Netsurion™ | EventTracker

EventTracker v9.x Change Audit

User Guide

Publication Date: September 11, 2019

Abstract

This guide provides you with the information for configuring Change Audit and the associated protocols in EventTracker. Change Audit is the important element of security. With Change Audit feature, you get complete auditing, in-depth security monitoring, and detailed tracking for user activity, authentications via system snap shots. Change Auditor tracks changes covering; file servers, folders, registry items and other key services to enhance threat detection and threat prevention across your enterprise.

Audience

This guide is intended for Administrators and Operations personnel who are responsible for managing and investigating network security.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

Table of Contents

1. Getting Started

1.1 About EventTracker - Change Audit

EventTracker - Change Audit is a diagnostic tool that targets a 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, it provides the user information regarding the changes that could be harmful. During the day, there are thousands of changes happening on the Windows system. Using an effective change management solution, changes can be viewed 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.

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

1.1.1 Capabilities of EventTracker - Change Audit

- Configuring Change Audit to log Snapshot results, as Change Audit events locally (Windows Application logs).
- Configuring Configuration Policies (Configuration Policy Editor).
- Comparing systems based on Configuration Policies. Compare systems can be used to generate a report if there are discrepancies between the existing configuration and the actual configuration of the systems.
- Exporting / Importing Configuration Policies.
- Scheduling Policy comparison.
- Identify and cure the systems of new viruses before the 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 restores “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. Filters can be turned off at any time.
- 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 more control 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 reduces 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 provides detailed change reports that 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 helps in reverting to a good configuration if any problem occurs.

1.2 EventTracker - Change Audit Architecture

EventTracker - Change Audit architecture is completely centralized and provides control to manage all the systems on the network from one console.

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.

1.3 Ports used by EventTracker - Change Audit

EventTracker - Change Audit uses two TCP ports 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 a golden snapshot located at the server.

NOTE: Enabling firewall on the EventTracker - Change Audit Manager computer adds the ports 14502 and 14508 to the firewall exceptions list.

1.4 EventTracker - Change Audit Events

Event ID	Cause of Event	Resolution
3400	After taking the system snapshot if Change Audit detects that any new file is added then this event is generated.	Take appropriate action for the detected change.
3401	After taking the system snapshot if Change Audit detects that any file is modified then this event is generated.	Check if the changes made to file are intentional and then take appropriate action for the detected change.
3402	After taking the system snapshot if Change Audit detects that any file is deleted then this event is generated	Take appropriate action for the detected change.
3403	After taking the system snapshot Change Audit generates this event to summarize all the detected file changes.	Take appropriate action for the detected change.
3404	After taking the system snapshot if Change Audit detects that any new registry key is added then this event is generated.	Take appropriate action for the detected change.

Event ID	Cause of Event	Resolution
3405	After taking the system snapshot if Change Audit detects that any registry key is modified then this event is generated.	Take appropriate action for the detected change.
3406	After taking the system snapshot if Change Audit detects that any registry key is deleted then this event is generated.	Take appropriate action for the detected change.
3407	After taking the system snapshot Change Audit generates this event to summarize all the detected registry changes.	Take appropriate action for the detected change.
3408	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.	Take appropriate action for the detected change.
3409	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.	Take appropriate action for the detected change.
3410	When Change Audit evaluates a category and its result is true then this event is generated.	Take appropriate action.

Event ID	Cause of Event	Resolution
3411	When the change type of an object is modified then this event is generated.	Take appropriate action.
3412	When the Change Audit engine takes a snapshot.	Take appropriate action.
3413	When the Change Audit engine sends snapshot files to manager.	Take appropriate action.
3414	When the Change Audit engine performs a scheduled policy comparison.	Take appropriate action.
3415	When the Change Audit engine performs inventory updation.	Take appropriate action.
3416	When the Change Audit engine executes the policy comparison request from manager.	Take appropriate action.

1.5 Starting Change Browser

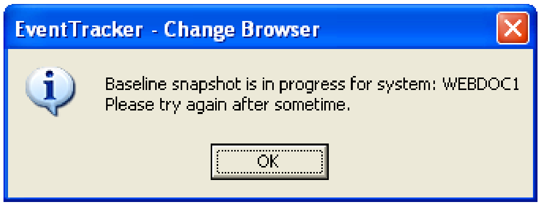
This option helps to start EventTracker – Change Browser from the Manager and the Client computers.

To start Change Browser follow the below steps :

1. Select **EventTracker Control Panel**, select **Change Audit**, and then select the **Change Browser**.

(OR)

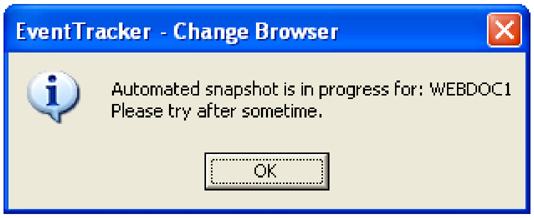
1. Double-click **Change Audit** on the desktop EventTracker Control Panel.
2. EventTracker displays the **Results Summary Console**.
3. Click **Change Browser** on the toolbar.
4. EventTracker - Change Audit displays the **Change Browser** console indicating that the Baseline snapshot is in progress.



Baseline snapshot is in progress for system: WEBDOC1
Please try again after sometime.

Figure 1

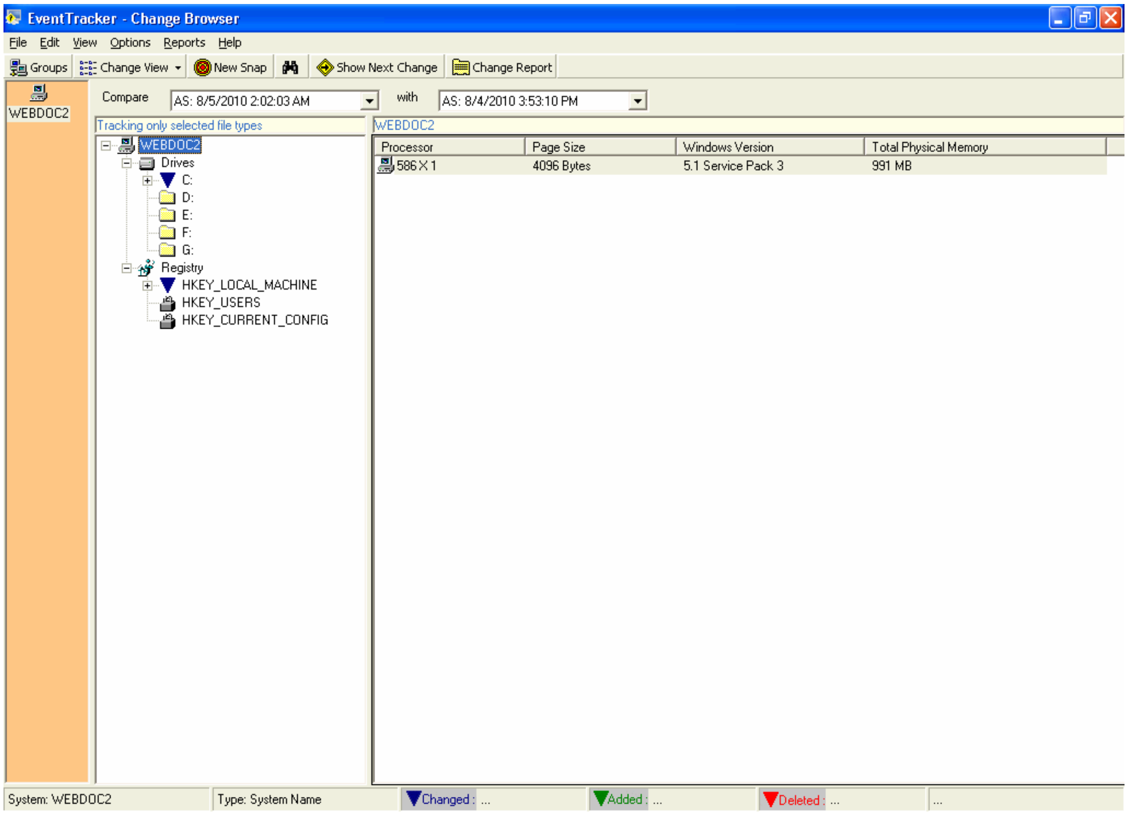
5. EventTracker - Change Audit displays the Change Browser console indicating that the Automated snapshot is in progress.



Automated snapshot is in progress for: WEBDOC1
Please try after sometime.

Figure 2

6. After successful installation, EventTracker - Change Audit takes a baseline Snapshot at 2 A.M.
7. If the Baseline and Automated snapshots are over, EventTracker - Change Audit loads the system, compares the two snapshots and displays the **Change View.**



Compare AS: 8/5/2010 2:02:03 AM with AS: 8/4/2010 3:53:10 PM

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.1 Service Pack 3	991 MB

System: WEBDOC2

Type: System Name

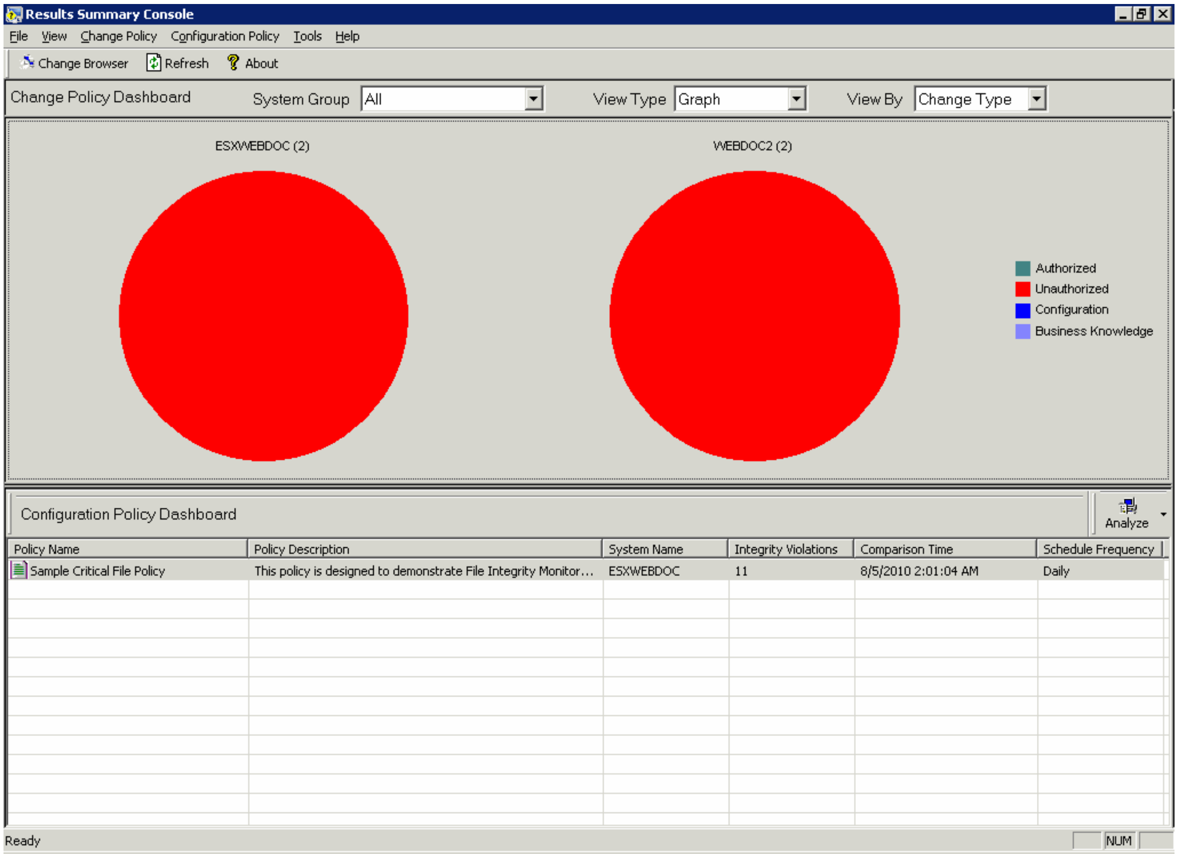
Figure 3

1.6 Starting Results Summary Console

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

To start Results Summary Console follow the below steps :

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.



System Group: All
View Type: Graph
View By: Change Type

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 4

Field	Description
System Group	This drop-down list displays all the system groups discovered by the Client Manager.
View Type	Select an option to view chart or data on the console.

Field	Description	
View By		
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 is made to the computer configuration, or able to restore the configuration of that computer back to a known valid restore point.
	Business Knowledge	The concept in which an enterprise consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills.
Object Type	Files Added	
	Files Deleted	
	Files Modified	
	Registry Added	Registry keys added
	Registry Deleted	Registry keys deleted

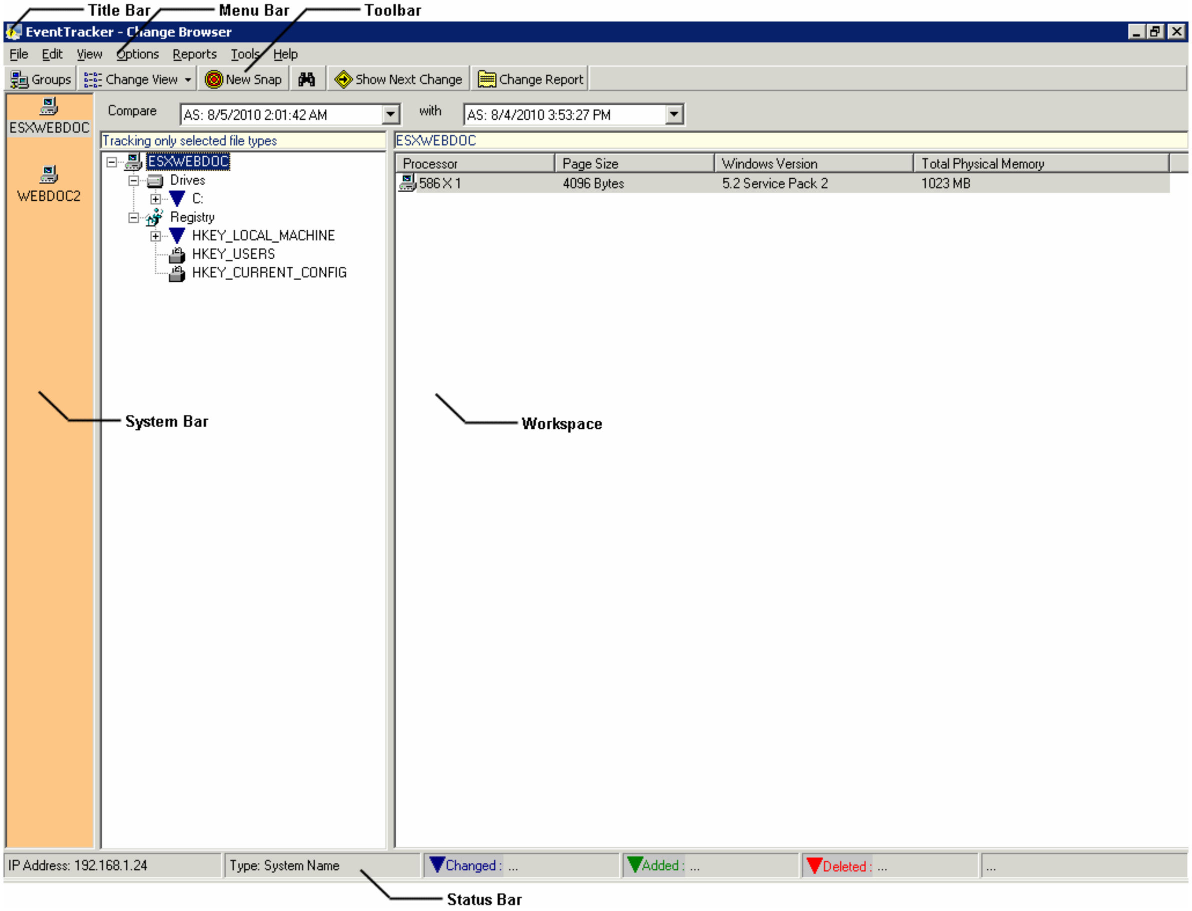
Field	Description	
	Registry Modified	Registry keys modified

NOTE:

- By default, data is not populated for **Change Type**: Authorized, configuration and Business Knowledge, as the default file types contain only the unauthorized file extensions.
- From v9.0 onwards, for **Object Type**, we are not **monitoring Registry Added/Registry Deleted/Registry Modified** by default.

1.7 Change Browser User Interface

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



Compare AS: 8/5/2010 2:01:42 AM with AS: 8/4/2010 3:53:27 PM

Tracking only selected file types

ESXWEBDOC

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.2 Service Pack 2	1023 MB

IP Address: 192.168.1.24 | Type: System Name | Changed : ... | Added : ... | Deleted : ... | ...

Figure 1

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

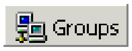
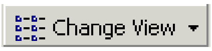
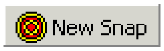
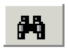
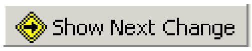
The strip next to Title Bar is the Menu Bar. Menu Bar contains menus. Each Menu contains a list of commands and shortcut keys to carry out a specific task. You cannot customize, move, or drag the Menu Bar.

System Bar

System pane displays the monitored systems.

Toolbar

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

Click	To
	Switch to Groups view.
	Toggle between Full View and Change View.
	Take new Snapshots of the selected system.
	Search strings in File System or Registry.
	View consecutive changes in File System and Registry.

Click	To
Change Report	View change reports based on Snapshots and change reports based on policies.

Hover the mouse on the ToolTip to know the function of the buttons.

Workspace

The Workspace consists of the left pane, 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, Displays Drives, and Registry trees on the left pane and hardware details on the right pane.

Expand and select items under Drives or Registry tree, EventTracker – Change Audit compares the Snapshots, the 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, in this Change View. 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.

1.8 EventTracker - Change Audit Icons

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

Icon	Represents
▼	Total count of all items added to the File System or Registry.
▼	Total count of all items modified in the File System or Registry.

Icon	Represents
🔻	Total count of all items deleted from the File System or Registry.
🟩	An item added to the File System or Registry.
↻	An item modified in the File System or Registry.
✕	An item deleted from the File System or Registry.
📄	Unaltered item.
🗄	Folders.
▭	Files.
⚙	Registry.
📁	File system folders and Registry keys.
🖥	Computer Groups.
🔴	Snapshot in progress.
📋	File changes found.
⚙	Registry changes found.
📋	File and registry changes found.
🟢	No changes found.

Icon	Represents
?	Fresh item.
✓	Items accepted.
ⓘ	Items ignored.
✗	Items rejected.

1.9 Change Audit Components

1.9.1 Change Browser

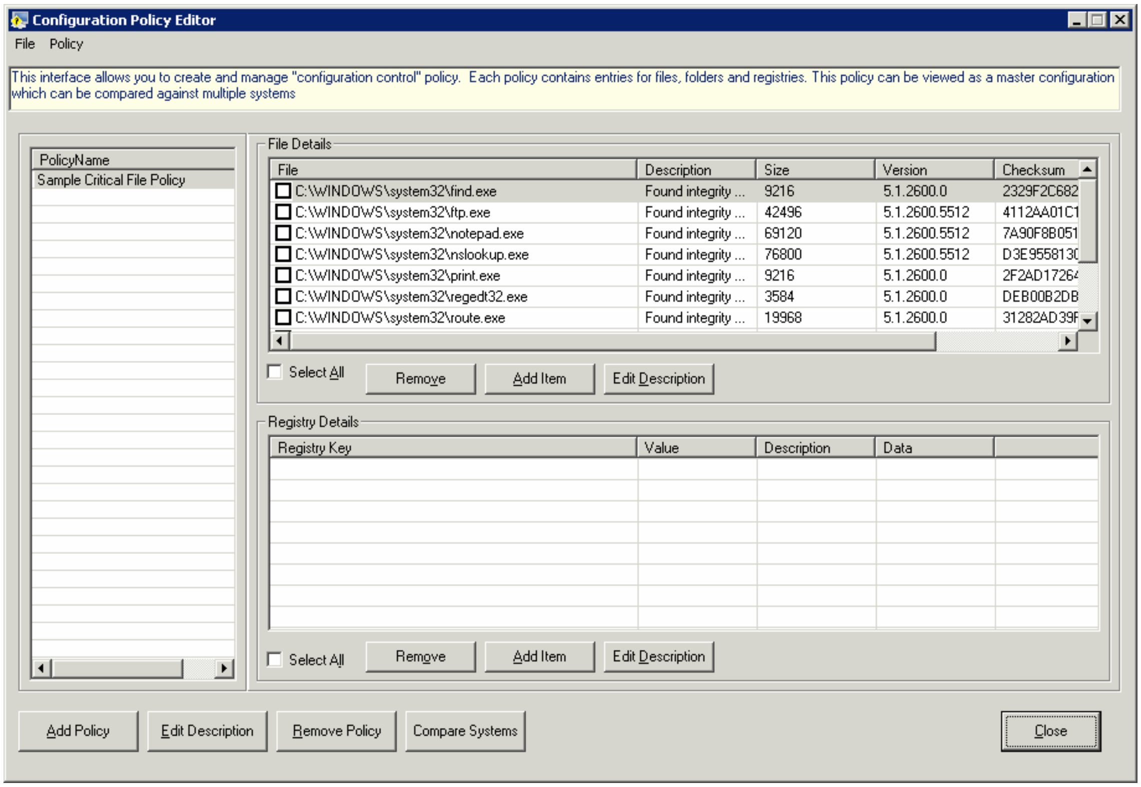
The Change Browser is an information-rich browser that displays a comparison of current versus previous snapshots.

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 in resolving the problems quickly.

In the Result Summary Console window, click the **Configuration Policy tab** in the menu bar and select **Configuration Policy Editor** option to open **Configuration Policy Editor** dialog box**.**

1.9.2 Configuration Policy Editor

Configuration Policy Editor helps in setting Configuration Policies for the enterprise environment. Policies are grouping 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 policy is indicated as a change to the Policy. It is easy to monitor changes through Policies rather than run through the entire file system and registry.



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
Sample Critical File Policy

File Details

File	Description	Size	Version	Checksum
□ C:\WINDOWS\system32\find.exe	Found integrity ...	9216	5.1.2600.0	2329F2C682
□ C:\WINDOWS\system32\ftp.exe	Found integrity ...	42496	5.1.2600.5512	4112AA01C1
□ C:\WINDOWS\system32\notepad.exe	Found integrity ...	69120	5.1.2600.5512	7A90F8B051
□ C:\WINDOWS\system32\nslookup.exe	Found integrity ...	76800	5.1.2600.5512	D3E955813C
□ C:\WINDOWS\system32\print.exe	Found integrity ...	9216	5.1.2600.0	2F2AD17264
□ C:\WINDOWS\system32\regedt32.exe	Found integrity ...	3584	5.1.2600.0	DEB00B2DB
□ C:\WINDOWS\system32\route.exe	Found integrity ...	19968	5.1.2600.0	31282AD39F

Registry Key	Value	Description	Data

Figure 2

Click	To
Add Policy	Create a new Policy.
Edit Description	Edit description of the Policy.
Remove Policy	Delete the selected Policy.
Compare Systems	Compare the monitored computers against the selected policy.
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	

Click	To
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 keys.

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.

2. 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.

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

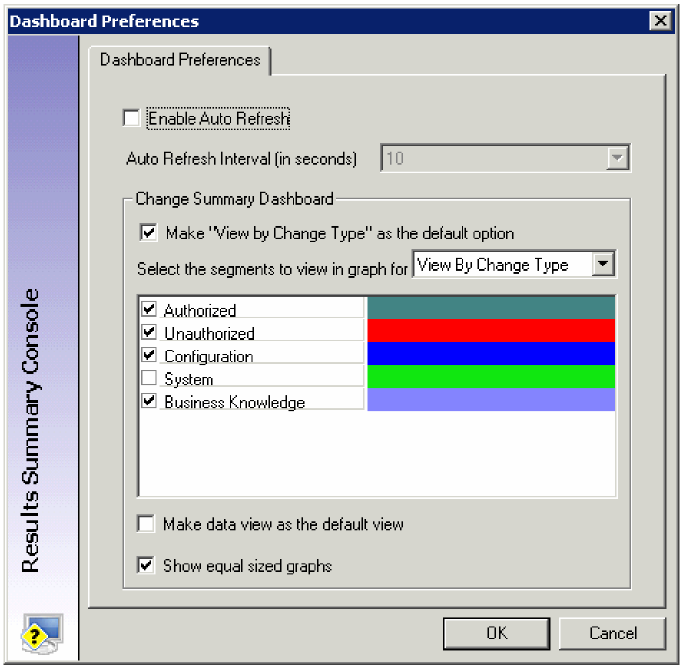
2.1 Setting Dashboard Preferences

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

To set dashboard preferences follow the below steps :

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

   Reports Summary Console displays the Dashboard Preferences window.



☐ Enable Auto Refresh

Auto Refresh Interval (in seconds) 10

Change Summary Dashboard

☑ Make "View by Change Type" as the default option

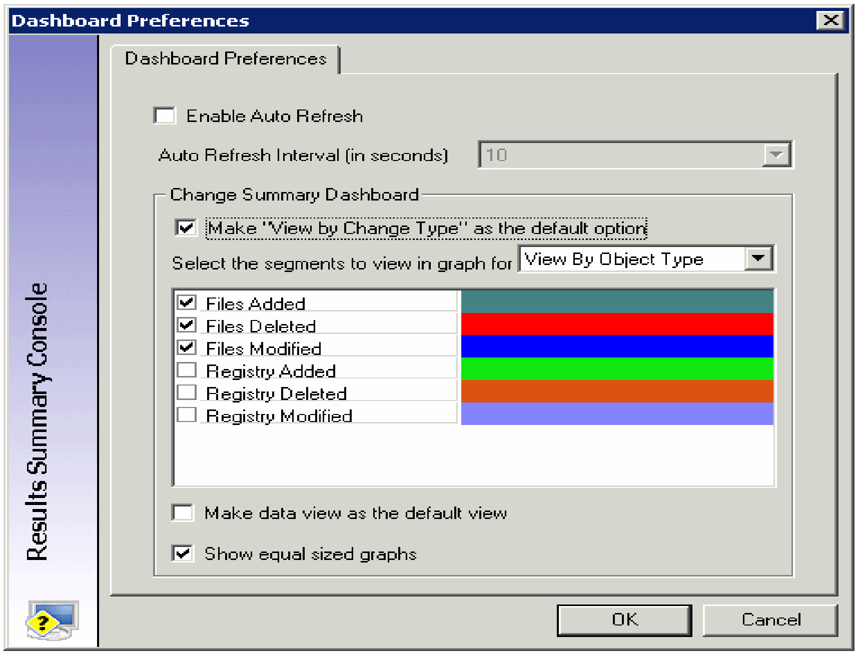
Select the segments to view in graph for View By Change Type

☑ Authorized
☑ Unauthorized
☑ Configuration
☐ System
☑ Business Knowledge

☐ Make data view as the default view

☑ Show equal sized graphs

Figure 3

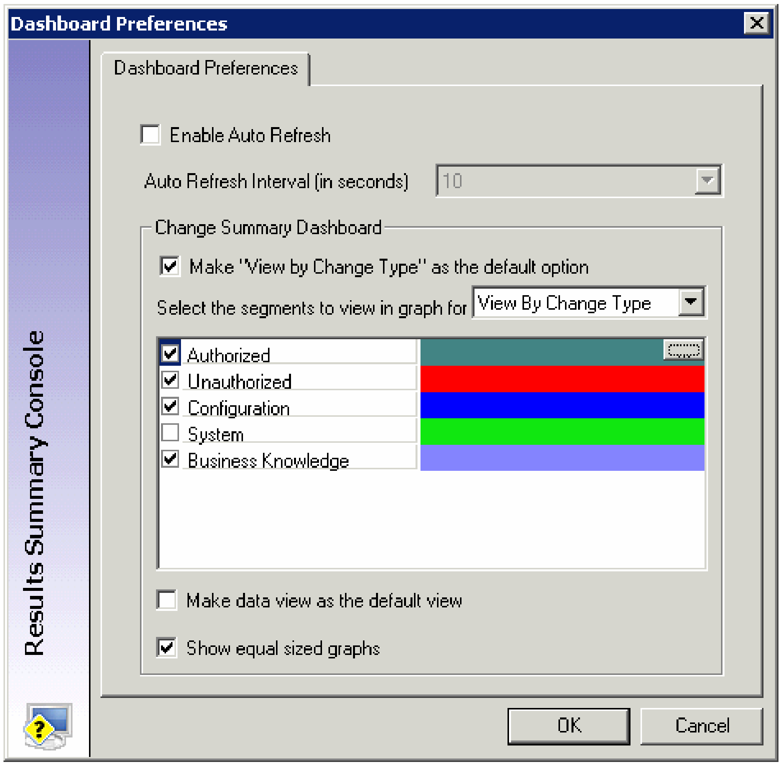
Field	Description
Enable Auto Refresh	Select this check box if you prefer EventTracker – Change Audit to refresh the Results Summary Console automatically. EventTracker - Change Audit enables the “Auto Refresh Interval [in seconds]” drop-down list. Set the interval for EventTracker - Change Audit to 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.  Dashboard Preferences Results Summary Console Dashboard Preferences ☐ Enable Auto Refresh Auto Refresh Interval (in seconds) 10 Change Summary Dashboard ☑ Make "View by Change Type" as the default option Select the segments to view in graph for View By Object Type ☑ Files Added ☑ Files Deleted ☑ Files Modified ☐ Registry Added ☐ Registry Deleted ☐ Registry Modified ☐ Make data view as the default view ☑ Show equal sized graphs OK Cancel Figure 8
Make data view as the default view	Select this check box if you prefer to view “Data View” by default. Otherwise, EventTracker - Change Audit displays the “Graph View” as default view.

Field	Description
Show equal sized graphs	EventTracker - Change Audit selects this check box by default. Clear this check box if preferred to view unequal sized graphs.

NOTE: To get data for authorized, configuration and Business Knowledge, the user must add it manually by:

- Navigating to EventTracker **Change Browser-> Options->Global Configuration->File Type**
- Adding the file types.

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.



Dashboard Preferences

Dashboard Preferences

☐ Enable Auto Refresh

Auto Refresh Interval (in seconds) 10

Change Summary Dashboard

☑ Make "View by Change Type" as the default option

Select the segments to view in graph for View By Change Type

☑ Authorized	🟩 ...
☑ Unauthorized	🟥
☑ Configuration	🟦
☐ System	🟩
☑ Business Knowledge	🟪

☐ Make data view as the default view

☑ Show equal sized graphs

Figure 9

4. Click the browse button.
   EventTracker - Change Audit displays the color palette.

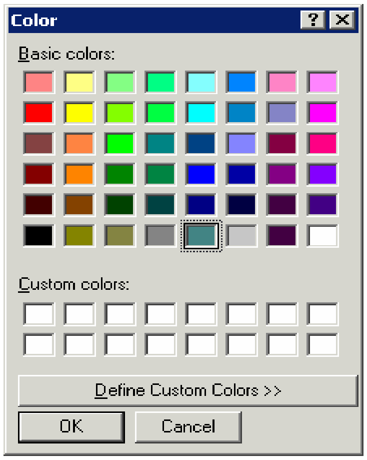


Figure 10

5. Select the color and then click **OK**.

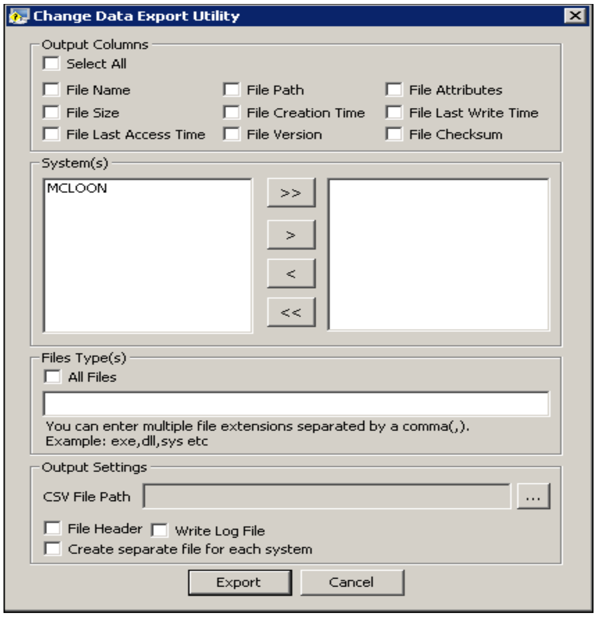
2.2 Export Change Data

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

To export Change Data follow the below steps :

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

   Change Data Export Utility window displays.

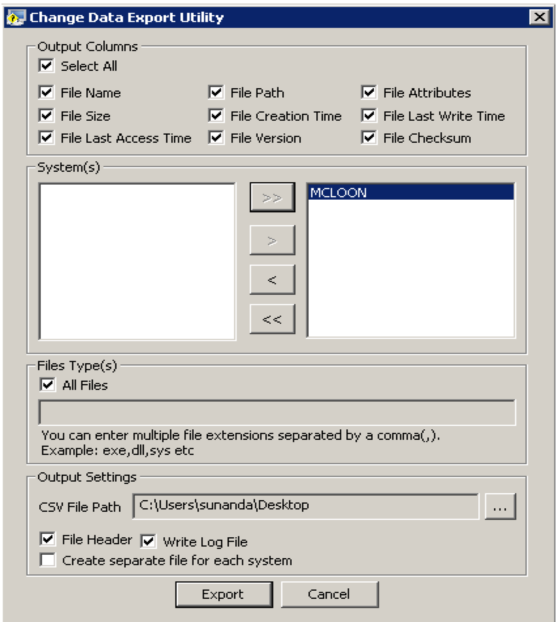


MCLOON

You can enter multiple file extensions separated by a comma(,).
Example: exe,dll,sys etc

Figure 11

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 a comma.
5. In **Output Settings** pane, browse the **CSV File Path**.
6. If required select **File Header, Write Log File, Create a separate file for each system option**.



Change Data Export Utility

Output Columns
☑ Select All

☑ File Name	☑ File Path	☑ File Attributes
☑ File Size	☑ File Creation Time	☑ File Last Write Time
☑ File Last Access Time	☑ File Version	☑ File Checksum

System(s)
MCLOON

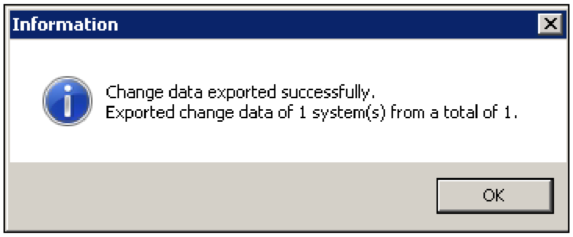
Files Type(s)
☑ All Files

You can enter multiple file extensions separated by a comma(,).
Example: exe,dll,sys etc

Output Settings
CSV File Path C:\Users\sunanda\Desktop
☑ File Header ☑ Write Log File
☐ Create separate file for each system

Figure 4

7. Select the **Export** button.
   A successful message displays.



Information

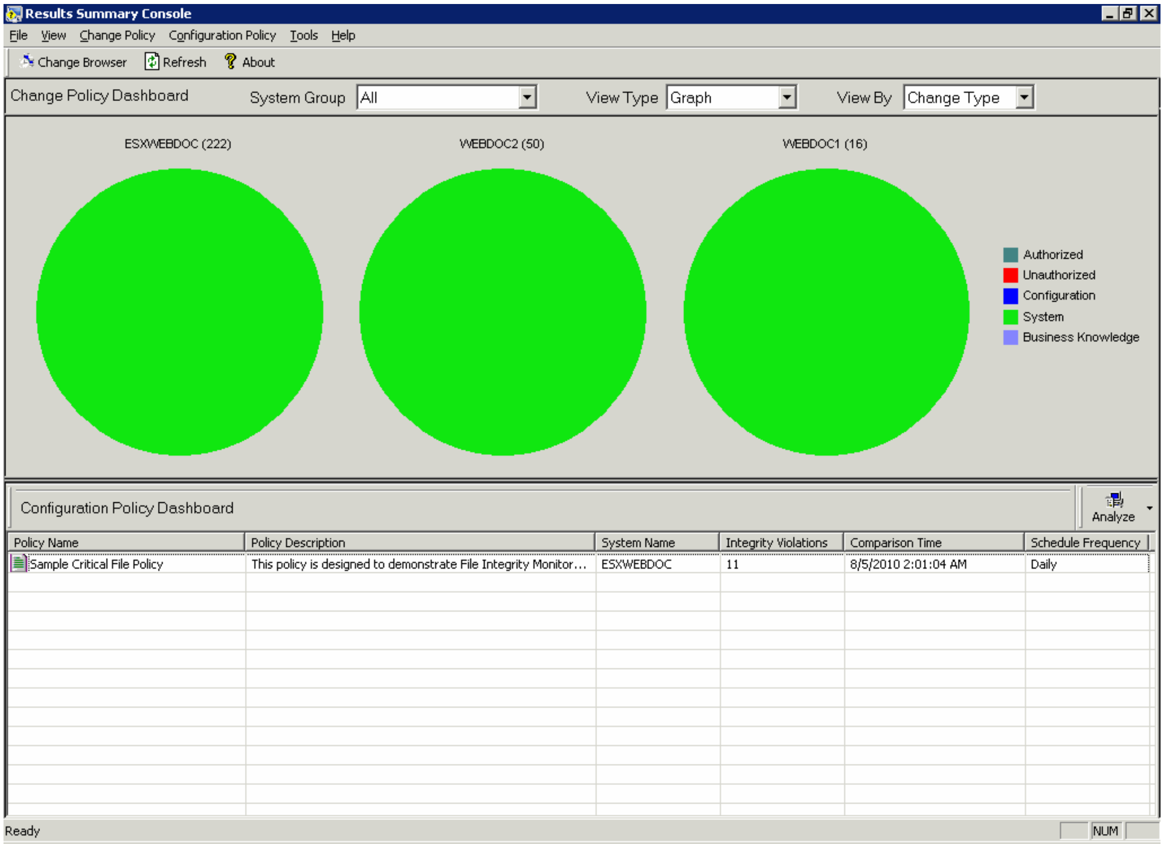
Change data exported successfully.
Exported change data of 1 system(s) from a total of 1.

Figure 13

Data can be viewed regarding the files in the respective CSV file. List can be imported as discussed in in the Active Watch List.

2.3 Viewing the summary of the Change Details

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



Change Policy Dashboard

System Group: All

View Type: Graph

View By: Change Type

Configuration Policy Dashboard

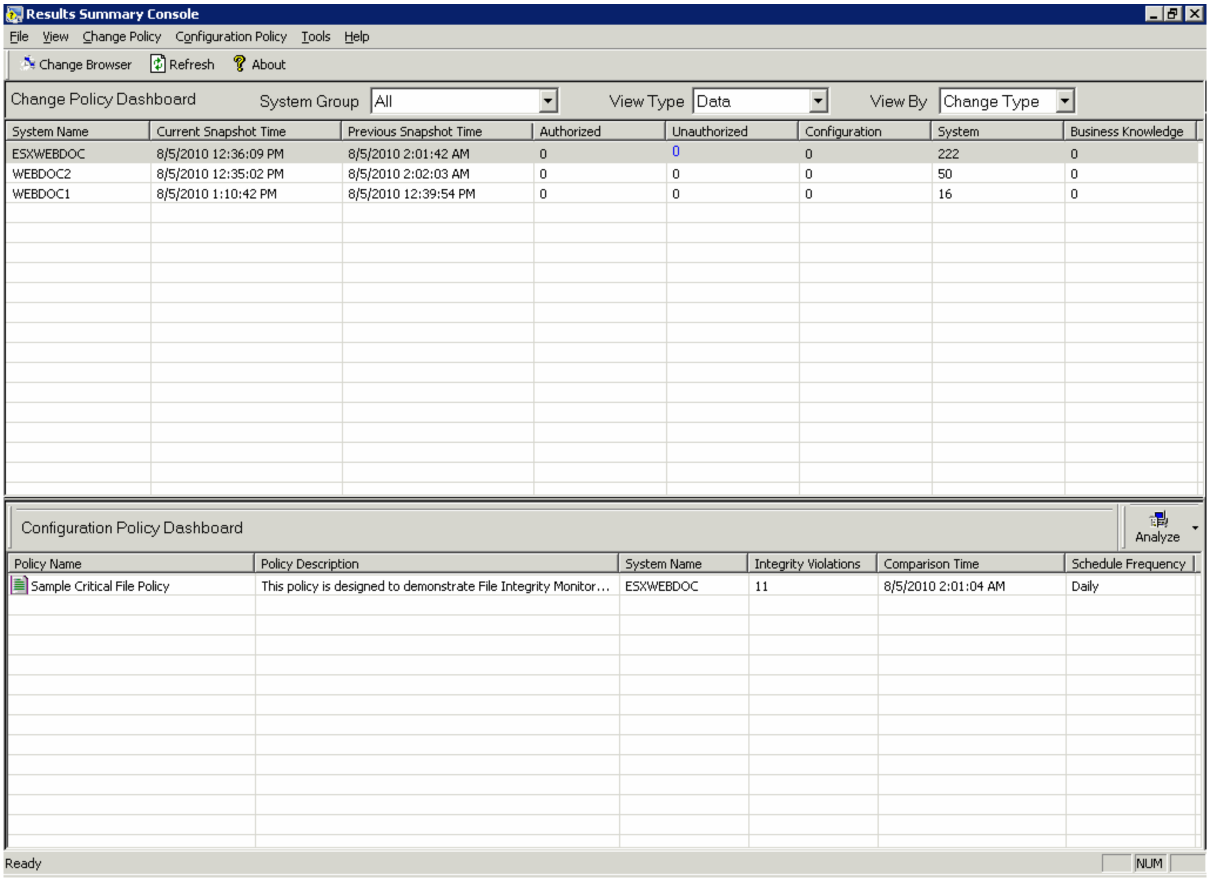
Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor...	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 14

NOTE: Depending on the Configuration settings, the graph varies.

To view statistical data of Change Type, follow the below steps :

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.



Change Policy Dashboard

System Group: All

View Type: Data

View By: Change Type

System Name	Current Snapshot Time	Previous Snapshot Time	Authorized	Unauthorized	Configuration	System	Business Knowledge
ESXWEBDOC	8/5/2010 12:36:09 PM	8/5/2010 2:01:42 AM	0	0	0	222	0
WEBDOC2	8/5/2010 12:35:02 PM	8/5/2010 2:02:03 AM	0	0	0	50	0
WEBDOC1	8/5/2010 1:10:42 PM	8/5/2010 12:39:54 PM	0	0	0	16	0

Configuration Policy Dashboard

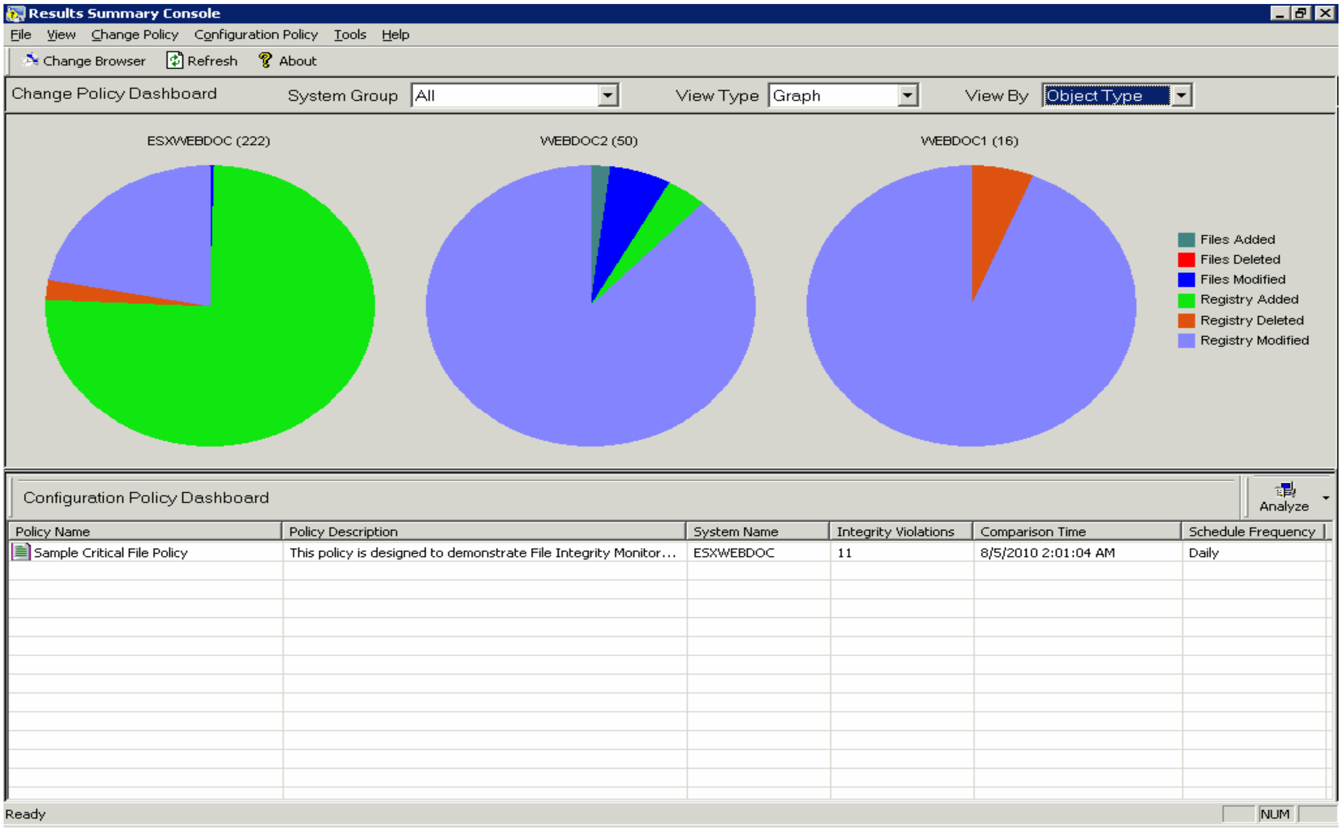
Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 15

To view chart view summary of Object Type, follow the below steps :

1. Select the **Object Type** option from the **View By** drop-down list.

   EventTracker displays the chart view summary of Object Type.



System Group: All

View Type: Graph

View By: Object Type

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

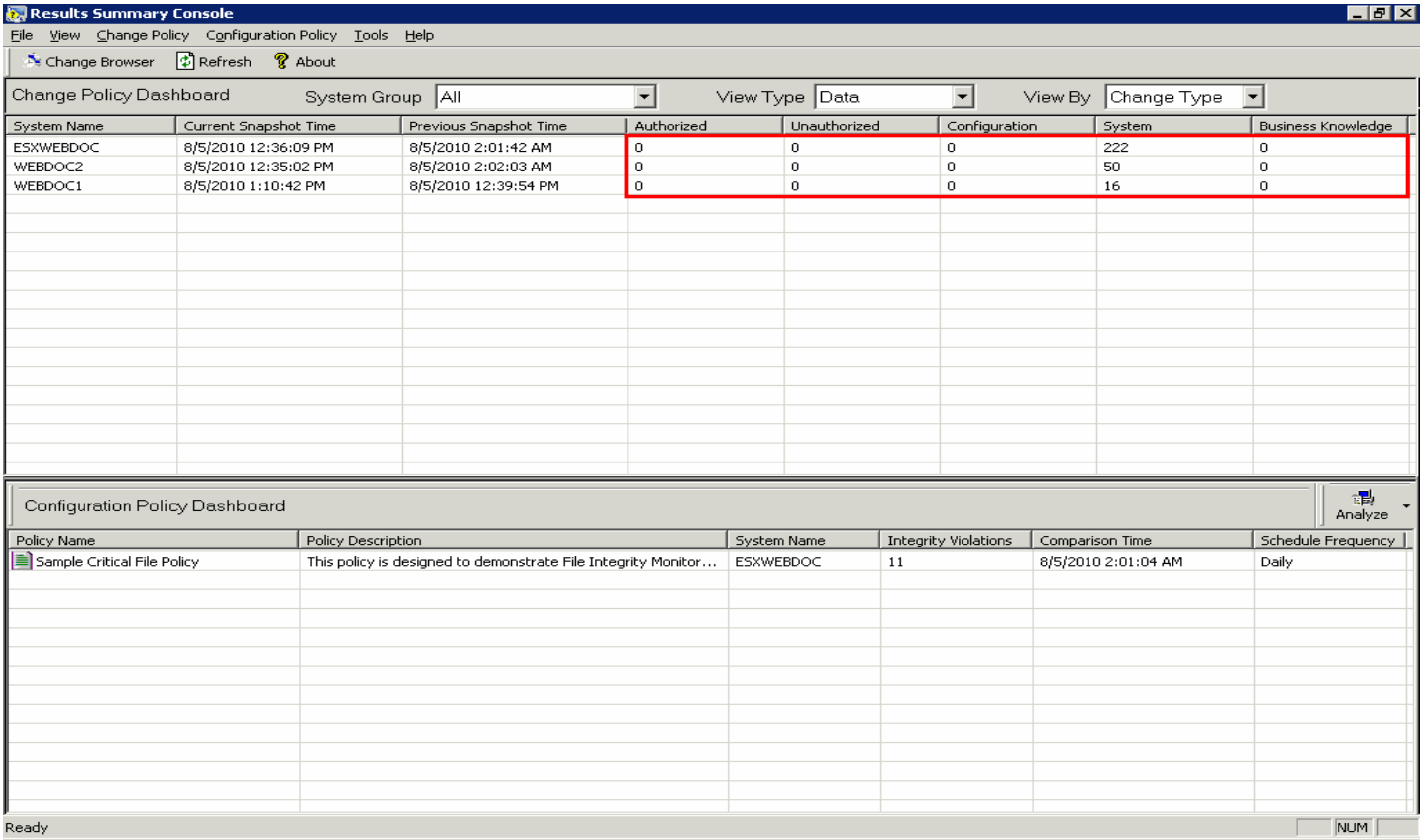
Figure16

NOTE: Depending on the Configuration settings, the graph varies.

