this Policy, EventTracker - Change Audit will compare the same drive and folders.

Sometimes files and folders may not be located on the same drive. In those circumstances, you can remove the drive letter so that EventTracker - Change Audit will search in all the drives.

Example: Had you entered C:\Program Files\SQL\abcd.exe,

EventTracker - Change Audit will search the abcd.exe in C:\Program Files\SQL
Had you entered Program Files\SQL\abcd.exe, EventTracker - Change Audit will search the abcd.exe in Program Files\SQL

Had you entered abcd.exe, EventTracker - Change Audit will search the abcd.exe in all drives and folder.

4. Click **Finish**.

   EventTracker - Change Audit adds the selected file and displays the Configuration Policy Editor.

5. Click **Close**.

To Search a Folder

1. Select the **Add particular folder** option as the item type.
2. Click **Next**.

   EventTracker - Change Audit displays the Configuration Policy Editor window.

![Configuration Policy Editor](image)

**Figure 179**

3. Select the drive, select the folder and then click **OK**.

   Example: EventTracker

   EventTracker - Change Audit displays the File/Folder Search tab.
4. **Click Search.**

   EventTracker - Change Audit saves the file information and displays the progress.

5. **Select All** check box is selected by default.

   You can also remove files by clearing the check boxes against the items that you wish to remove.
6. Click **Finish**.

EventTracker - Change Audit displays the Configuration Policy Editor with the File Details.
To Search a Folder and Sub-folder

1. Select the **Add folder and sub-folder** option as the item type.

2. Click **Next**.

   EventTracker - Change Audit displays the Configuration Policy Editor.

3. Select the drive, select the folder and then click **OK**. Example: EventTracker

   EventTracker - Change Audit displays the File/Folder Search tab.

4. Click **Search**.

   EventTracker - Change Audit saves the file information and displays the progress.

5. **Select All** check box is selected by default.
You can also remove files by clearing the check boxes against the items that you wish to remove.

6. Click **Finish**.

EventTracker - Change Audit displays the Configuration Policy Editor with the File Details.

![Configuration Policy Editor](image)

**Figure 183**

To Search Registry Key in Hive

1. Select the Search for Registry Key in Hive as the item type.

2. Click Next.

EventTracker - Change Audit displays the Registry Search tab.
3. Type the name of the key in the Key Name field as shown in the following figure. Example: EventTracker

4. Click Search.

EventTracker - Change Audit searches for the Key name and displays the progress of search.

EventTracker - Change Audit displays the Registry Search tab with the list of hives.
5. Select the keys and then Finish.

EventTracker - Change Audit displays the Configuration Policy Editor with the Registry Details.
**Edit Policy Description**

1. Open the **Configuration Policy Editor**.

2. Select a Policy.

3. Click **Edit Description**.

   EventTracker - Change Audit displays Item Description window.
4. Edit the description and then click **Save**.

5. Click **Close**.

**Edit File/Registry Key Description**

1. Open the Configuration Policy Editor.

2. Select an item on the File Details or Registry Details pane.

3. Click **Edit Description**.

   EventTracker - Change Audit displays Item Description window.

4. Edit the description and then click **Save**.

5. Click **Close**.
Add Policy Items

This option helps you add file/folder and registry key details to a Policy.

To add policy items

1. To add file items, click **Add Item** on the **File Details** pane.

   EventTracker displays the Configuration Policy Editor window.

2. Select an appropriate option and then add file items.

3. To add file items, click **Add Item** on the **Registry Details** pane.

   EventTracker displays the Configuration Policy Editor window.
Compare Systems

This option helps you compare Policies between monitored computers.

To compare systems

1. Open the Change Browser.
2. Click the **Tools** menu and select the **Compare Systems** option.

   (OR)

   Open the Configuration Policy Editor and then click Compare Systems.

EventTracker - Change Audit displays the Compare Systems window.
3. Select a Policy and then click Next.

**NOTE:** You can select only one Policy for comparison.

EventTracker - Change Audit displays the Systems tab.
NOTE:

Select the domain from the drop-down list. EventTracker – Change Audit displays all the monitored computers members of that domain. By default, EventTracker - Change Audit displays all the monitored computers irrespective of domains. You can select any number of systems for comparison.

4. Select the computers and then click Add.

(OR)

Click Add All to add all the computers.

EventTracker - Change Audit displays the Systems tab with the selected computers.

5. Click OK.

EventTracker - Change Audit displays the comparison progress.
### Compare Systems

**Policy Name:** ET

<table>
<thead>
<tr>
<th>System</th>
<th>Policy Item</th>
<th>Search Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>ES/WeBL</td>
<td>Policy Item: C:\Program Files\Palm Ml...</td>
<td></td>
</tr>
<tr>
<td>WEBDoc1</td>
<td>Policy Item: C:\Program Files\Palm Ml...</td>
<td></td>
</tr>
<tr>
<td>WEBDoc2</td>
<td>Policy Item: C:\Program Files\Palm Ml...</td>
<td></td>
</tr>
</tbody>
</table>

Compare Agent systems with the Manager's Configuration

![EventTracker - Compare Systems](image)

**Figure 192**
After comparing, EventTracker - Change Audit displays the result in the Policy Comparison Results window.
Open the Results Summary Console to view configuration policy comparison results.
Schedule Policy Comparison
This option helps you schedule Policy comparison.