2.4 Viewing the Change Details – Change Details Console

To view change details in the Change Details console, follow the below steps :

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


Results Summary Console
File View Change Policy Configuration Policy Tools Help
Change Browser Refresh About
Analyze
Ready
NUM

Change Policy Dashboard — System Group: All — View Type: Data — View By: Change Type

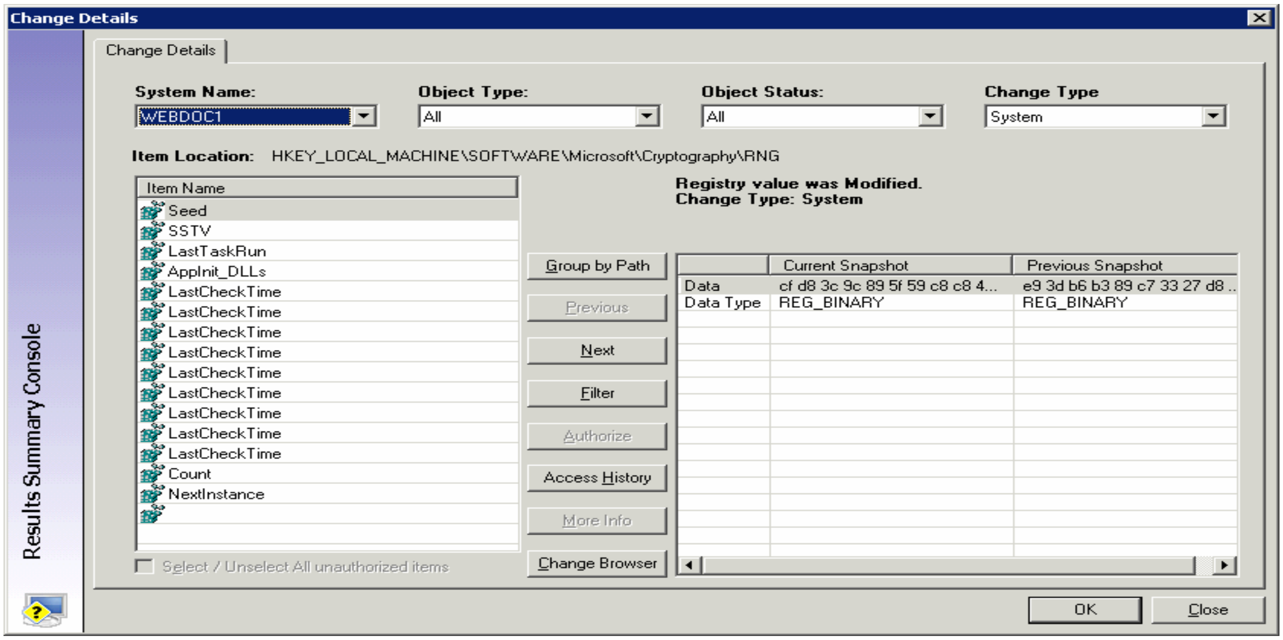
System Name	Current Snapshot Time	Previous Snapshot Time	Authorized	Unauthorized	Configuration	System	Business Knowledge
ESXWEBDOC	8/5/2010 12:36:09 PM	8/5/2010 2:01:42 AM	0	0	0	222	0
WEBDOC2	8/5/2010 12:35:02 PM	8/5/2010 2:02:03 AM	0	0	0	50	0
WEBDOC1	8/5/2010 1:10:42 PM	8/5/2010 12:39:54 PM	0	0	0	16	0

Configuration Policy Dashboard

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 17

Results Summary Console displays the Change Details console.



Change Details

System Name: WEBDOC1
Object Type: All
Object Status: All
Change Type: System

Item Location: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG

Registry value was Modified.
Change Type: System

Item Name
Seed
SSTV
LastTaskRun
AppInit_DLLs
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
LastCheckTime
Count
NextInstance

	Current Snapshot	Previous Snapshot
Data	cf d8 3c 9c 89 5f 59 c8 c8 4...	e9 3d b6 b3 89 c7 33 27 d8 ..
Data Type	REG_BINARY	REG_BINARY

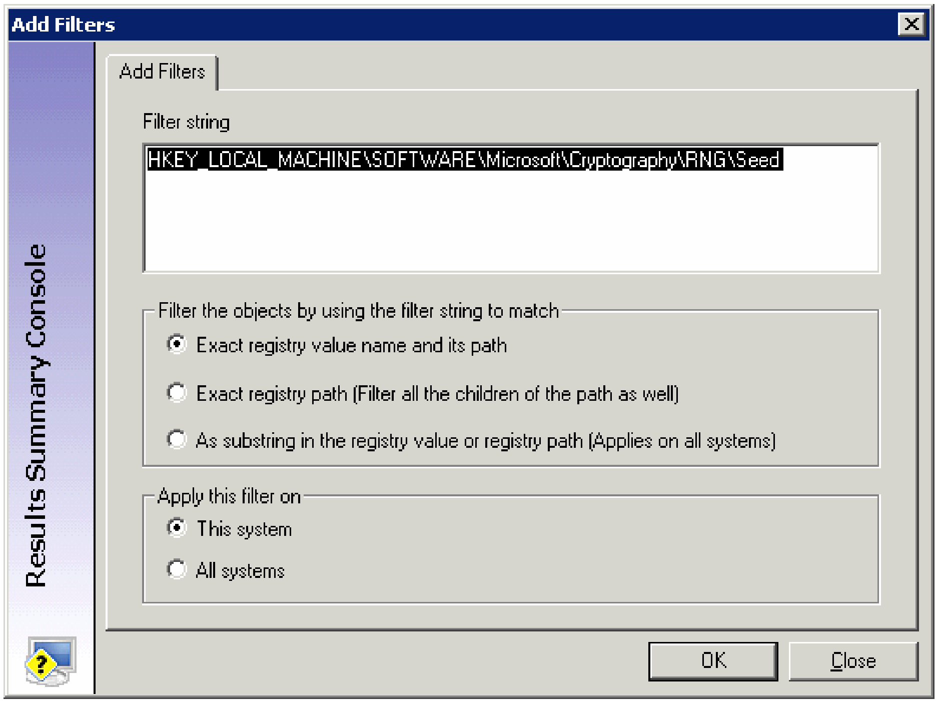
□ Select / Unselect All unauthorized items

Figure 18

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 a new filter to System or Global Configuration. Results Summary Console displays the Add Filters console.



Filter string

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed

Filter the objects by using the filter string to match

● Exact registry value name and its path

○ Exact registry path (Filter all the children of the path as well)

○ As substring in the registry value or registry path (Applies on all systems)

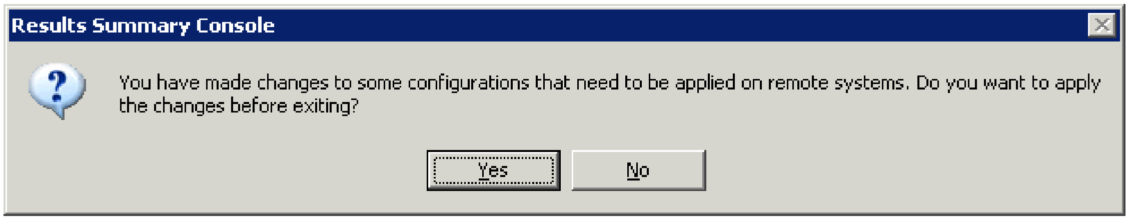
Apply this filter on

● This system

○ All systems

Figure 5

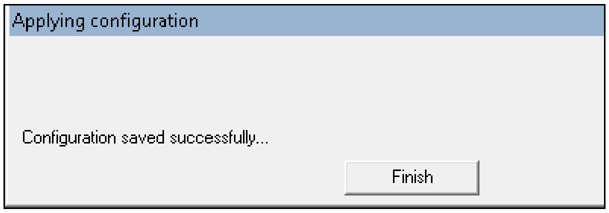
4. Select an appropriate option under “Filter the objects by using the filter string to match”.
5. Select “**All systems**” option under “**Apply this filter on**” to add this filter to Global Configuration. Click **OK** on the Change Details console. Results Summary Console displays the confirmation message box.



You have made changes to some configurations that need to be applied on remote systems. Do you want to apply the changes before exiting?

Figure 20

6. Click **Yes**. Results Summary Console displays the **Applying Configuration** dialog box with the appropriate message.

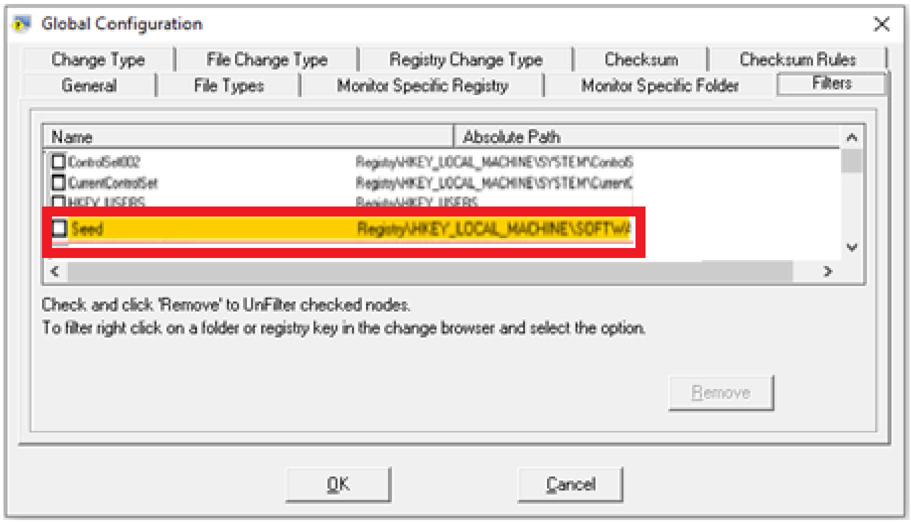


Configuration saved successfully...

Figure 21

7. Click **Finish** on the **Applying Configuration** dialog box.
8. Open the **Change Browser**. (From the Result Summary Console refer fig 17)
9. Click the **Options** menu and select the **Global Configuration** option.
10. Click the **Filters** tab.

    EventTracker - Change Audit displays the newly added Global Filter.

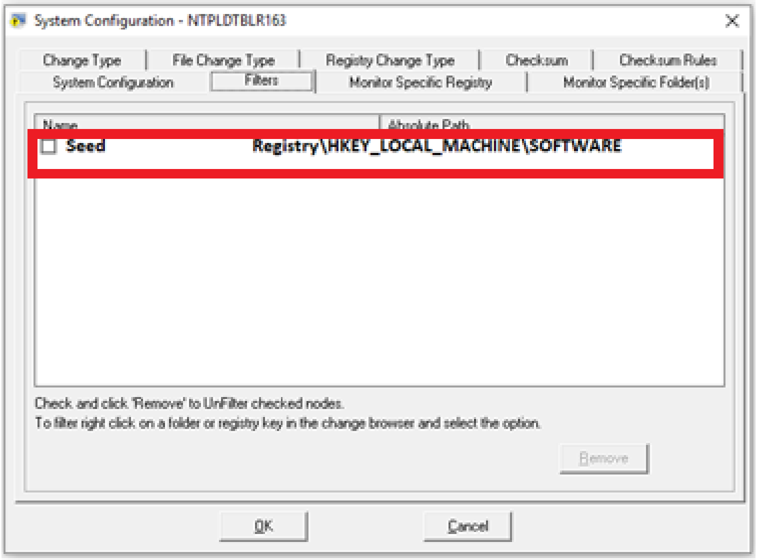


Name	Absolute Path
□ ControlSet002	Registry\HKEY_LOCAL_MACHINE\SYSTEM\ControlS
□ CurrentControlSet	Registry\HKEY_LOCAL_MACHINE\SYSTEM\CurrentC
□ HKEY_USERS	Registry\HKEY_USERS
□ Seed	Registry\HKEY_LOCAL_MACHINE\SOFTWA

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 22

11. Select "**This system'** option under "**Apply this filter on'** to add this filter to the System Configuration. (In the results summary console, refer fig 17)
12. Open the **Change Browser**.
13. Load the system that you want to view the newly added filter.
14. Click the **Options** menu and select the **System Configuration** option.
15. Click the **Filters** tab.



Name	Absolute Path
□ Seed	Registry\HKEY_LOCAL_MACHINE\SOFTWARE

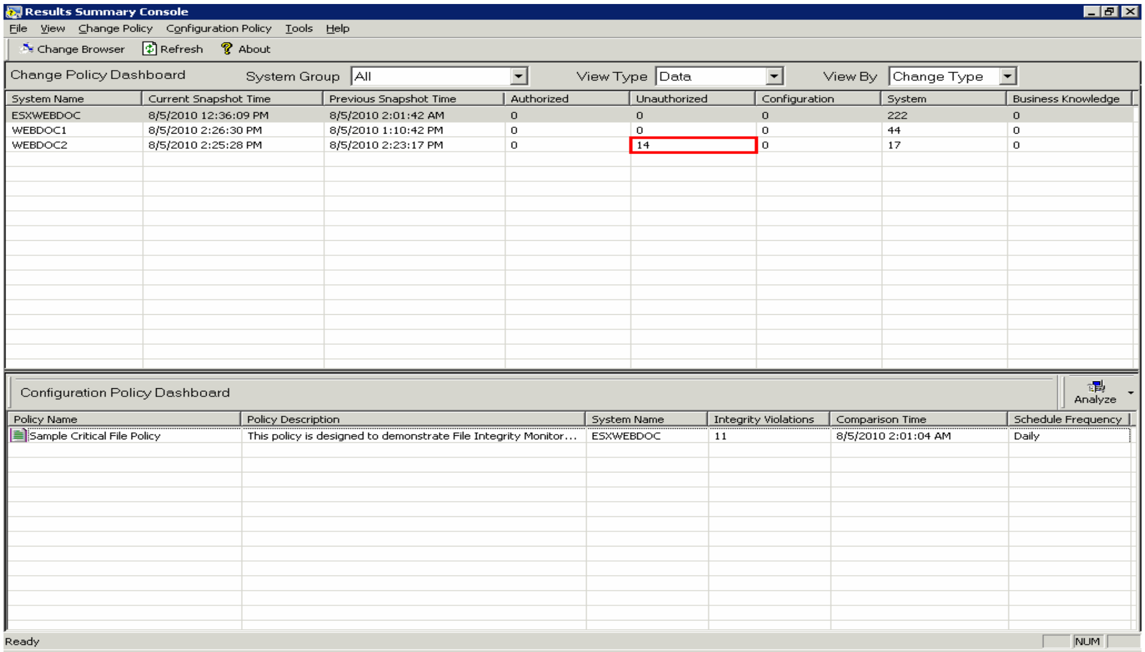
Check and click 'Remove' to UnFilter checked nodes.
To filter right click on a folder or registry key in the change browser and select the option.

Figure 23

2.5 Authorizing Unauthorized Changes

To authorize unauthorized changes, follow the below steps :

1. Click the hyperlink in the **Unauthorized** column.



Change Policy Dashboard System Group All View Type Data View By Change Type

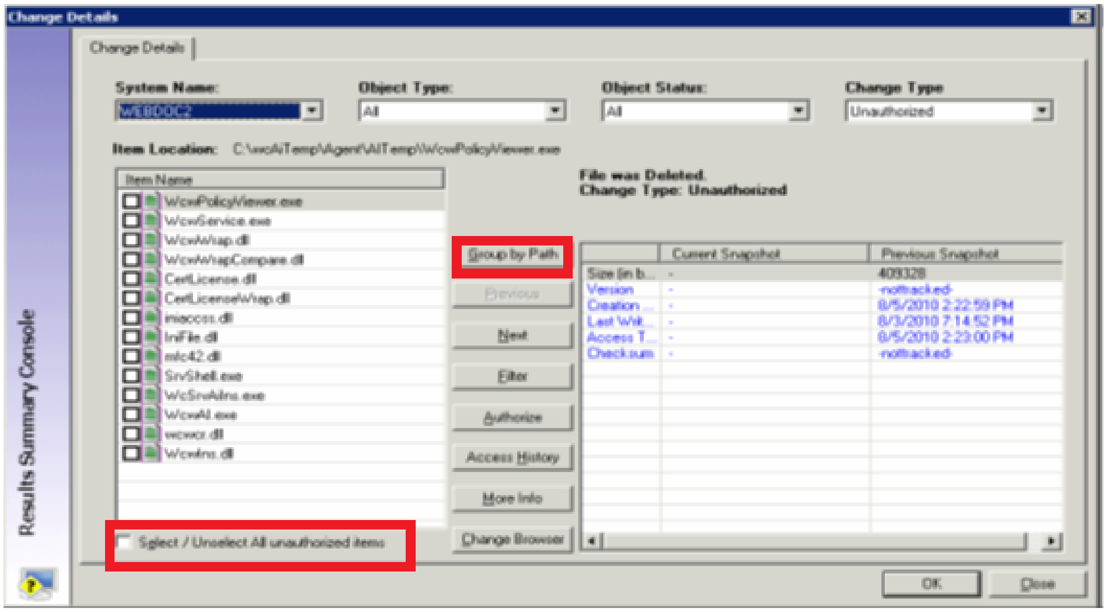
System Name	Current Snapshot Time	Previous Snapshot Time	Authorized	Unauthorized	Configuration	System	Business Knowledge
ESXWEBDOC	8/5/2010 12:36:09 PM	8/5/2010 2:01:42 AM	0	0	0	222	0
WEBDOC1	8/5/2010 2:26:30 PM	8/5/2010 1:10:42 PM	0	0	0	44	0
WEBDOC2	8/5/2010 2:25:28 PM	8/5/2010 2:23:17 PM	0	14	0	17	0

Configuration Policy Dashboard

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 24

2. Results Summary Console displays the Change Details console.



Change Details

Change Details

System Name: WEBDOC2

Object Type: All

Object Status: All

Change Type: Unauthorized

Item Location: C:\wcAiTemp\Agent\AITemp\WcwPolicyViewer.exe

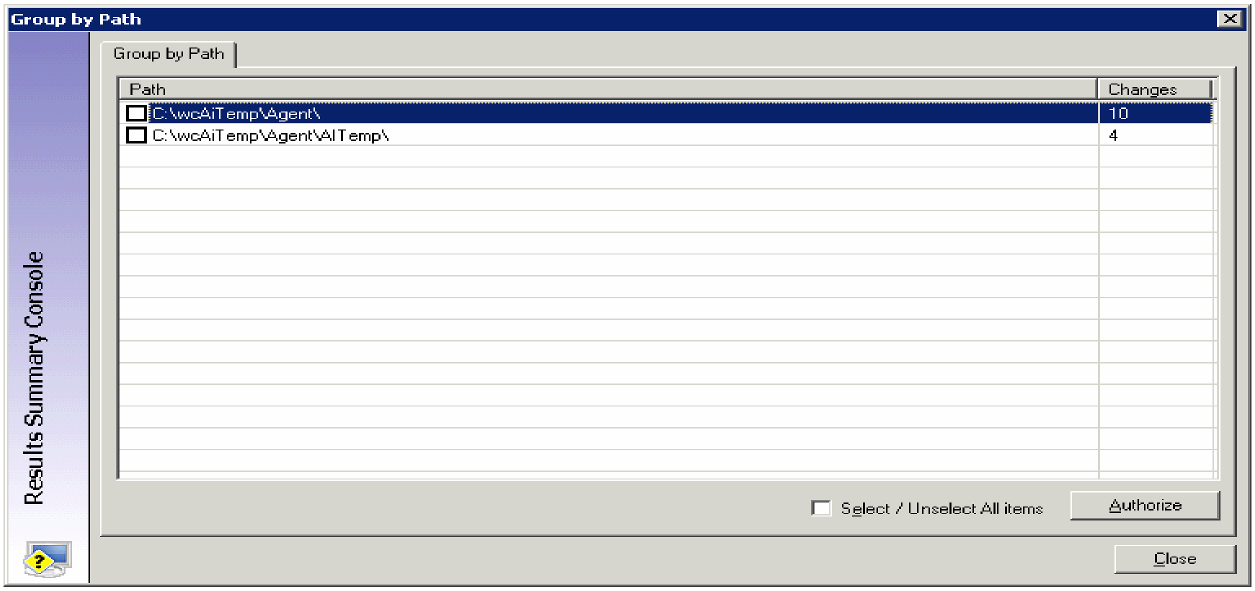
File was Deleted.
Change Type: Unauthorized

Item Name
□ WcwPolicyViewer.exe
□ WcwService.exe
□ WcwWrap.dll
□ WcwWrapCompare.dll
□ CertLicense.dll
□ CertLicenseWrap.dll
□ iniaccess.dll
□ IniFile.dll
□ mlc42.dll
□ SrvShell.exe
□ WcSrvAdms.exe
□ WcwAll.exe
□ wcwcr.dll
□ Wcwlns.dll

	Current Snapshot	Previous Snapshot
Size (in b...	-	409328
Version	-	-nottracked-
Creation ...	-	8/5/2010 2:22:59 PM
Last Writ...	-	8/3/2010 7:14:52 PM
Access T...	-	8/5/2010 2:23:00 PM
Checksum	-	-nottracked-

Figure 25

3. Select the **Select / Unselect All unauthorized items** checkbox to select all unauthorized items if not selected.
   You can also select/unselect individual items by selecting or clearing the respective checkbox.
   (OR)
   Click **Group by Path** to view all unauthorized changes based on the location.
   Results Summary Console displays the Group by Path window.



Group by Path

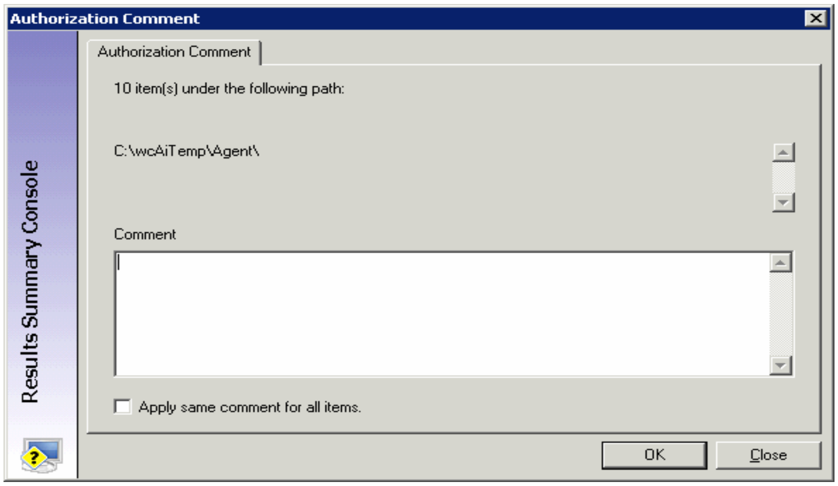
Path	Changes
□ C:\wcAiTemp\Agent\	10
□ C:\wcAiTemp\Agent\AITemp\	4

Figure 26

4. Select the items and then click **Authorize**.

Results Summary Console displays the Authorization Comment window.

Note: Each path selected, Results Summary Console displays a separate **Authorization Comment** window.



10 item(s) under the following path:

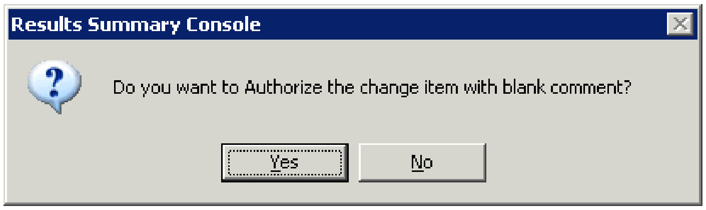
C:\wcAiTemp\Agent\

Comment

☐ Apply same comment for all items.

Figure 27

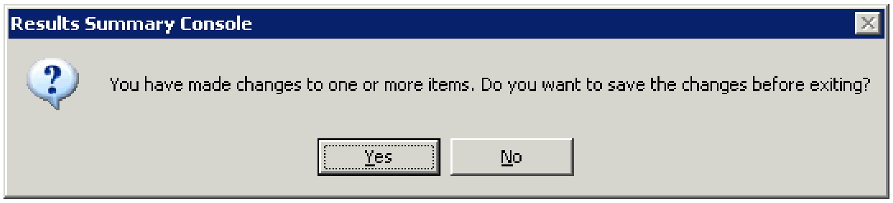
5. Type an appropriate comment.
6. Select the **Apply same comment for all items** check box if you wish to apply the comment for all items.
7. Click **OK**.
   If you leave the comment field empty, Results Summary Console displays the confirmation message box.



Do you want to Authorize the change item with blank comment?

Figure 28

8. Click **Close** on the Group by Path window.
9. Click **OK** on the Change Details window.
   Results Summary Console displays the confirmation message box.

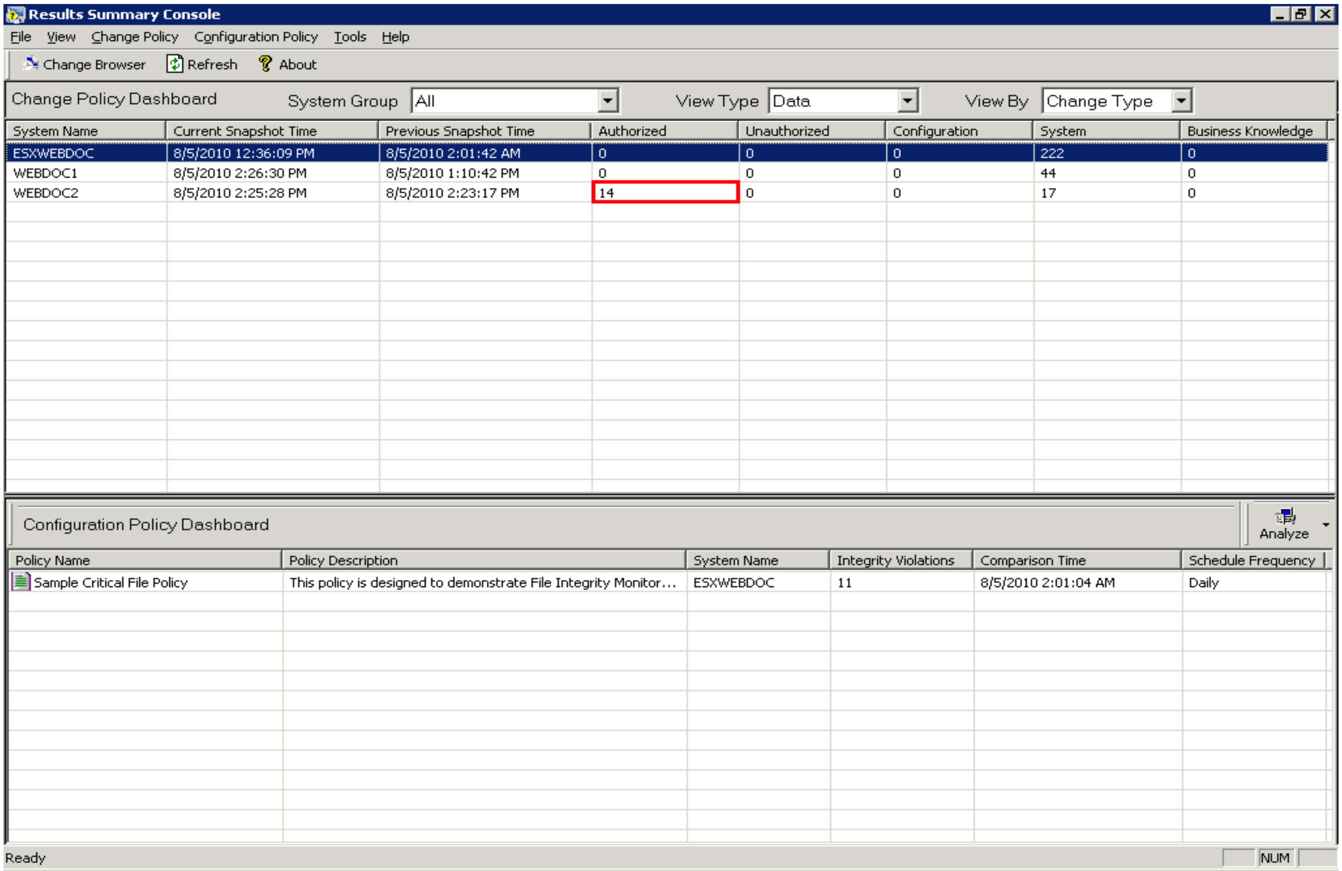


You have made changes to one or more items. Do you want to save the changes before exiting?

Figure 29

10. Click **Yes** to save the changes.

    EventTracker - Change Audit authorizes the unauthorized changes.


Results Summary Console
File View Change Policy Configuration Policy Tools Help
Change Browser Refresh About
Change Policy Dashboard
System Group All
View Type Data
View By Change Type

System Name	Current Snapshot Time	Previous Snapshot Time	Authorized	Unauthorized	Configuration	System	Business Knowledge
ESXWEBDOC	8/5/2010 12:36:09 PM	8/5/2010 2:01:42 AM	0	0	0	222	0
WEBDOC1	8/5/2010 2:26:30 PM	8/5/2010 1:10:42 PM	0	0	0	44	0
WEBDOC2	8/5/2010 2:25:28 PM	8/5/2010 2:23:17 PM	14	0	0	17	0

Configuration Policy Dashboard
Analyze

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor...	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 30

2.6 Viewing the change details in the Change Browser

To view change details in the Change Browser, follow the below steps :

1. Click a hyperlink under the **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 window.

   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 window.

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

2.7 Viewing Change Report

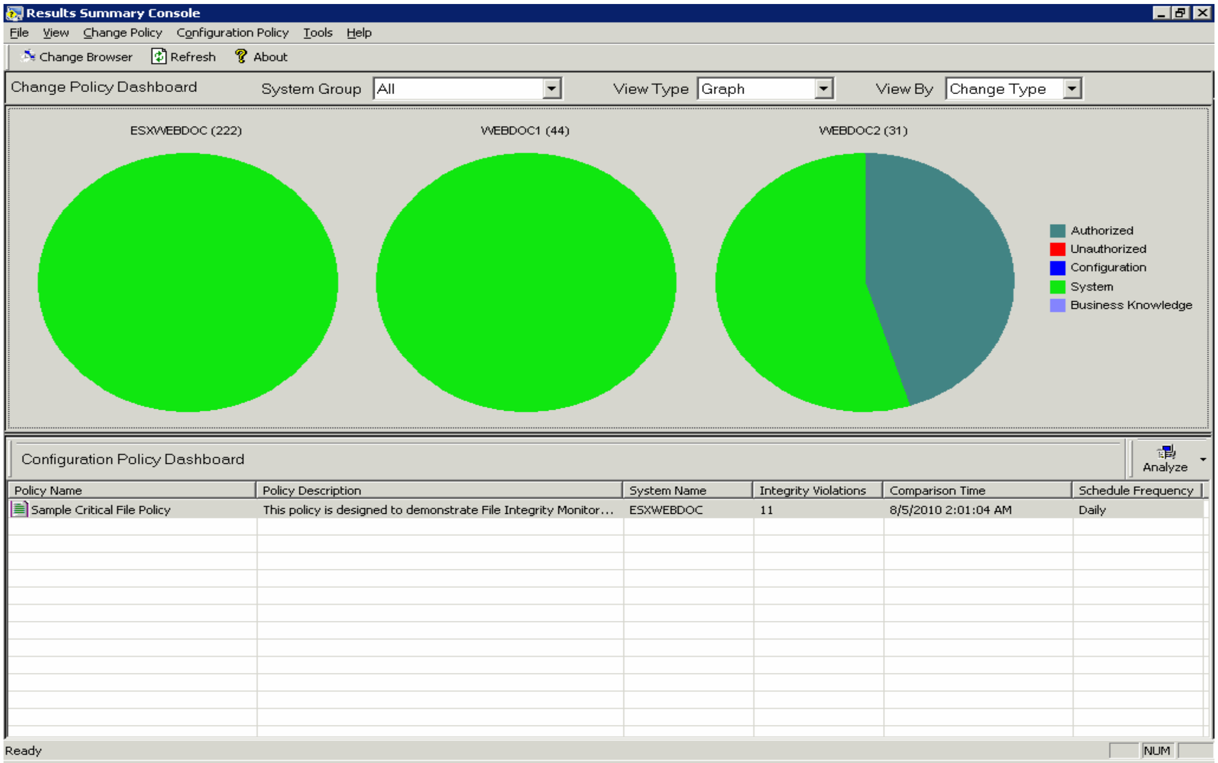
To view change report, follow the below steps :

1. Select a system (In the **Change Policy Dashboard)**
2. Click the **Change Policy** menu and select the **View Report** option.

   Results Summary Console displays the report in the Notepad.

2.8 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.



System Group: All
View Type: Graph
View By: Change Type

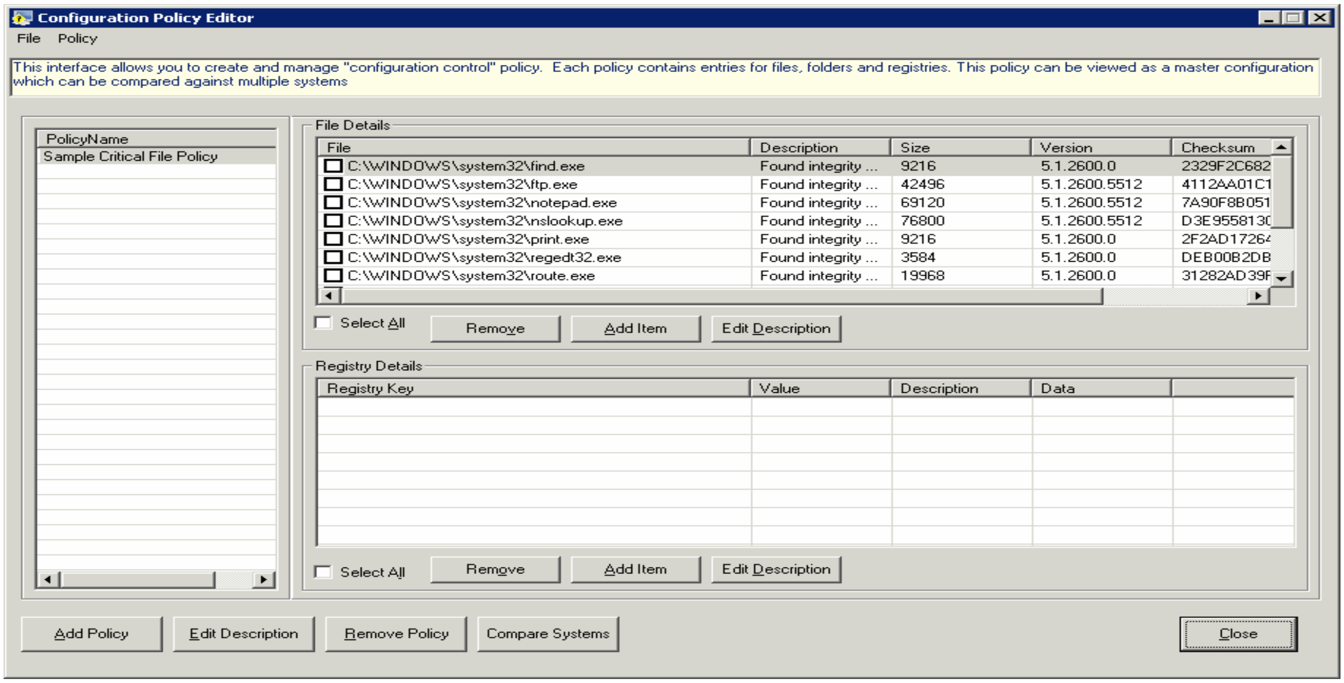
Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/5/2010 2:01:04 AM	Daily

Figure 31

NOTE: Depending on the Configuration settings, the graph varies.

Icon	Represents
🔴	Snapshot in progress.
🟢	No changes found.
🗎	File changes found.
⚙	Registry changes found.
🗎⚙	File and registry changes found.

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**.



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

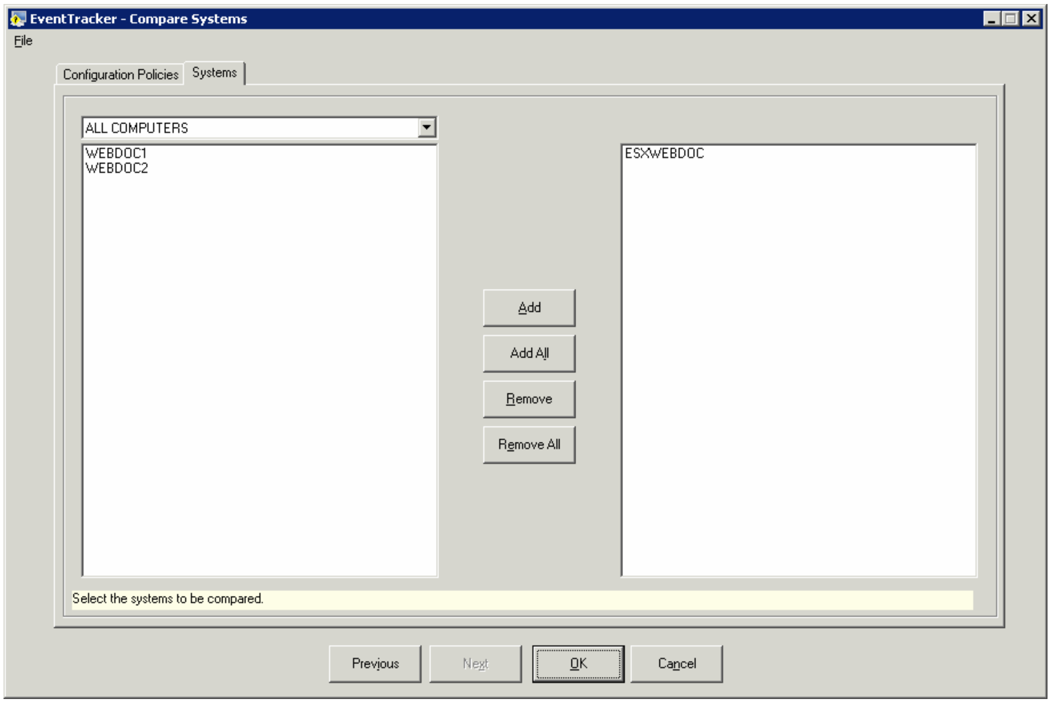
PolicyName
Sample Critical File Policy

File Details

File	Description	Size	Version	Checksum
□ C:\WINDOWS\system32\find.exe	Found integrity ...	9216	5.1.2600.0	2329F2C682
□ C:\WINDOWS\system32\ftp.exe	Found integrity ...	42496	5.1.2600.5512	4112AA01C1
□ C:\WINDOWS\system32\notepad.exe	Found integrity ...	69120	5.1.2600.5512	7A90F8B051
□ C:\WINDOWS\system32\nslookup.exe	Found integrity ...	76800	5.1.2600.5512	D3E955813C
□ C:\WINDOWS\system32\print.exe	Found integrity ...	9216	5.1.2600.0	2F2AD17264
□ C:\WINDOWS\system32\regedt32.exe	Found integrity ...	3584	5.1.2600.0	DEB00B2DB
□ C:\WINDOWS\system32\route.exe	Found integrity ...	19968	5.1.2600.0	31282AD39F

Figure 32

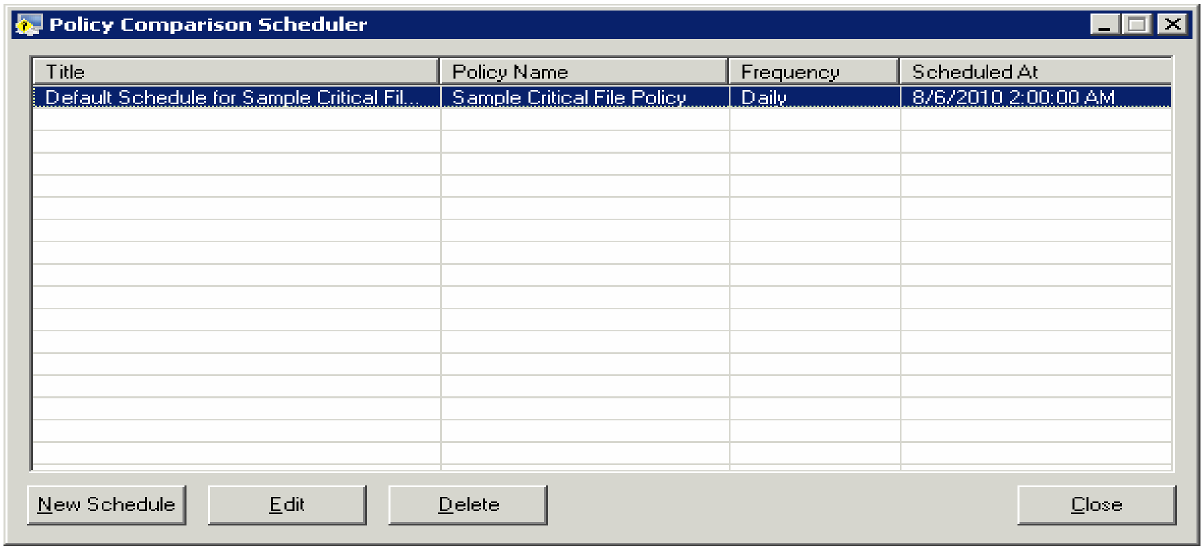
2. Click the name of the system in the **System Name** column to view compare system details. You can also compare policies on systems on demand.
   (OR)
   Click the **Analyze** drop-down button.
   EventTracker - Change Audit displays the shortcut menu.
   From the shortcut menu, choose **Run**.
 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



Select the systems to be compared.

Figure 33

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**.



Policy Comparison Scheduler

Title	Policy Name	Frequency	Scheduled At
Default Schedule for Sample Critical Fil...	Sample Critical File Policy	Daily	8/6/2010 2:00:00 AM

Figure 34

2.9 Analyzing the Policy Comparison Results

To analyze policy comparison results, follow the below steps :

1. Click an item in the **Integrity Violations** column. (Present in the Configuration Policy Dashboard)

   (OR)

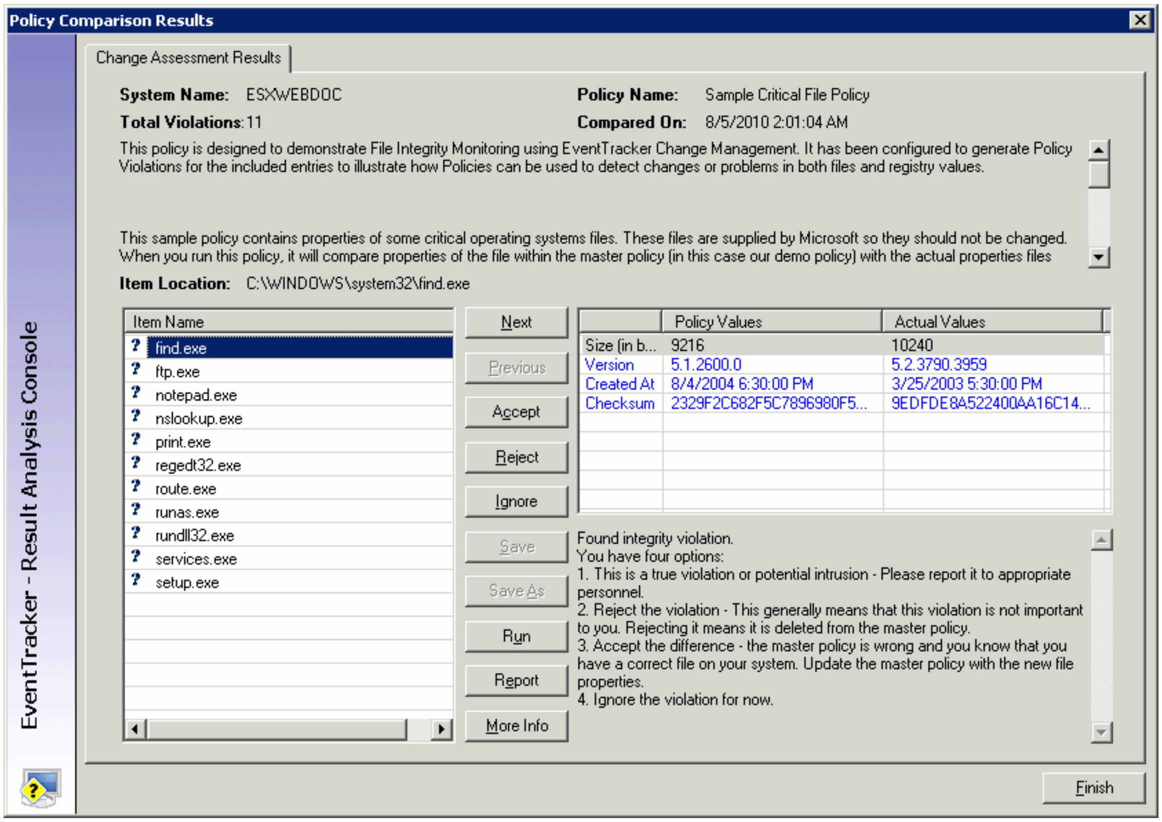
   Select an item.

   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.


Policy Comparison Results
EventTracker - Result Analysis Console
Change Assessment Results
Next
Previous
Accept
Reject
Ignore
Save
Save As
Run
Report
More Info
Finish

System Name: ESXWEBDOC

Total Violations: 11

Policy Name: Sample Critical File Policy

Compared On: 8/5/2010 2:01:04 AM

This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values.

This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When you run this policy, it will compare properties of the file within the master policy (in this case our demo policy) with the actual properties files

Item Location: C:\WINDOWS\system32\find.exe

Item Name
find.exe
ftp.exe
notepad.exe
nslookup.exe
print.exe
regedt32.exe
route.exe
runas.exe
rundll32.exe
services.exe
setup.exe

	Policy Values	Actual Values
Size (in b...	9216	10240
Version	5.1.2600.0	5.2.3790.3959
Created At	8/4/2004 6:30:00 PM	3/25/2003 5:30:00 PM
Checksum	2329F2C682F5C7896980F5...	9EDFDE8A522400AA16C14...

Found integrity violation.
You have four options:
1. This is a true violation or potential intrusion - Please report it to appropriate personnel.
2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy.
3. Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties.
4. Ignore the violation for now.

Figure 35

Field	Description
Top pane	
System Name	Name of the target system where the policy is compared.
Policy Name	Name of the policy compared on the target system.
Total Violations	Total number of violations detected.
Compared on	Date and time when the policy was compared.
Policy Description	Description of the policy.
Left pane	
Item Name	Name of the policy item.
Right pane	
Policy Values	Values of the policy item selected in the left pane when the policy was configured.

Field	Description
Actual Values	Actual Values of the policy item selected in the left pane after the policy comparison is done. This reflects any change in the value of the policy item.
Item Description	Description of the item selected in the left pane is displayed at the bottom of the right pane.

Field	Description
Tool tips are provided to understand the purpose of buttons. Move the mouse cursor on the buttons.	
Next	Move to the next item.
Previous	Move to the previous item.
Accept	If changes are found for the selected item, you can update the master policy with the new value.
Reject	If you find an item to be irrelevant to the present context, you can select and remove that item from the master policy.
Ignore	When you generate a report, ignored items is not considered for report generation. **Note**: These items are not removed from the master policy.
Save	Save the policy with the same name.
Save As	Save the policy with a different name.
Run	Manually run the policy again on the same system. This opens the Compare Systems window. The result displays as Manual Comparison in the Results Summary Console -> Configuration Policy Dashboard.
Report	Generate report. **Note:** Ignored items are not included in the report.
More Info	Click to view additional information on the selected process.
Finish	To close the Policy Comparison Results window.

Icon	Represents
🟢	No changes found.
?	Fresh item.

✓	Items accepted.
ⓘ	Items ignored.
✗	Items rejected.