To schedule Policy comparison

1. Open the Change Browser.

2. Click the Tools menu and select the Schedule Policy Comparison option.

(OR)
Open the Results Summary Console.
Click the Configuration Policy menu and select the Schedule Policy Comparison option.
EventTracker - Change Audit displays the Policy Comparison Scheduler.

3. Click **New Schedule**.

   EventTracker - Change Audit displays the Policy Schedule window.
4. Type the name of the schedule in the **Title** field.

5. Select a policy from the **Policy Name** drop-down list, for example, ET.

6. Select the **Systems**.

7. Select the start date and time from the **Start from** spin box.

8. Select how often you want the report to be generated from the **Frequency** drop-down list.

   **NOTE:**

   EventTracker - Change Audit enables **Week Day** drop-down list only when you select **Frequency** as **Weekly**.

9. Click **Save**.

   EventTracker - Change Audit displays the **PolicyScheduler message box**.
10. Click **OK**.

EventTracker - Change Audit displays the Policy Comparison Scheduler with the newly configured schedule.

11. Select a schedule and then click **Edit** to change the settings.

12. Select a schedule and then click **Delete** to delete the schedule details.
Export Configuration Policies
This option helps you export configuration Policies to a desired location.

To export configuration Policies
1. Open the Change Browser.
2. Click the Tools menu and select the Configuration Policy Editor option.
   EventTracker - Change Audit displays the Configuration Policy Editor.
3. Click the Policy menu and select the Export option.
   EventTracker - Change Audit displays the Export Configuration Policy window.
4. Select a Policy and then click Export.
   EventTracker - Change Audit displays the Select Export File window.
5. Go to the appropriate folder, enter the name in File name field and then click Save.

   NOTE:
Valid export file format is .ispol.

After exporting successfully, EventTracker - Change Audit displays the message box.

![Successful export message]

Figure 200

Import Configuration Policies
This option helps you import configuration Policies to monitored computers.

To import configuration Policies
1. Open the Change Browser.
2. Click the **Tools** menu and select the **Configuration Policy Editor** option.

   EventTracker - Change Audit displays the Configuration Policy Editor.

3. Click the **Policy** menu and select the **Import** option.

   EventTracker - Change Audit displays the Select Import File window.

4. Go to appropriate folder, select the file and then click **Open**.

   After importing successfully, EventTracker - Change Audit displays the message box.

   ![EventTracker - Configuration Policy Editor](image)

   **Figure 201**

---

### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change Management</td>
<td>The practice of administering changes with the help of tested methods and techniques in order to avoid new errors and minimize the impact of changes.</td>
</tr>
<tr>
<td>Change View</td>
<td>EventTracker - Change Audit displays the items that are Added, modified and deleted in File System and Registry.</td>
</tr>
<tr>
<td>Client</td>
<td>Tiny footprint installed in monitored systems to track changes.</td>
</tr>
<tr>
<td>Computer Logical Groups</td>
<td>User-defined groups. These groups are logical in the sense you can group computers in different domains of your interest for easy management.</td>
</tr>
<tr>
<td>Edit Snapshots</td>
<td>Helps to keep the selected Snapshot forever or delete when the Snapshot limit exceeds.</td>
</tr>
<tr>
<td><strong>File System</strong></td>
<td>A system for organizing directories and files, generally in terms of how it is implemented in the disk operating system.</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Filters</strong></td>
<td>Filters are set to exclude folders and files from tracking.</td>
</tr>
<tr>
<td><strong>Full View</strong></td>
<td>EventTracker - Change Audit displays the items that are Added, modified and deleted in File System and Registry. Also, displays the unaltered items in File System and Registry.</td>
</tr>
<tr>
<td><strong>Global Configuration</strong></td>
<td>Configure and apply folders / files to track and apply filters to all the monitored computers from the Manager console.</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>Helps to group and track registry hives and directories of an application.</td>
</tr>
<tr>
<td><strong>Reinitialize Snapshots</strong></td>
<td>EventTracker - Change Audit removes all the Snapshots including the Snapshots selected to keep forever and takes a new baseline Snapshot.</td>
</tr>
<tr>
<td><strong>Removing Client Components</strong></td>
<td>Helps to clean-up database entries and other components when clients are removed manually from the remote computers.</td>
</tr>
<tr>
<td><strong>Snapshot</strong></td>
<td>Snapshot is an image of File System and Registry.</td>
</tr>
<tr>
<td><strong>System Configuration</strong></td>
<td>Configure Snapshot automation, Snapshot limit and filters to the current system. System Configuration can also be propagated to all other system in the network.</td>
</tr>
<tr>
<td><strong>Windows Registry</strong></td>
<td>In computing, the Windows registry is a database, which stores settings and options for the operating system. It contains information and settings for all the hardware, software, users, and preferences of the PC. Whenever a user makes changes to &quot;Control Panel&quot; settings, or file associations, system policies, or installed software, the changes</td>
</tr>
</tbody>
</table>
are reflected and stored in the registry.