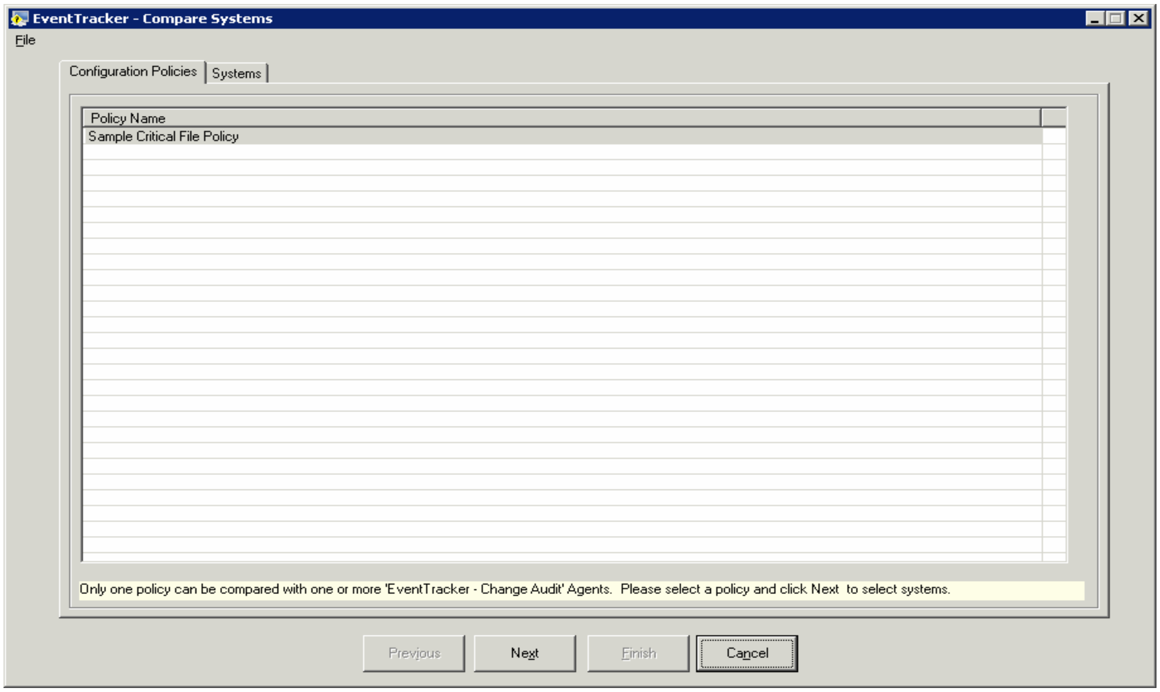
2.10 Compare Policies

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

To compare policies on demand, follow the below steps :

1. Select a record.
2. Click the **Configuration Policy** tab in the menu bar and select the **Compare Systems** option.

   Results Summary Console displays the Compare Systems window.



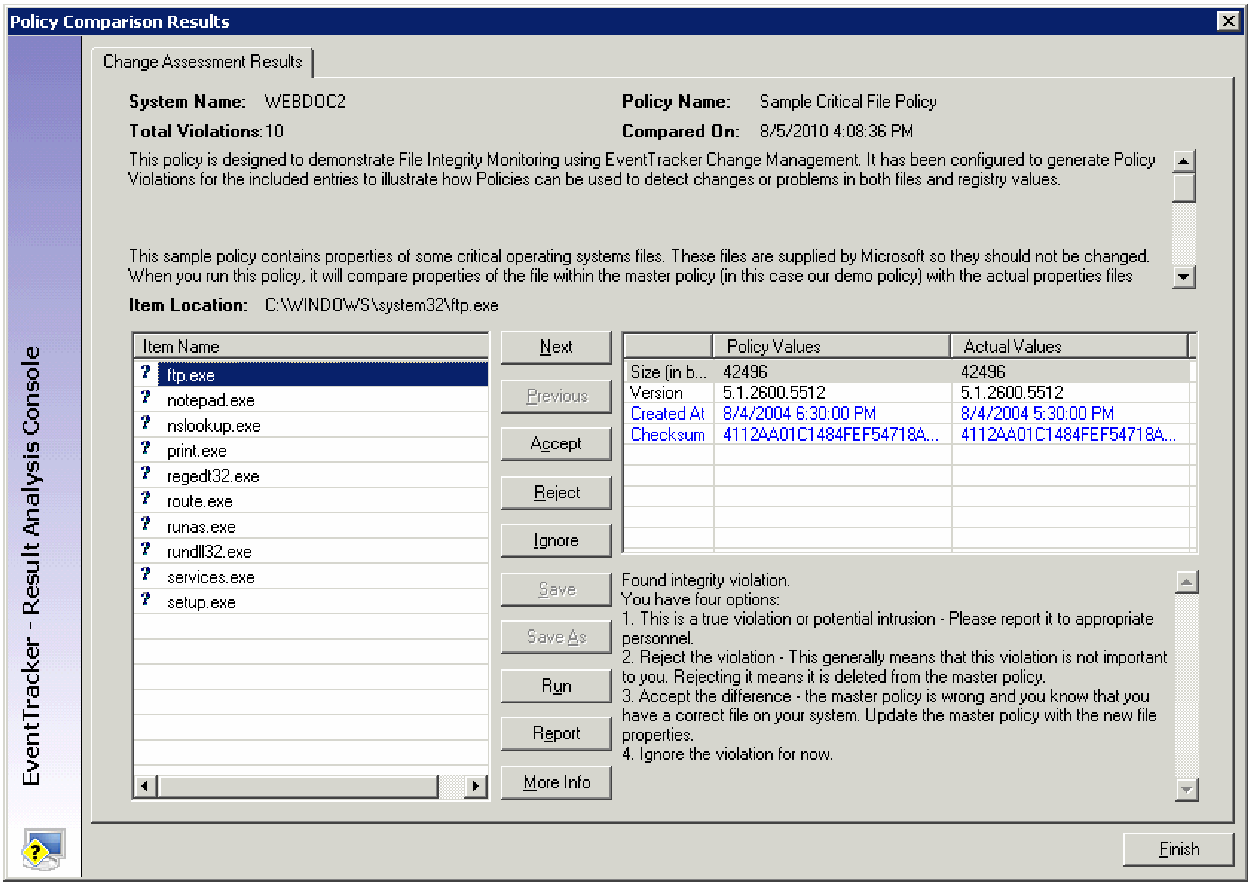
Sample Critical File Policy

Only one policy can be compared with one or more 'EventTracker - Change Audit' Agents. Please select a policy and click Next to select systems.

Figure 36

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.


Policy Comparison Results
Change Assessment Results
EventTracker - Result Analysis Console
Next
Previous
Accept
Reject
Ignore
Save
Save As
Run
Report
More Info
Finish

System Name: WEBDOC2

Total Violations: 10

Policy Name: Sample Critical File Policy

Compared On: 8/5/2010 4:08:36 PM

This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values.

This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When you run this policy, it will compare properties of the file within the master policy (in this case our demo policy) with the actual properties files

Item Location: C:\WINDOWS\system32\ftp.exe

Item Name
ftp.exe
notepad.exe
nslookup.exe
print.exe
regedt32.exe
route.exe
runas.exe
rundll32.exe
services.exe
setup.exe

	Policy Values	Actual Values
Size (in b...	42496	42496
Version	5.1.2600.5512	5.1.2600.5512
Created At	8/4/2004 6:30:00 PM	8/4/2004 5:30:00 PM
Checksum	4112AA01C1484FEF54718A...	4112AA01C1484FEF54718A...

Found integrity violation.
You have four options:
1. This is a true violation or potential intrusion - Please report it to appropriate personnel.
2. Reject the violation - This generally means that this violation is not important to you. Rejecting it means it is deleted from the master policy.
3. Accept the difference - the master policy is wrong and you know that you have a correct file on your system. Update the master policy with the new file properties.
4. Ignore the violation for now.

Figure 37

2.11 Scheduling the Policy Comparison

To schedule policy comparison, follow the below steps :

1. Right-click a record.

   Results Summary Console displays the shortcut menu.

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

   (OR)

   Click the **Analyze** button.

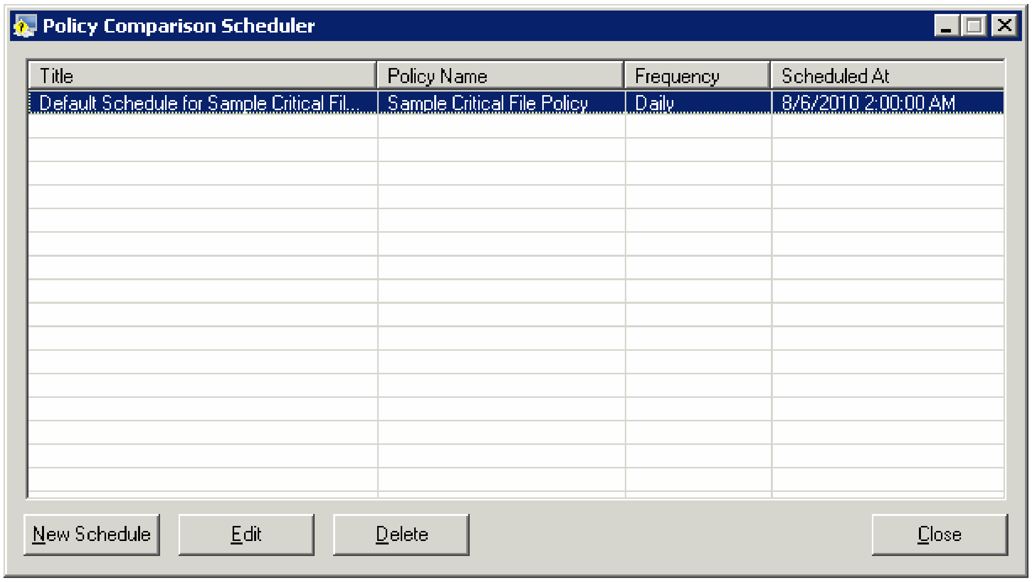
   Results Summary Console displays the shortcut menu.

   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.



Title	Policy Name	Frequency	Scheduled At
Default Schedule for Sample Critical Fil...	Sample Critical File Policy	Daily	8/6/2010 2:00:00 AM

Figure 38

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.

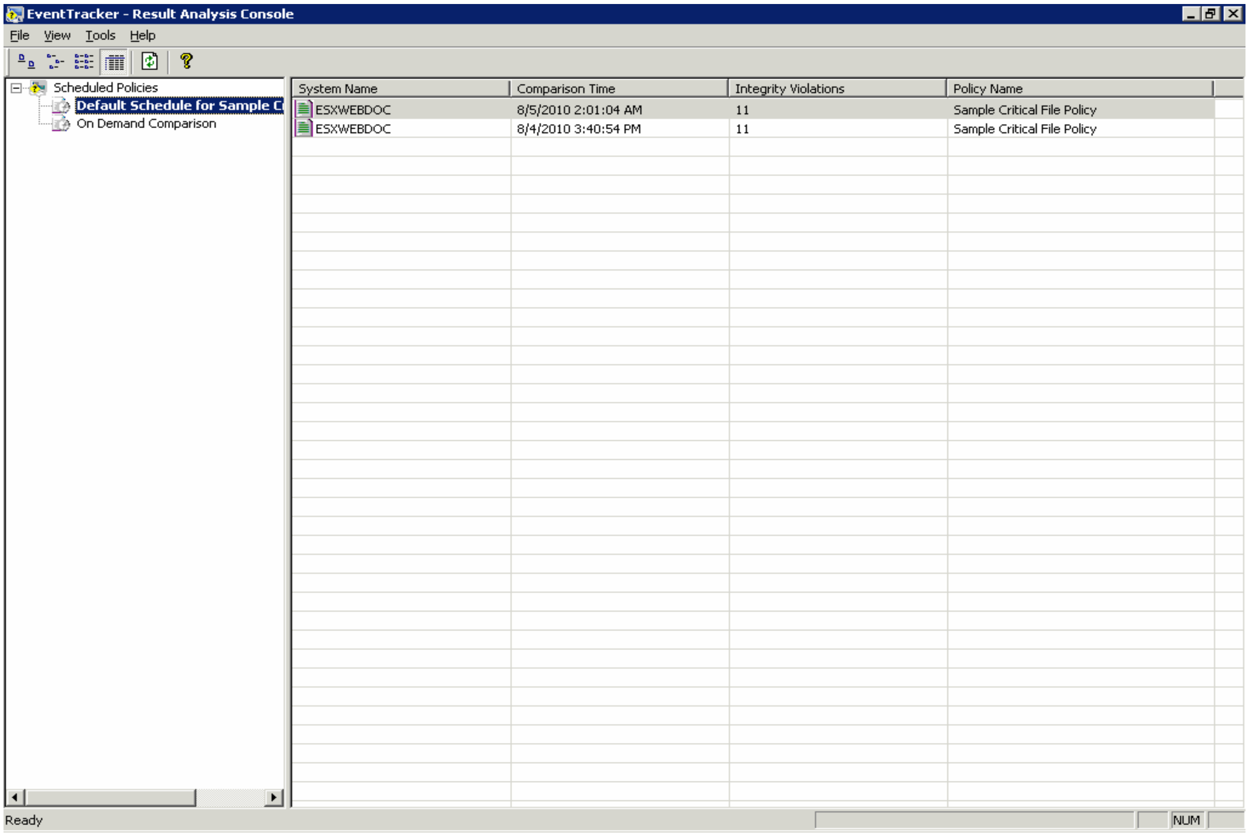
2.12 Accessing the Result Analysis Console

To access Result Analysis Console, follow the below steps :

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.



- Scheduled Policies
  - Default Schedule for Sample C
  - On Demand Comparison

System Name	Comparison Time	Integrity Violations	Policy Name
ESXWEBDOC	8/5/2010 2:01:04 AM	11	Sample Critical File Policy
ESXWEBDOC	8/4/2010 3:40:54 PM	11	Sample Critical File Policy

Figure 39

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.

3. Change Browser

3.1 View Groups option

This option helps you switch to the Groups view.

Follow the below steps, to Switch to the Groups view

1. Open the Change Browser.

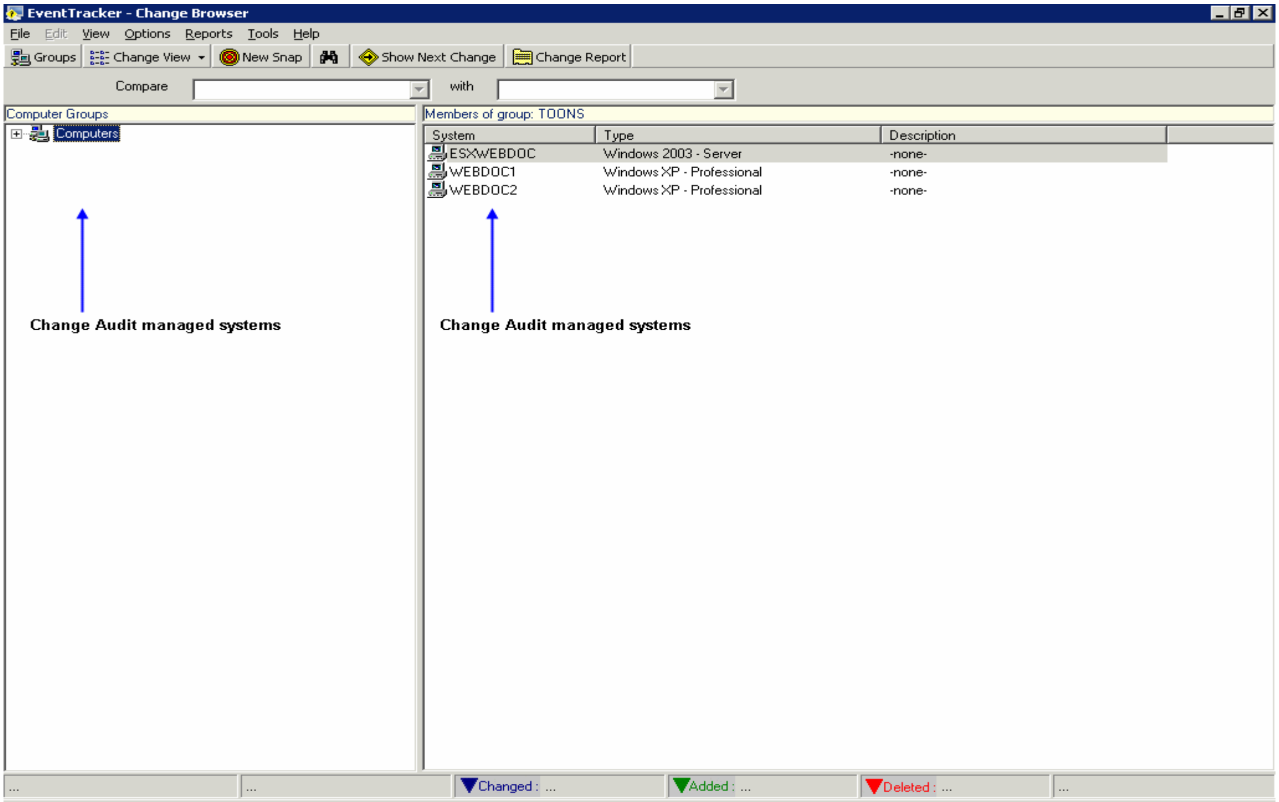
   Note:

   When the Change Browser is open for the first time after installation, EventTracker - Change Audit displays the File System 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 the keyboard.
   EventTracker - Change Audit displays the **Groups** view.
   (OR)
   Click **Groups** on the toolbar.



System	Type	Description
ESXWEBDOC	Windows 2003 - Server	-none-
WEBDOC1	Windows XP - Professional	-none-
WEBDOC2	Windows XP - Professional	-none-

Figure 40

1. To view Groups, expand the **Computers** node on the left pane.
2. 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.

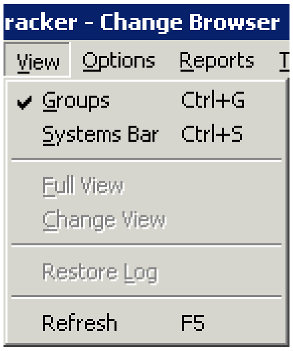
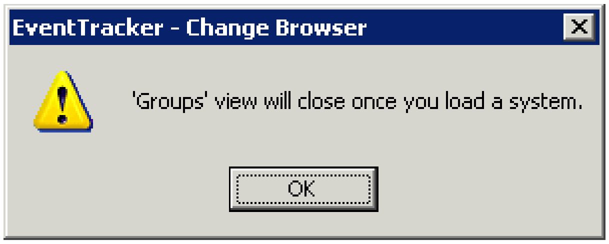


Figure 41

If you try to clear the tick mark, EventTracker - Change Audit displays the Change Browser message box.



EventTracker - Change Browser

'Groups' view will close once you load a system.

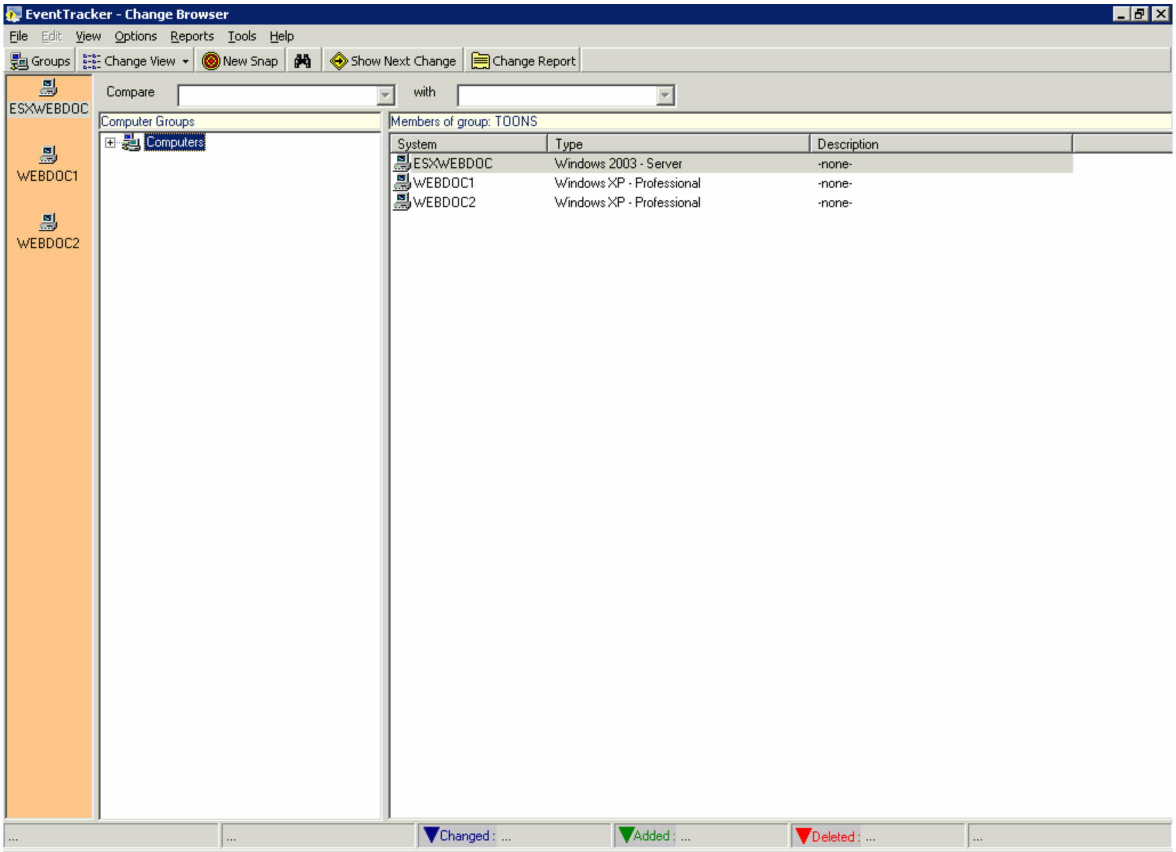
Figure 42

3. 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.

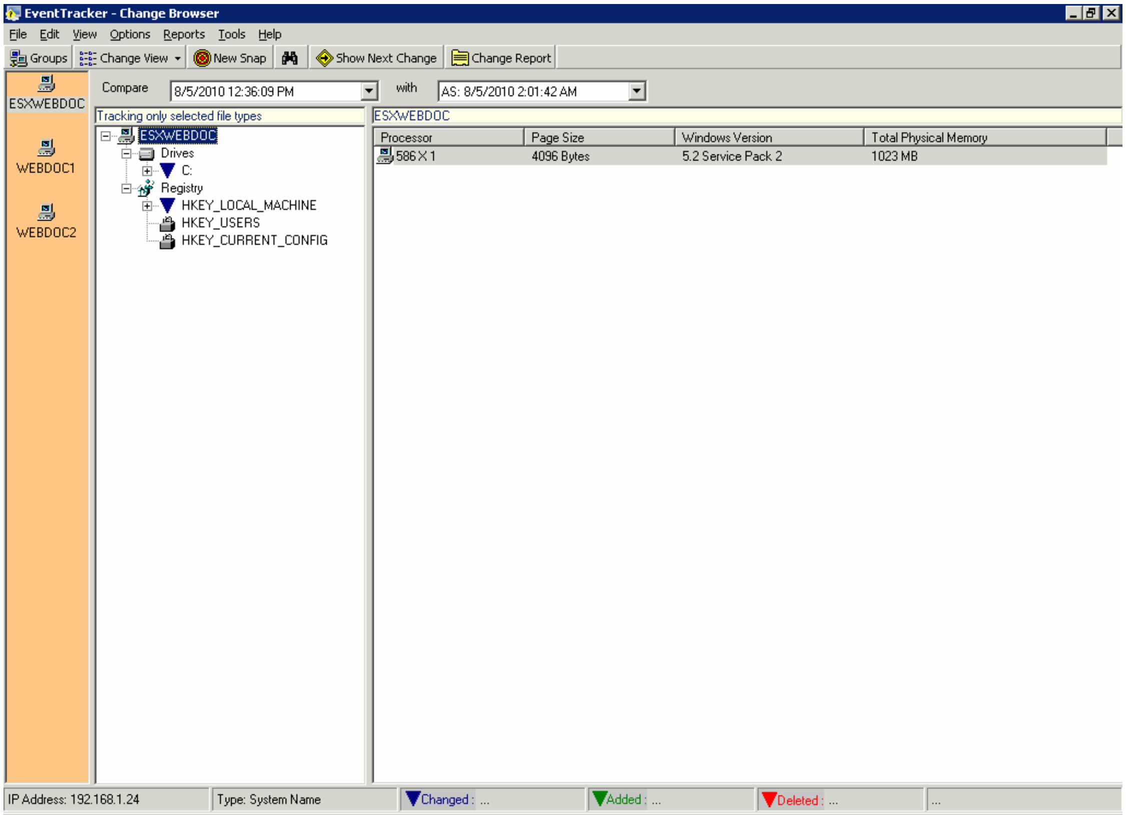


System	Type	Description
ESXWEBDOC	Windows 2003 - Server	-none-
WEBDOC1	Windows XP - Professional	-none-
WEBDOC2	Windows XP - Professional	-none-

Figure 43

4. 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.



Compare 8/5/2010 12:36:09 PM with AS: 8/5/2010 2:01:42 AM

ESXWEBDOC

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.2 Service Pack 2	1023 MB

IP Address: 192.168.1.24 Type: System Name

Figure 44

3.2 Viewing System Details

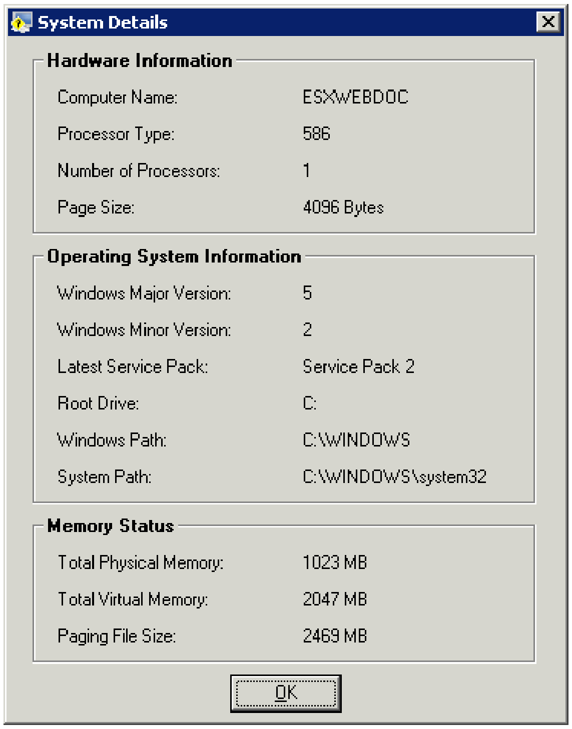
This option helps you view Hardware Information, Operating System Information and Memory Status of the selected system.

To view system details, follow the below steps :

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.



System Details

Hardware Information

Computer Name:	ESXWEBDOC
Processor Type:	586
Number of Processors:	1
Page Size:	4096 Bytes

Operating System Information

Windows Major Version:	5
Windows Minor Version:	2
Latest Service Pack:	Service Pack 2
Root Drive:	C:
Windows Path:	C:\WINDOWS
System Path:	C:\WINDOWS\system32

Memory Status

Total Physical Memory:	1023 MB
Total Virtual Memory:	2047 MB
Paging File Size:	2469 MB

Figure 45

3. If there is no Snapshot for the selected system, then EventTracker – Change the Audit displays the error message.

3.3 Viewing the File System Changes

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

To Viewing the File System Changes, follow the below steps :

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.

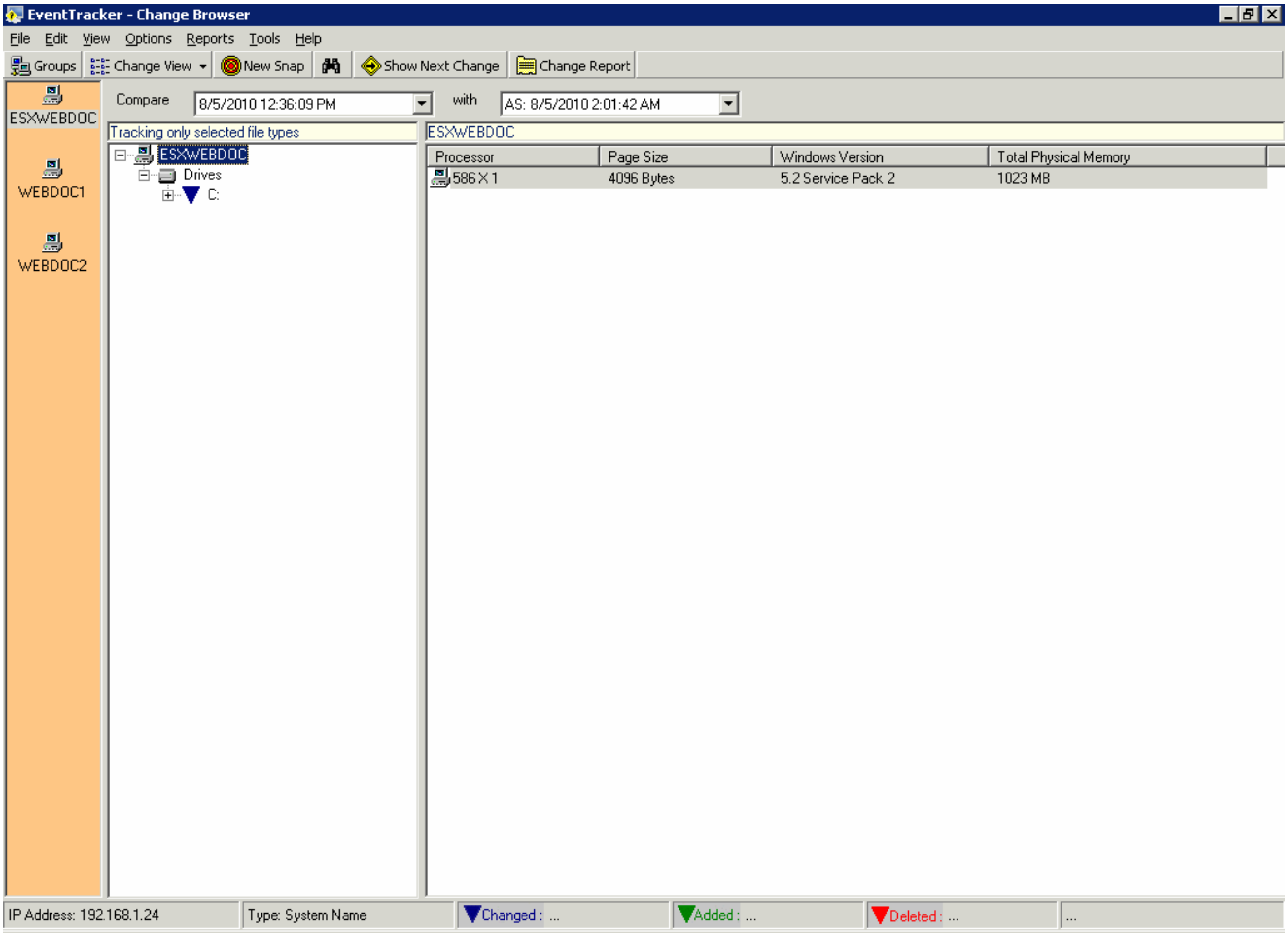


Figure 46

3.4 Viewing the Registry Changes

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

To View the Registry Changes, follow the below steps :

1. Select a system on the System Bar.

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

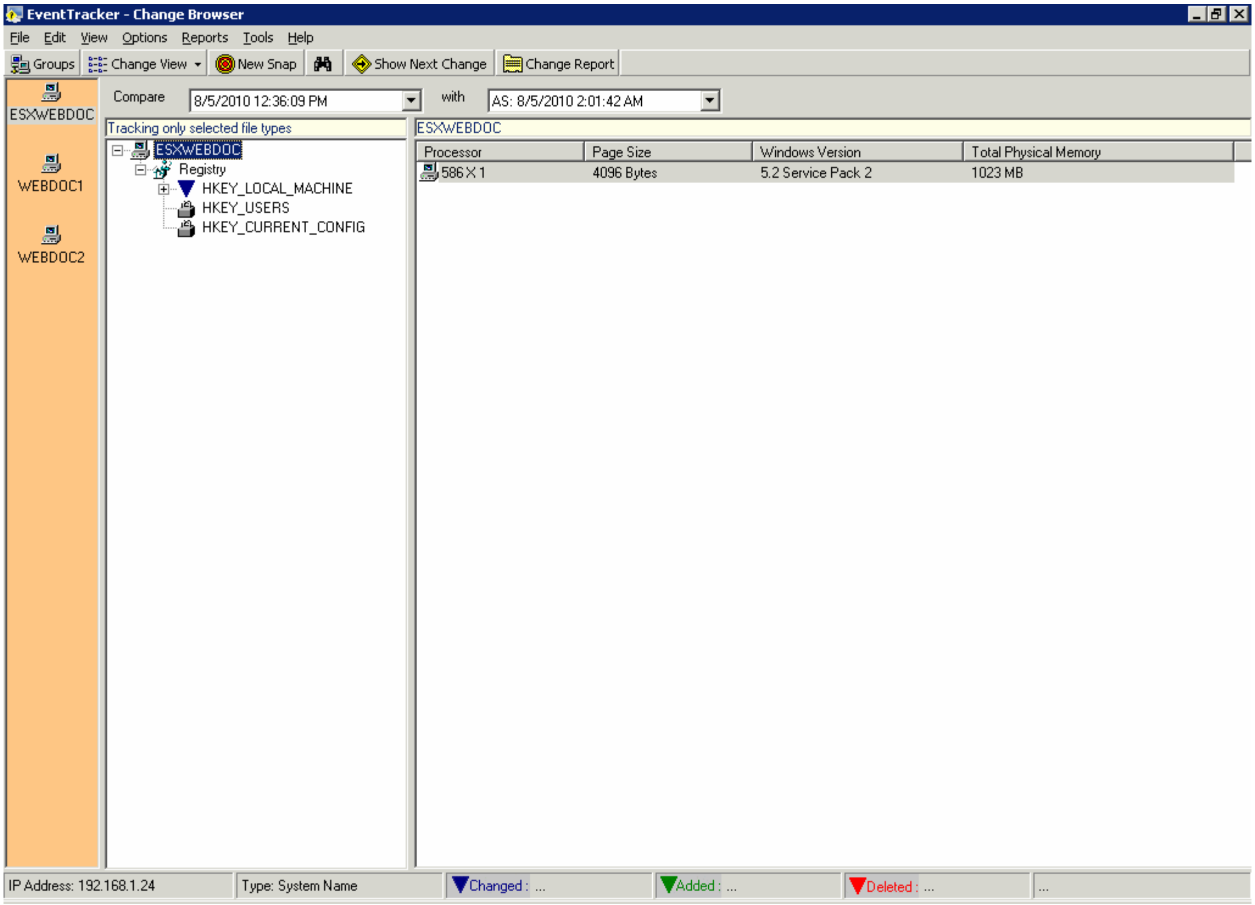
   (OR)

   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.



Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.2 Service Pack 2	1023 MB

Figure 47

3.5 Full View option

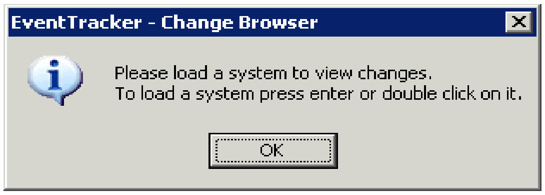
This option helps you fully/completely View the monitored computers. In Full View, EventTracker - Change Audit compares two latest Snapshots and displays the difference in Snapshots that includes Addition, Deletion or Modification of files, folders and registry keys, filtered items and all other unaltered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

To view the Full View of the monitored computers, follow the below steps :

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.



Please load a system to view changes.
To load a system press enter or double click on it.

Figure 48

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.

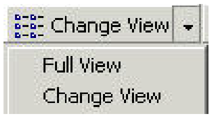
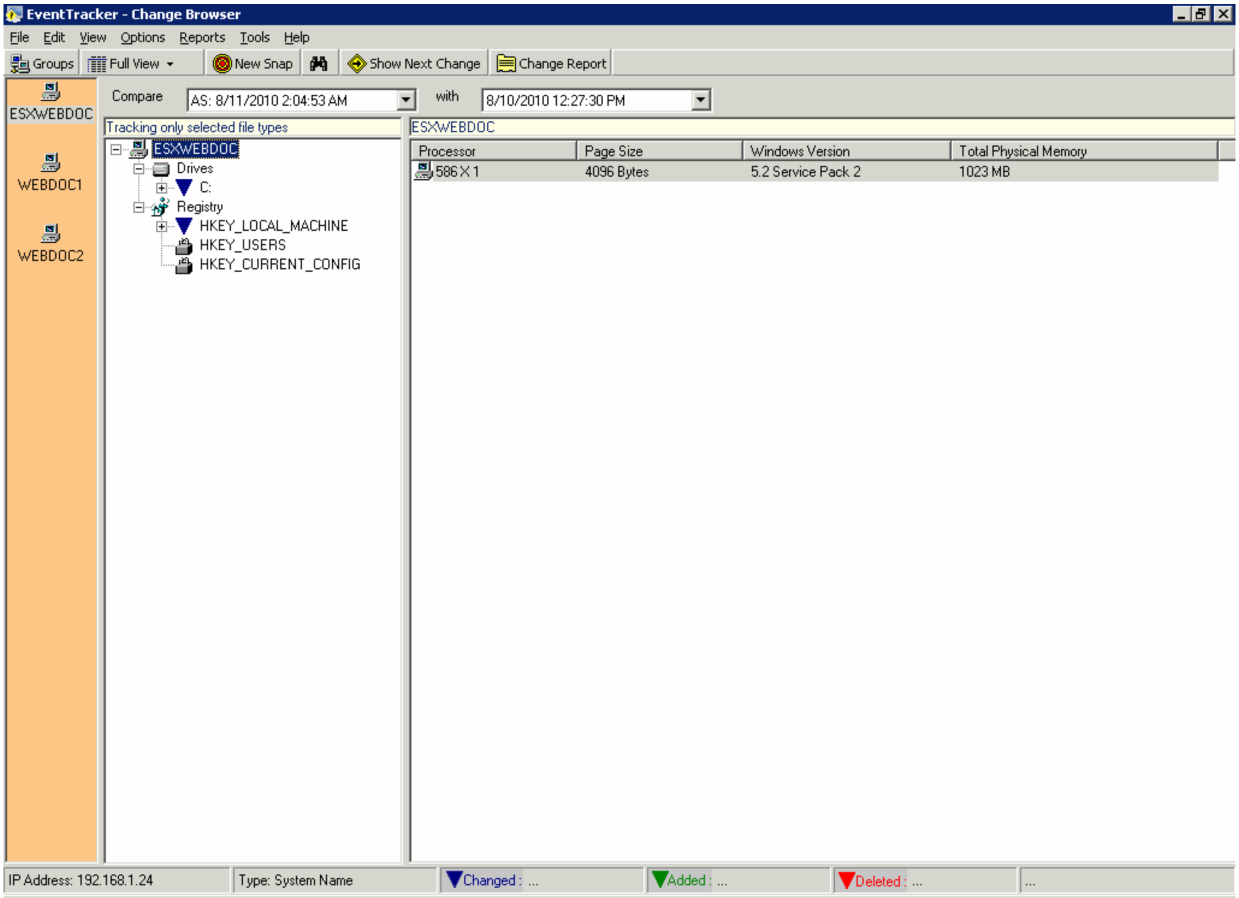


Figure 49

   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.



Compare AS: 8/11/2010 2:04:53 AM with 8/10/2010 12:27:30 PM

Tracking only selected file types

ESXWEBDOC

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.2 Service Pack 2	1023 MB

IP Address: 192.168.1.24

Type: System Name

Figure 50

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

   EventTracker - Change Audit displays the mouse over tooltip about the status of the item.

3.6 Viewing the Compare Details

This option helps you view Compare Details of folders and files.

To view compare details of File system items, follow the below steps :

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.

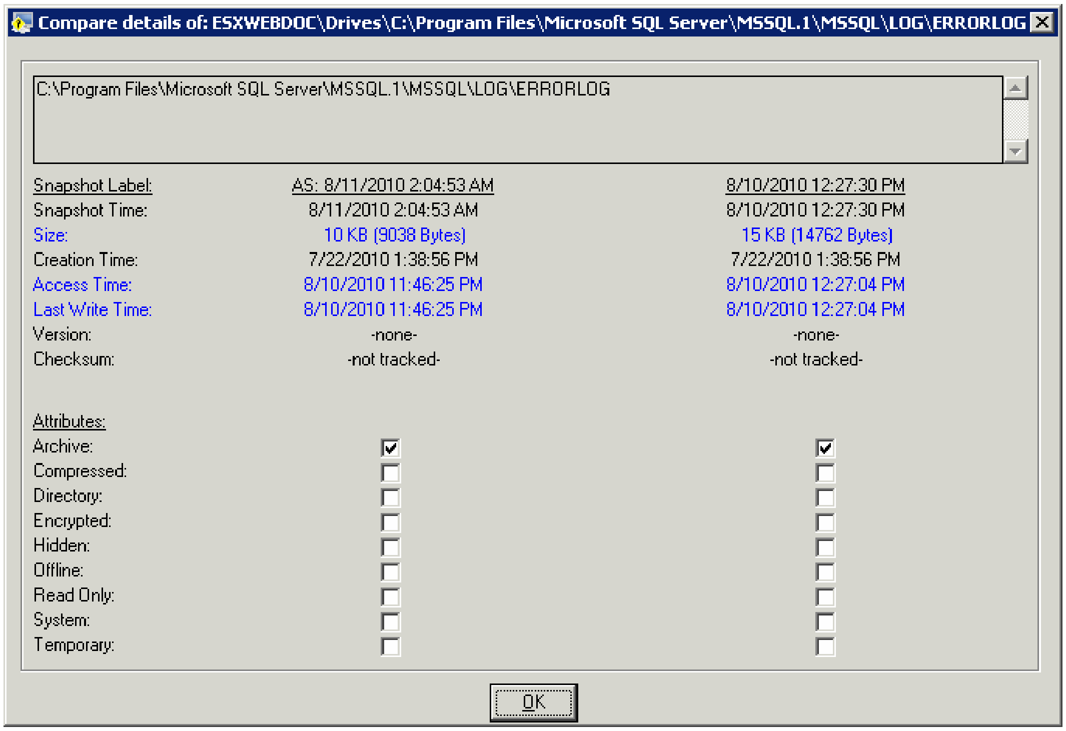
(OR)

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.

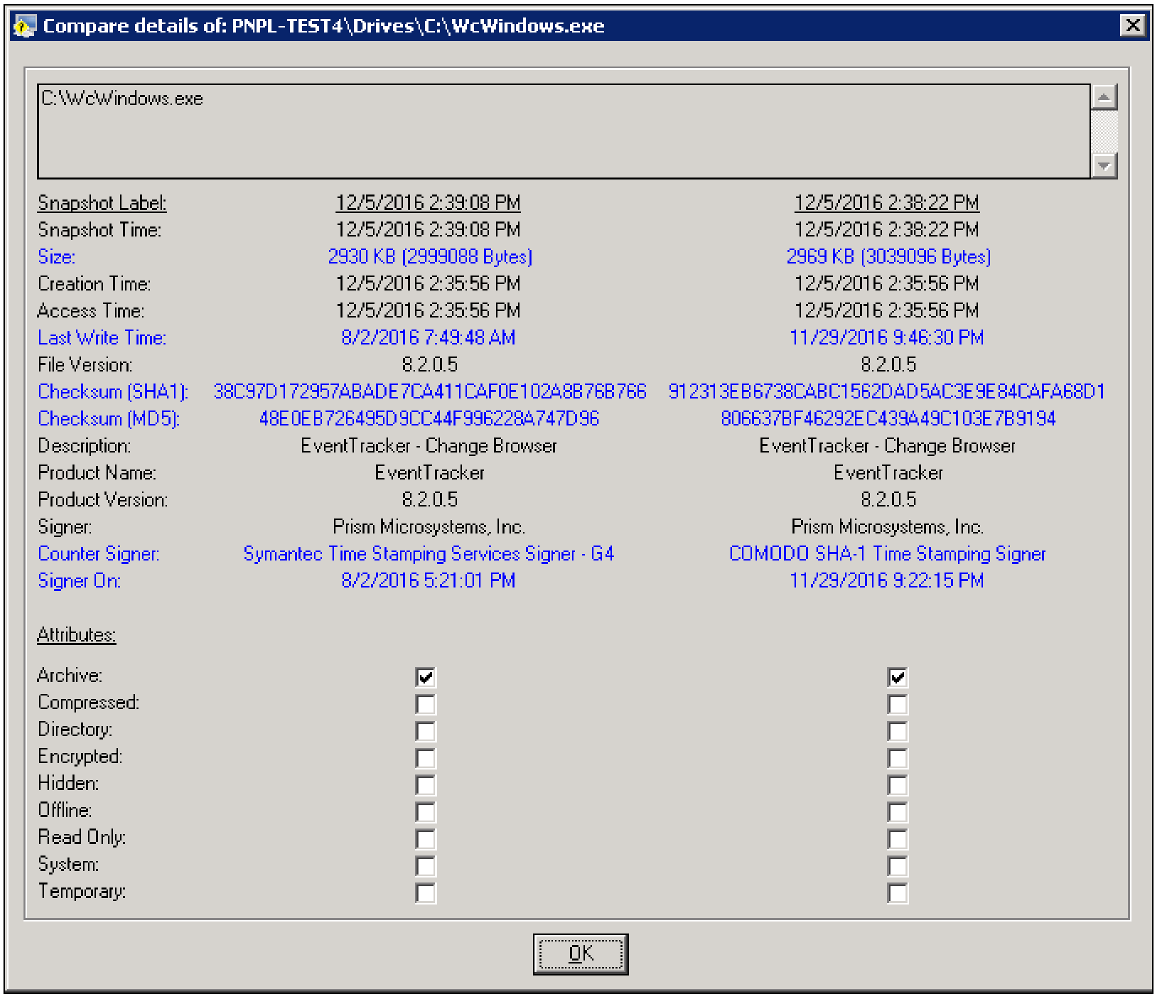


Compare details of: ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\ERRORLOG

C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG\ERRORLOG

Snapshot Label:	AS: 8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM
Snapshot Time:	8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM
Size:	10 KB (9038 Bytes)	15 KB (14762 Bytes)
Creation Time:	7/22/2010 1:38:56 PM	7/22/2010 1:38:56 PM
Access Time:	8/10/2010 11:46:25 PM	8/10/2010 12:27:04 PM
Last Write Time:	8/10/2010 11:46:25 PM	8/10/2010 12:27:04 PM
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 51



C:\WcWindows.exe

Snapshot Label:	12/5/2016 2:39:08 PM	12/5/2016 2:38:22 PM
Snapshot Time:	12/5/2016 2:39:08 PM	12/5/2016 2:38:22 PM
Size:	2930 KB (2999088 Bytes)	2969 KB (3039096 Bytes)
Creation Time:	12/5/2016 2:35:56 PM	12/5/2016 2:35:56 PM
Access Time:	12/5/2016 2:35:56 PM	12/5/2016 2:35:56 PM
Last Write Time:	8/2/2016 7:49:48 AM	11/29/2016 9:46:30 PM
File Version:	8.2.0.5	8.2.0.5
Checksum (SHA1):	38C97D172957ABADE7CA411CAF0E102A8B76B766	912313EB6738CABC1562DAD5AC3E9E84CAFA68D1
Checksum (MD5):	48E0EB726495D9CC44F996228A747D96	806637BF46292EC439A49C103E7B9194
Description:	EventTracker - Change Browser	EventTracker - Change Browser
Product Name:	EventTracker	EventTracker
Product Version:	8.2.0.5	8.2.0.5
Signer:	Prism Microsystems, Inc.	Prism Microsystems, Inc.
Counter Signer:	Symantec Time Stamping Services Signer - G4	COMODO SHA-1 Time Stamping Signer
Signer On:	8/2/2016 5:21:01 PM	11/29/2016 9:22:15 PM
Attributes:		
Archive:	☑	☑
Compressed:	☐	☐
Directory:	☐	☐
Encrypted:	☐	☐
Hidden:	☐	☐
Offline:	☐	☐
Read Only:	☐	☐
System:	☐	☐
Temporary:	☐	☐

Figure 52

- MD5 Checksum
- File Description
- Product Name
- Product Version
- Signer
- Counter Signer
- Signed On

3.7 Comparing the details of the Registry Items

This option helps you Compare Details of the Registry items.

To view compare details of the Registry items, follow the below steps :

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.

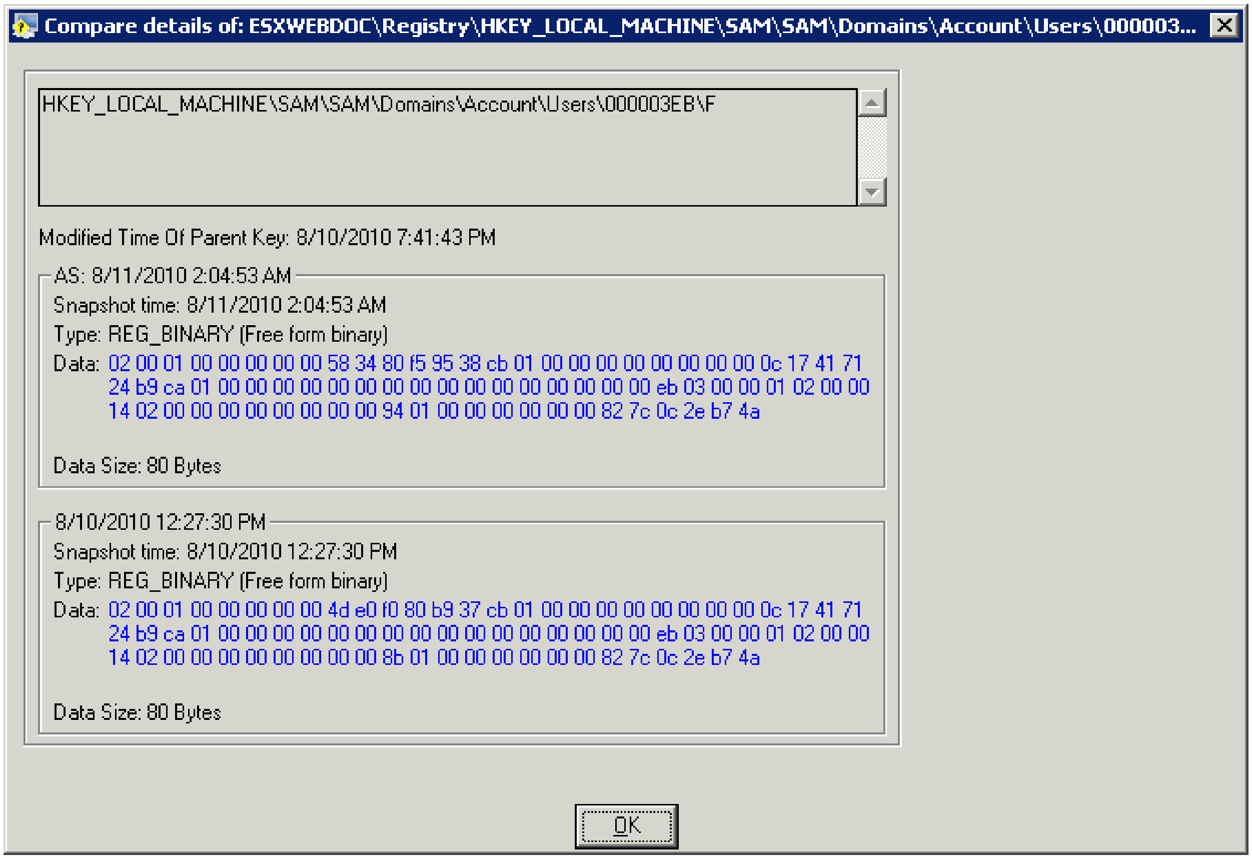
   (OR)

   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.



Compare details of: ESXWEBDOC\Registry\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003...

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003EB\F

Modified Time Of Parent Key: 8/10/2010 7:41:43 PM

AS: 8/11/2010 2:04:53 AM

```
Snapshot time: 8/11/2010 2:04:53 AM
Type: REG_BINARY (Free form binary)
Data: 02 00 01 00 00 00 00 00 58 34 80 f5 95 38 cb 01 00 00 00 00 00 00 00 00 0c 17 41 71
      24 b9 ca 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 eb 03 00 00 01 02 00 00
      14 02 00 00 00 00 00 00 00 00 94 01 00 00 00 00 00 00 82 7c 0c 2e b7 4a

Data Size: 80 Bytes
```

8/10/2010 12:27:30 PM

```
Snapshot time: 8/10/2010 12:27:30 PM
Type: REG_BINARY (Free form binary)
Data: 02 00 01 00 00 00 00 00 4d e0 f0 80 b9 37 cb 01 00 00 00 00 00 00 00 00 0c 17 41 71
      24 b9 ca 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 eb 03 00 00 01 02 00 00
      14 02 00 00 00 00 00 00 00 00 8b 01 00 00 00 00 00 00 82 7c 0c 2e b7 4a

Data Size: 80 Bytes
```

Figure 53

3.8 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.

3.9 Find Changes option

This option helps you find addition, deletion, and modification of folders, files, 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 the keyboard.

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

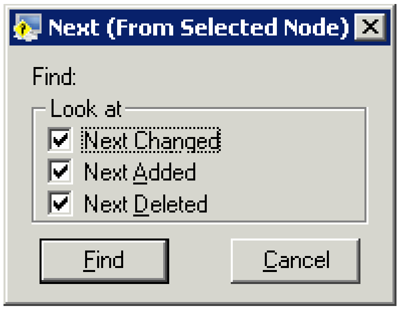
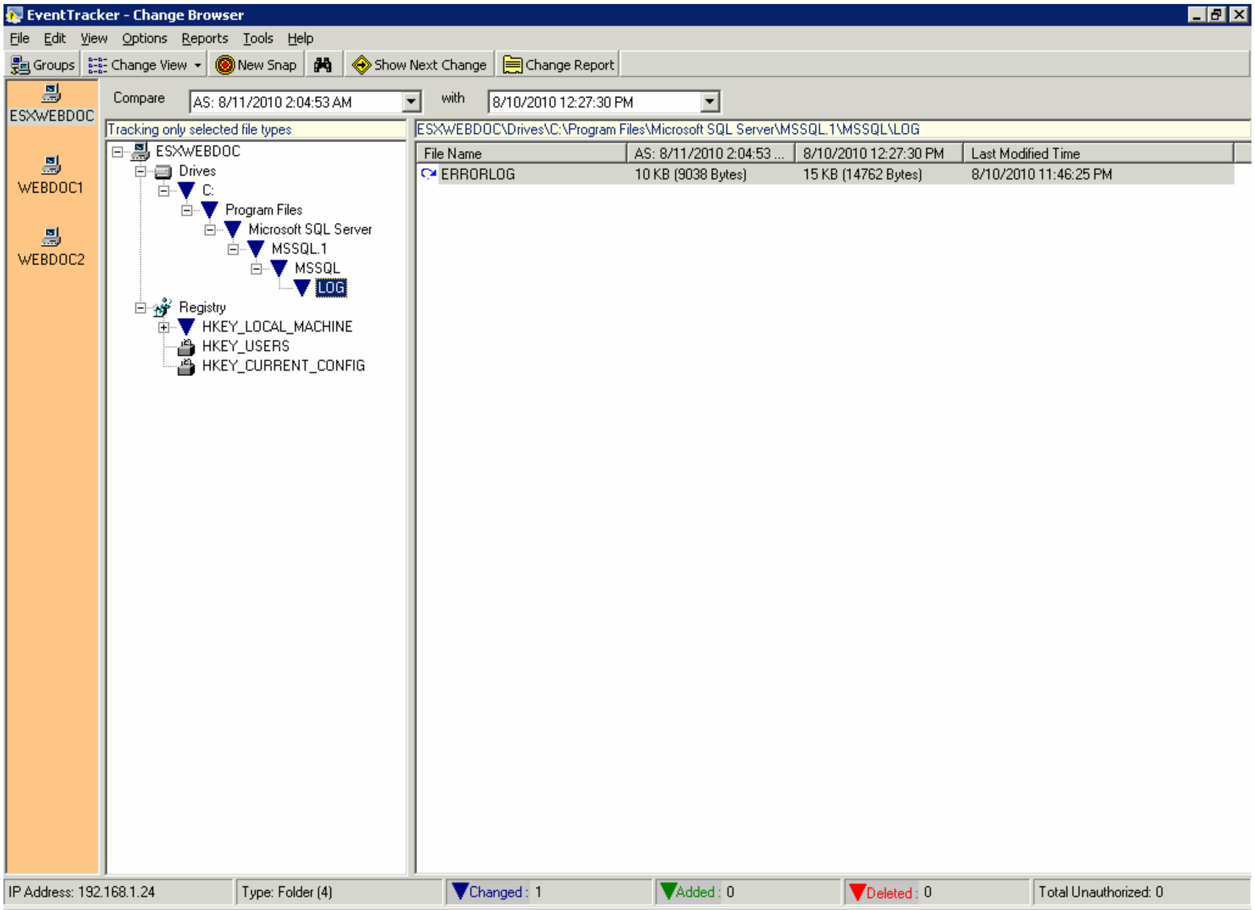


Figure 54

Field	Description
Next Changed	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.
Next Added	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.
Next Deleted	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.

2. Select the option appropriately and then click **Find**.

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



Compare AS: 8/11/2010 2:04:53 AM with 8/10/2010 12:27:30 PM

Tracking only selected file types

ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG

File Name	AS: 8/11/2010 2:04:53 ...	8/10/2010 12:27:30 PM	Last Modified Time
ERRORLOG	10 KB (9038 Bytes)	15 KB (14762 Bytes)	8/10/2010 11:46:25 PM

IP Address: 192.168.1.24 | Type: Folder (4) | Changed : 1 | Added : 0 | Deleted : 0 | Total Unauthorized: 0

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.

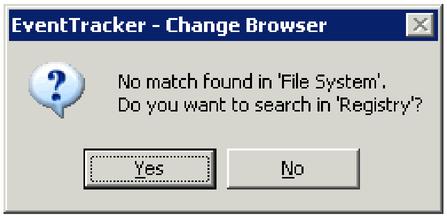
3. To view the next change, click the **Edit** menu and select the **Next Change** option.

   (OR)

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

   EventTracker - Change Audit displays the next change.

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

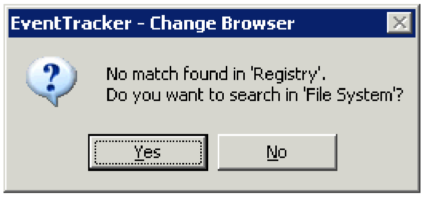


EventTracker - Change Browser

No match found in 'File System'.
Do you want to search in 'Registry'?

Figure 56

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



EventTracker - Change Browser

No match found in 'Registry'.
Do you want to search in 'File System'?

Figure 57

3.10 Search Strings

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

To Search Strings in File System, follow the below steps :

1. Open the Change Browser.
2. Click the **Edit** menu and select the **Find** option.

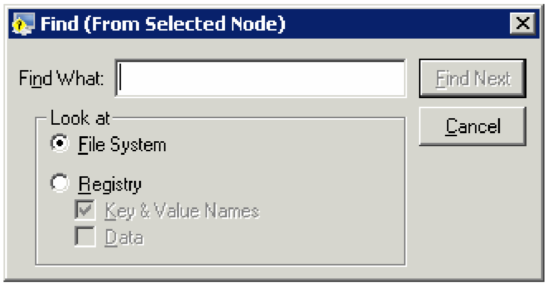
   (OR)

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

   (OR)

   Click on the toolbar.

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



Find (From Selected Node)

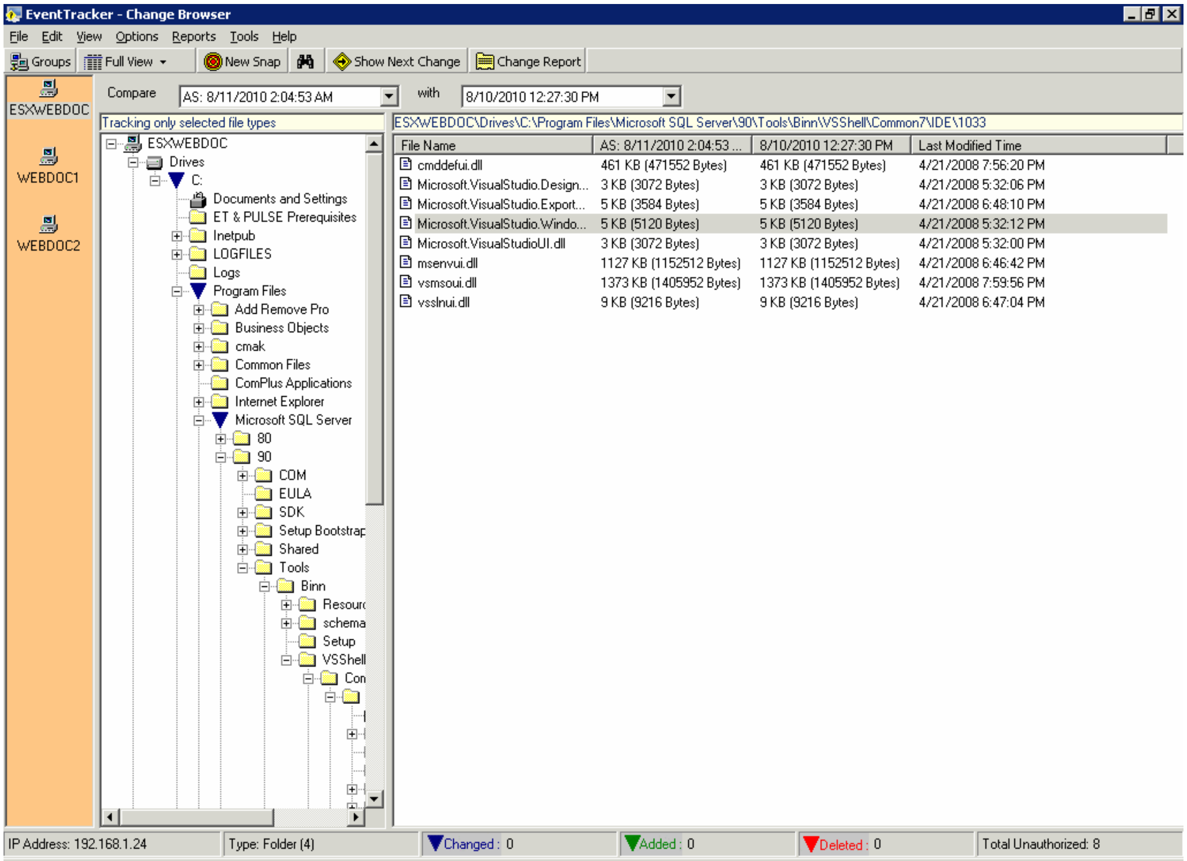
Find What:

Look at
● File System
○ Registry
☑ Key & Value Names
□ Data

Figure 58

3. Enter the string in **Find What** field.
   Example: Windows.
4. Click **Find Next**.

   EventTracker - Change Audit displays the search result.



Compare AS: 8/11/2010 2:04:53 AM with 8/10/2010 12:27:30 PM

Tracking only selected file types

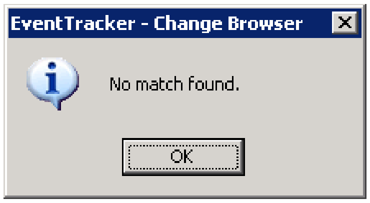
ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\90\Tools\Binn\VSShell\Common7\IDE\1033

File Name	AS: 8/11/2010 2:04:53 ...	8/10/2010 12:27:30 PM	Last Modified Time
cmddefui.dll	461 KB (471552 Bytes)	461 KB (471552 Bytes)	4/21/2008 7:56:20 PM
Microsoft.VisualStudio.Design...	3 KB (3072 Bytes)	3 KB (3072 Bytes)	4/21/2008 5:32:06 PM
Microsoft.VisualStudio.Export...	5 KB (3584 Bytes)	5 KB (3584 Bytes)	4/21/2008 6:48:10 PM
Microsoft.VisualStudio.Windo...	5 KB (5120 Bytes)	5 KB (5120 Bytes)	4/21/2008 5:32:12 PM
Microsoft.VisualStudioUI.dll	3 KB (3072 Bytes)	3 KB (3072 Bytes)	4/21/2008 5:32:00 PM
msenvui.dll	1127 KB (1152512 Bytes)	1127 KB (1152512 Bytes)	4/21/2008 6:46:42 PM
vsmsoui.dll	1373 KB (1405952 Bytes)	1373 KB (1405952 Bytes)	4/21/2008 7:59:56 PM
vsslnui.dll	9 KB (9216 Bytes)	9 KB (9216 Bytes)	4/21/2008 6:47:04 PM

IP Address: 192.168.1.24 | Type: Folder (4) | Changed : 0 | Added : 0 | Deleted : 0 | Total Unauthorized: 8

Figure 59

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



No match found.

Figure 60

5. 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.

3.11 Searching the Strings in the 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.

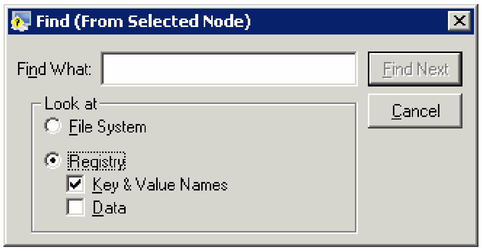
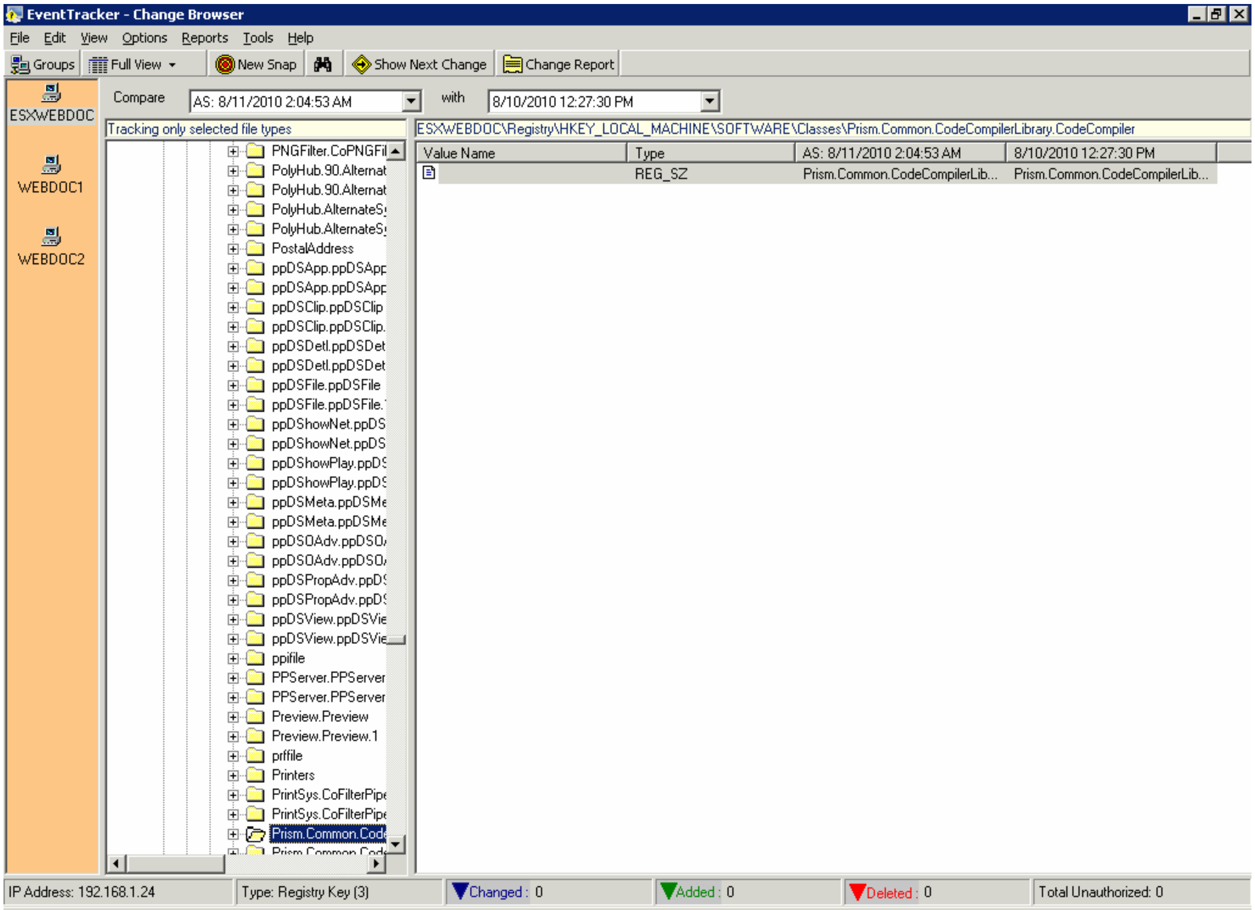


Figure 61

4. Type the string in **Find What** field.
   Example: Prism.
5. Click **Find Next**.

   EventTracker - Change Audit displays the search result.



Compare AS: 8/11/2010 2:04:53 AM with 8/10/2010 12:27:30 PM

Tracking only selected file types

ESXWEBDOC\Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Prism.Common.CodeCompilerLibrary.CodeCompiler

Value Name	Type	AS: 8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM
	REG_SZ	Prism.Common.CodeCompilerLib...	Prism.Common.CodeCompilerLib...

IP Address: 192.168.1.24 | Type: Registry Key (3) | Changed : 0 | Added : 0 | Deleted : 0 | Total Unauthorized: 0

Figure 62

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.

3.12 Generating the Change Report

This option helps in viewing the reports generated by EventTracker - Change Audit based on Snapshots and Policies. Reports can be viewed based on Snapshots either in a text file or in the Excel file.

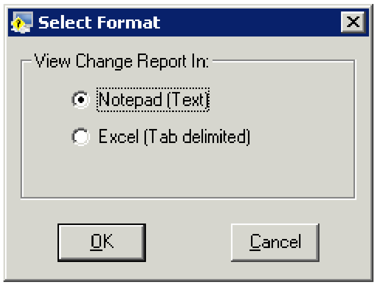
To Generate Change report, follow the steps below:

1. Open the Change Browser.
2. On the System Bar, double-click the system for which you want to generate a change report.
3. Select the Snapshots from the drop-down lists.
4. Click the **Reports** menu and select the **View Reports** option.

(OR)

Click Change Report on the toolbar.

EventTracker - Change Audit displays the Select Format window.



View Change Report In:

● Notepad (Text)

○ Excel (Tab delimited)

Figure 63

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 the Excel format.

6. Click **OK**.

   EventTracker - Change Audit generates and displays the change report.

3.13 Track File Checksum Feature

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 this feature is enabled, EventTracker - Change Audit tracks file checksum for all files and sub-folders associated with the chosen folder, in this case for the system32 folder.

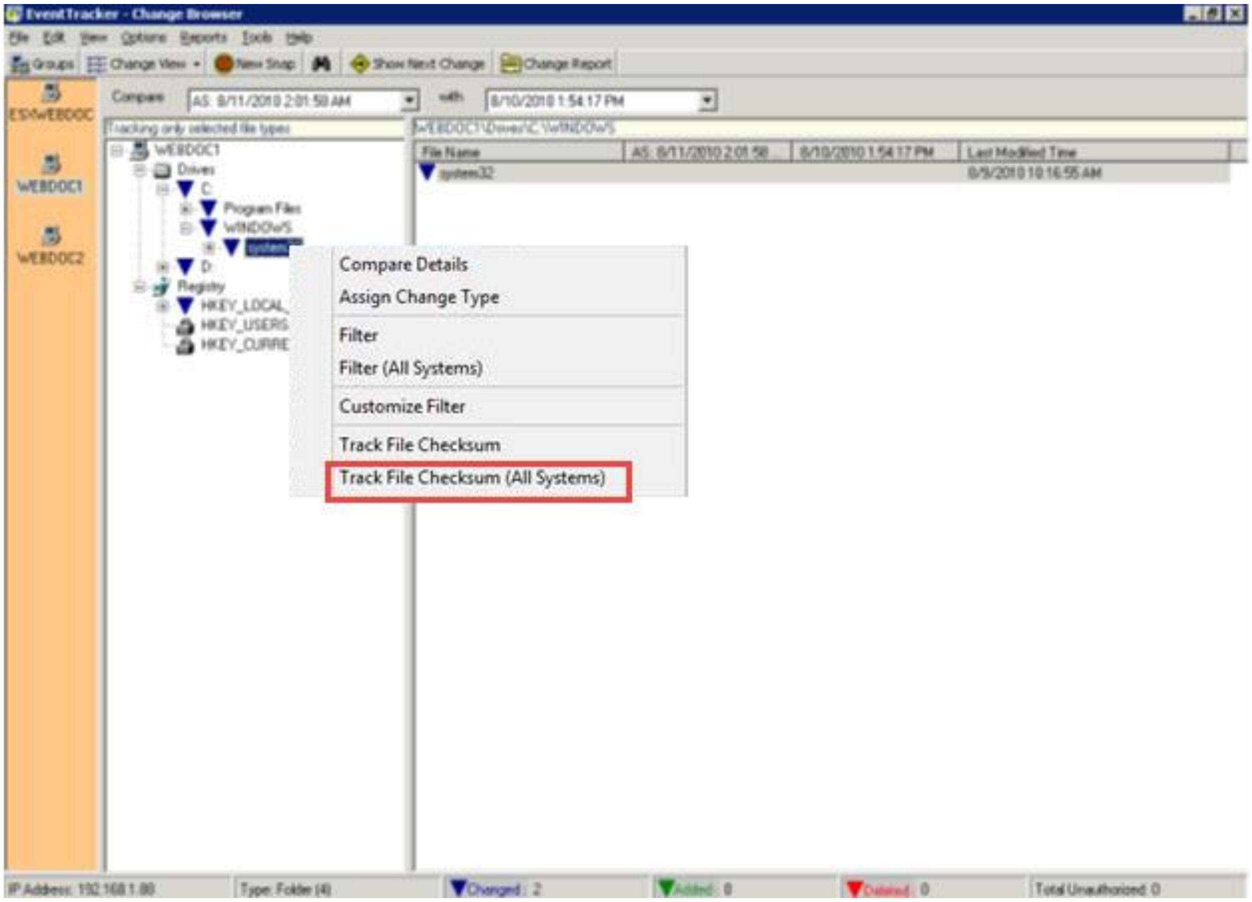
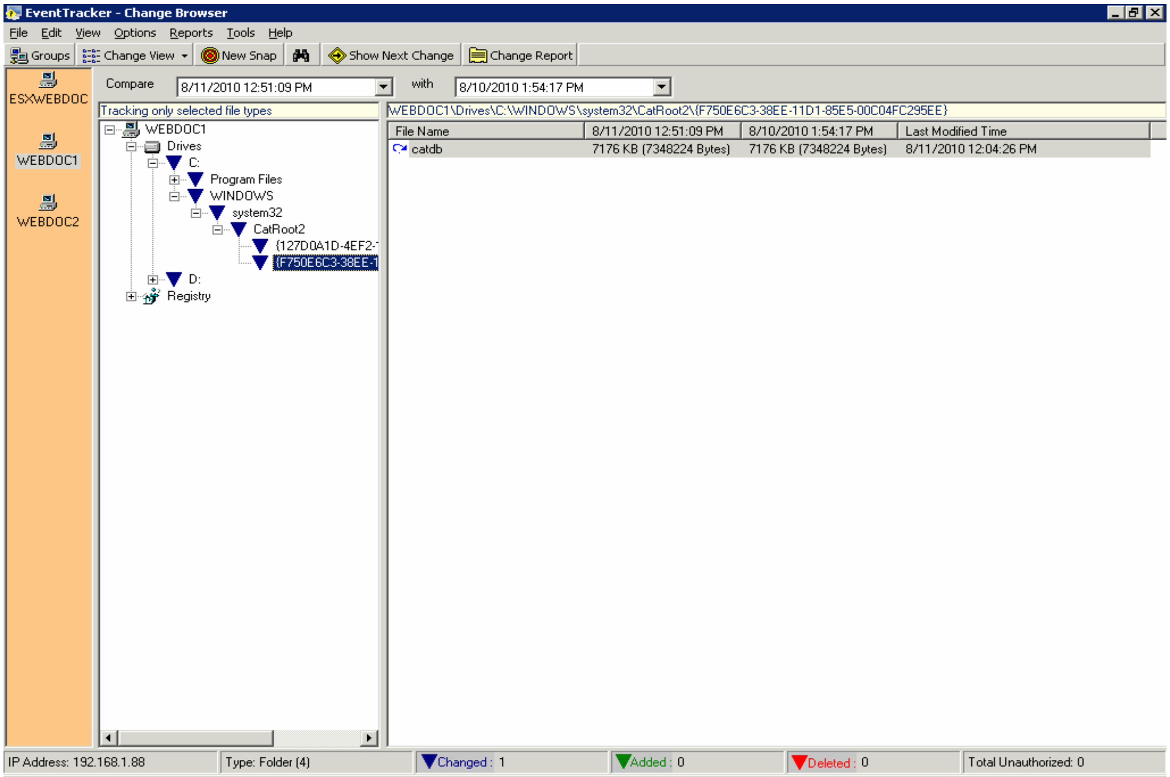


Figure 64

To view the file checksum, follow the steps below:

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.



Compare 8/11/2010 12:51:09 PM with 8/10/2010 1:54:17 PM

Tracking only selected file types

WEBDOC1\Drives\C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}

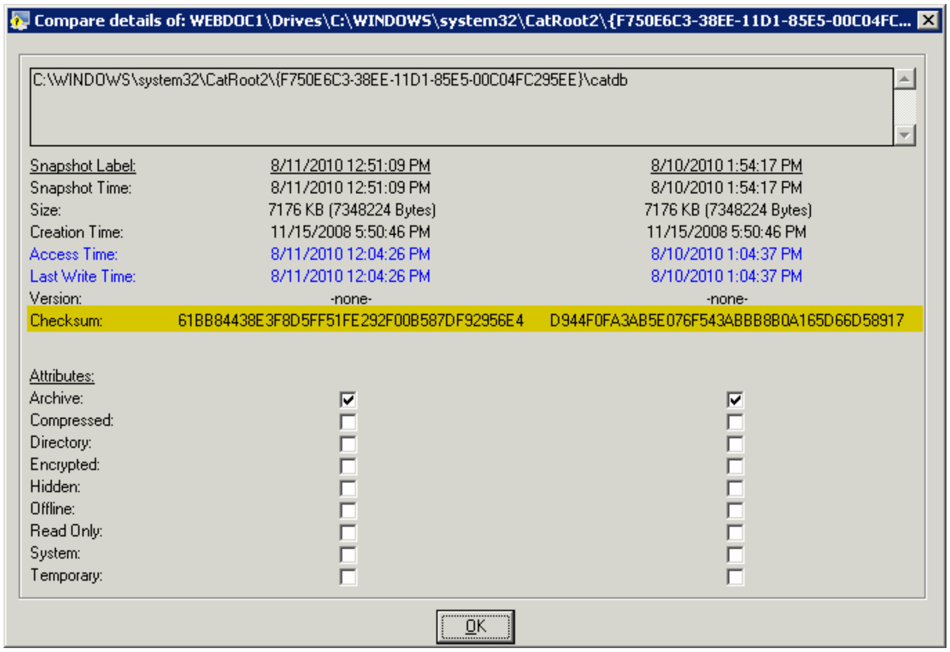
File Name	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM	Last Modified Time
catdb	7176 KB (7348224 Bytes)	7176 KB (7348224 Bytes)	8/11/2010 12:04:26 PM

IP Address: 192.168.1.88 | Type: Folder (4) | Changed : 1 | Added : 0 | Deleted : 0 | Total Unauthorized: 0

Figure 65

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

   EventTracker - Change Audit displays the Compare Details window with checksum details.


Compare details of: WEBDOC1\Drives\C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC...
OK

C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb

Snapshot Label:	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM
Snapshot Time:	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM
Size:	7176 KB (7348224 Bytes)	7176 KB (7348224 Bytes)
Creation Time:	11/15/2008 5:50:46 PM	11/15/2008 5:50:46 PM
Access Time:	8/11/2010 12:04:26 PM	8/10/2010 1:04:37 PM
Last Write Time:	8/11/2010 12:04:26 PM	8/10/2010 1:04:37 PM
Version:	-none-	-none-
Checksum:	61BB84438E3F8D5FF51FE292F00B587DF92956E4	D944F0FA3AB5E076F543ABBB8B0A165D66D58917
Attributes:		
Archive:	☑	☑
Compressed:	☐	☐
Directory:	☐	☐
Encrypted:	☐	☐
Hidden:	☐	☐
Offline:	☐	☐
Read Only:	☐	☐
System:	☐	☐
Temporary:	☐	☐

Figure 66

3.13.1 Enabling the 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.

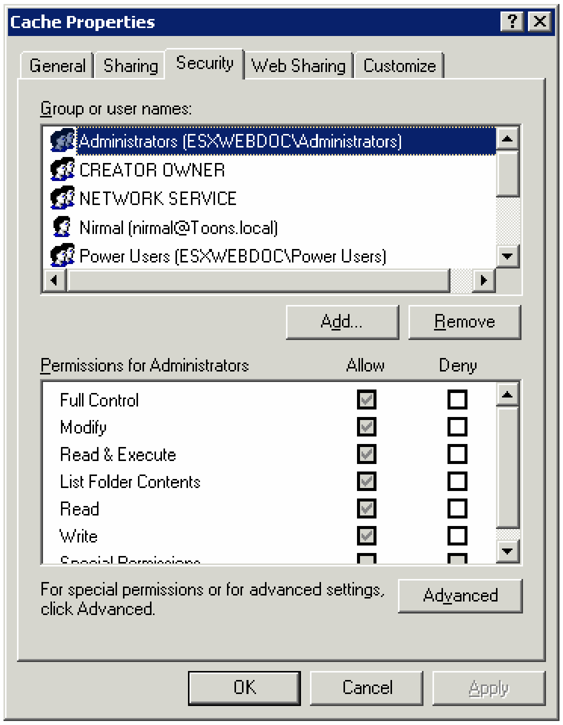
   From the shortcut menu, choose **Track File Checksum** to track file checksum for the local system.

   (OR)

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

3.13.2 Enabling the O/S Audit on Files and Folders

1. Right-click the folder 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.



Cache Properties

General | Sharing | Security | Web Sharing | Customize

Group or user names:

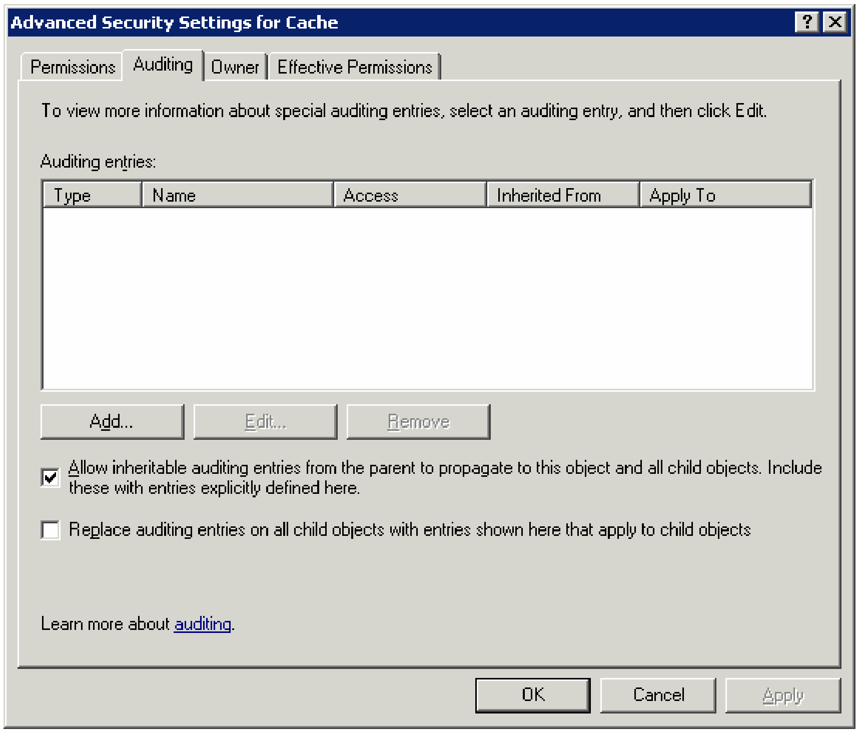
- Administrators (ESXWEBDOC\Administrators)
- CREATOR OWNER
- NETWORK SERVICE
- Nirmal (nirmal@Toons.local)
- Power Users (ESXWEBDOC\Power Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Figure 67

4. Click **Advanced**.
5. Click the **Auditing** tab on the Advanced Security Settings window.



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

Auditing entries:

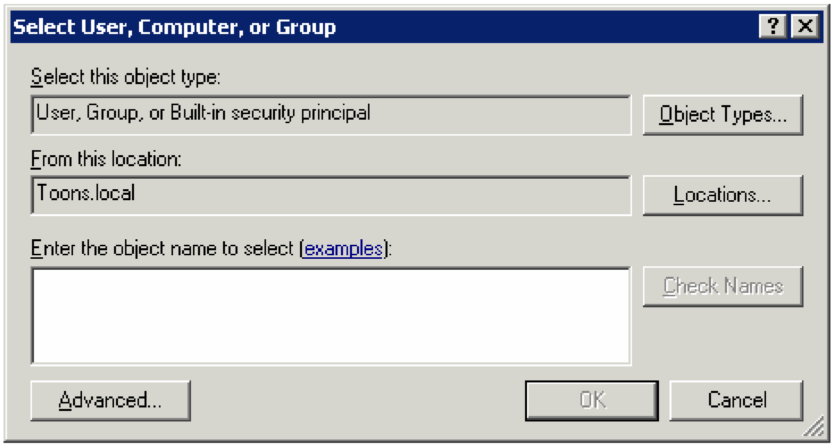
☑ Allow inheritable auditing entries from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

☐ Replace auditing entries on all child objects with entries shown here that apply to child objects

Learn more about auditing.

Figure 68

6. Click **Add**.
   Select User, Computer, or Group window is displayed.



Select this object type: User, Group, or Built-in security principal

From this location: Toons.local

Enter the object name to select (examples):

Figure 69

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

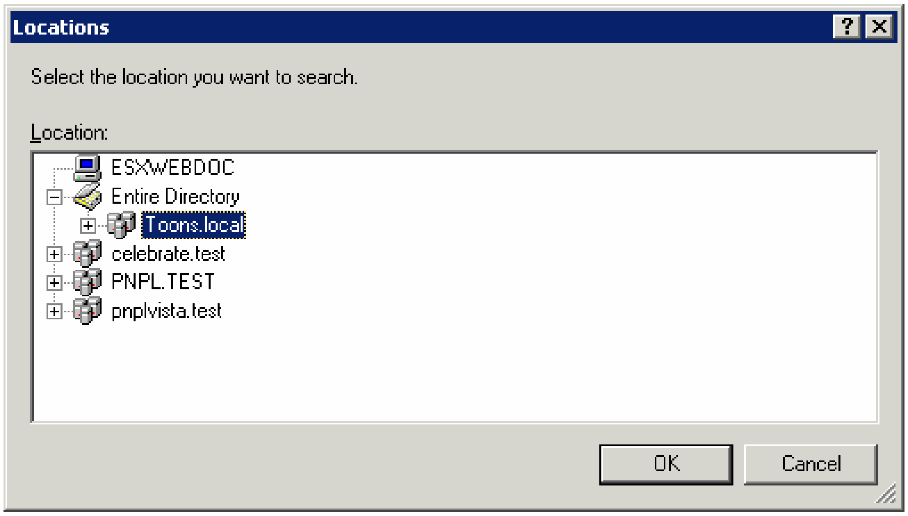
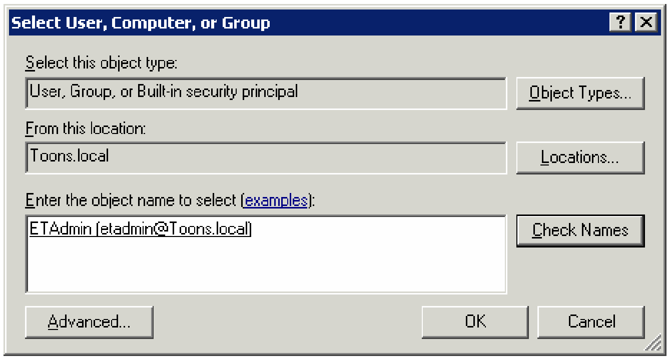


Figure 70

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.

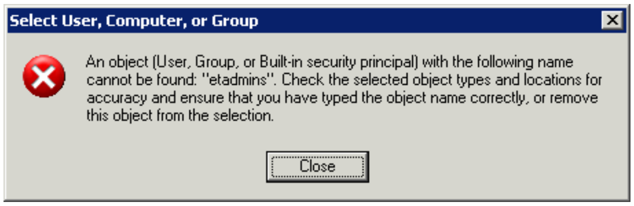


Select this object type:
User, Group, or Built-in security principal

From this location:
Toons.local

Enter the object name to select (examples):
ETAdmin (etadmin@Toons.local)

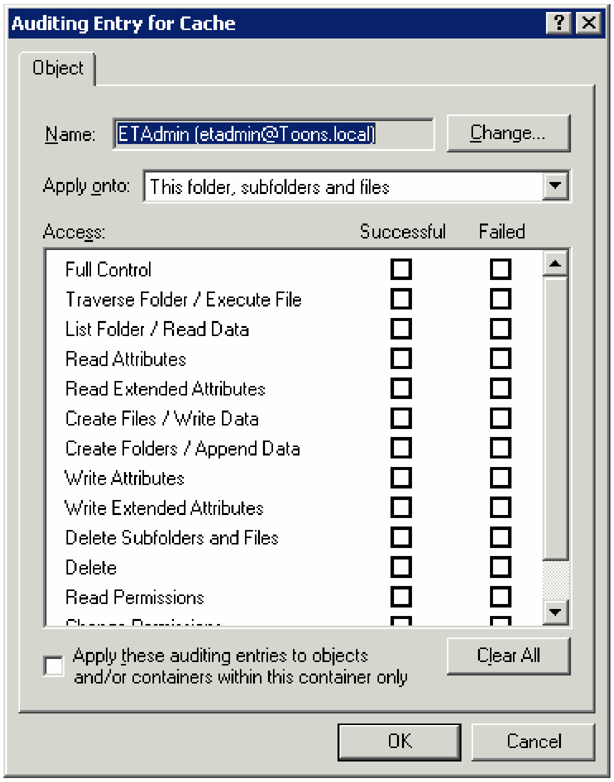
Figure 71



An object (User, Group, or Built-in security principal) with the following name cannot be found: "etadmins". Check the selected object types and locations for accuracy and ensure that you have typed the object name correctly, or remove this object from the selection.

Figure 72

11. Click **OK**.
    Auditing Entry for… the window is displayed.



Auditing Entry for Cache

Object

Name: ETAdmin (etadmin@Toons.local) Change...

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full Control	□	□
Traverse Folder / Execute File	□	□
List Folder / Read Data	□	□
Read Attributes	□	□
Read Extended Attributes	□	□
Create Files / Write Data	□	□
Create Folders / Append Data	□	□
Write Attributes	□	□
Write Extended Attributes	□	□
Delete Subfolders and Files	□	□
Delete	□	□
Read Permissions	□	□

□ Apply these auditing entries to objects and/or containers within this container only

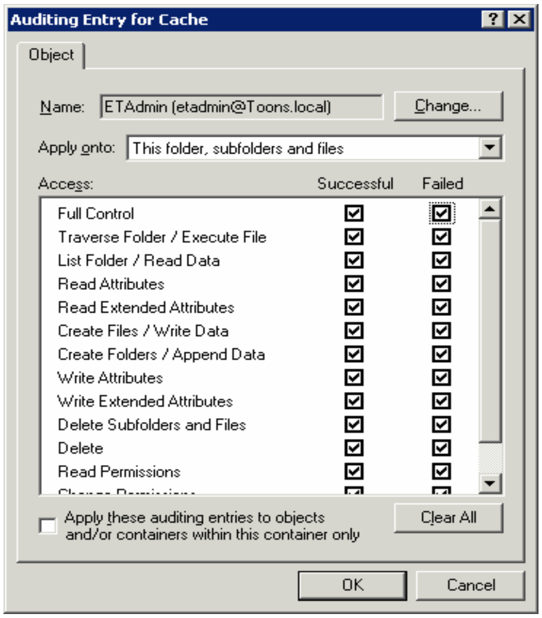
Clear All

OK Cancel

Figure 73

12. Select **Full Control** under **Successful** and **Failed**.

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



Auditing Entry for Cache

Object

Name: ETAdmin (etadmin@Toons.local) Change...

Apply onto: This folder, subfolders and files

Access:	Successful	Failed
Full Control	☑	☑
Traverse Folder / Execute File	☑	☑
List Folder / Read Data	☑	☑
Read Attributes	☑	☑
Read Extended Attributes	☑	☑
Create Files / Write Data	☑	☑
Create Folders / Append Data	☑	☑
Write Attributes	☑	☑
Write Extended Attributes	☑	☑
Delete Subfolders and Files	☑	☑
Delete	☑	☑
Read Permissions	☑	☑

□ Apply these auditing entries to objects and/or containers within this container only

Clear All

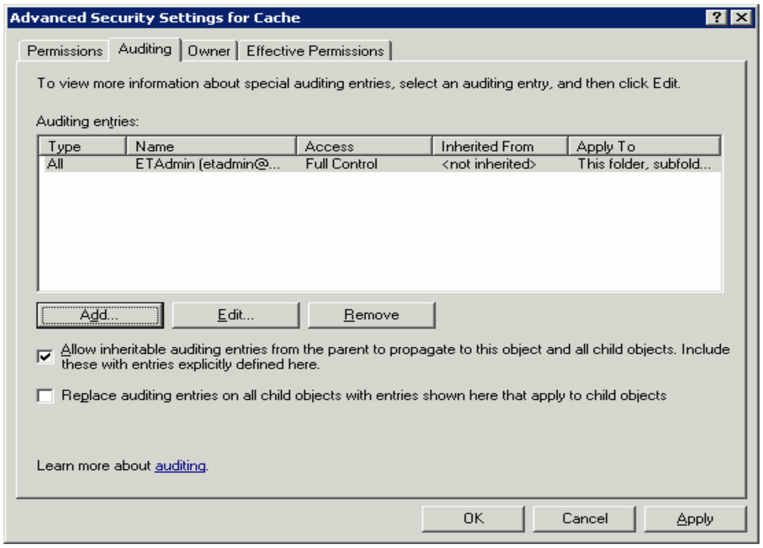
OK Cancel

Figure 74

NOTE: You don’t need to select the Full Control check box. Select the options as per the requirement.

13. Click **OK**.

    Advanced Security Settings window is displayed with the newly added user.



Advanced Security Settings for Cache

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

Auditing entries:

Type	Name	Access	Inherited From	Apply To
All	ETAdmin (etadmin@...	Full Control	<not inherited>	This folder, subfold...

☑ 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.

Figure 75

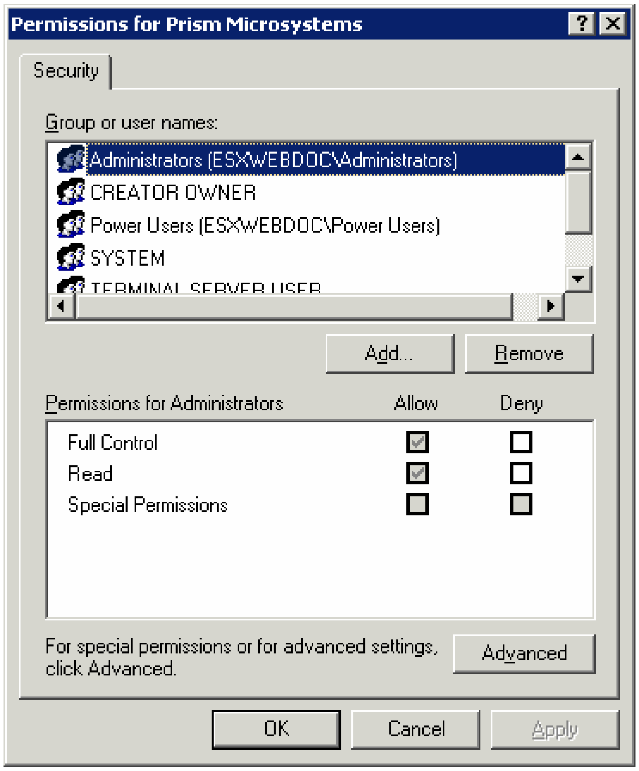
14. Click **Apply** and then click **OK**.
15. Click **OK** on the Properties window.

    NOTE: Similarly, enable auditing for file or registry keys.

3.13.3 Enabling the O/S Audit on the Registry Keys

To enable O/S audit on registry keys, follow the steps below:

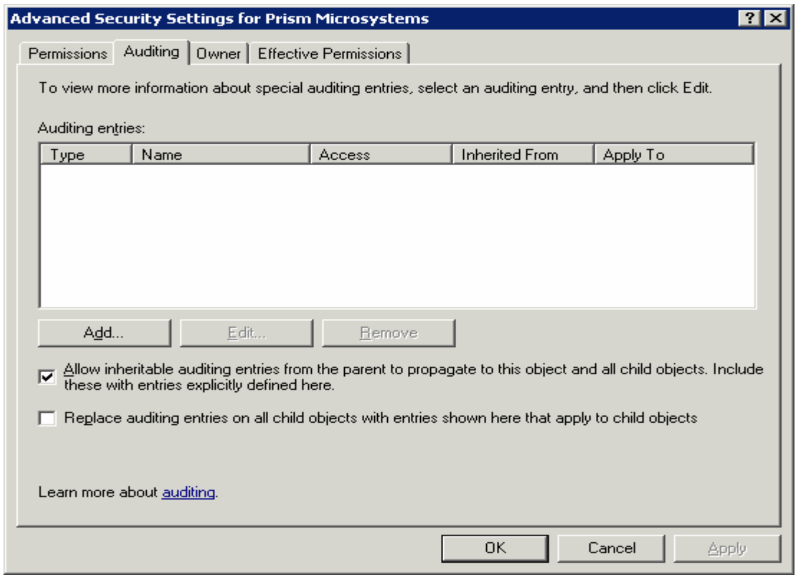
1. Open the Registry Editor.
2. Right-click the key that you want to audit.
3. From the shortcut menu, choose **Permissions**.


Permissions for Prism Microsystems
Security
Group or user names:
Administrators (ESXWEBDOC\Administrators)
CREATOR OWNER
Power Users (ESXWEBDOC\Power Users)
SYSTEM
TERMINAL SERVER USER
Add...
Remove
Permissions for Administrators
Allow
Deny
Full Control
Read
Special Permissions
For special permissions or for advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Read	☑	□
Special Permissions	□	□

Figure 76

4. Click **Advanced**.
5. Click the **Auditing** tab on the Advanced Security Settings window.



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

☑ 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

Figure 77

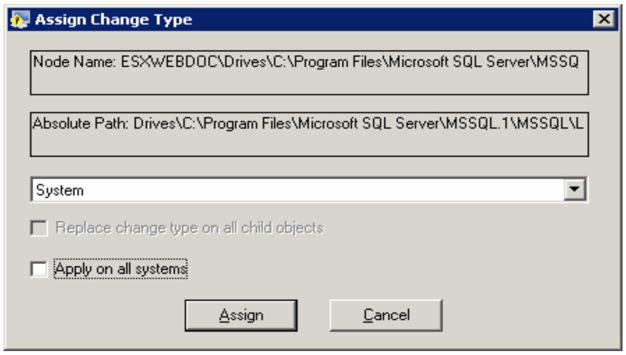
6. Add users as explained in the previous section.

3.14 Assign Change Type

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

To modify Change Type, follow the steps below:

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 the **Assign Change Type**.
   EventTracker - Change Audit displays the Assign Change Type window.



Assign Change Type

Node Name: ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\MSSQ

Absolute Path: Drives\C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\L

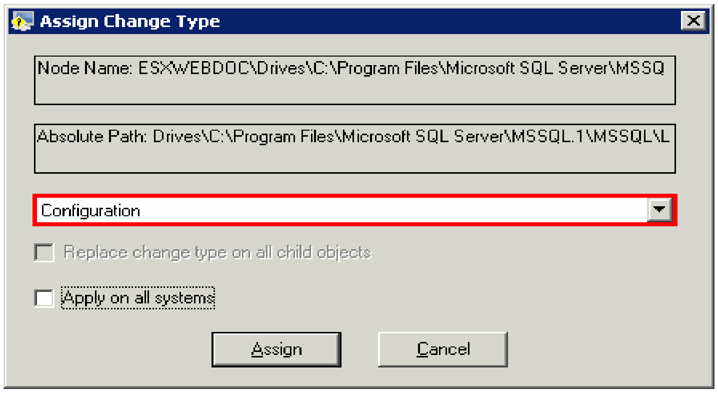
System

□ Replace change type on all child objects

□ Apply on all systems

Figure 78

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.



Assign Change Type

Node Name: ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\MSSQ

Absolute Path: Drives\C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\L

Configuration

□ Replace change type on all child objects

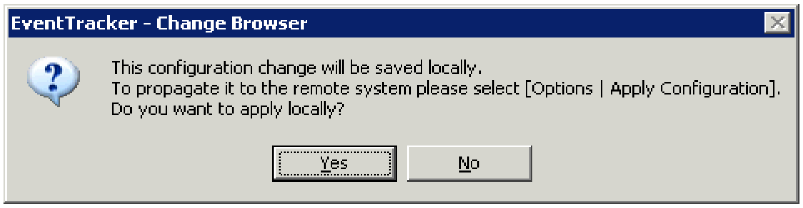
□ Apply on all systems

Figure 79

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.



EventTracker - Change Browser

This configuration change will be saved locally.
To propagate it to the remote system please select [Options | Apply Configuration].
Do you want to apply locally?

Figure 80

4. Snapshots

Snapshot is a read-only copy of File System structure, Registry structure, and System configuration.

After successful installation, EventTracker - Change Audit takes a baseline Snapshot. EventTracker - Change Audit takes one or 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 is not deleted in any of the earlier Snapshots and will not attempt to take the new Snapshot.

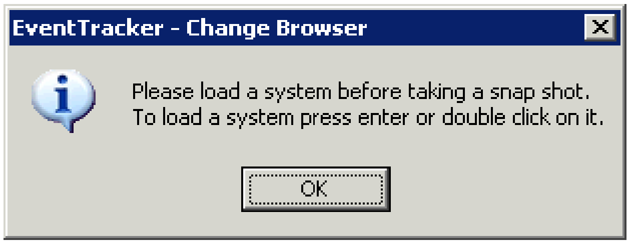
4.1 Take Snapshots on Demand

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

To take Snapshots on demand, follow the steps below:

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 before taking the Snapshots.



EventTracker - Change Browser

Please load a system before taking a snap shot.
To load a system press enter or double click on it.

Figure 81

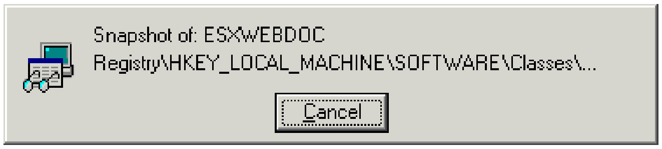
   EventTracker - Change Audit loads the details of the selected system.

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

   (OR)

Click New Snap on the toolbar.

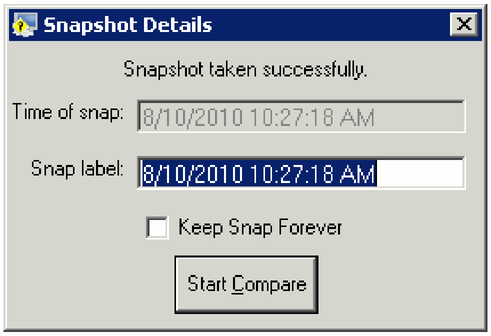
EventTracker - Change Audit displays Snapshot progress.



Snapshot of: ESXWEBDOC
Registry\HKEY_LOCAL_MACHINE\SOFTWARE\Classes\...

Figure 82

After completion of taking the Snapshot, EventTracker - Change Audit displays the Snapshot Details dialog box.



Snapshot Details

Snapshot taken successfully.

Time of snap: 8/10/2010 10:27:18 AM

Snap label: 8/10/2010 10:27:18 AM

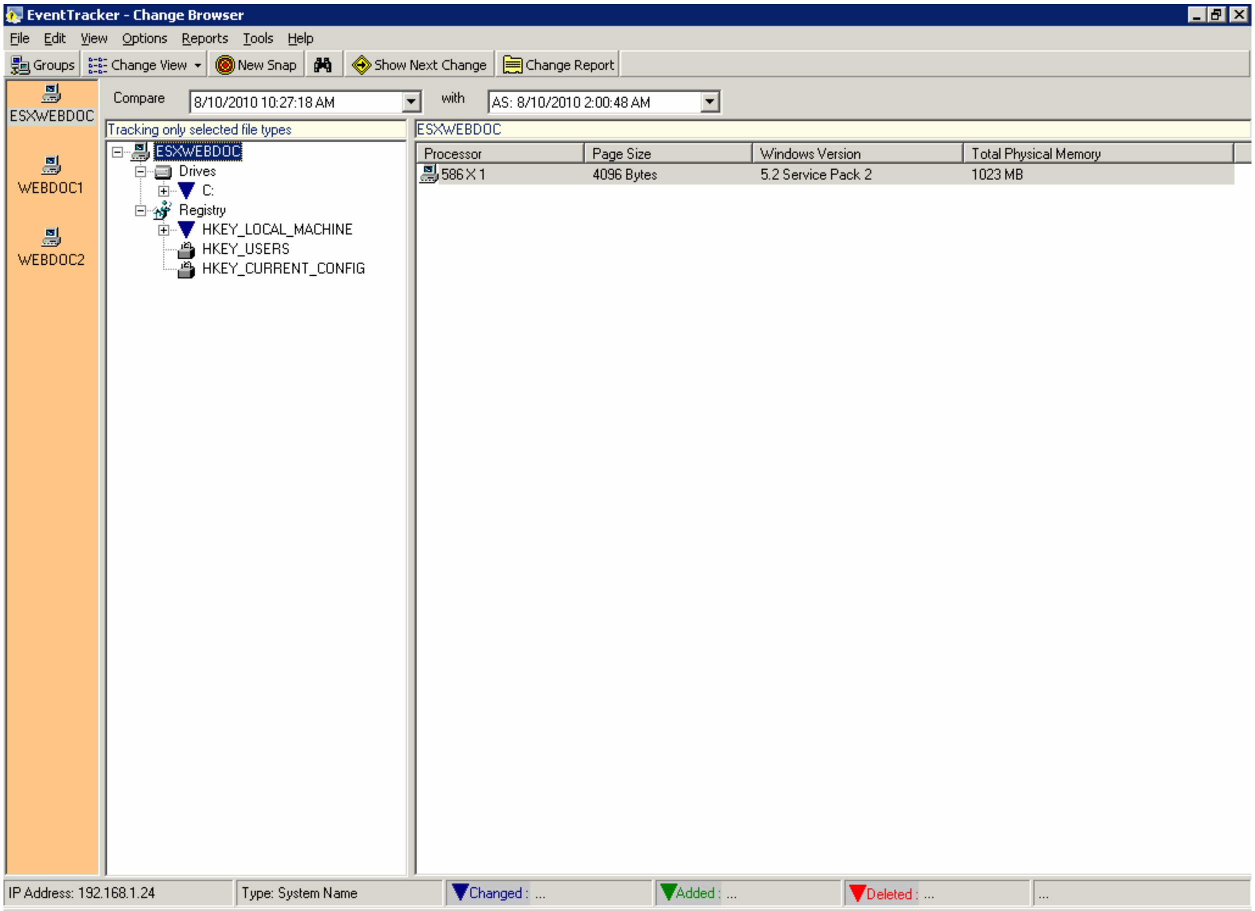
□ Keep Snap Forever

Figure 83

Field	Description
Time of snap	Display box displays the date and time when the Snapshot was taken.
Snap label	Text box displays the EventTracker - Change Audit name of the Snapshot. You can edit and rename the Snapshot.
Keep Snap Forever	Select this check box, if you want to preserve the Snapshot forever.
Start Compare	Click this button for the EventTracker - Change Audit to start comparing with the immediate previous Snapshot.

4. Type an appropriate name for the new Snapshot in the **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.



Compare 8/10/2010 10:27:18 AM with AS: 8/10/2010 2:00:48 AM

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.2 Service Pack 2	1023 MB

IP Address: 192.168.1.24

Type: System Name

Figure 84

4.2 Edit Snapshots

This option helps you edit Snapshot settings.

To edit Snapshot settings, follow the steps below:

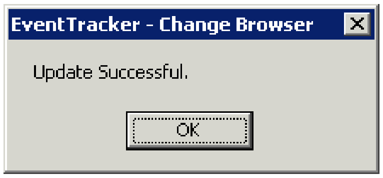
1. Open the Change Browser.
2. Double-click a computer on the System Bar.
3. Click the **Options** menu and select the **Edit Snapshots** option.

EventTracker - Change Audit displays the Snap Editor.

Field	Description
List of snapshots for current system	Displays the list of Snapshots taken for the selected Computer.
Time of snap	Display box displays the date and time when the Snapshot was taken.
Snap label	Displays the name of the selected Snapshot.
Keep Snap Forever	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. Select and clear for all the Snapshots, whenever needed.
Update	After making appropriate changes, click this button for the EventTracker - Change Audit to update the changes.
Close	Click this button to close Snap Editor.

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

   EventTracker - Change Audit displays the message box.

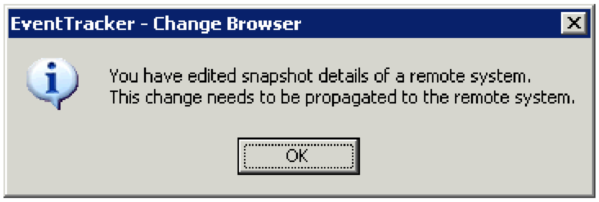


Update Successful.

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 the remote system.

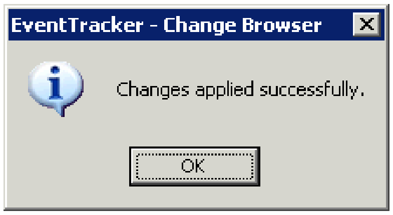


You have edited snapshot details of a remote system.
This change needs to be propagated to the remote system.

Figure 86

6. Click **OK**.

   EventTracker - Change Audit displays the message box.



EventTracker - Change Browser

Changes applied successfully.

Figure 87

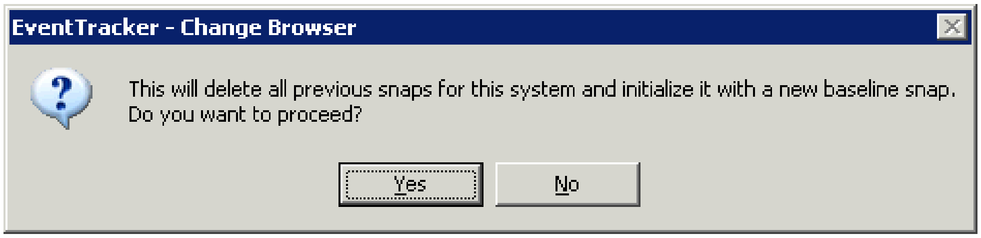
4.3 Reinitialize Snapshots

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, follow the steps below:

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.



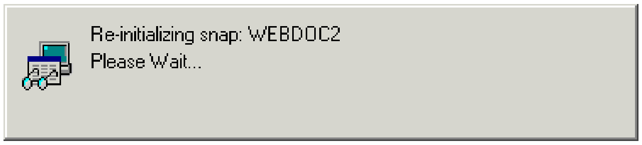
EventTracker - Change Browser

This will delete all previous snaps for this system and initialize it with a new baseline snap.
Do you want to proceed?

Figure 88

4. Click **Yes** to proceed.

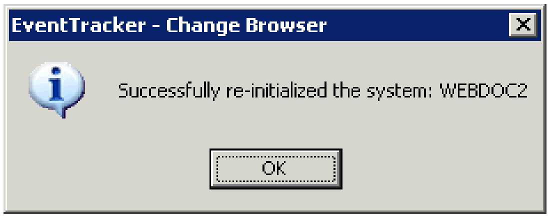
   EventTracker - Change Audit displays the re-initialization process progress.



Re-initializing snap: WEBDOC2
Please Wait...

Figure 89

After successfully re-initializing the Snapshots, EventTracker - Change Audit displays the message box.

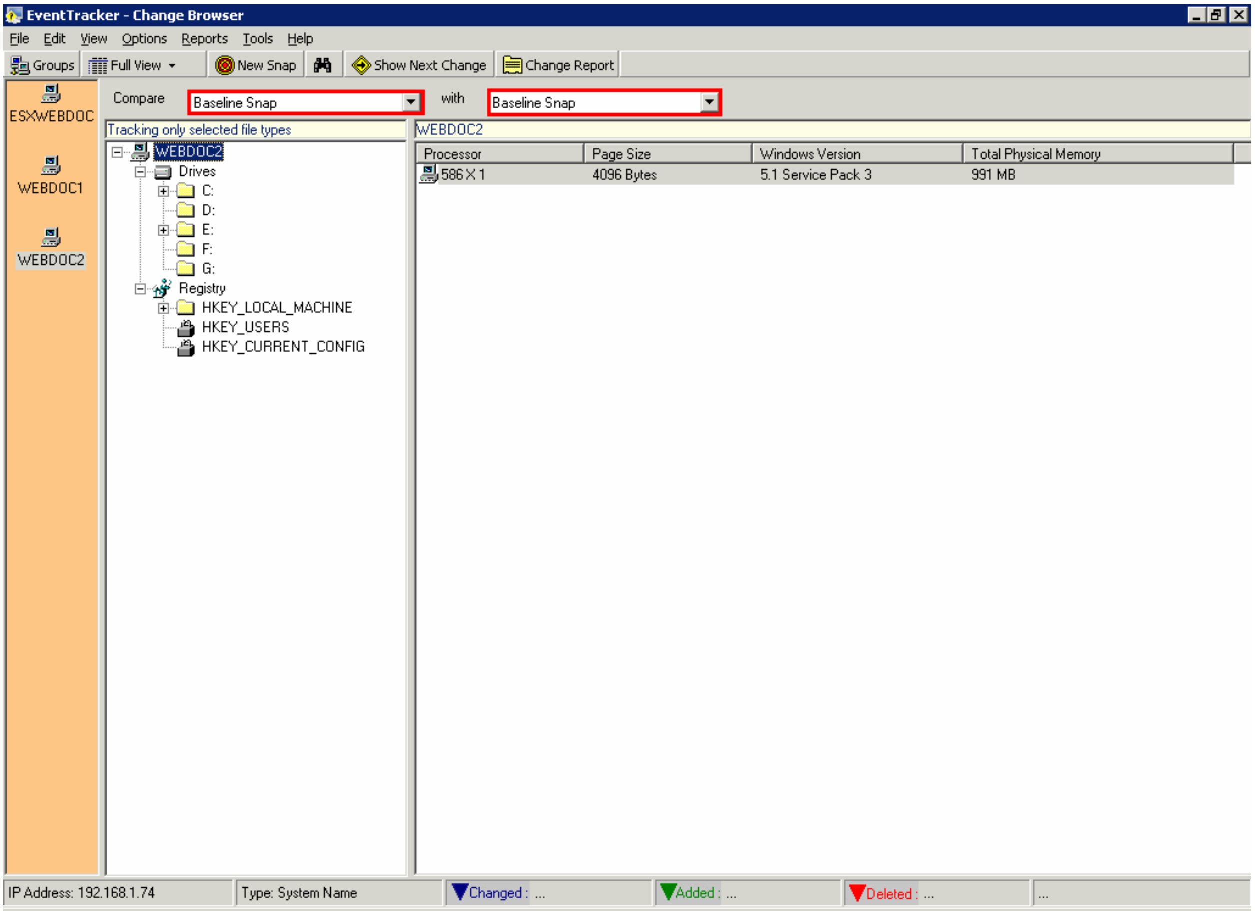


Successfully re-initialized the system: WEBDOC2

Figure 90

5. Click **OK**.

   EventTracker - Change Audit displays the Change Browser.



Compare Baseline Snap with Baseline Snap

Tracking only selected file types

WEBDOC2

Processor	Page Size	Windows Version	Total Physical Memory
586 X 1	4096 Bytes	5.1 Service Pack 3	991 MB

IP Address: 192.168.1.74 Type: System Name

Figure 91

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**.

4.4 Back up the Snapshots

This option helps you back up Snapshots.

To back up Snapshot, follow the steps below:

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.

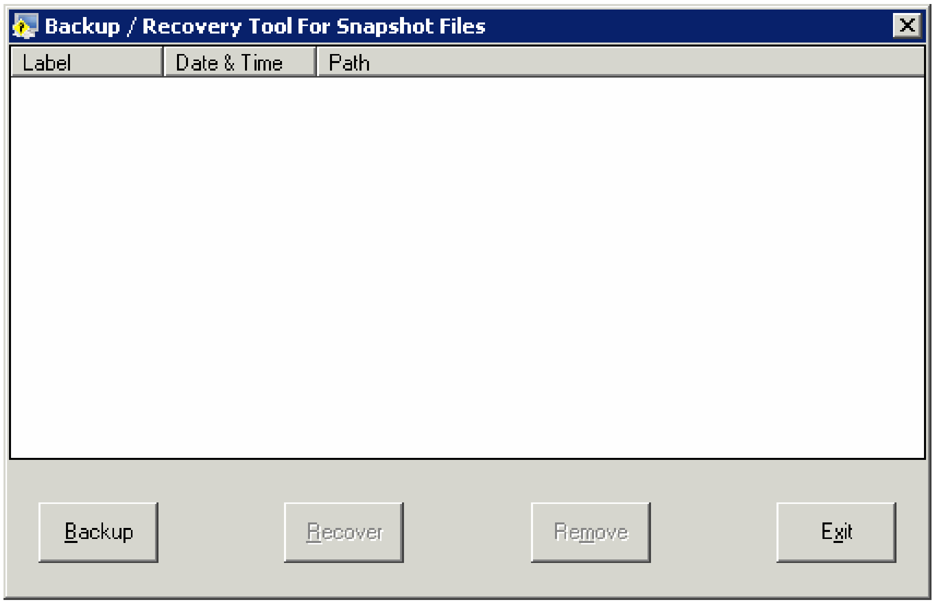


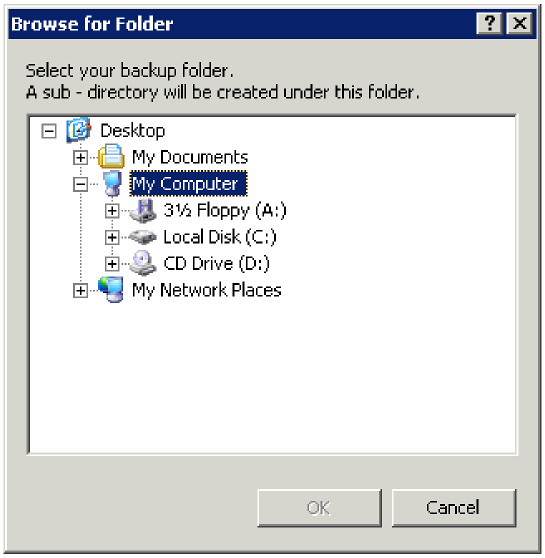
Figure 92

Click	To
Backup	Back up the Snapshots of the current system.
Recover	Select the backup file from the list and then click to recover the Snapshots.

Click	To
Remove	Select the backup 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.



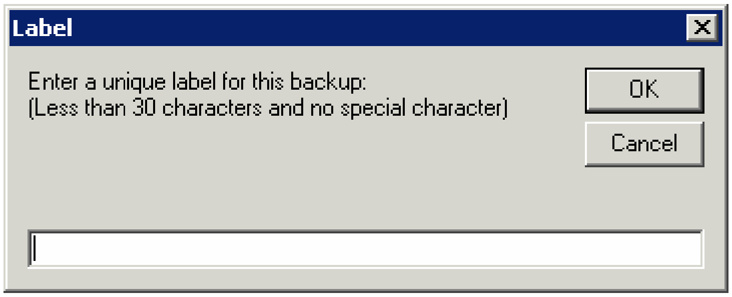
Browse for Folder

Select your backup folder.
A sub - directory will be created under this folder.

Figure 93

5. Select the appropriate folder and then click **OK**.

   EventTracker - Change Audit displays the Label window.



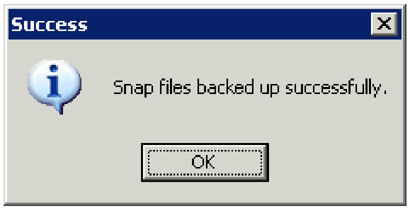
Label

Enter a unique label for this backup:
(Less than 30 characters and no special character)

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.

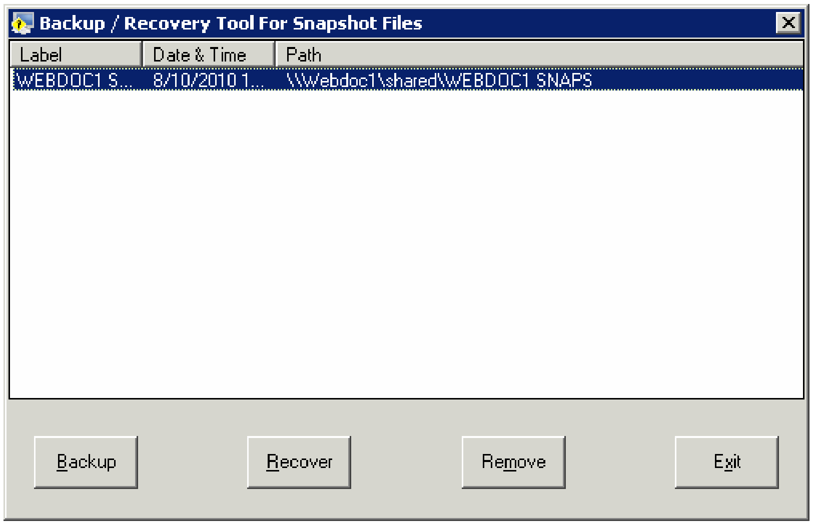


Snap files backed up successfully.

Figure 95

7. Click **OK**.

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



Label	Date & Time	Path
WEBDOC1 S...	8/10/2010 1...	\\Webdoc1\shared\WEBDOC1 SNAPS

Figure 96

8. Click **Exit**.

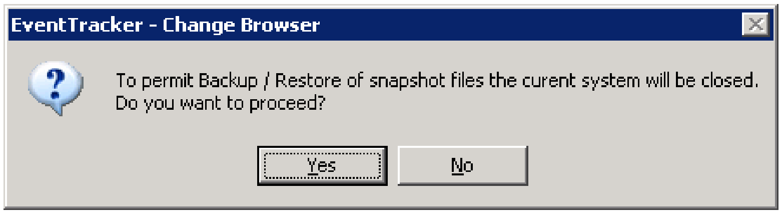
4.5 Recover Snapshots

This option helps you recover Snapshots.

To recover Snapshots, follow the steps below:

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.

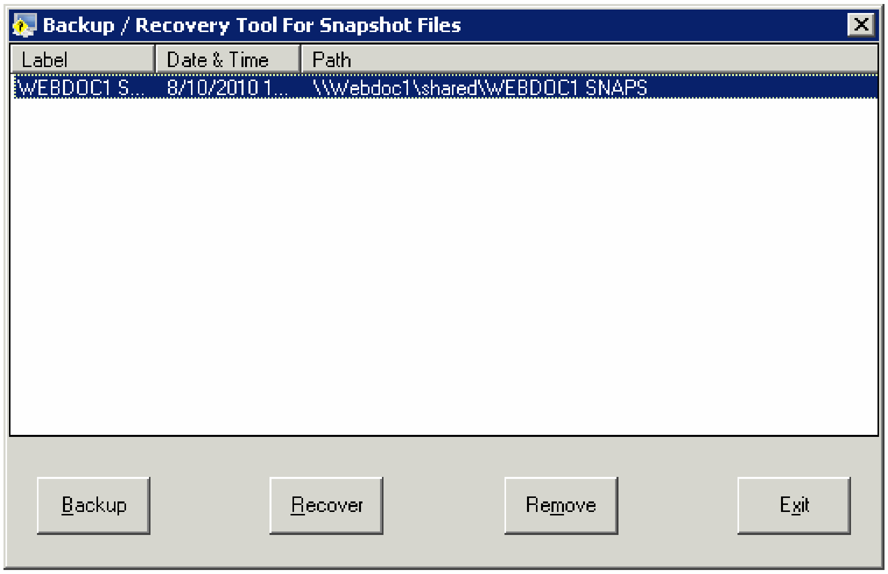

EventTracker - Change Browser

To permit Backup / Restore of snapshot files the curent system will be closed.
Do you want to proceed?

Figure 97

3. Click **Yes** to proceed.

   EventTracker - Change Audit displays the Backup / Recovery Tool.

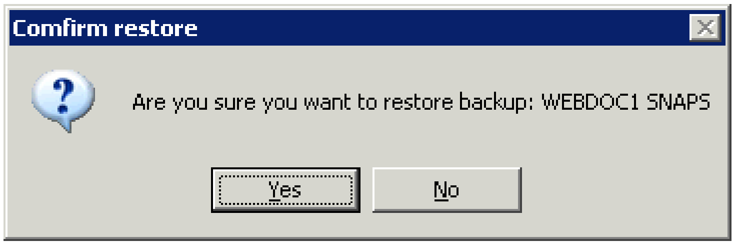

Backup / Recovery Tool For Snapshot Files

Label	Date & Time	Path
WEBDOC1 S...	8/10/2010 1...	\\Webdoc1\shared\WEBDOC1 SNAPS

Figure 98

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

   EventTracker - Change Audit displays the Confirm restore message box.

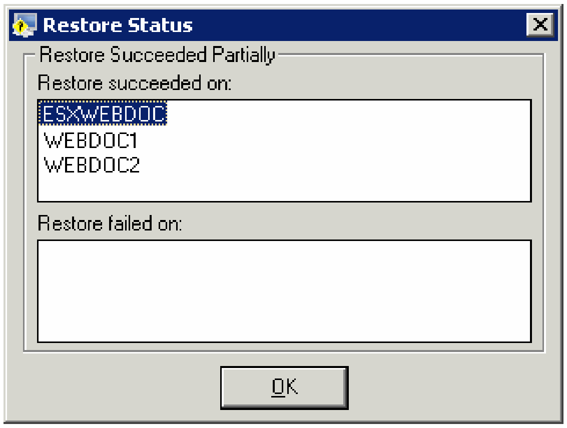

Comfirm restore

Are you sure you want to restore backup: WEBDOC1 SNAPS

Figure 99

5. Click **Yes** to proceed.

   After a successful recovery, EventTracker - Change Audit displays the Restore Status.



Restore Status

Restore Succeeded Partially

Restore succeeded on:

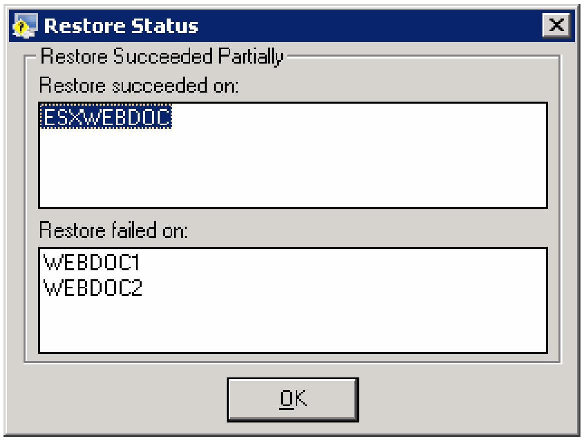
ESXWEBDOC
WEBDOC1
WEBDOC2

Restore failed on:

Figure 100

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 the appropriate message.



Restore Status

Restore Succeeded Partially

Restore succeeded on:

ESXWEBDOC

Restore failed on:

WEBDOC1
WEBDOC2

Figure 101

5. Configuration

The administrator can configure any Client through the 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.

5.1 Global Configuration

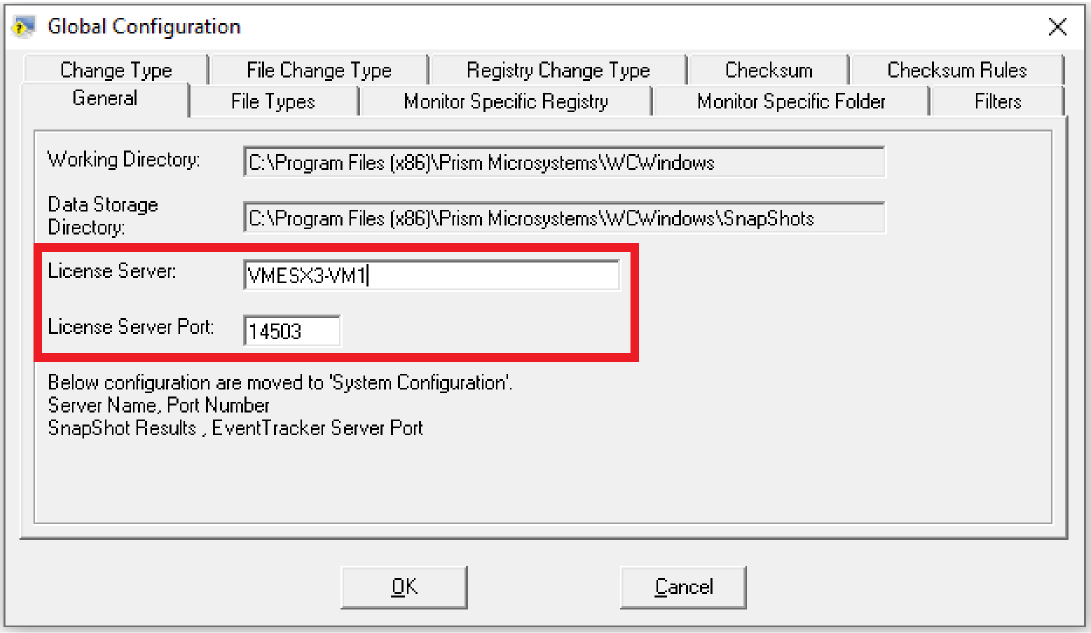
This option helps to set the Global Configuration.

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

To set up Global Configuration, follow the steps below:

1. Open the Change Browser.
2. Click the **Options** menu and select the **Global Configuration** option.

   Change Audit displays the Global Configuration window.



Working Directory: C:\Program Files (x86)\Prism Microsystems\WCWindows

Data Storage Directory: C:\Program Files (x86)\Prism Microsystems\WCWindows\SnapShots

License Server: VMESX3-VM1

License Server Port: 14503

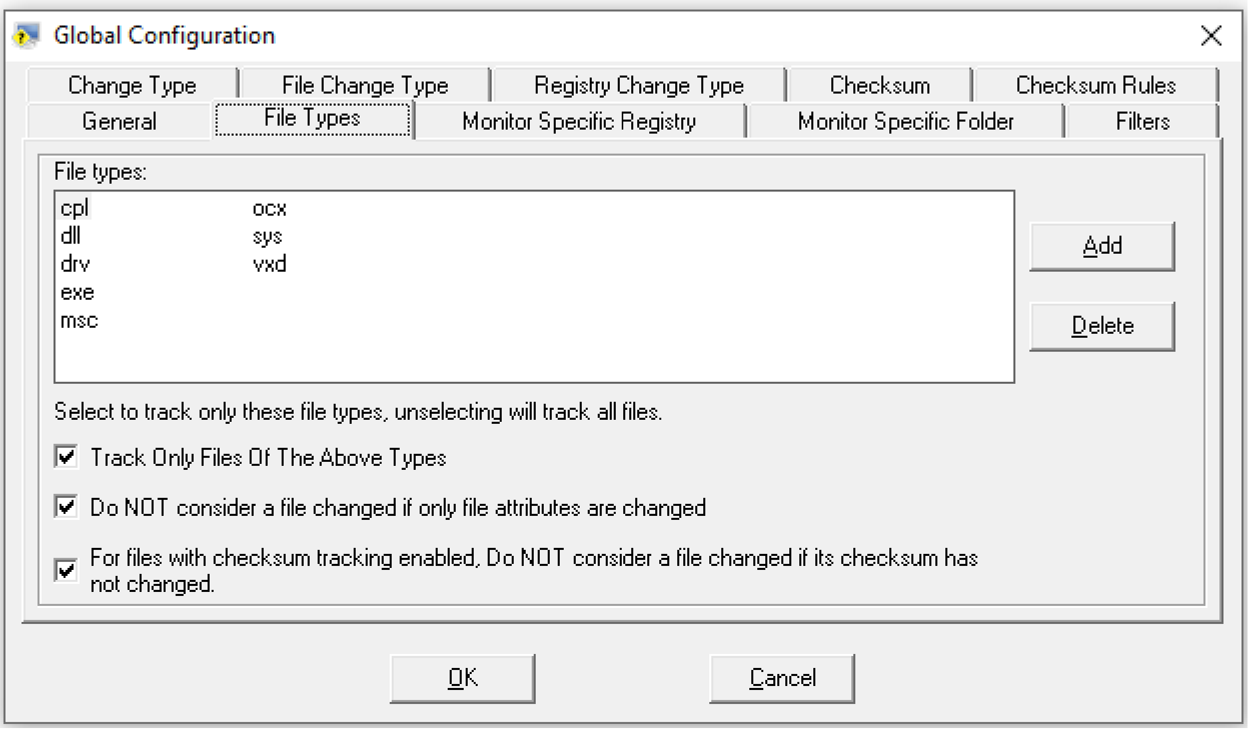
Below configuration are moved to 'System Configuration'.
Server Name, Port Number
SnapShot Results , EventTracker Server Port

Figure 102

Field	Description
General	General Change Audit selects this tab by default and displays information about the Working Directory path, Data Store directory path.

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

   EventTracker - Change Audit displays the File Types tab.



File types:

cpl	ocx
dll	sys
drv	vxd
exe	
msc	

Select to track only these file types, unselecting will track all files.

☑ Track Only Files Of The Above Types

☑ Do NOT consider a file changed if only file attributes are changed

☑ For files with checksum tracking enabled, Do NOT consider a file changed if its checksum has not changed.

Figure 103

Field	Description
File Types	Click this tab to view the Files 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 tacking 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, do not consider a file changed if its checksum has not	Clear this check box to exclude checksum tracking enabled files, if the checksum has not changed.

Field	Description
changed	

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

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

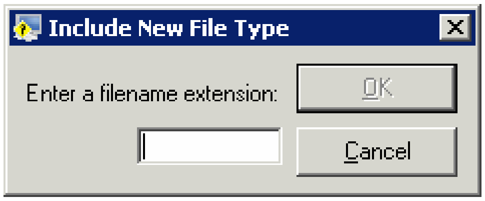
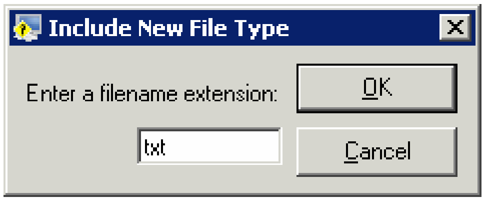


Figure 104

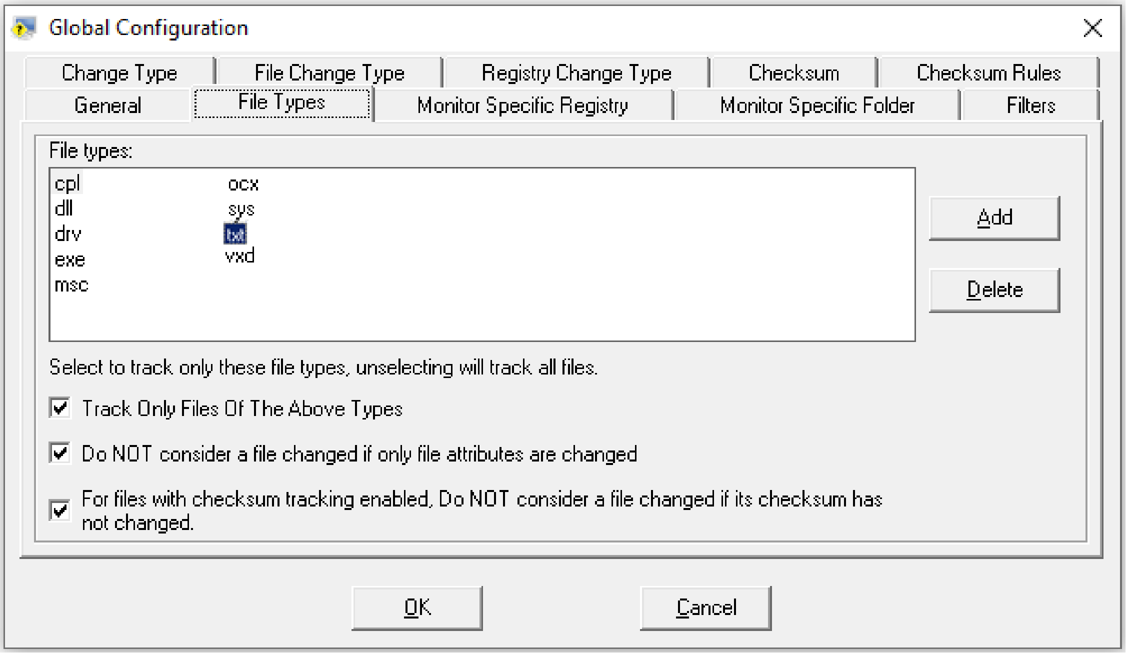
5. Type the filename extension and then click **OK**.



Enter a filename extension: txt

Figure 105

EventTracker - Change Audit includes the file type and displays the File Types tab.



File types:

cpl, dll, drv, exe, msc, ocx, sys, txt, vxd

Select to track only these file types, unselecting will track all files.

☑ Track Only Files Of The Above Types

☑ Do NOT consider a file changed if only file attributes are changed

☑ For files with checksum tracking enabled, Do NOT consider a file changed if its checksum has not changed.

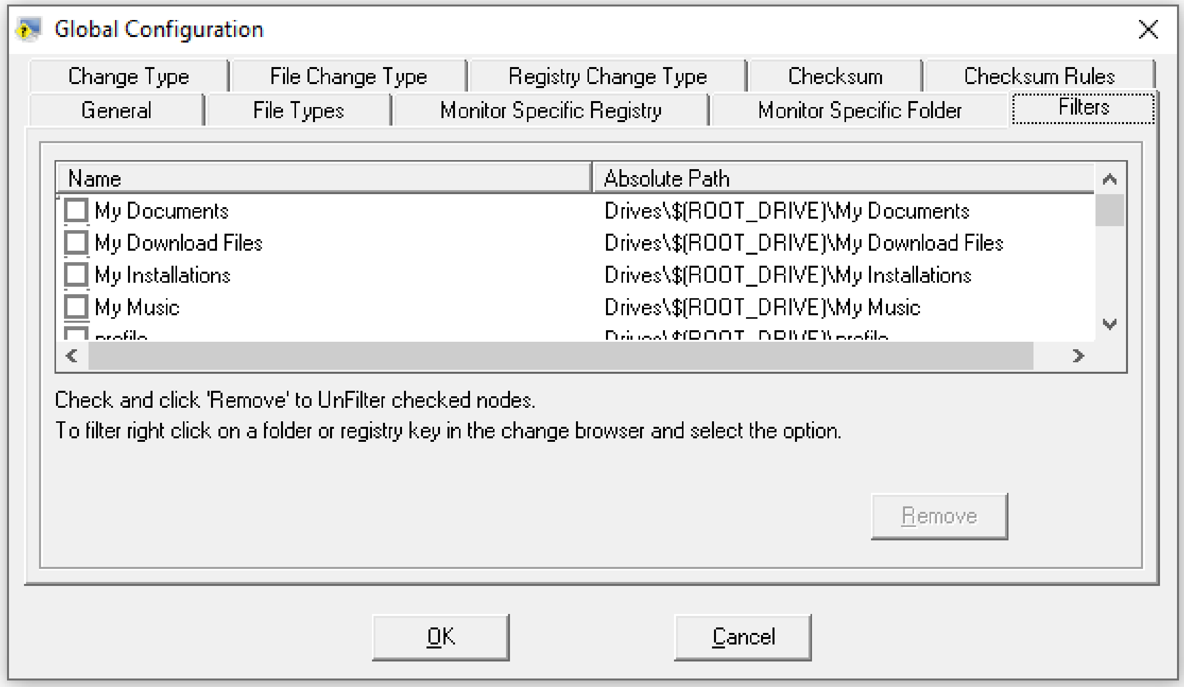
Figure 106

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.



Name	Absolute Path
□ My Documents	Drives\$(ROOT_DRIVE)\My Documents
□ My Download Files	Drives\$(ROOT_DRIVE)\My Download Files
□ My Installations	Drives\$(ROOT_DRIVE)\My Installations
□ My Music	Drives\$(ROOT_DRIVE)\My Music
□ profile	Drives\$(ROOT_DRIVE)\profile

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 107

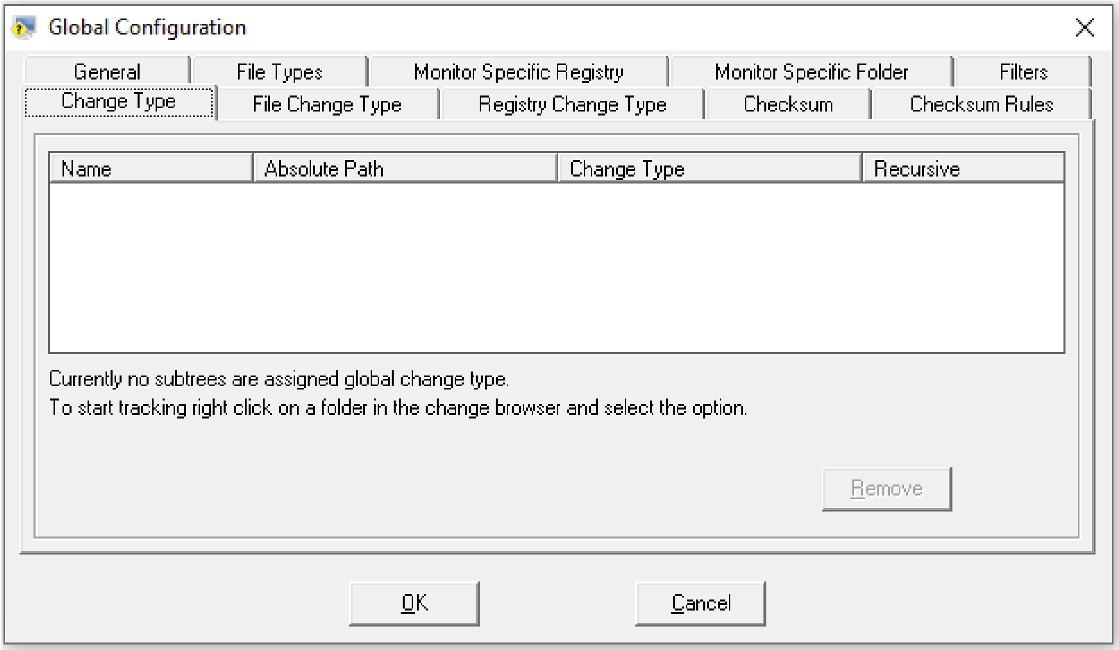
Field	Description
Filters	Click this tab to view files, folders, registry hives and keys filtered by EventTracker - Change Audit. Select the check box against items in the list and click **Remove** to exclude it from the Filters list. To learn more about Filters, refer the Filters chapter.

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.



Currently no subtrees are assigned global change type.
To start tracking right click on a folder in the change browser and select the option.

Figure 108

Field	Description
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 is made to the 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.

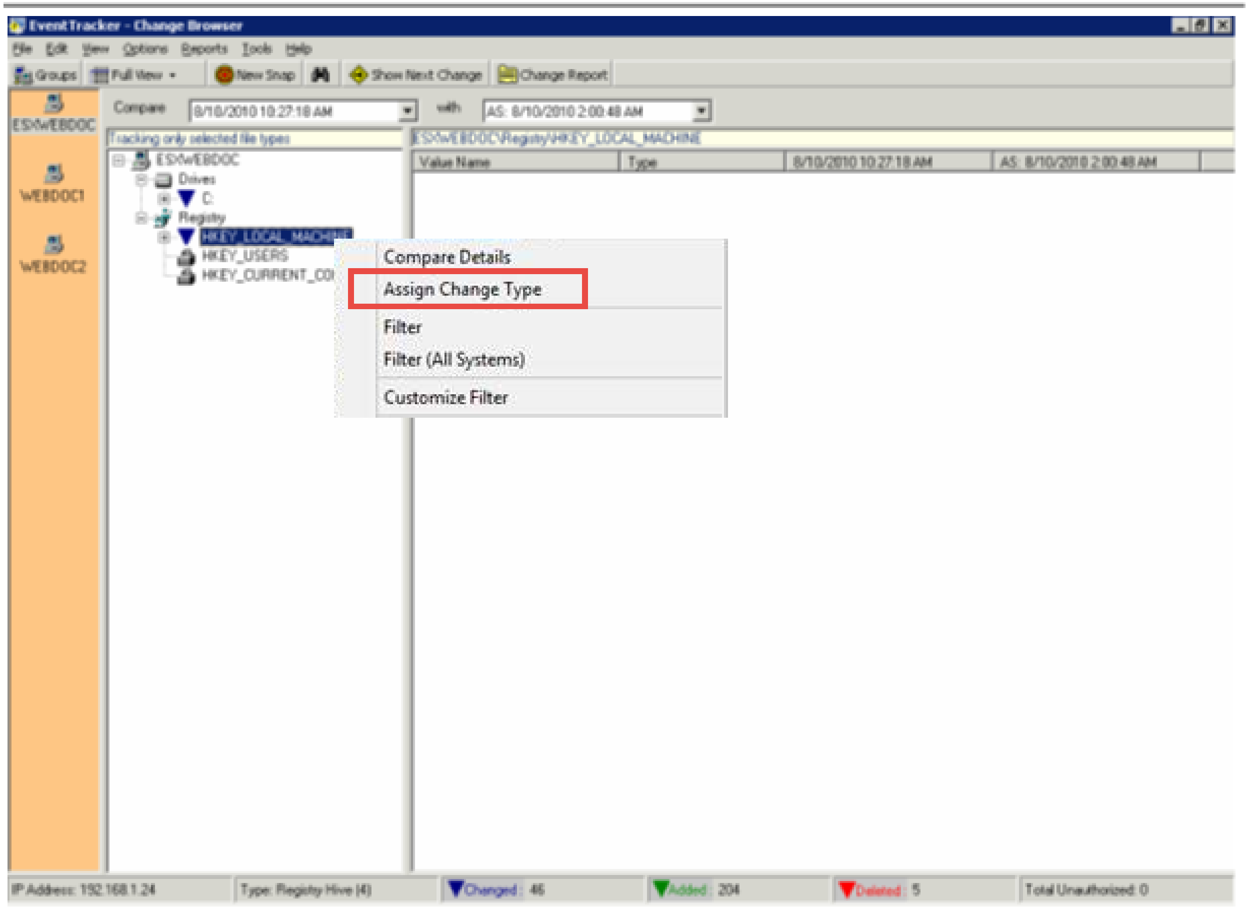


Figure 109

2. From the shortcut menu, choose **Assign Change Type**.

   EventTracker - Change Audit displays the Assign Change Type window.

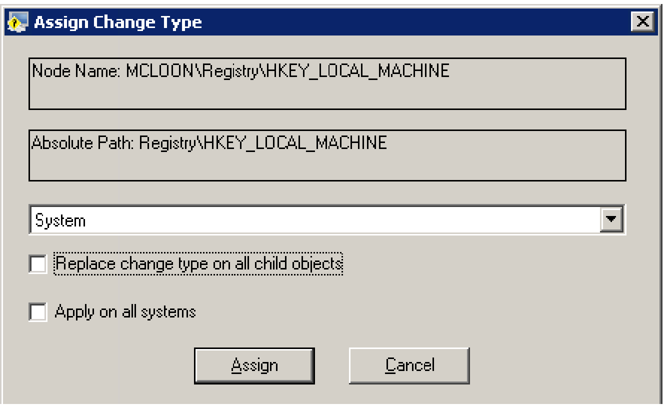
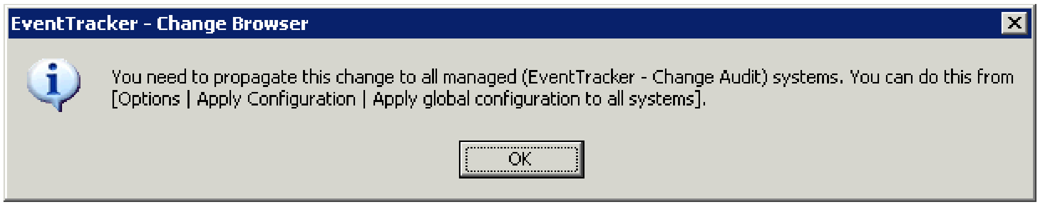

Assign Change Type
Node Name: MCLOON\Registry\HKEY_LOCAL_MACHINE
Absolute Path: Registry\HKEY_LOCAL_MACHINE
System
☐ Replace change type on all child objects
☐ Apply on all systems
Assign
Cancel

Figure 110

Field	Description
Change Type	But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc, *.xlsx, *.docx, *.ppt, *.pptx, *.pdf, *.pps, *.ppsx, *.dotx, *.dot, *.odt 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**.

   If **Apply** is selected on all the systems check box, EventTracker - Change Audit displays the confirmation message box.



EventTracker - Change Browser

You need to propagate this change to all managed (EventTracker - Change Audit) systems. You can do this from [Options | Apply Configuration | Apply global configuration to all systems].

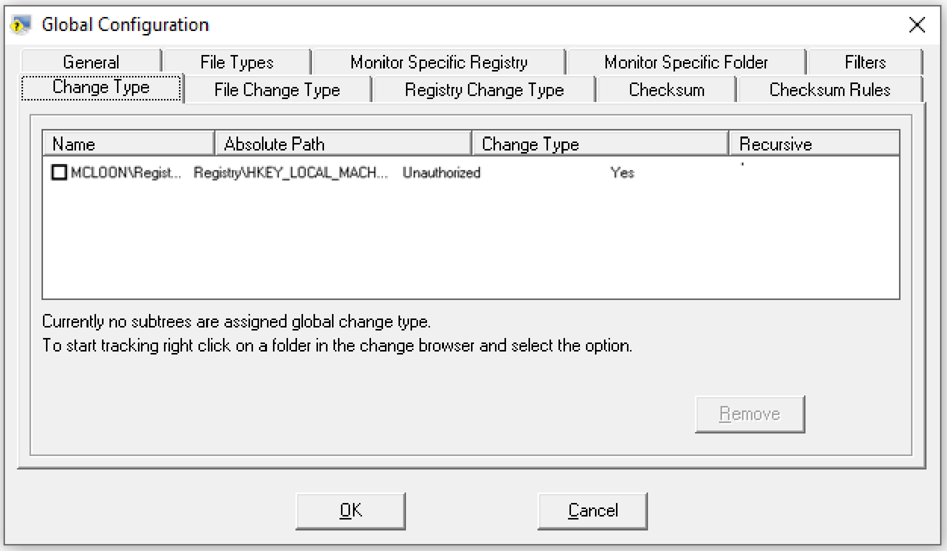
Figure 111

4. Click **OK** to continue.

   EventTracker - Change Audit applies the change to 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.



Name	Absolute Path	Change Type	Recursive
□ MCLOON\Regist...	Registry\HKEY_LOCAL_MACH...	Unauthorized	Yes

Currently no subtrees are assigned global change type.
To start tracking right click on a folder in the change browser and select the option.

Figure 112

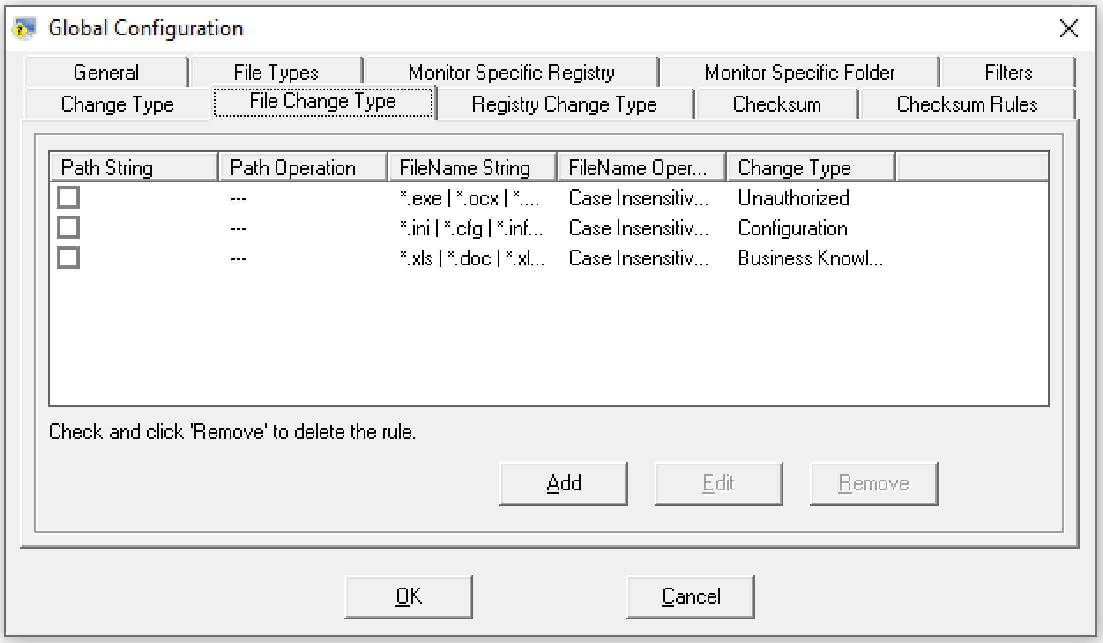
6. Select an object and then click **Remove**.

   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.



Path String	Path Operation	FileName String	FileName Oper...	Change Type
□	---	*.exe | *.ocx | *....	Case Insensitiv...	Unauthorized
□	---	*.ini | *.cfg | *.inf...	Case Insensitiv...	Configuration
□	---	*.xls | *.doc | *.xl...	Case Insensitiv...	Business Knowl...

Check and click 'Remove' to delete the rule.

Figure 113

Field	Description
File Change Type	But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc, *.xlsx, *.docx, *.ppt, *.pptx, *.pdf, *.pps, *.ppsx, *.dotx, *.dot, *.odt

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

   EventTracker - Change Audit removes the selected item.

5.1.1 Adding/Editing File Change Type

To add/edit File Change Type, follow the steps below:

1. Click **Add/Edit** to add a new File Name String.

   EventTracker - Change Audit displays the File Change Type window.

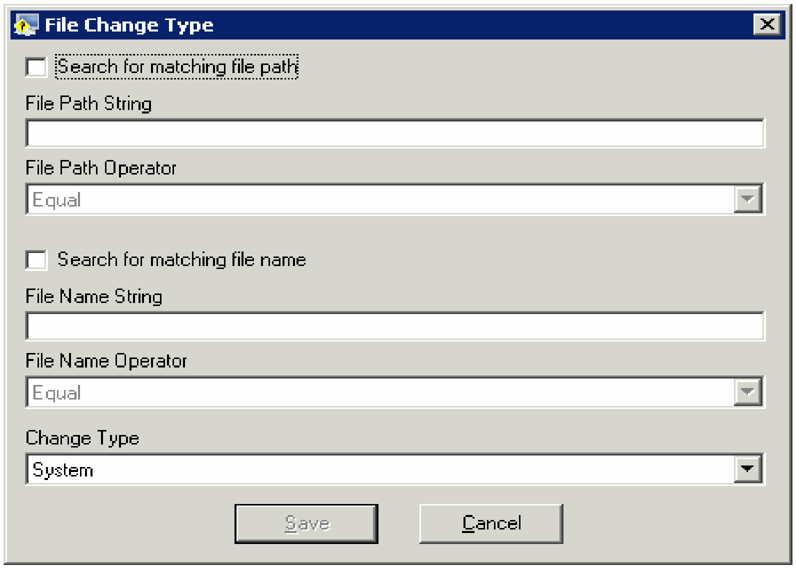


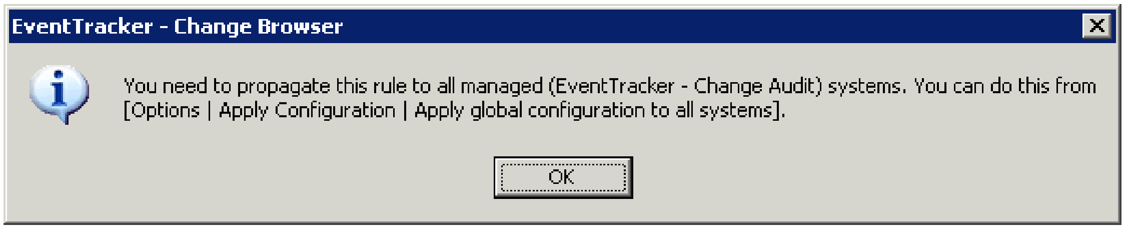
Figure 114

Field	Description
Search for matching file path	Select this check box. EventTracker - Change Audit enables File Path String and File Path Operator fields.
File Path String	Type the location of the file.
File Path Operator	Select an operator from this drop-down list.
Search for matching file name	Select this check box. EventTracker - Change Audit enables File Name String and File Name Operator fields.
File Name String	Type the name of the file.
File Name Operator	Select an operator from this drop-down list.

Field	Description
Change Type	Select a change type from this drop-down list.

2. Enter/select appropriate options.
3. Click **Save** to save changes.

   EventTracker - Change Audit displays the message box.



EventTracker - Change Browser

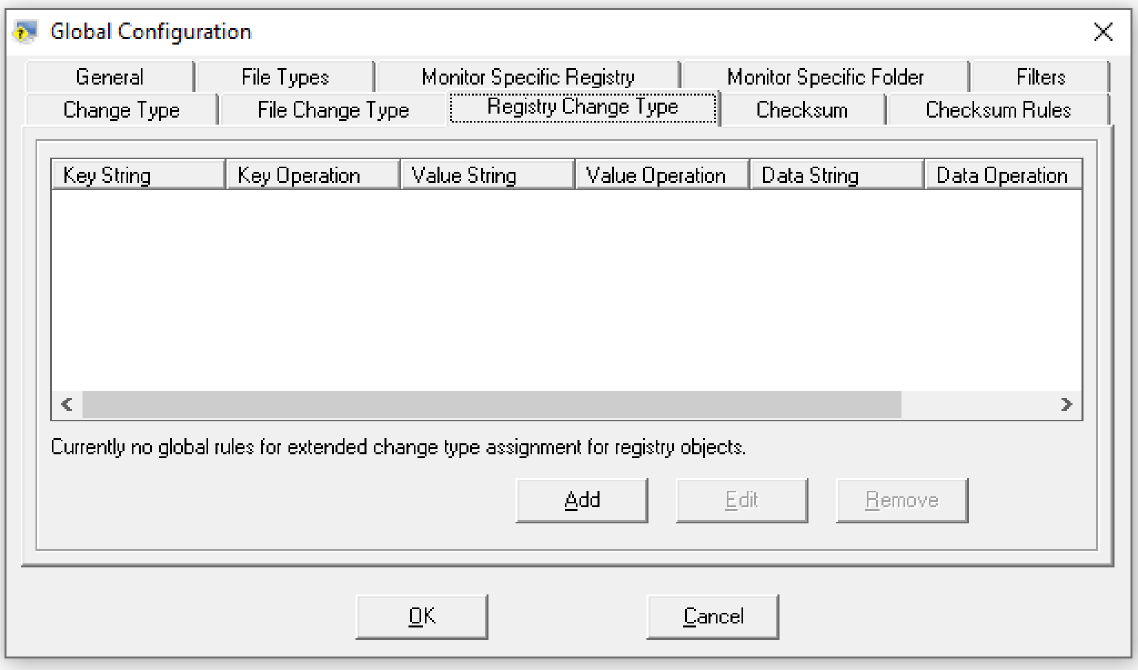
You need to propagate this rule to all managed (EventTracker - Change Audit) systems. You can do this from [Options | Apply Configuration | Apply global configuration to all systems].

Figure 115

4. Click **OK** and follow the message 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.



Global Configuration

Key String	Key Operation	Value String	Value Operation	Data String	Data Operation

Currently no global rules for extended change type assignment for registry objects.

Figure 116

Field	Description
Registry Change Type	But for the following classification of Change Type, EventTracker - Change Audit considers all else as System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc, *.xlsx, *.docx, *.ppt, *.pptx, *.pdf, *.pps, *.ppsx, *.dotx, *.dot, *.odt

6. Click **Add/Edit** to add new registry keys or update existing registry keys.

   EventTracker - Change Audit displays the Registry Change Type window.

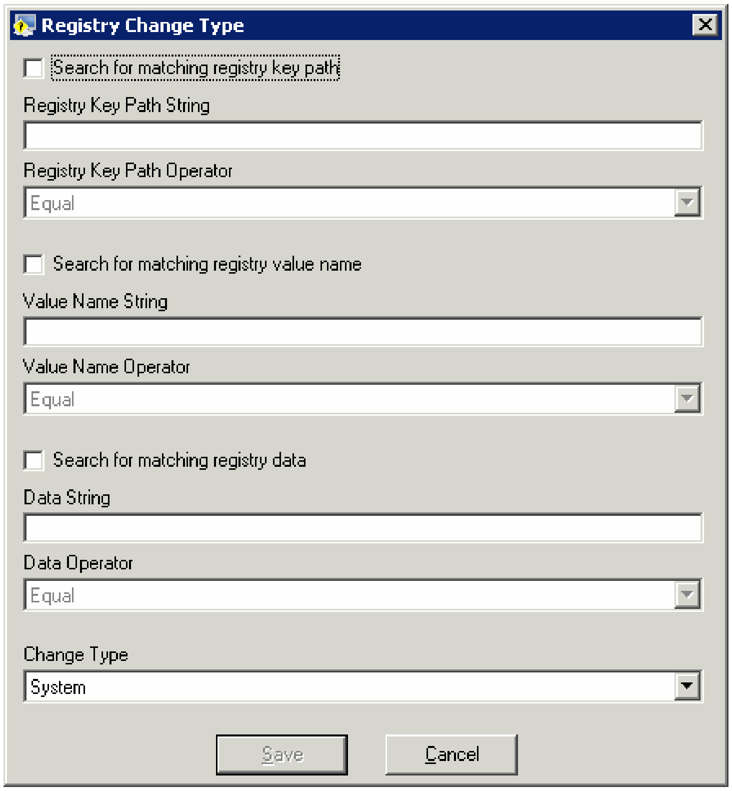


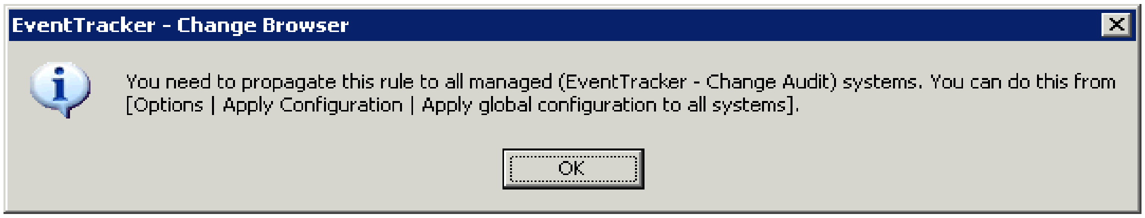
Figure 117

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.
Value Name Operator	Select an operator from this drop-down list.
Search for matching registry data	Select this check box. EventTracker - Change Audit enables Data String and Data Operator fields.
Data String	Type the data string.
Data Operator	Select an operator from this drop-down list.
Change Type	Select a change type from this drop-down list.

7. Enter/select appropriate options.

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

   EventTracker - Change Audit displays the message box.

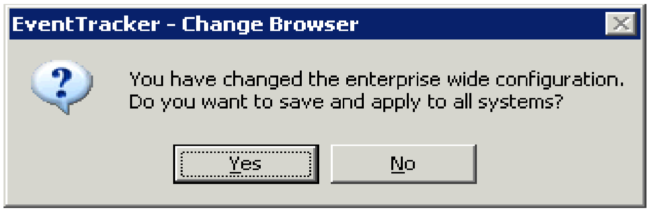


You need to propagate this rule to all managed (EventTracker - Change Audit) systems. You can do this from [Options | Apply Configuration | Apply global configuration to all systems].

Figure 118

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

   EventTracker - Change Audit displays the confirmation message box.



EventTracker - Change Browser

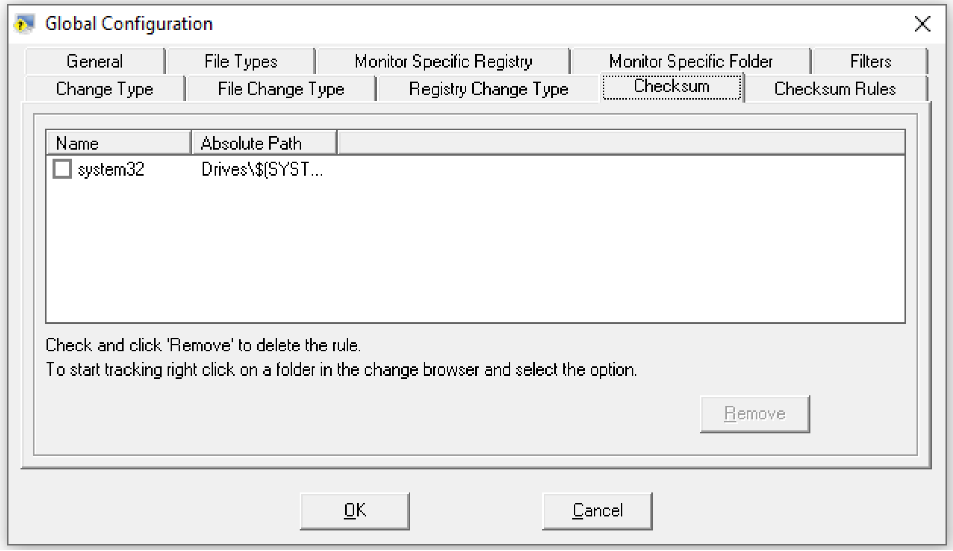
You have changed the enterprise wide configuration.
Do you want to save and apply to all systems?

Figure 119

10. Click **Yes** to apply to all the systems.

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

For the Checksum tab,



Global Configuration

Name	Absolute Path
□ system32	Drives\$(SYST...

Check and click 'Remove' to delete the rule.
To start tracking right click on a folder in the change browser and select the option.

Figure 120

5.1.2 Configuring the Change Type

1. Right-click a folder, file.

   EventTracker - Change Audit displays the shortcut menu.

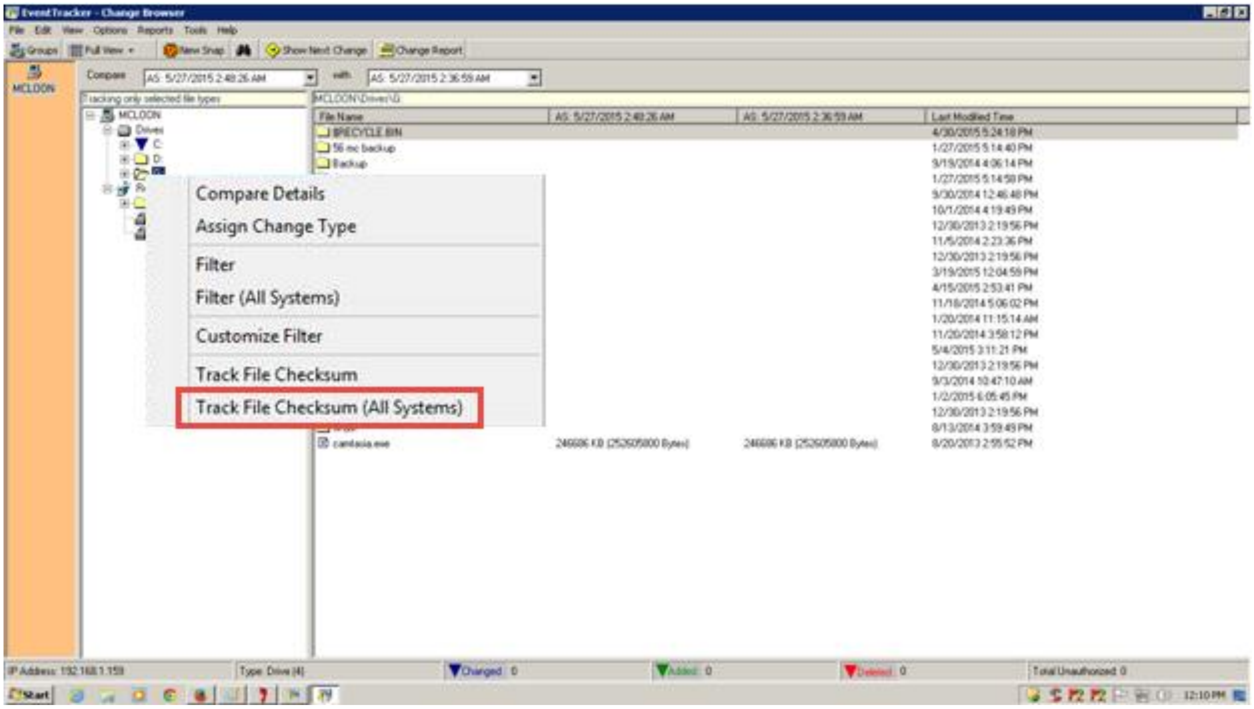
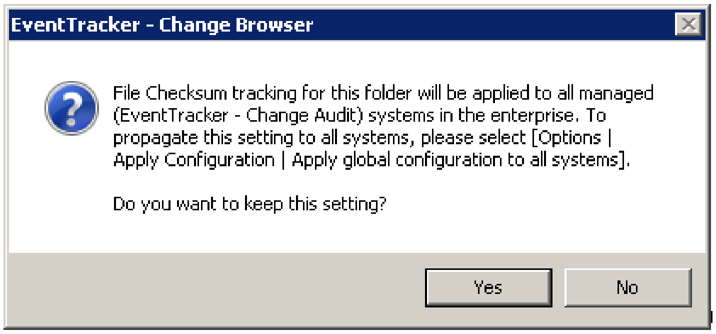


Figure 121

2. From the shortcut menu, choose **Track File Checksum (All Systems)**.

   EventTracker - Change Audit displays a message box window.



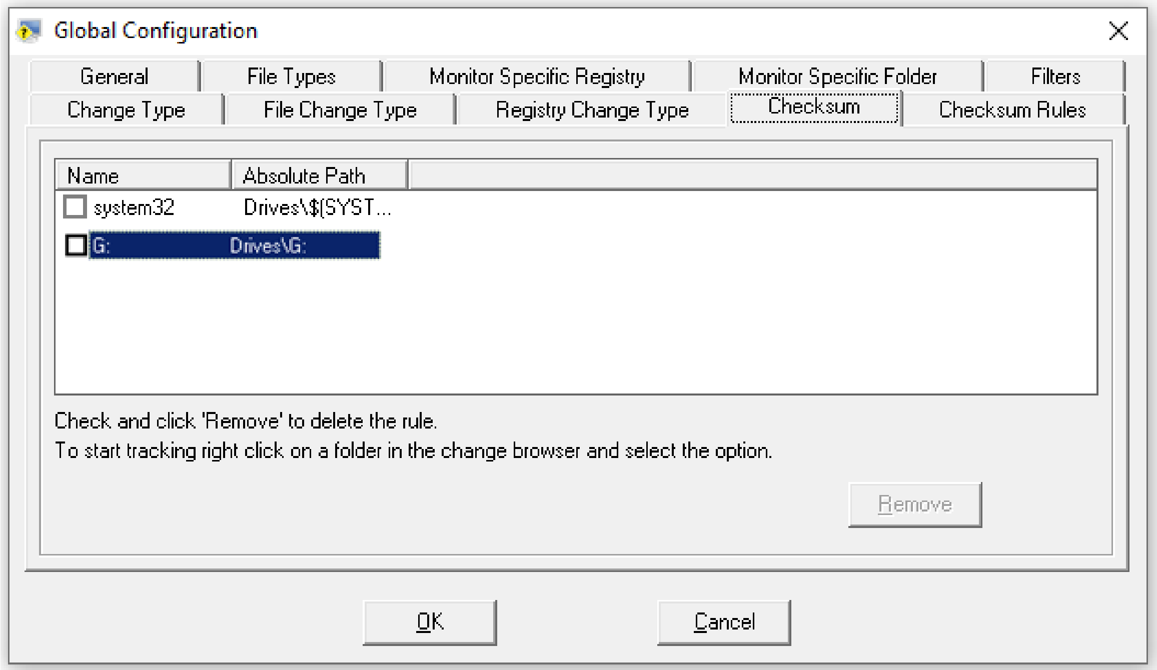
EventTracker - Change Browser

File Checksum tracking for this folder will be applied to all managed (EventTracker - Change Audit) systems in the enterprise. To propagate this setting to all systems, please select [Options | Apply Configuration | Apply global configuration to all systems].

Do you want to keep this setting?

Figure 122

3. Click **Yes** to apply the configuration.
   OR, click **No** to close the window.
4. In the checksum tab, select the system by clicking the checkbox.



Name	Absolute Path
□ system32	Drives\$(SYST...
□ G:	Drives\G:

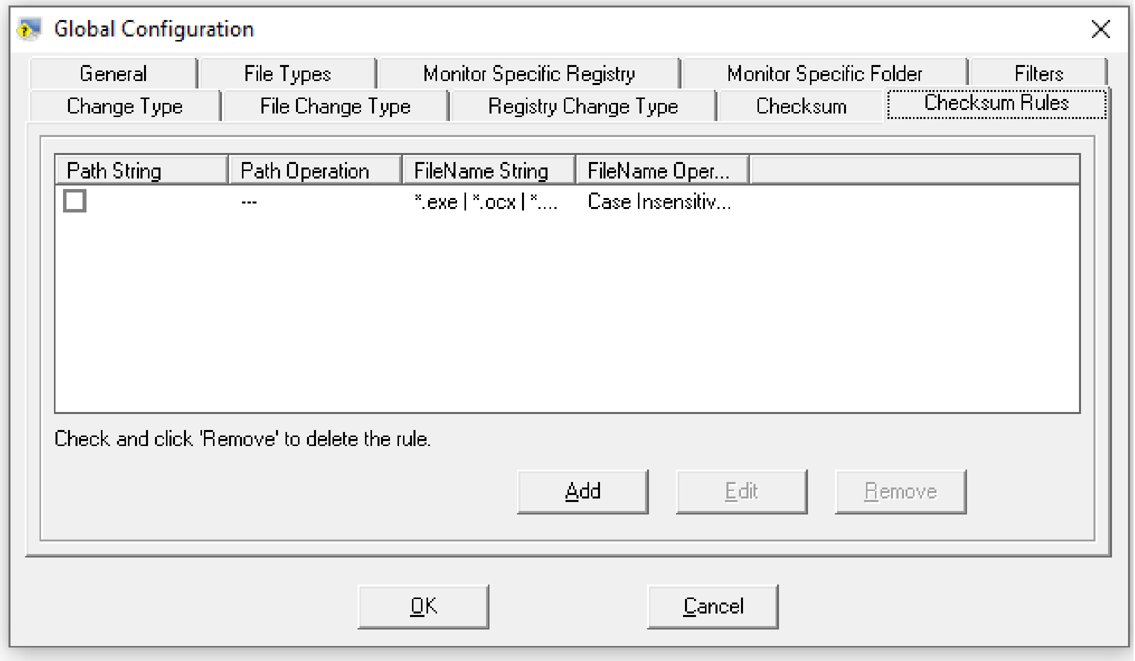
Check and click 'Remove' to delete the rule.
To start tracking right click on a folder in the change browser and select the option.

Figure 123

5. To remove it, click the **Remove** button.

5.1.3 Checksum Rules tab

1. The Checksum tracking is enabled by default for all executable files (*.exe, *.dll etc.).

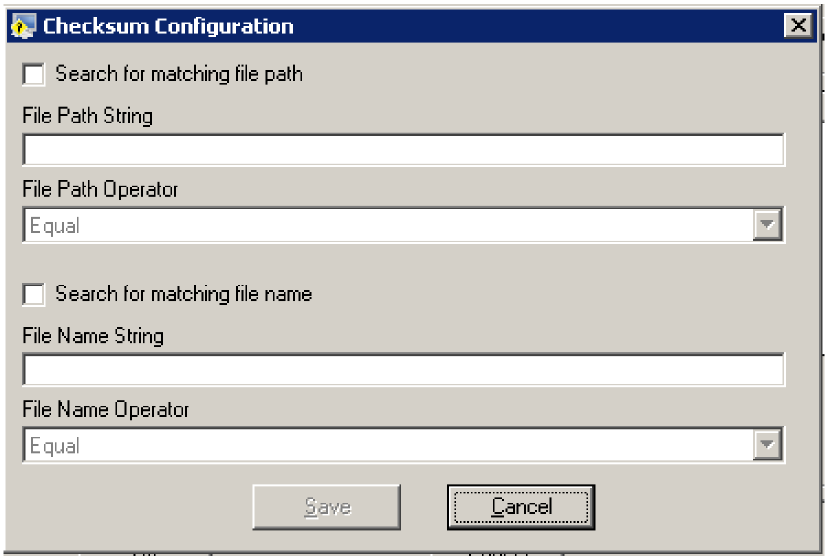


Path String	Path Operation	FileName String	FileName Oper...
□	---	*.exe | *.ocx | *....	Case Insensitiv...

Check and click 'Remove' to delete the rule.

Figure 124

2. Click the **Add** button and the Checksum configuration page displays.



Checksum Configuration

☐ Search for matching file path

File Path String

File Path Operator: Equal

☐ Search for matching file name

File Name String

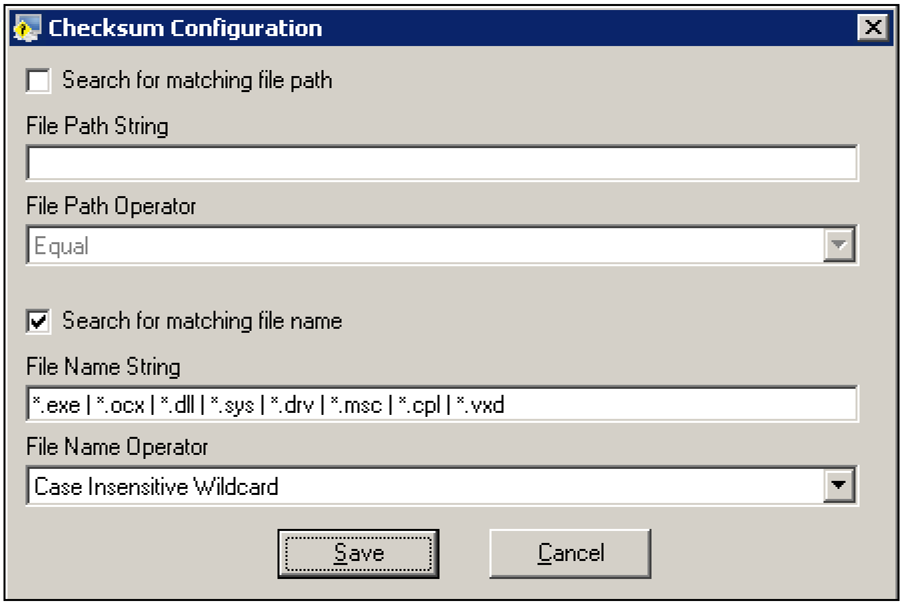
File Name Operator: Equal

Figure 125

3. Enter the configuration details and click the **Save** button.

Similarly, for editing,

4. Click the **Edit** button and make changes in the existing configuration.



Checksum Configuration

☐ Search for matching file path

File Path String

File Path Operator: Equal

☑ Search for matching file name

File Name String: *.exe | *.ocx | *.dll | *.sys | *.drv | *.msc | *.cpl | *.vxd

File Name Operator: Case Insensitive Wildcard

Figure 126

5. After making the changes, click the **Save** button.

5.2 Apply Global Configuration

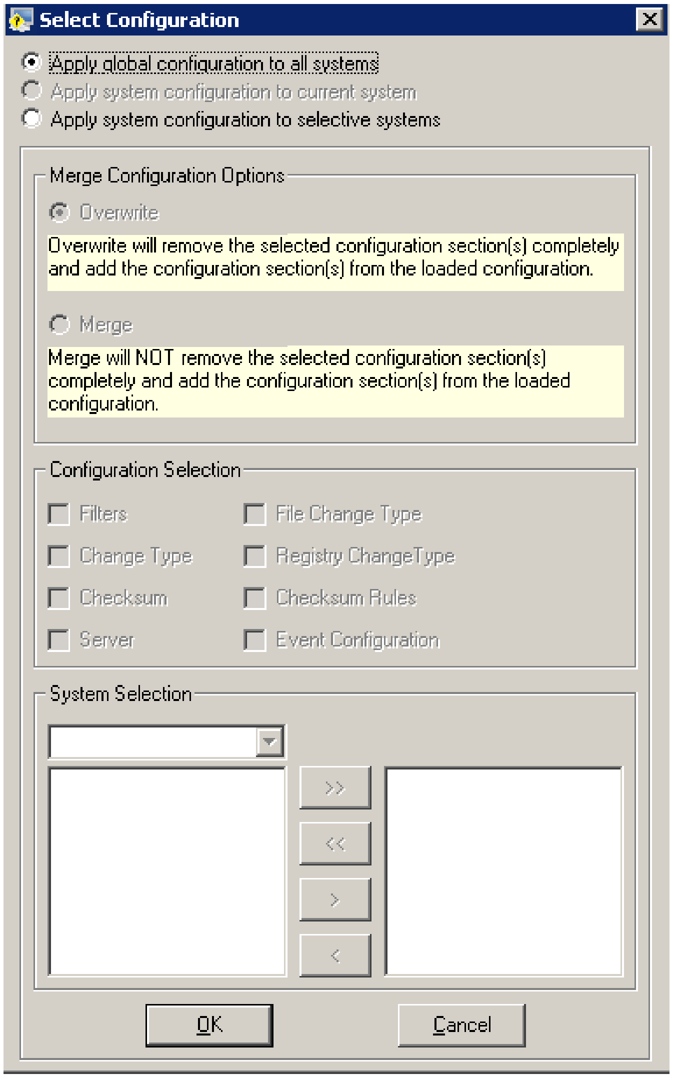
This option helps you to apply the Global Configuration to all the monitored systems.

To apply Global Configuration, follow the steps below:

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 the option to apply global configuration alone.



Select Configuration

● Apply global configuration to all systems
○ Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

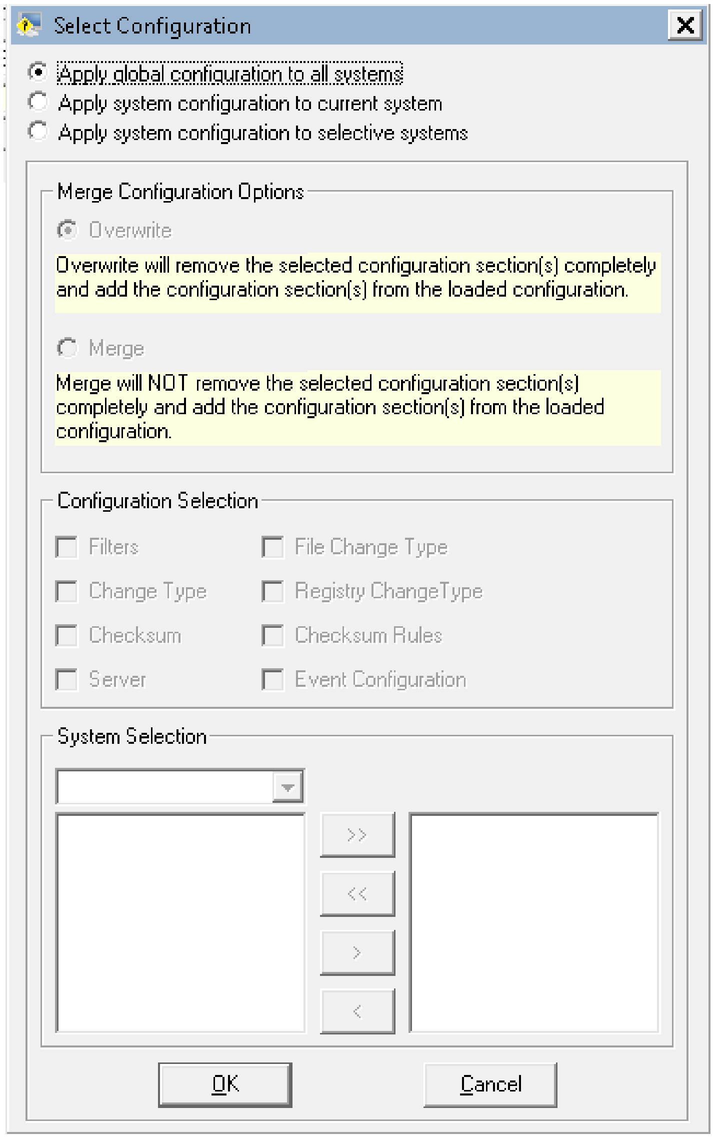
Configuration Selection

□ Filters □ File Change Type
□ Change Type □ Registry ChangeType
□ Checksum □ Checksum Rules
□ Server □ Event Configuration

System Selection

Figure 127

If the selected Computer is a remote system, then EventTracker - Change Audit displays the Select Configuration window with an additional option.



Select Configuration

● Apply global configuration to all systems
○ Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

Configuration Selection

□ Filters □ File Change Type
□ Change Type □ Registry ChangeType
□ Checksum □ Checksum Rules
□ Server □ Event Configuration

System Selection

Figure 128

3. Select the **Apply global configuration to all systems** option and then click **OK**. If you select the **Apply system configuration to the current system** option, then EventTracker - Change Audit is applied to the system configuration to the current system.

4. **Apply system configuration to selected systems** allows the user to apply selected configuration on a group of systems. The **'Merge Configuration Options'** provides the user to overwrite the existing configuration or merge a new configuration with existing configurations. In the '**Configuration**

Selections' pane, select different sections to be applied to the systems. **System Selection** group provides system groups and system list that user can select and apply the configuration.

EventTracker - Change Audit applies the global configuration to all the monitored systems.

5.3 System Configuration

This option helps you set the 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.

Once the filter is set either through System Configuration or Global Configuration, EventTracker - Change Audit will not consider the filtered items for Snapshots.

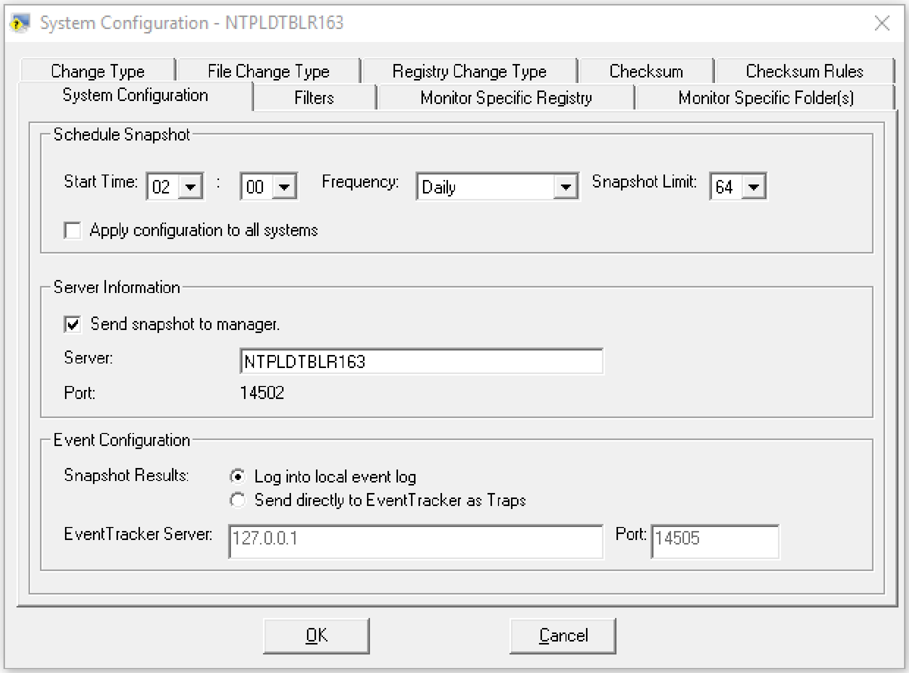
To set up System Configuration, follow the steps below:

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.



Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

□ Apply configuration to all systems

☑ Send snapshot to manager.

Server: NTPLDTBLR163

Port: 14502

Snapshot Results: ● Log into local event log ○ Send directly to EventTracker as Traps

EventTracker Server: 127.0.0.1 Port: 14505

Figure 129

Field	Description
System Configuration	
Start Time	By default, EventTracker - Change Audit selects 2 A.M. 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.
Send Snapshot to manager	Select this checkbox to take back up of snapshot on a manager system.
Server	Provide the server name on which back up of snapshots should be taken.
Snapshot Result	EventTracker - Change Audit client logs the 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’.
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

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

4. To set Filters, refer Filters.

5.3.1 Apply System Configuration – Local System

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

To apply System Configuration to the current system, follow the steps below:

1. Open the Change Browser.

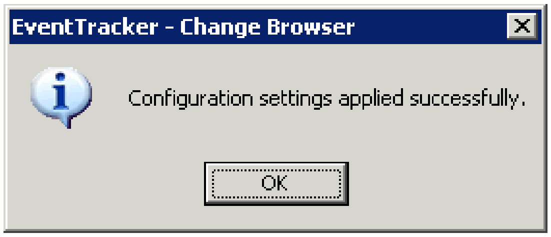
2. On the System Bar, double-click the local computer.

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.



EventTracker - Change Browser

Configuration settings applied successfully.

Figure 130

5. Click **OK**.

5.3.2 Apply System Configuration – Remote Systems

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

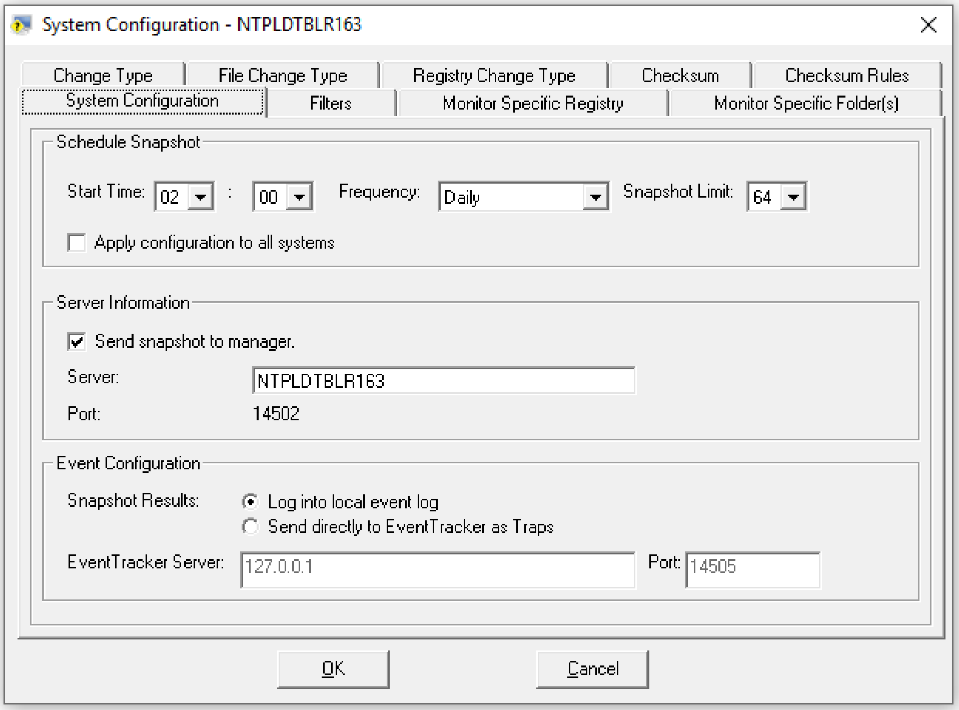
To apply System Configuration to remote systems, follow the steps below:

1. Open the Change Browser.

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

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

   EventTracker - Change Audit displays the System Configuration window.



System Configuration - NTPLDTBLR163

Schedule Snapshot

Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

□ Apply configuration to all systems

Server Information

☑ Send snapshot to manager.

Server: NTPLDTBLR163

Port: 14502

Event Configuration

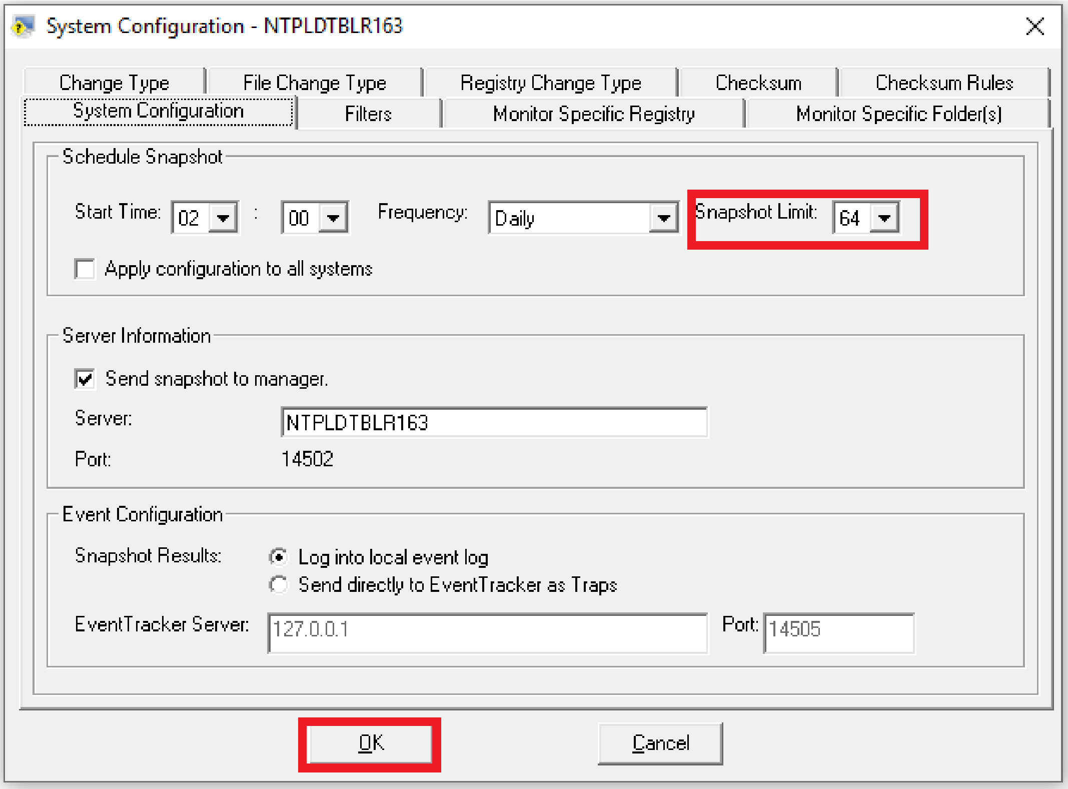
Snapshot Results: ● Log into local event log

○ Send directly to EventTracker as Traps

EventTracker Server: 127.0.0.1 Port: 14505

Figure 131

4. Modify the Snapshot Automation settings and then click **OK**.



System Configuration - NTPLDTBLR163

Schedule Snapshot

Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

□ Apply configuration to all systems

Server Information

☑ Send snapshot to manager.

Server: NTPLDTBLR163

Port: 14502

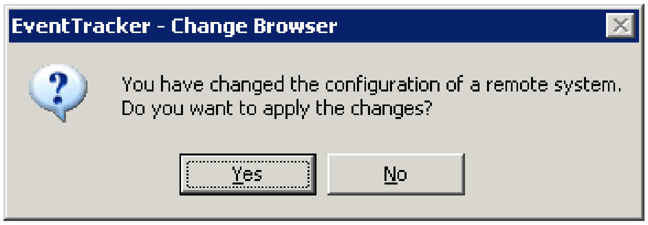
Event Configuration

Snapshot Results: ● Log into local event log ○ Send directly to EventTracker as Traps

EventTracker Server: 127.0.0.1 Port: 14505

Figure 132

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



EventTracker - Change Browser

You have changed the configuration of a remote system.
Do you want to apply the changes?

Figure 133

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.

5.3.3 Apply System Configuration – All Systems

This option helps you apply Snapshot settings to all systems.

To apply System Configuration to all systems, follow the steps below:

1. Open the Change Browser.

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

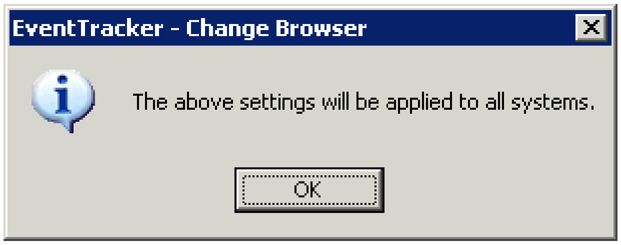
3. Click the **Options** menu and select the **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.

4. Modify the Snapshot Automation settings.

5. Select the **Apply configuration to all systems** check box.

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



EventTracker - Change Browser

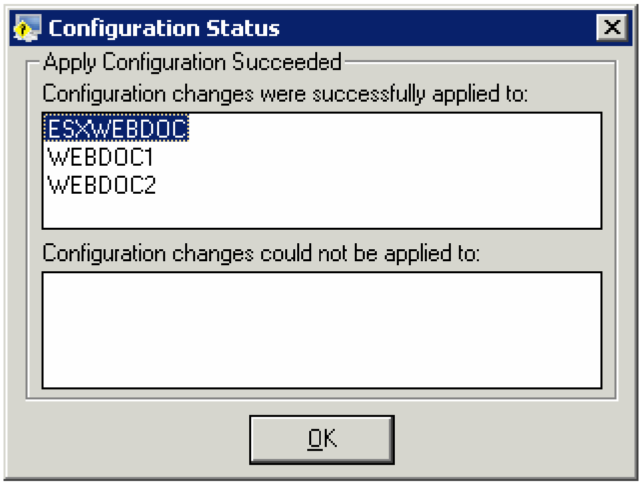
The above settings will be applied to all systems.

Figure 134

6. Click **OK**.

7. Click **OK** on the System Configuration window.

   EventTracker - Change Audit displays the Configuration Status window.



Configuration Status

Apply Configuration Succeeded

Configuration changes were successfully applied to:

ESXWEBDOC
WEBDOC1
WEBDOC2

Configuration changes could not be applied to:

Figure 135

8. Click **OK**.

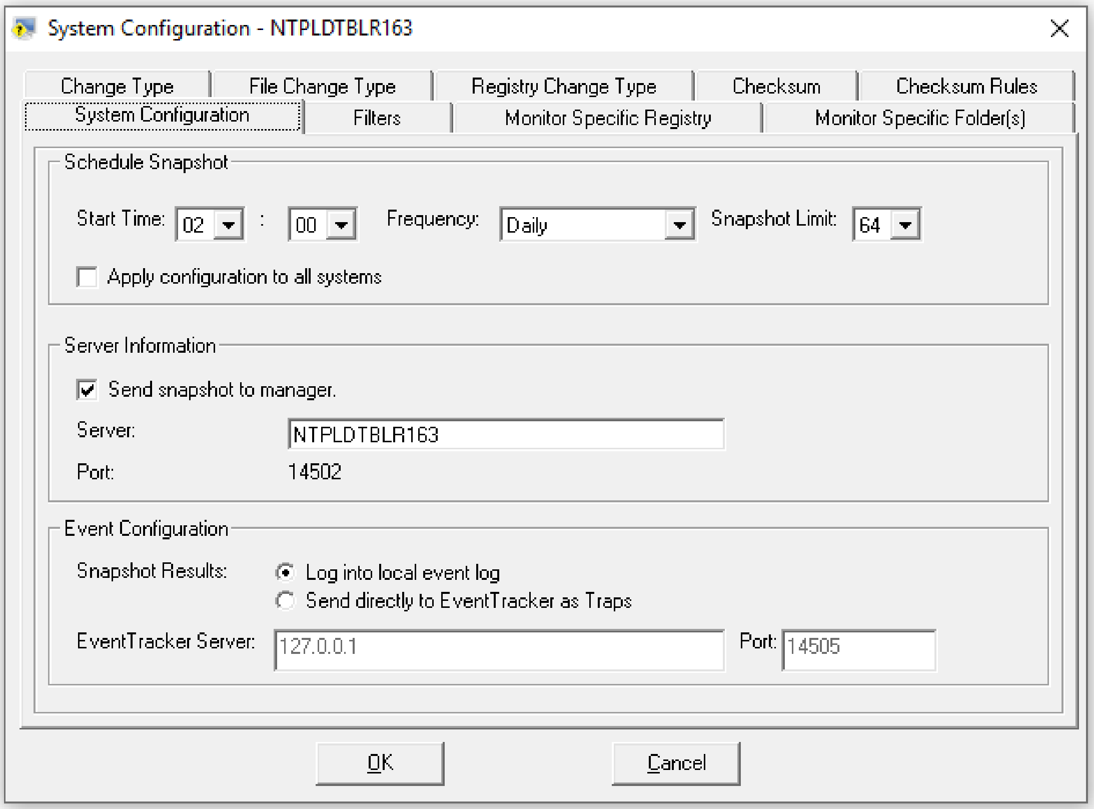
5.4 Search the Change Events (EventTracker Search Interface)

5.4.1 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 **System Configuration** option.

   EventTracker - Change Audit displays the System Configuration window.



System Configuration - NTPLDTBLR163

Schedule Snapshot

Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

☐ Apply configuration to all systems

Server Information

☑ Send snapshot to manager.

Server: NTPLDTBLR163

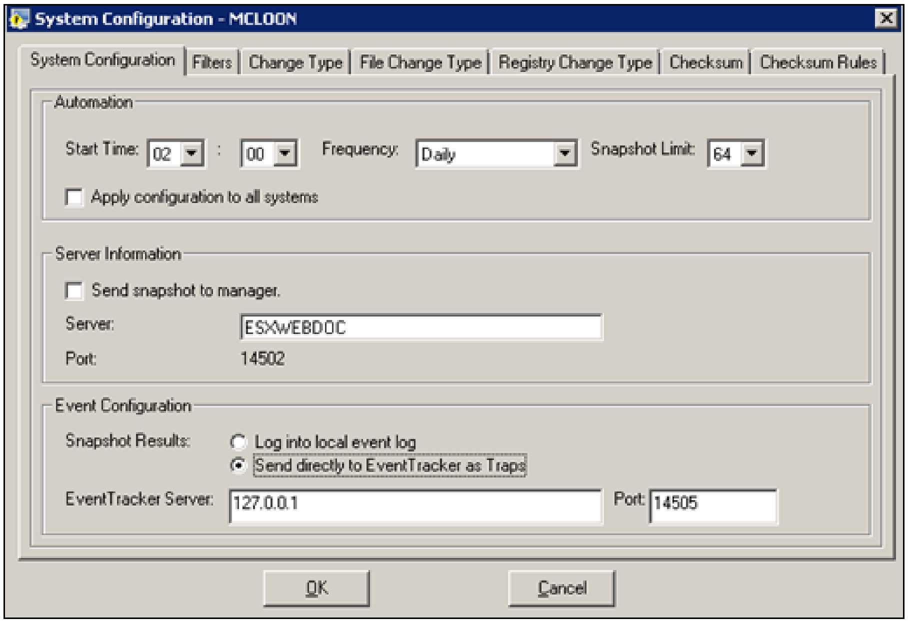
Port: 14502

Event Configuration

Snapshot Results: ● Log into local event log ○ Send directly to EventTracker as Traps

EventTracker Server: 127.0.0.1 Port: 14505

Figure 136



Automation

Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

□ Apply configuration to all systems

Server Information

□ Send snapshot to manager.

Server: ESXWEBDOC

Port: 14502

Event Configuration

Snapshot Results: ○ Log into local event log

● Send directly to EventTracker as Traps

EventTracker Server: 127.0.0.1 Port: 14505

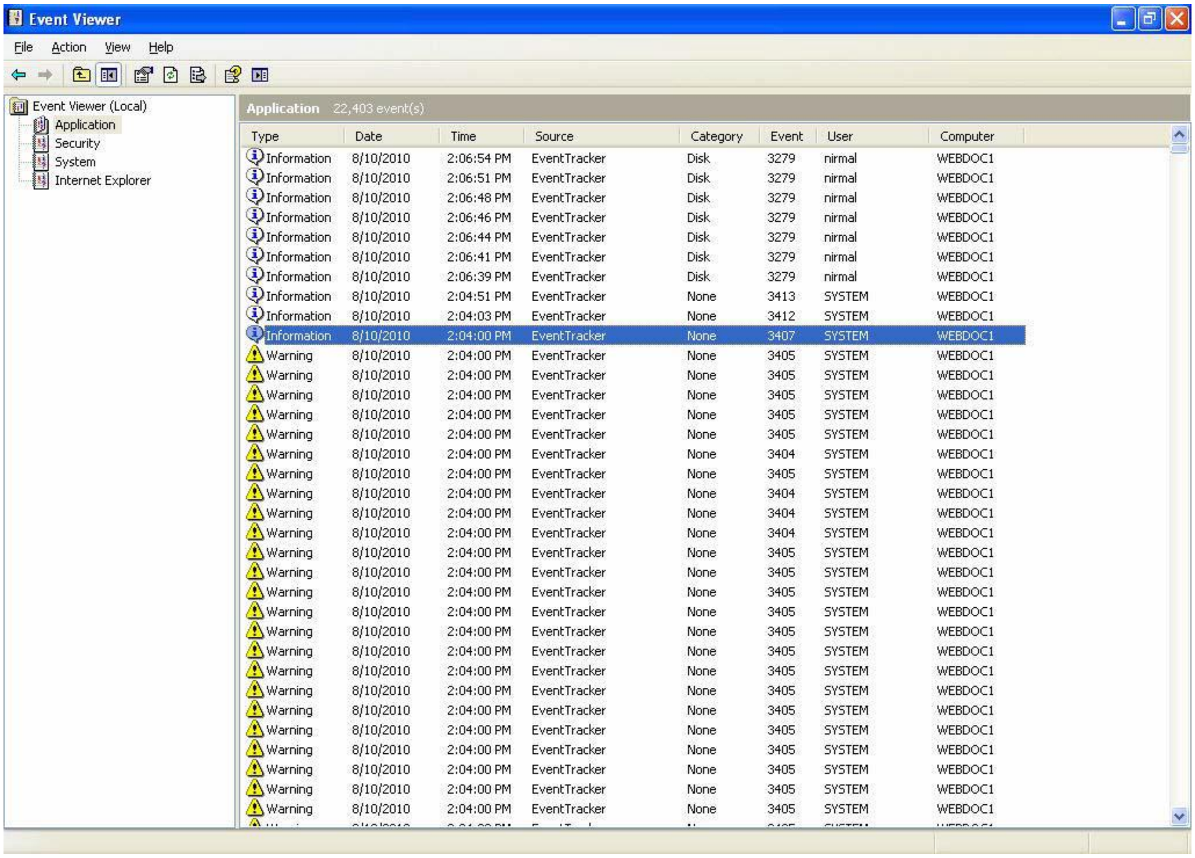
Figure 137

Field	Description
Snapshot Results: Change Audit client logs the 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’.	
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

Field	Description
	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.

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

4. Open the Event Viewer to view Change Audit events.

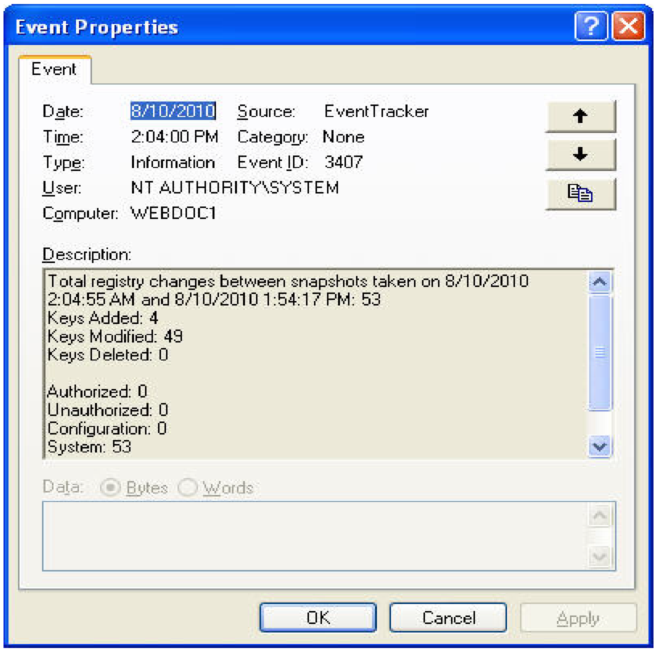


Application 22,403 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Information	8/10/2010	2:06:54 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:51 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:48 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:46 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:44 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:41 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:06:39 PM	EventTracker	Disk	3279	nirmal	WEBDOC1
Information	8/10/2010	2:04:51 PM	EventTracker	None	3413	SYSTEM	WEBDOC1
Information	8/10/2010	2:04:03 PM	EventTracker	None	3412	SYSTEM	WEBDOC1
Information	8/10/2010	2:04:00 PM	EventTracker	None	3407	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1
Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1

Figure 138

5. Double-click an event in the right pane to view event properties.



Date: 8/10/2010 Source: EventTracker
Time: 2:04:00 PM Category: None
Type: Information Event ID: 3407
User: NT AUTHORITY\SYSTEM
Computer: WEBDOC1

Description:

Total registry changes between snapshots taken on 8/10/2010
2:04:55 AM and 8/10/2010 1:54:17 PM: 53
Keys Added: 4
Keys Modified: 49
Keys Deleted: 0

Authorized: 0
Unauthorized: 0
Configuration: 0
System: 53

Figure 139

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.

5.5 Generating 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 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.

12. Crosscheck Report cost details.

13. Crosscheck Report details and then click **Generate Report**.

6. 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.

6.1 Normal Filters

Adding a normal filter does not remove the filtered node from the snapshots i.e. the changes detected so far is 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 contains the changes that were detected before it was filtered, and the changes detected since it has been unfiltered.

6.2 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.

6.3 Difference between Customized Filters and Normal Filters

Normal Filter	Customized Filter
This can be applied at both the levels system level as well as global level.	This can only be added at the global level.
This can only be added when the complete path of a file or registry system object is known.	This can be added even if a substring within the path of file or registry system is known.
Adding a normal filter does not remove the filtered node from	When we declare a customized filter, it

Normal Filter	Customized Filter
the snapshots i.e. the changes detected so far is retained; it only stops monitoring any changes in the object from the time it is filtered.	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.

6.3.1 Demonstration

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

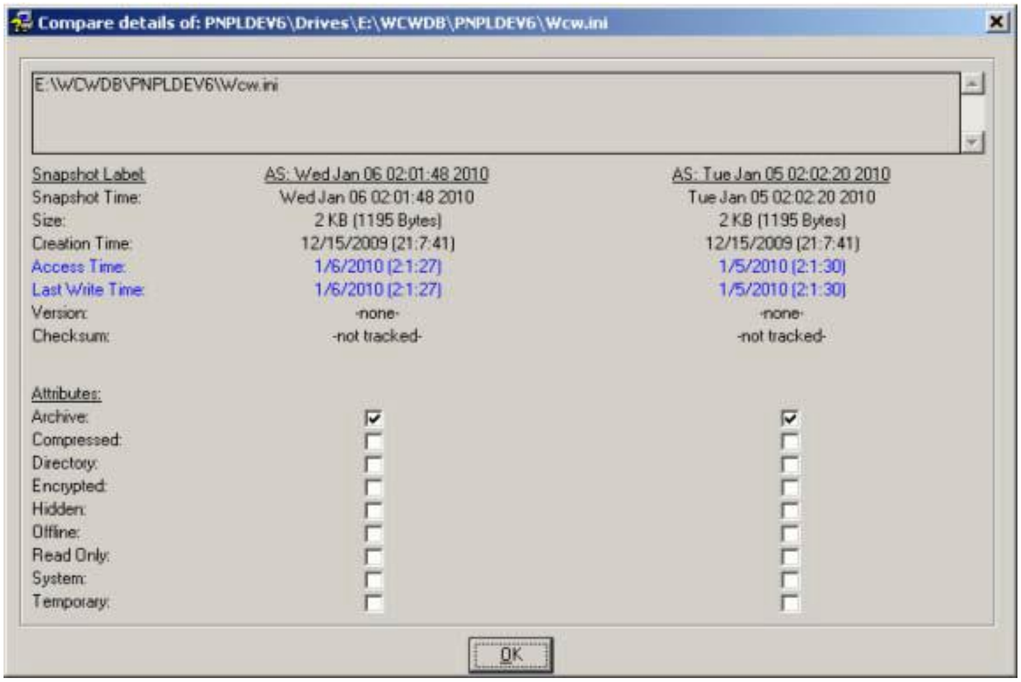
2. Add a customized filter to filter the file “E:\WCWDB\PNPLDEV6\wcw.ini’.

   Note: 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

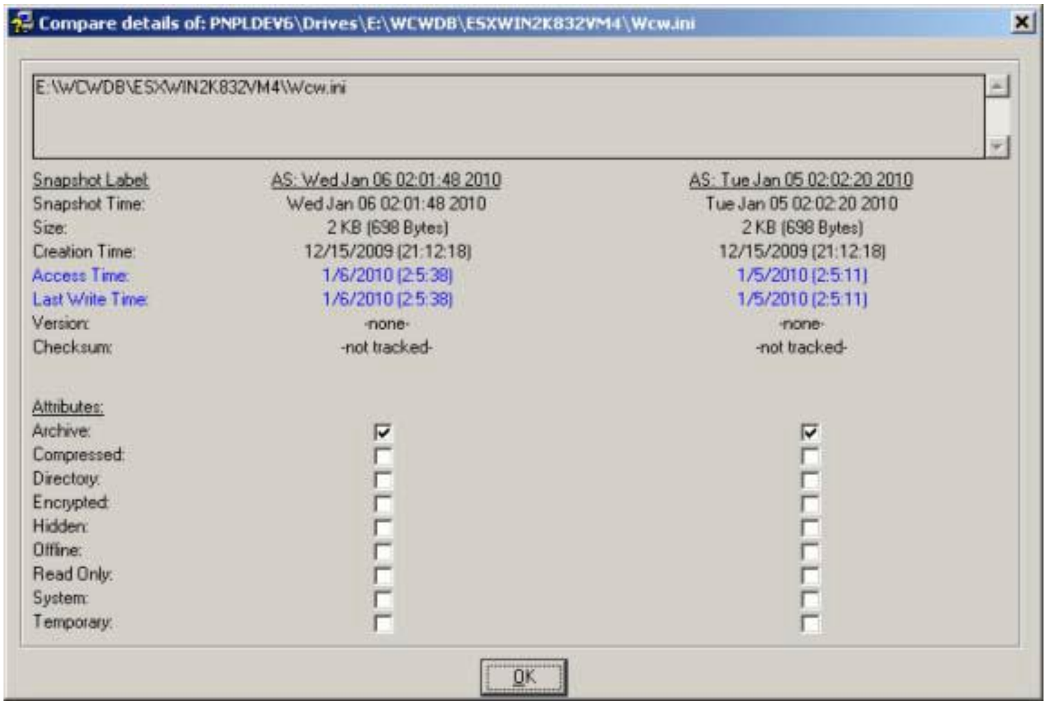


Compare details of: PNPLDEV6\Drives\E:\WCWDB\PNPLDEV6\Wcw.ini

E:\WCWDB\PNPLDEV6\Wcw.ini

Snapshot Label:	AS: Wed Jan 06 02:01:48 2010	AS: Tue Jan 05 02:02:20 2010
Snapshot Time:	Wed Jan 06 02:01:48 2010	Tue Jan 05 02:02:20 2010
Size:	2 KB (1195 Bytes)	2 KB (1195 Bytes)
Creation Time:	12/15/2009 (21:7:41)	12/15/2009 (21:7:41)
Access Time:	1/6/2010 (2:1:27)	1/5/2010 (2:1:30)
Last Write Time:	1/6/2010 (2:1:27)	1/5/2010 (2:1:30)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	☐	☐
Directory:	☐	☐
Encrypted:	☐	☐
Hidden:	☐	☐
Offline:	☐	☐
Read Only:	☐	☐
System:	☐	☐
Temporary:	☐	☐

Figure 140



Compare details of: PNPLDEV6\Drives\E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

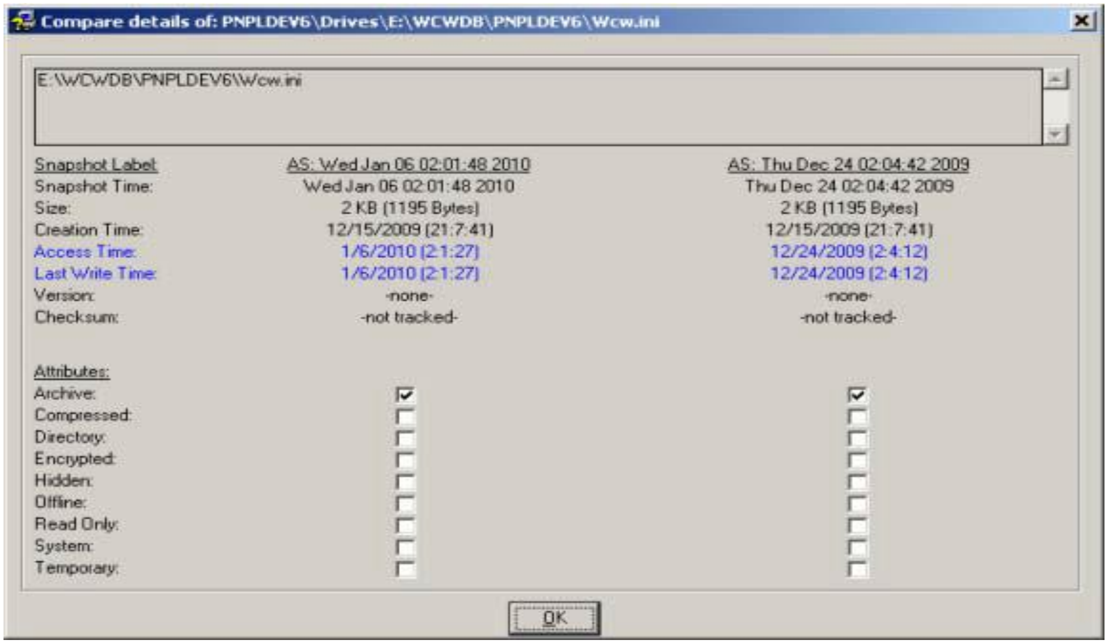
Snapshot Label:	AS: Wed Jan 06 02:01:48 2010	AS: Tue Jan 05 02:02:20 2010
Snapshot Time:	Wed Jan 06 02:01:48 2010	Tue Jan 05 02:02:20 2010
Size:	2 KB (698 Bytes)	2 KB (698 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (2:5:38)	1/5/2010 (2:5:11)
Last Write Time:	1/6/2010 (2:5:38)	1/5/2010 (2:5:11)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	☐	☐
Directory:	☐	☐
Encrypted:	☐	☐
Hidden:	☐	☐
Offline:	☐	☐
Read Only:	☐	☐
System:	☐	☐
Temporary:	☐	☐

Figure 141

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

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

Baseline Snapshot: 2009-12-24T02:04:42

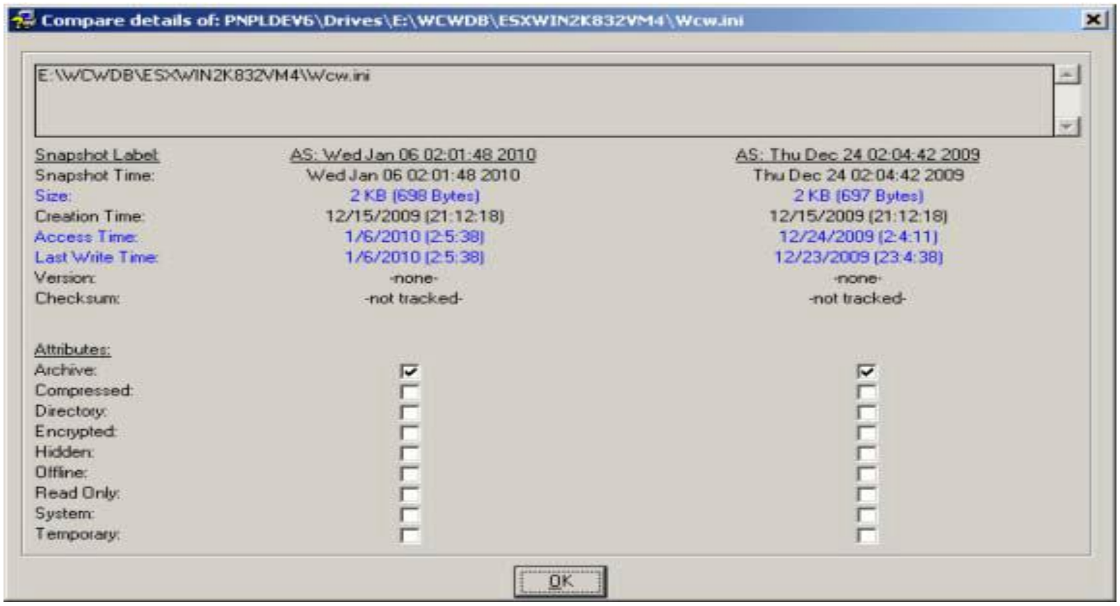


Compare details of: PNPLDEV6\Drives\E:\WCWDB\PNPLDEV6\Wcw.ini

E:\WCWDB\PNPLDEV6\Wcw.ini

Snapshot Label	AS: Wed Jan 06 02:01:48 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 02:01:48 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (1195 Bytes)	2 KB (1195 Bytes)
Creation Time:	12/15/2009 (21:7:41)	12/15/2009 (21:7:41)
Access Time:	1/6/2010 (2:1:27)	12/24/2009 (2:4:12)
Last Write Time:	1/6/2010 (2:1:27)	12/24/2009 (2:4:12)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 142



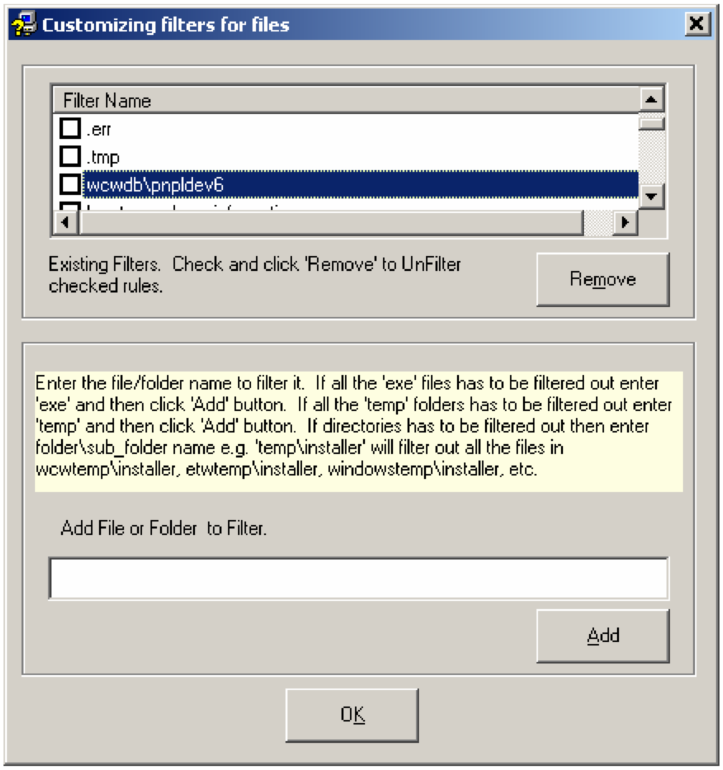
Compare details of: PNPLDEV6\Drives\E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

Snapshot Label	AS: Wed Jan 06 02:01:48 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 02:01:48 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (698 Bytes)	2 KB (697 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (2:5:38)	12/24/2009 (2:4:11)
Last Write Time:	1/6/2010 (2:5:38)	12/23/2009 (23:4:38)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 143

3. Add a customized filter to filter the folder “wcwdb\pnpldev6’.



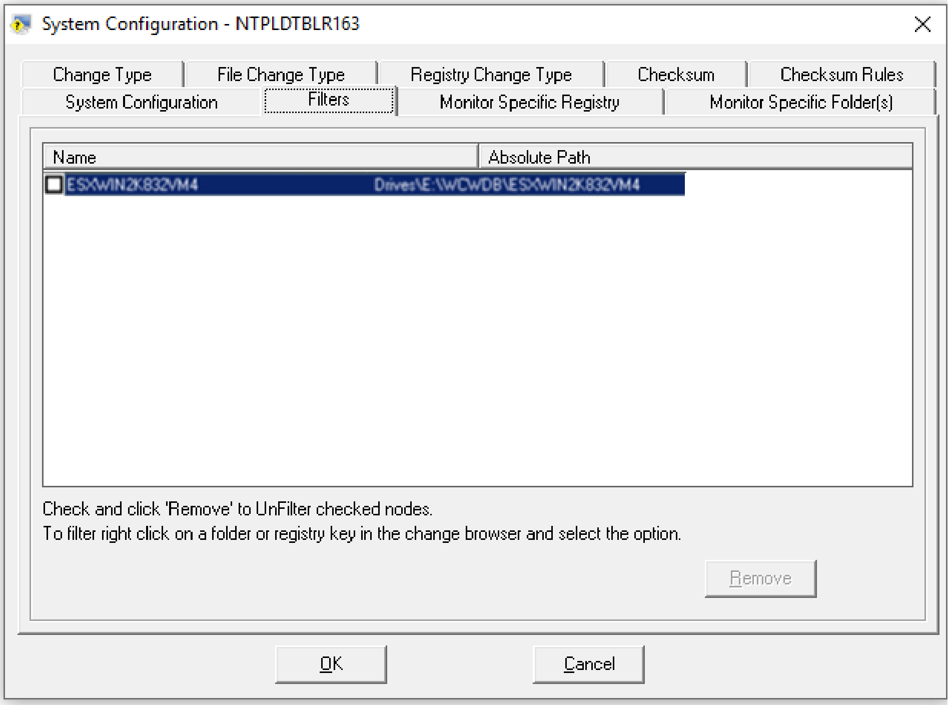
Existing Filters. Check and click 'Remove' to UnFilter checked rules.

Enter the file/folder name to filter it. If all the 'exe' files has to be filtered out enter 'exe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter 'temp' and then click 'Add' button. If directories has to be filtered out then enter folder\sub_folder name e.g. 'temp\installer' will filter out all the files in wcwtemp\installer, etwtemp\installer, windowstemp\installer, etc.

Add File or Folder to Filter.

Figure 144

4. Add a Normal filter to filter the folder “E:\WCWDB\ESXWIN2k832VM4\’.



Name	Absolute Path
□ ESXWIN2K832VM4	Drives\E:\WCWDB\ESXWIN2K832VM4

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 145

5. Make changes to the two files and take a new snapshot after adding the two filters.

   Neither of the file is reported as changed.

   Note 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.

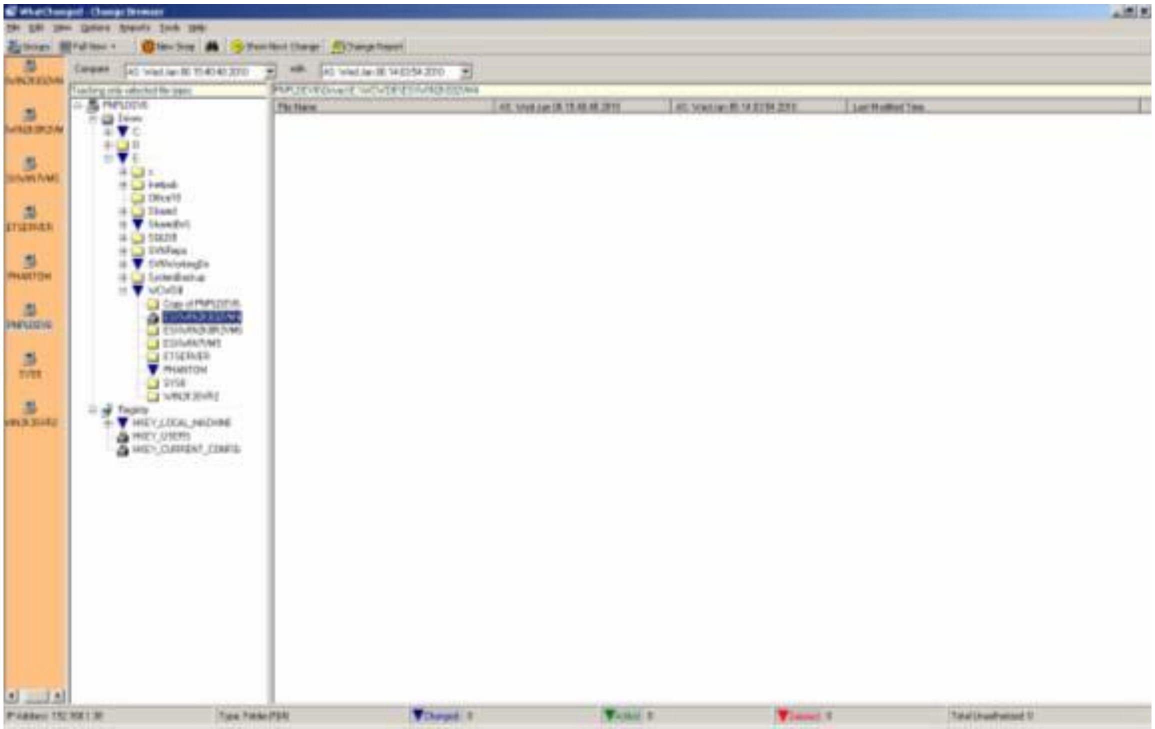


Figure 146

6. Remove both the filters and take a new snapshot.

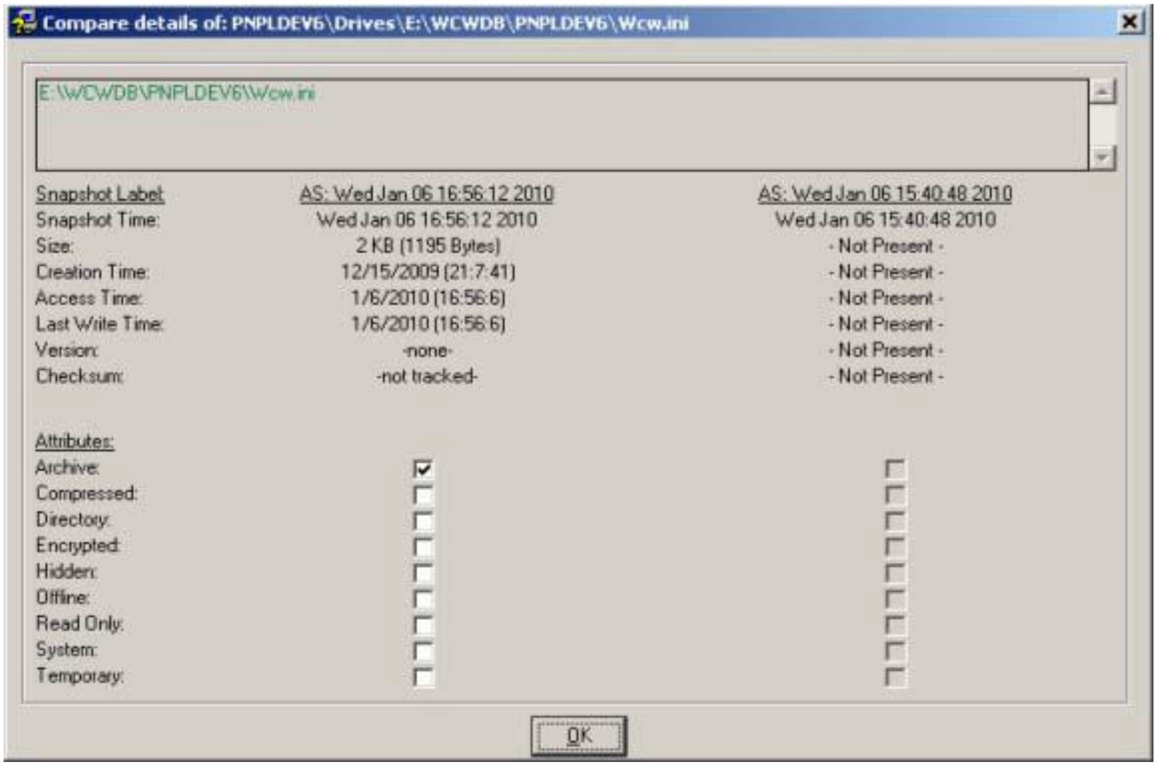
   The following screenshots display the properties of both the files after taking the snapshot without the filters.

   Note 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

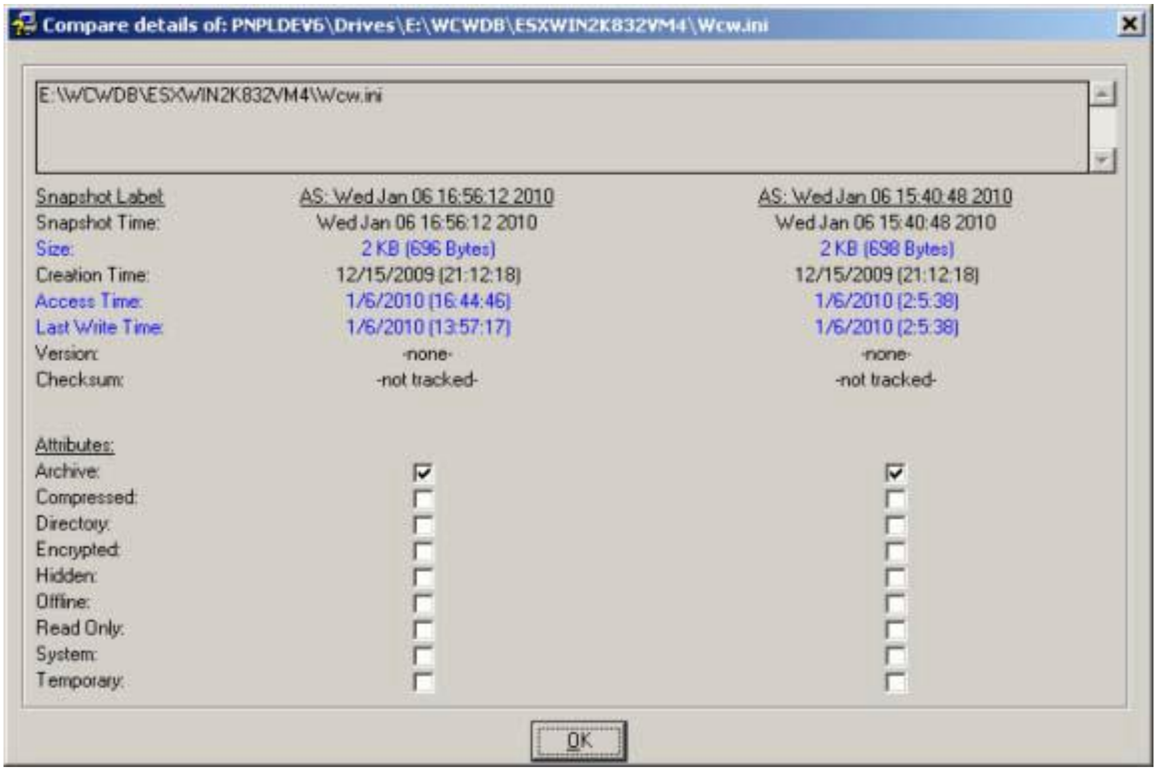


Compare details of: PNPLDEV6\Drives\E:\WCWDB\PNPLDEV6\Wcw.ini

E:\WCWDB\PNPLDEV6\Wcw.ini

Snapshot Label	AS: Wed Jan 06 16:56:12 2010	AS: Wed Jan 06 15:40:48 2010
Snapshot Time:	Wed Jan 06 16:56:12 2010	Wed Jan 06 15:40:48 2010
Size:	2 KB (1195 Bytes)	- Not Present -
Creation Time:	12/15/2009 (21:7:41)	- Not Present -
Access Time:	1/6/2010 (16:56:6)	- Not Present -
Last Write Time:	1/6/2010 (16:56:6)	- Not Present -
Version:	-none-	- Not Present -
Checksum:	-not tracked-	- Not Present -
Attributes:		
Archive:	☑	□
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 147



Compare details of: PNPLDEV6\Drives\E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

Snapshot Label	AS: Wed Jan 06 16:56:12 2010	AS: Wed Jan 06 15:40:48 2010
Snapshot Time:	Wed Jan 06 16:56:12 2010	Wed Jan 06 15:40:48 2010
Size:	2 KB (696 Bytes)	2 KB (698 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (16:44:46)	1/6/2010 (2:5:38)
Last Write Time:	1/6/2010 (13:57:17)	1/6/2010 (2:5:38)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

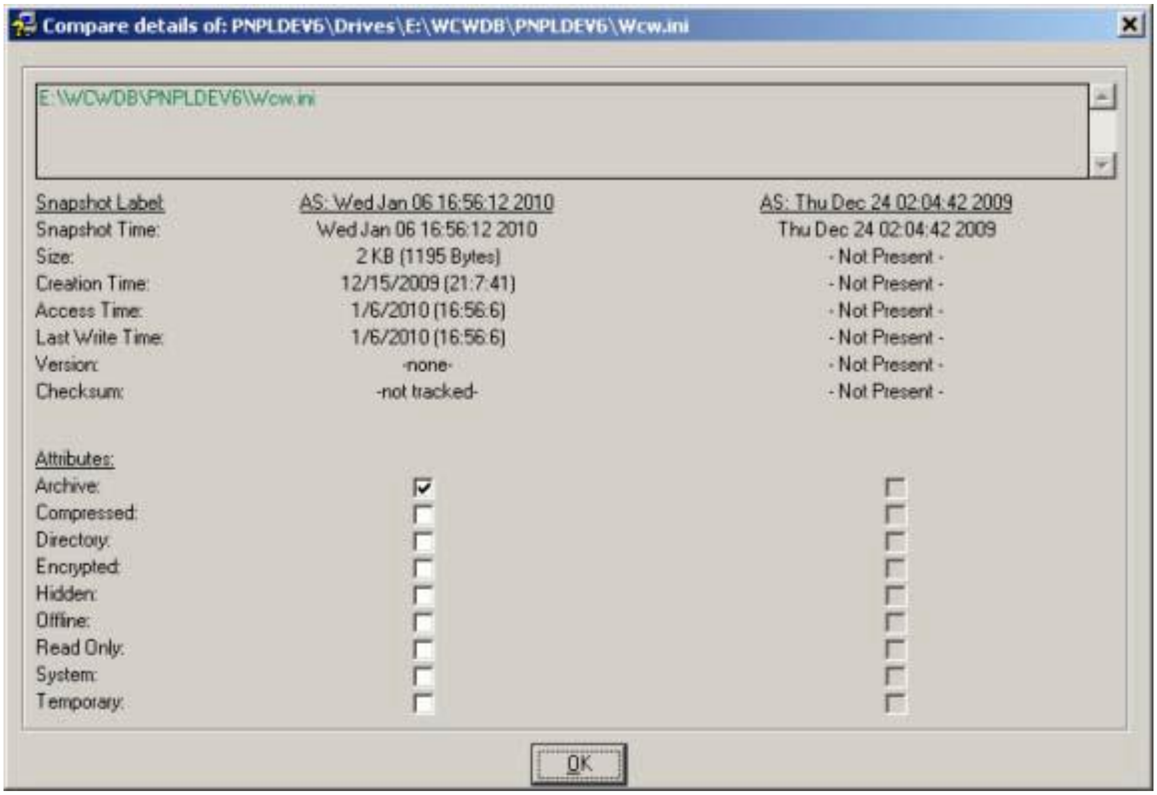
Figure 148

The following screenshots display the properties (with respect to baseline snapshot) of 2 files “E:\WCWDB\PNPLDEV6\wcw.in’ and “E:\WCWDB\ESXWIN2k832VM4\wcw.ini’ after removing both the filters.

Note 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

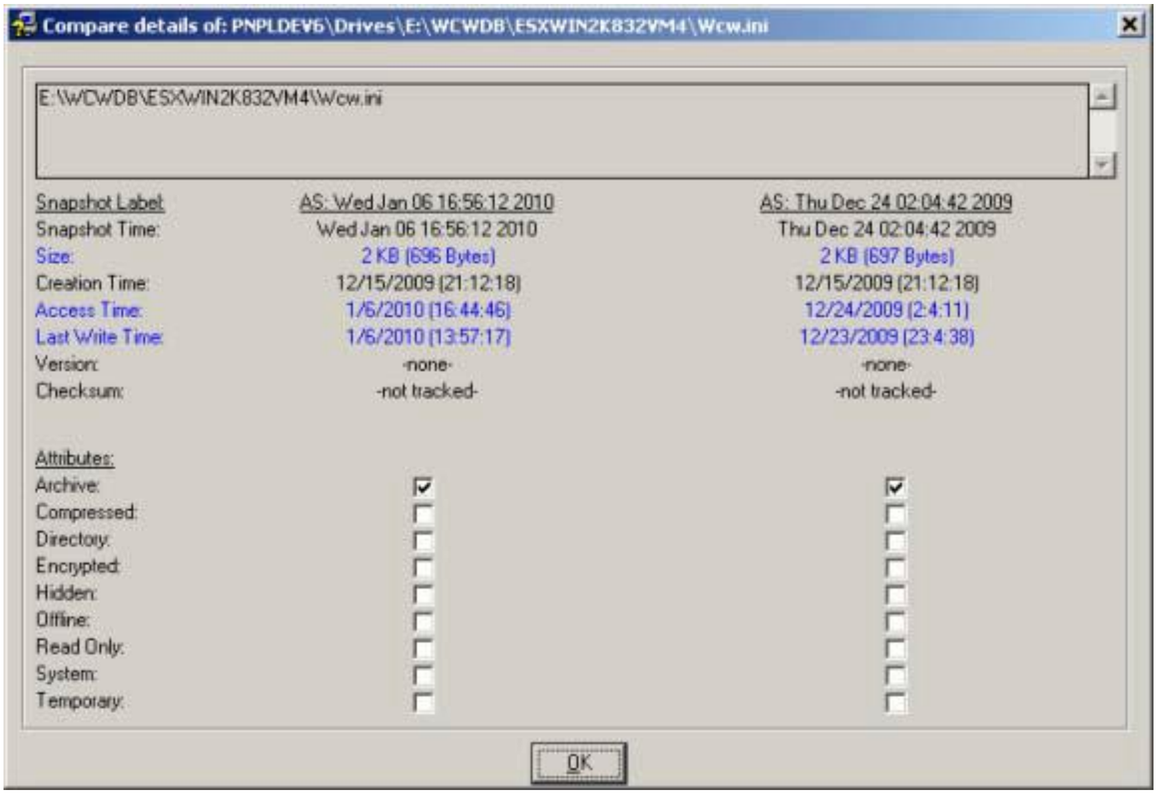


Compare details of: PNPLDEV6\Drives\E:\WCWDB\PNPLDEV6\Wcw.ini

E:\WCWDB\PNPLDEV6\Wcw.ini

Snapshot Label	AS: Wed Jan 06 16:56:12 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 16:56:12 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (1195 Bytes)	- Not Present -
Creation Time:	12/15/2009 (21:7:41)	- Not Present -
Access Time:	1/6/2010 (16:56:6)	- Not Present -
Last Write Time:	1/6/2010 (16:56:6)	- Not Present -
Version:	-none-	- Not Present -
Checksum:	-not tracked-	- Not Present -
Attributes:		
Archive:	☑	□
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 149



Compare details of: PNPLDEV6\Drives\E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

E:\WCWDB\ESXWIN2K832VM4\Wcw.ini

Snapshot Label	AS: Wed Jan 06 16:56:12 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 16:56:12 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (696 Bytes)	2 KB (697 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (16:44:46)	12/24/2009 (2:4:11)
Last Write Time:	1/6/2010 (13:57:17)	12/23/2009 (23:4:38)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	☑	☑
Compressed:	□	□
Directory:	□	□
Encrypted:	□	□
Hidden:	□	□
Offline:	□	□
Read Only:	□	□
System:	□	□
Temporary:	□	□

Figure 150

6.3.2 Customize Filters

This option helps you customize filters.

To customize filters, follow the steps below:

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)

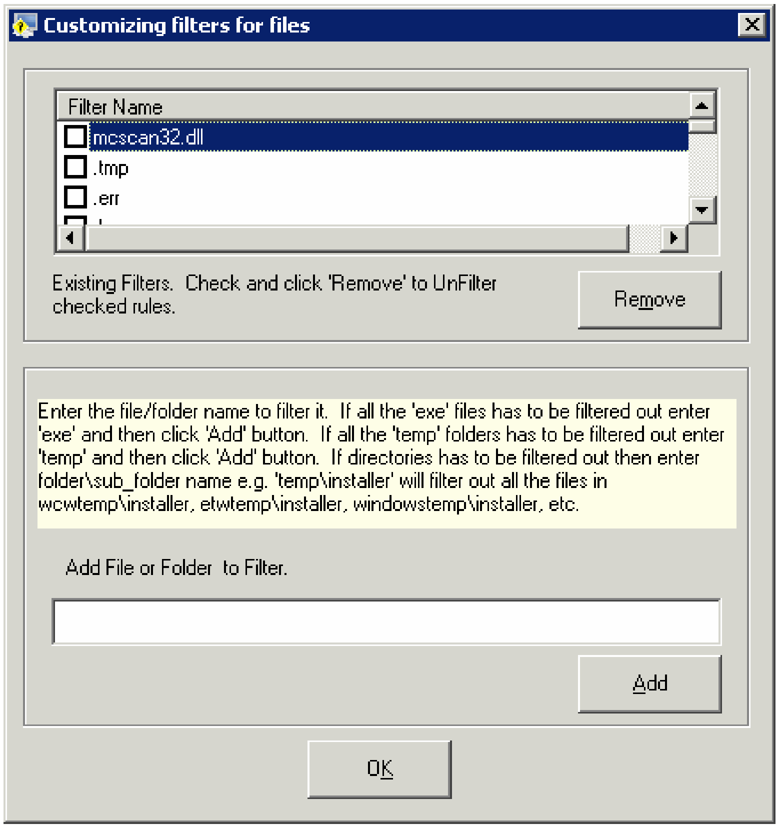
   Expand the Drives or Registry trees.

   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 the files window.



Customizing filters for files

Filter Name
□ mcscan32.dll
□ .tmp
□ .err

Existing Filters. Check and click 'Remove' to UnFilter checked rules.

Enter the file/folder name to filter it. If all the 'exe' files has to be filtered out enter 'exe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter 'temp' and then click 'Add' button. If directories has to be filtered out then enter folder\sub_folder name e.g. 'temp\installer' will filter out all the files in wcwtemp\installer, etwtemp\installer, windowstemp\installer, etc.

Add File or Folder to Filter.

Figure 151

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.

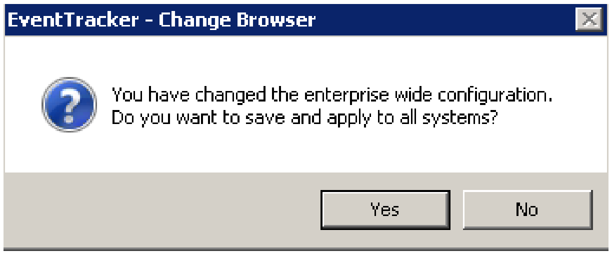
5. Click **OK**.

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**.



You have changed the enterprise wide configuration.
Do you want to save and apply to all systems?

Figure 152

9. Click **Yes**.

6.4 Apply Filters option– Local System

This option helps you apply filters to the local system.

To apply filters to the local system, follow the steps below:

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**.

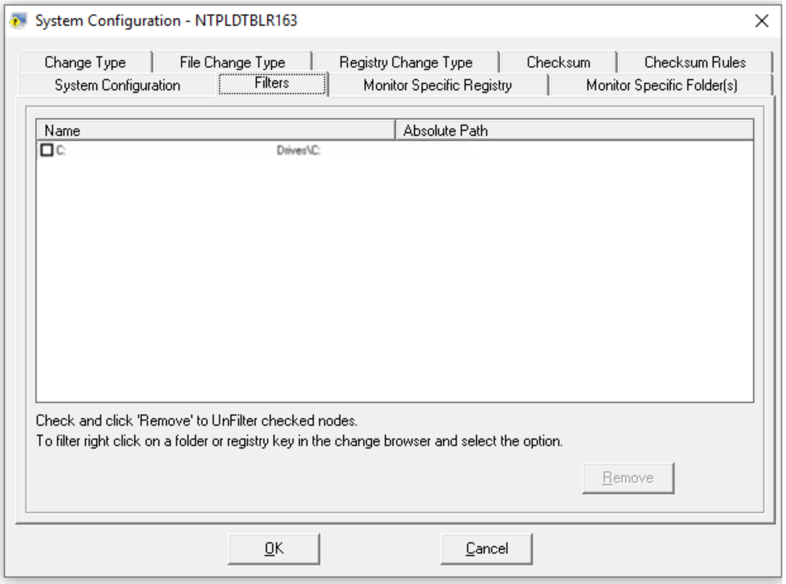
   EventTracker - Change Audit filters the selected drive.

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.



Name	Absolute Path
□ C:	Drives\C:

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 153

6.5 Apply Filters option – Remote Systems

This option helps you apply filters to the remote system.

To apply filters to the remote system, follow the steps below:

1. Open the Change Browser.

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

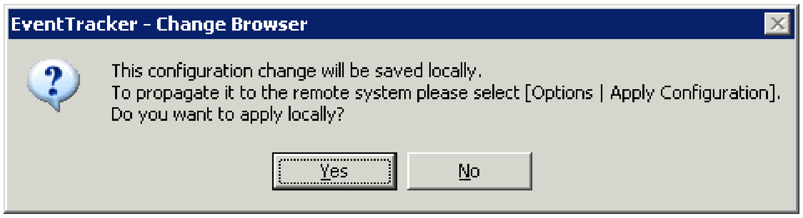
3. Right-click any item under Drives or Registry trees.

   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.



This configuration change will be saved locally.
To propagate it to the remote system please select [Options | Apply Configuration].
Do you want to apply locally?

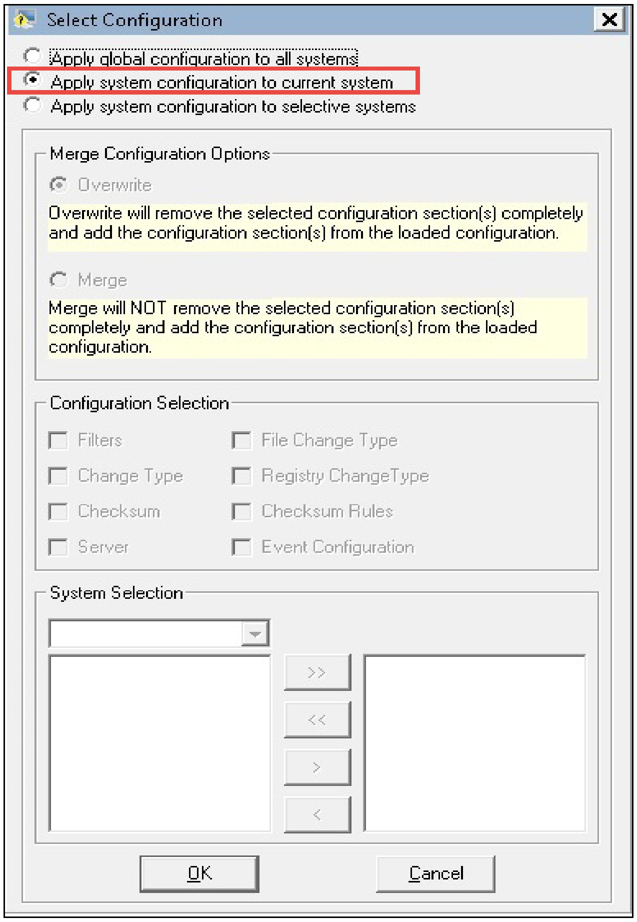
Figure 154

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.



Select Configuration

○ Apply global configuration to all systems
● Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

Configuration Selection

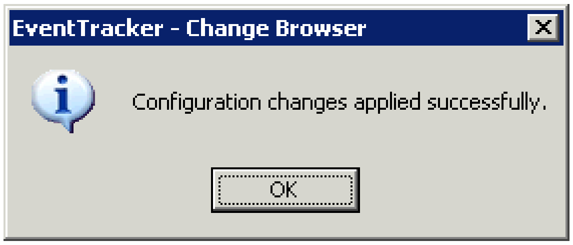
□ Filters □ File Change Type
□ Change Type □ Registry ChangeType
□ Checksum □ Checksum Rules
□ Server □ Event Configuration

System Selection

Figure 155

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

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



EventTracker - Change Browser

Configuration changes applied successfully.

Figure 156

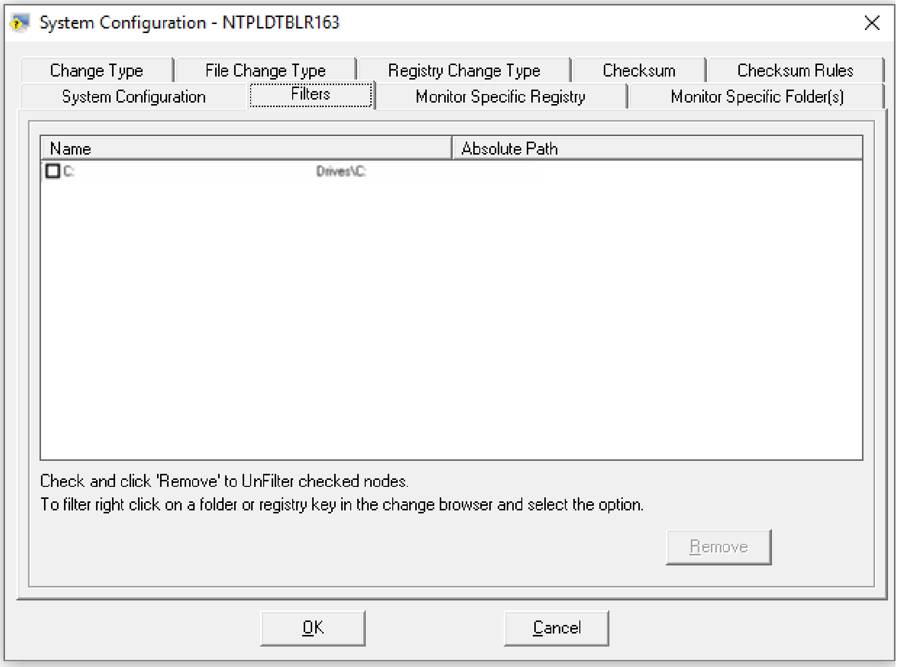
7. Click **OK**.

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.



Name	Absolute Path
□ C:	Drives\C:

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 157

6.6 Apply Filters option – All Systems

This option helps you apply filters to all systems.

To apply filters to all systems, follow the steps below:

1. Open the Change Browser.

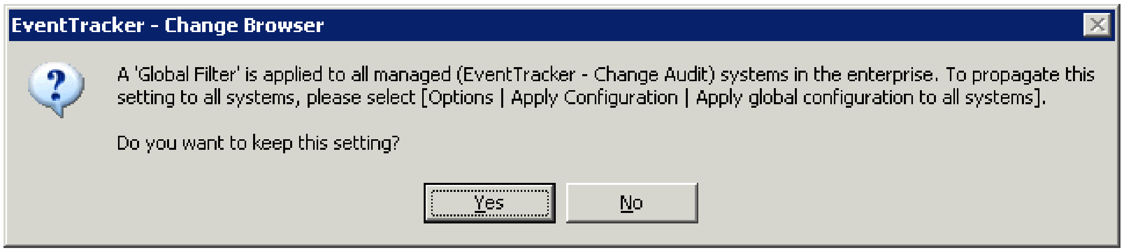
2. Double-click any Computer on the System Bar.

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.


EventTracker - Change Browser

A 'Global Filter' is applied to all managed (EventTracker - Change Audit) systems in the enterprise. To propagate this setting to all systems, please select [Options | Apply Configuration | Apply global configuration to all systems].

Do you want to keep this setting?

Figure 158

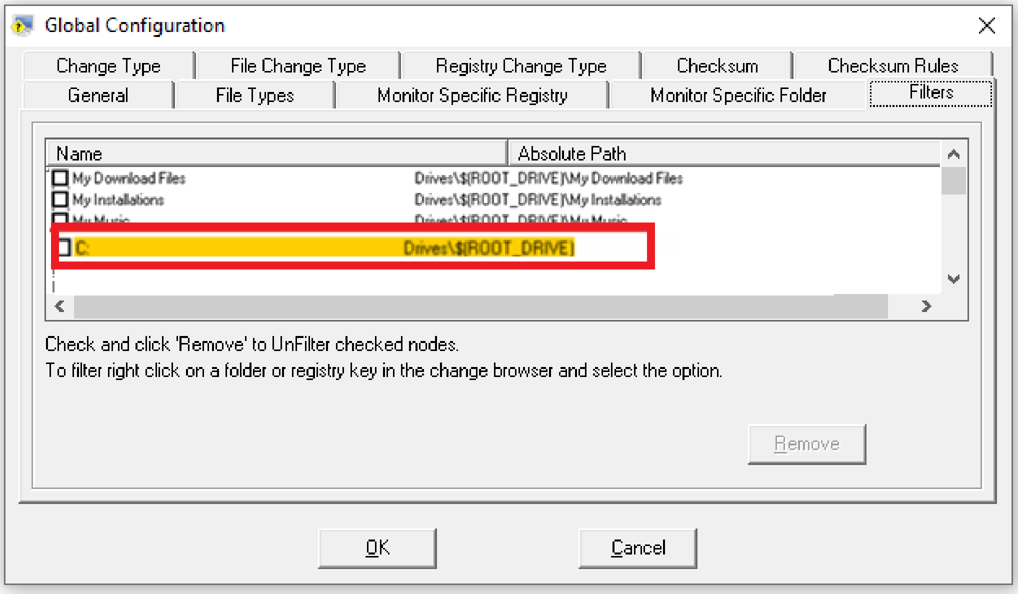
4. Click **Yes** to proceed.

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.


Global Configuration

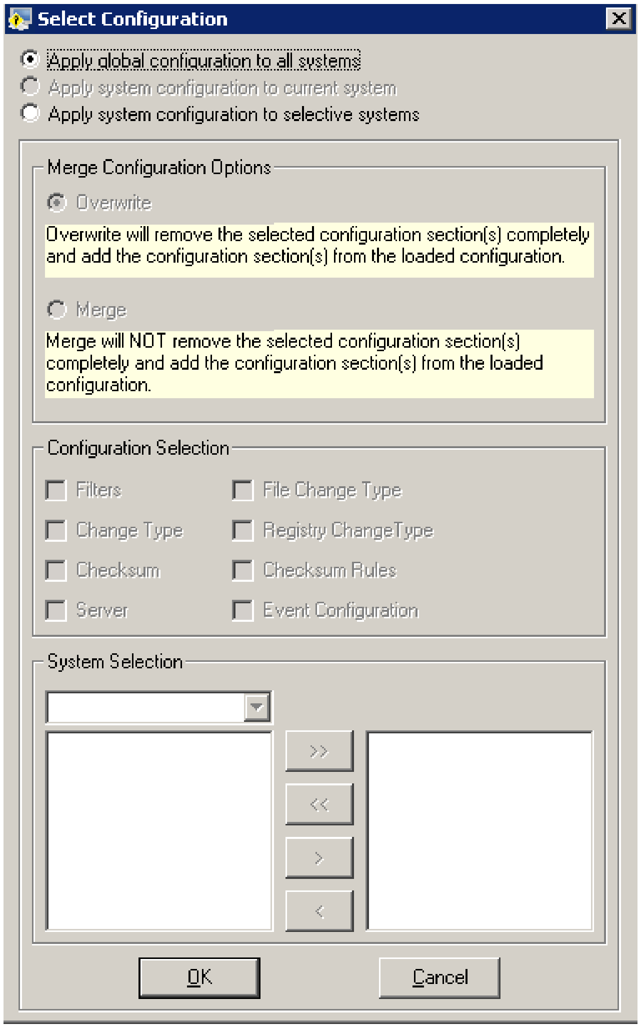
Name	Absolute Path
□ My Download Files	Drives\$(ROOT_DRIVE)\My Download Files
□ My Installations	Drives\$(ROOT_DRIVE)\My Installations
□ My Music	Drives\$(ROOT_DRIVE)\My Music
□ C:	Drives\$(ROOT_DRIVE)

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 159

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

● Apply global configuration to all systems
○ Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

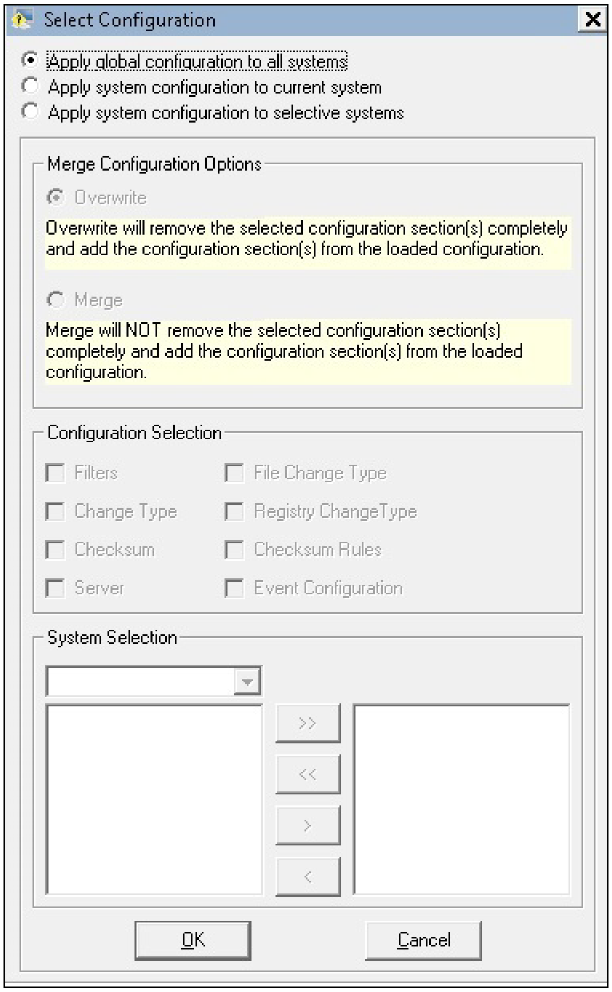
Configuration Selection

□ Filters
□ Change Type
□ Checksum
□ Server
□ File Change Type
□ Registry ChangeType
□ Checksum Rules
□ Event Configuration

System Selection

Figure 160

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



Select Configuration

● Apply global configuration to all systems
○ Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

Configuration Selection

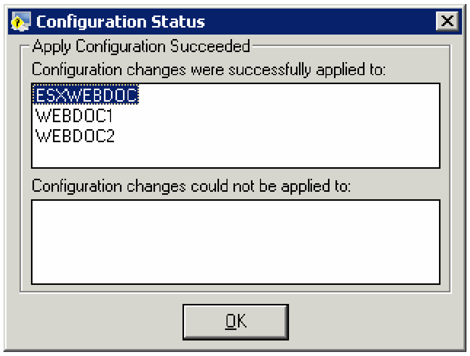
□ Filters □ File Change Type
□ Change Type □ Registry ChangeType
□ Checksum □ Checksum Rules
□ Server □ Event Configuration

System Selection

Figure 161

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.



Configuration Status

Apply Configuration Succeeded

Configuration changes were successfully applied to:

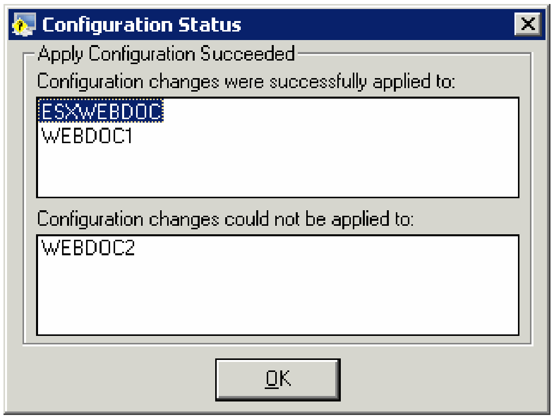
ESXWEBDOC
WEBDOC1
WEBDOC2

Configuration changes could not be applied to:

Figure 162

9. Click **OK**.

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



Apply Configuration Succeeded

Configuration changes were successfully applied to:

ESXWEBDOC
WEBDOC1

Configuration changes could not be applied to:

WEBDOC2

Figure 163

10. Double-click the remote system on the System Bar.

    EventTracker - Change Audit displays the remote system with the filtered drive.

6.7 Remove Filters option – Local System

This option helps you remove filters from the local system.

To remove filters in the local system, follow the steps below:

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.

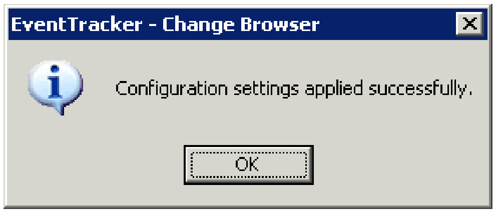
   Click the **Filters** tab.

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.



Configuration settings applied successfully.

Figure 164

Click **OK**.

6.8 Remove Filters – Remote Systems

This option helps you remove filters from remote systems.

To remove filters in remote systems, follow the steps below:

1. Open the Change Browser.

2. Double-click the remote computer on the System Bar for which you want to remove filters.

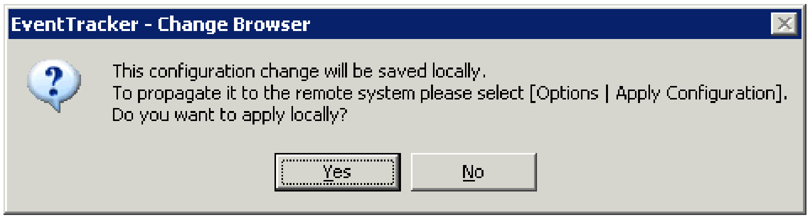
3. Right-click the drive.

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.



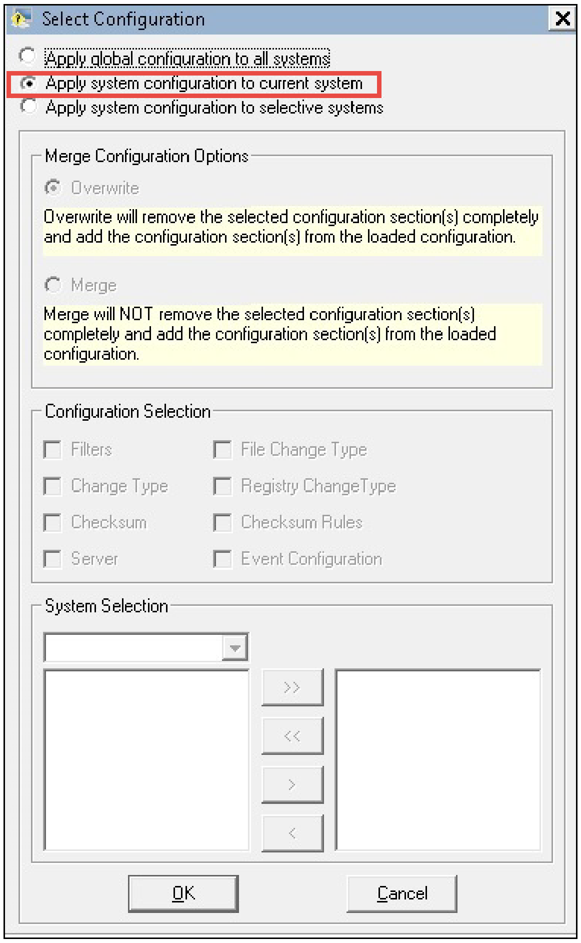
This configuration change will be saved locally.
To propagate it to the remote system please select [Options | Apply Configuration].
Do you want to apply locally?

Figure 165

4. Click **Yes**.

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

   EventTracker - Change Audit displays the Select Configuration window.



Select Configuration

○ Apply global configuration to all systems
● Apply system configuration to current system
○ Apply system configuration to selective systems

Merge Configuration Options

● Overwrite

Overwrite will remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

○ Merge

Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration.

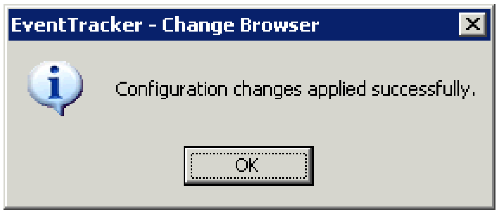
Configuration Selection

□ Filters □ File Change Type
□ Change Type □ Registry ChangeType
□ Checksum □ Checksum Rules
□ Server □ Event Configuration

Figure 166

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

   EventTracker - Change Audit displays the message box.



EventTracker - Change Browser

Configuration changes applied successfully.

Figure 167

7. Click **OK**.

EventTracker - Change Audit un-filters the selected drive.

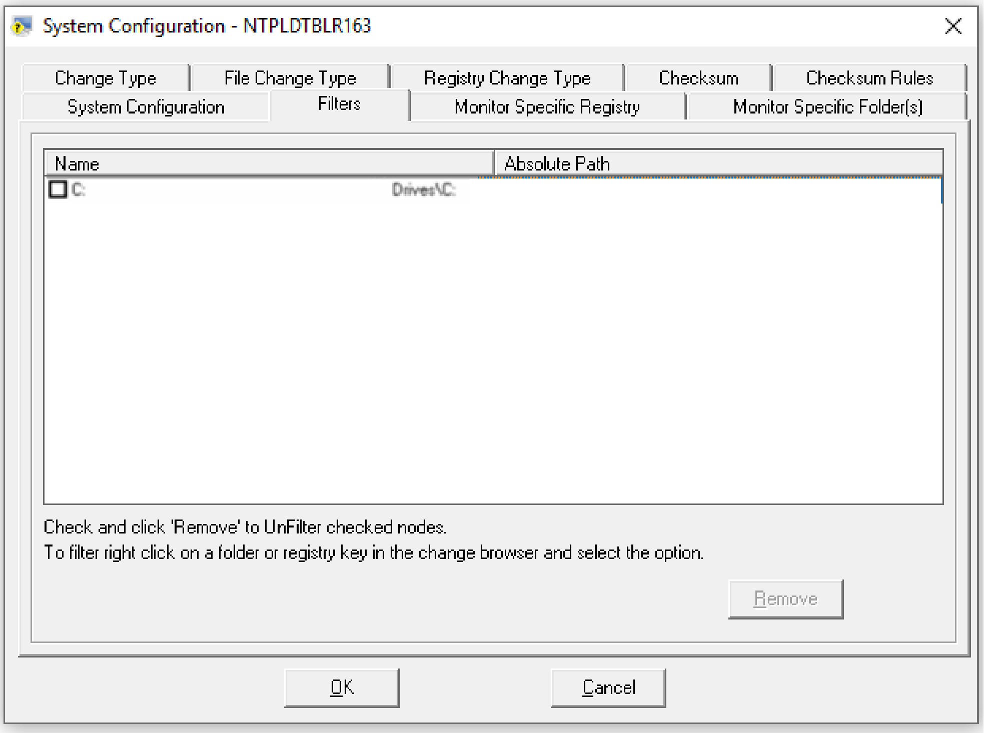
(OR)

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.



Name	Absolute Path
□ C:	Drives\C:

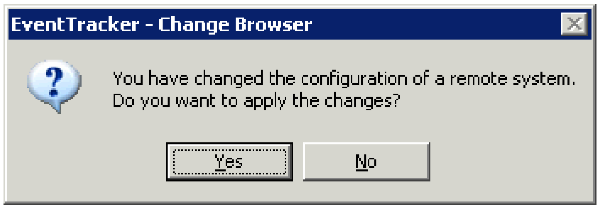
Check and click 'Remove' to UnFilter checked nodes.
To filter right click on a folder or registry key in the change browser and select the option.

Figure 168

9. Select the check box against the drive and then click **Remove**.

10. Click **OK**.

    EventTracker - Change Audit displays the confirmation message box.

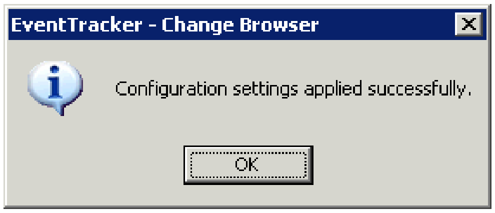


You have changed the configuration of a remote system.
Do you want to apply the changes?

Figure 169

11. Click **Yes**.

    EventTracker - Change Audit displays the message box.



EventTracker - Change Browser

Configuration settings applied successfully.

Figure 170

12. Click **OK**.

    EventTracker - Change Audit un-filters the selected drive.

6.9 Remove Filters – All Systems

This option helps you remove filters in all systems.

To remove filters in all systems, follow the steps below:

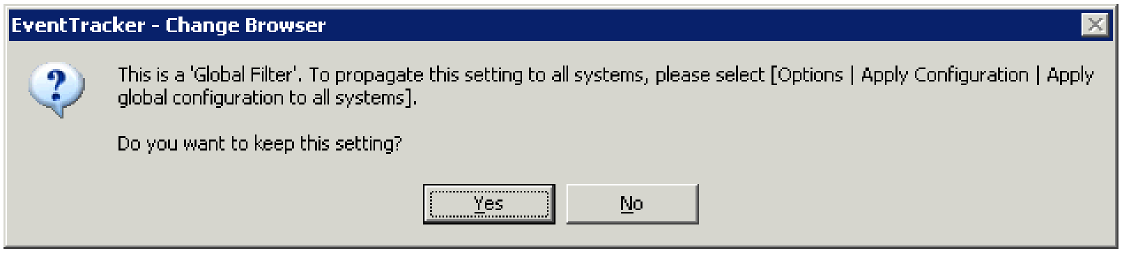
1. Open the Change Browser.

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.



EventTracker - Change Browser

This is a 'Global Filter'. To propagate this setting to all systems, please select [Options | Apply Configuration | Apply global configuration to all systems].

Do you want to keep this setting?

Figure 171

4. Click **Yes**.

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

6.10 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 the 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.

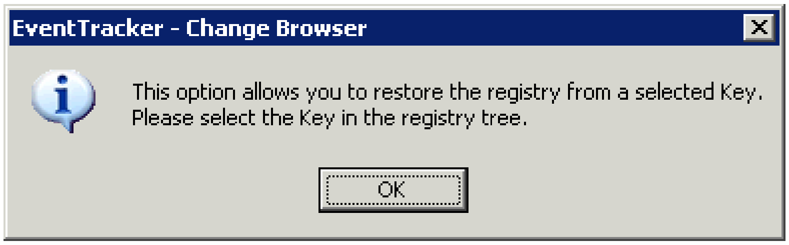
To restore registry sub tree, follow the steps below:

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.

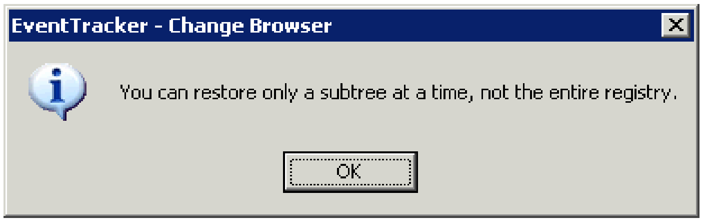


EventTracker - Change Browser

This option allows you to restore the registry from a selected Key.
Please select the Key in the registry tree.

Figure 172

EventTracker - Change Audit displays the EventTracker - Change Audit message box, had you tried to restore the entire registry.



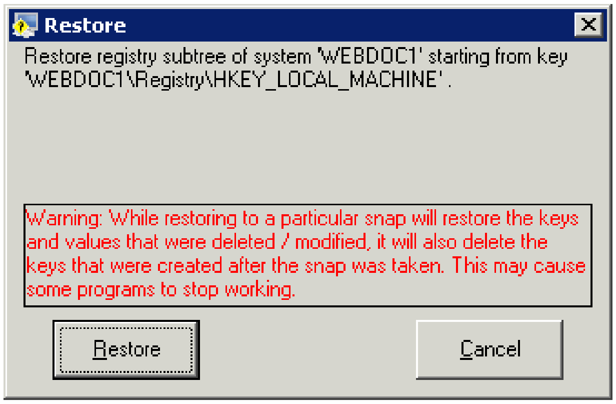
EventTracker - Change Browser

You can restore only a subtree at a time, not the entire registry.

Figure 173

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.



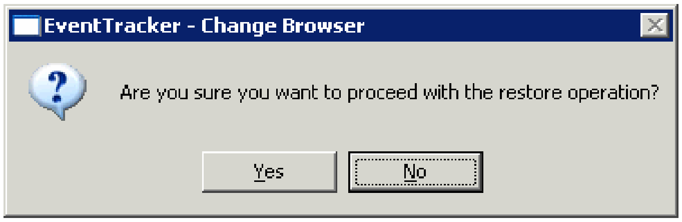
Restore registry subtree of system 'WEBDOC1' starting from key 'WEBDOC1\Registry\HKEY_LOCAL_MACHINE' .

Warning: While restoring to a particular snap will restore the keys and values that were deleted / modified, it will also delete the keys that were created after the snap was taken. This may cause some programs to stop working.

Figure 174

6. Click **Restore**.

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



Are you sure you want to proceed with the restore operation?

Figure 175

7. Click **Yes** to continue.

   EventTracker - Change Audit displays the Restore status.

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

6.11 Restore Logs

This option helps you view the restore logs.

To view restore logs, follow the steps below:

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 an appropriate message if no log exists.

6.12 Undo Restore

This option helps you undo the registry key restore.

To undo the restore, follow the steps below:

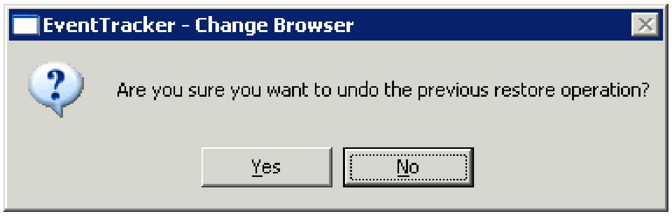
1. Open the Change Browser.

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.

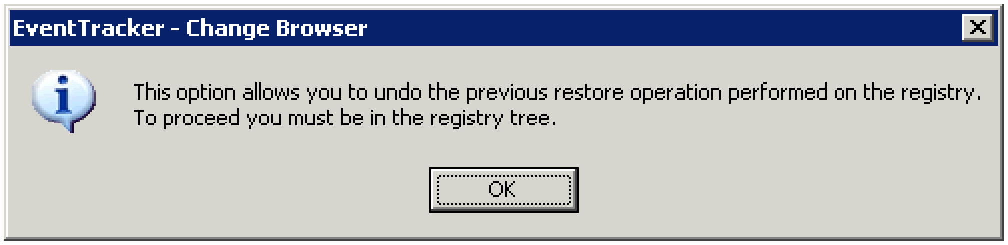


EventTracker - Change Browser

Are you sure you want to undo the previous restore operation?

Figure 176

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



EventTracker - Change Browser

This option allows you to undo the previous restore operation performed on the registry.
To proceed you must be in the registry tree.

Figure 177

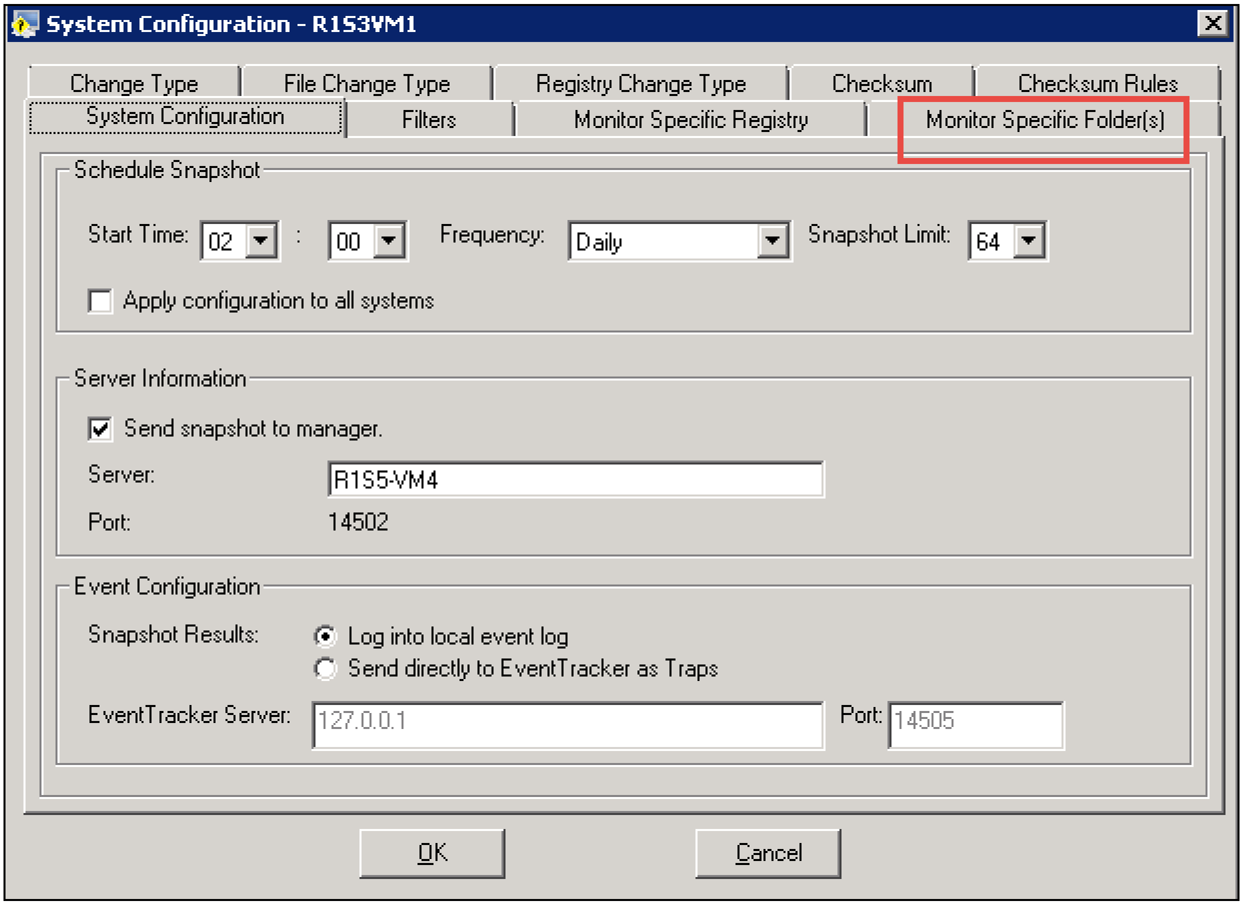
5. Click **Yes** to continue.

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

6.13 Support for monitoring a specific folder on the system

6.13.1 Process after applying the Update

1. In Change Audit, Click the **Change Browser** option.
2. Click the **Options** dropdown and select **System Configuration** .



Schedule Snapshot

Start Time: 02 : 00 Frequency: Daily Snapshot Limit: 64

□ Apply configuration to all systems

Server Information

☑ Send snapshot to manager.

Server: R1S5-VM4

Port: 14502

Event Configuration

Snapshot Results: ● Log into local event log
○ Send directly to EventTracker as Traps

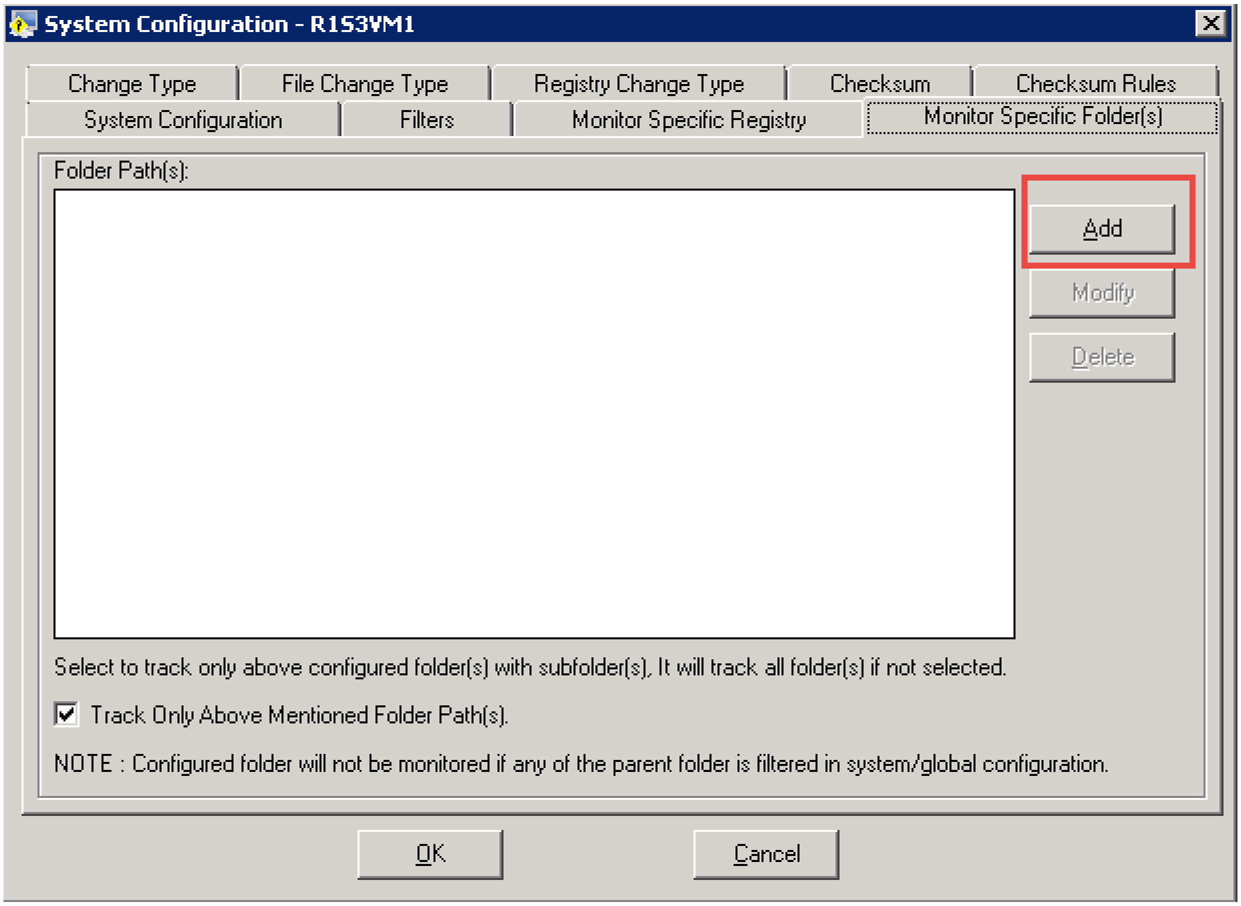
EventTracker Server: 127.0.0.1 Port: 14505

Figure 178

3. The new tab Monitor Specific Folder(s) is added.

Using this option, the user can monitor any specific folder(s) from a system.

4. Click the **Monitor Specific Folder(s)** and select the **Add** button to add folders**.**



Select to track only above configured folder(s) with subfolder(s), It will track all folder(s) if not selected.

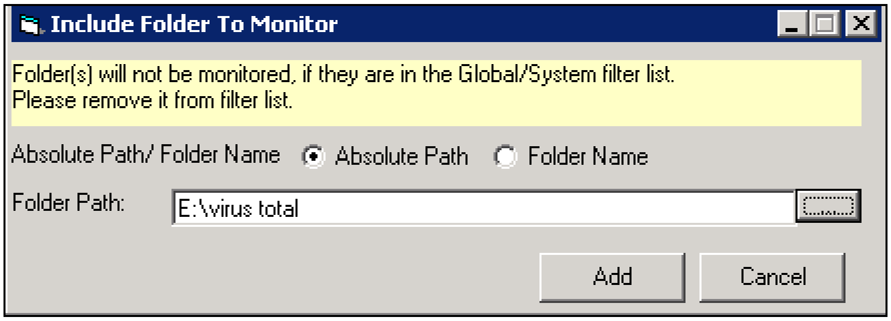
☑ Track Only Above Mentioned Folder Path(s).

NOTE : Configured folder will not be monitored if any of the parent folder is filtered in system/global configuration.

Figure 179

5. Browse the Folder path.

NOTE: Folders will not be monitored, if Global or System Filter is applied.



Folder(s) will not be monitored, if they are in the Global/System filter list.
Please remove it from filter list.

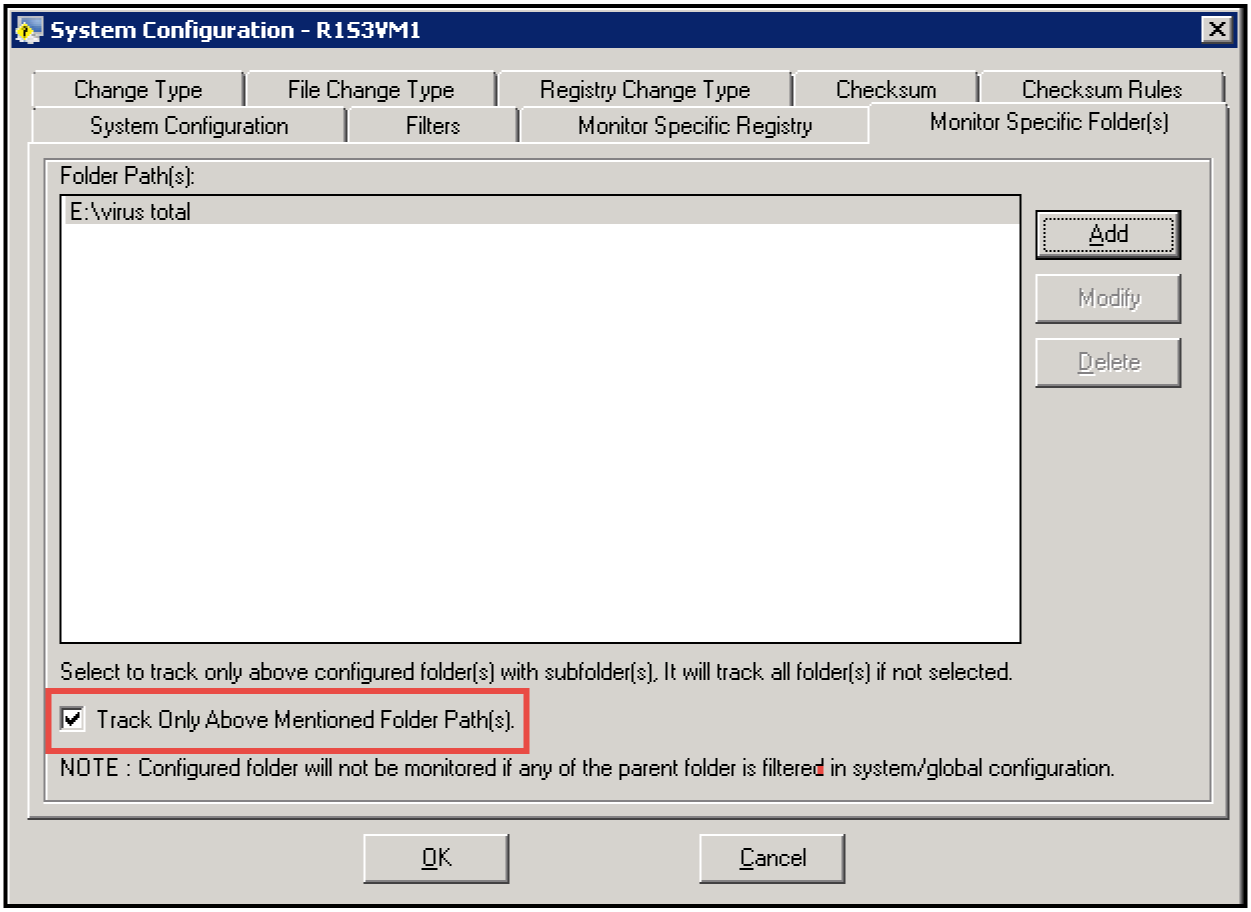
Absolute Path/ Folder Name ● Absolute Path ○ Folder Name

Folder Path: E:\virus total

Figure 180

6. Click **Add**.

It gets added.



System Configuration - R153VM1

Folder Path(s):

E:\virus total

Select to track only above configured folder(s) with subfolder(s). It will track all folder(s) if not selected.

☑ Track Only Above Mentioned Folder Path(s).

NOTE : Configured folder will not be monitored if any of the parent folder is filtered in system/global configuration.

Figure 181

7. Click the "**Track Only Above Mentioned Folder Path(s)"** check box and then click **OK**.
8. The user can now take a new snapshot and compare the changes.
9. Before taking new snapshot, user has to re-initialize the snapshot.

NOTE: The same option "**Monitor Specific Folder(s)"** has also been added in Global Configuration and it functions in the similar way mentioned for **System configuration**. For this, the global configuration should be applied to all other agents also through "**Apply Configuration**".

7. Configuration Policy Editor

7.1 Configuration Policy

Configuration Policies facilitate comparison of 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 the 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 must do is to configure a Configuration Policy and compare the systems. The report generated by

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

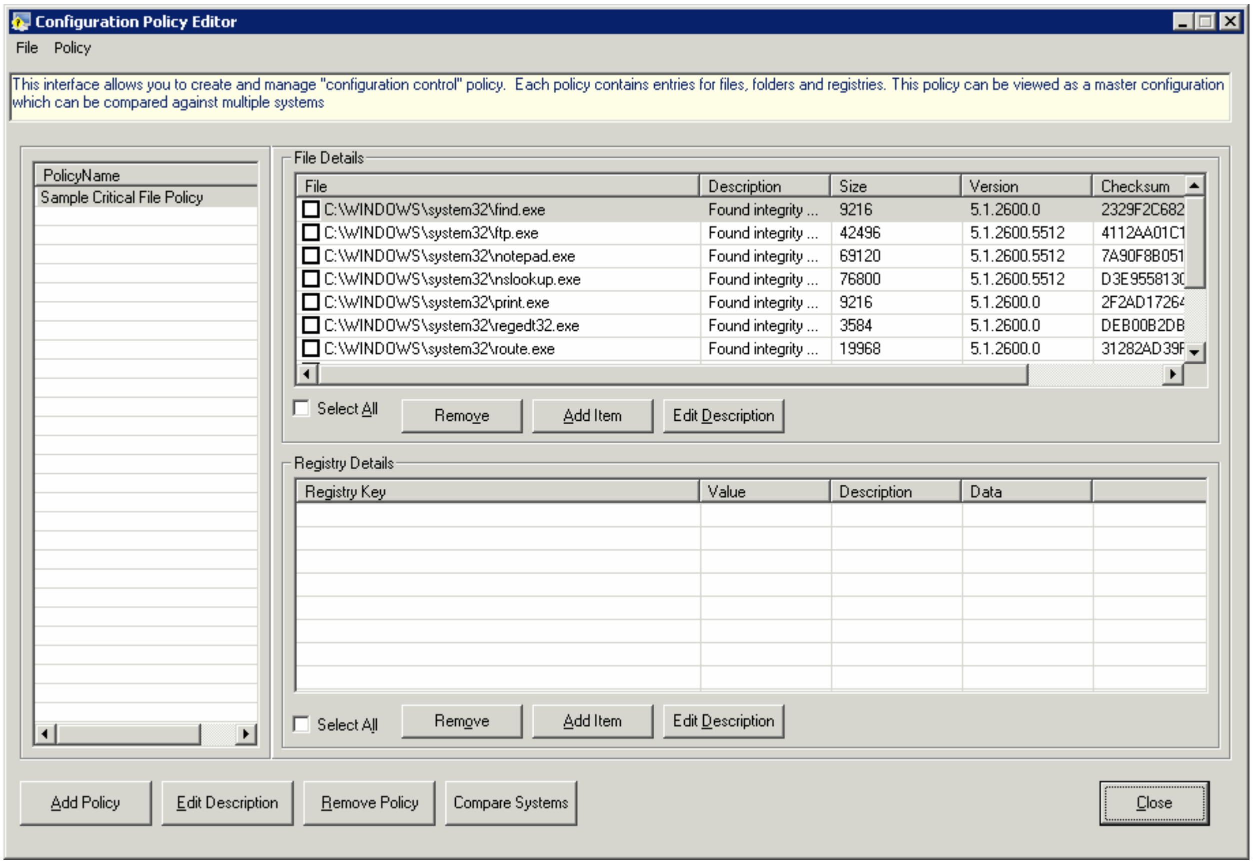
7.1.1 Creating Configuration Policies

To create Configuration Policies, follow the steps below:

1. Open the Change Browser.

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

   EventTracker - Change Audit displays Configuration Policy Editor.



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
Sample Critical File Policy

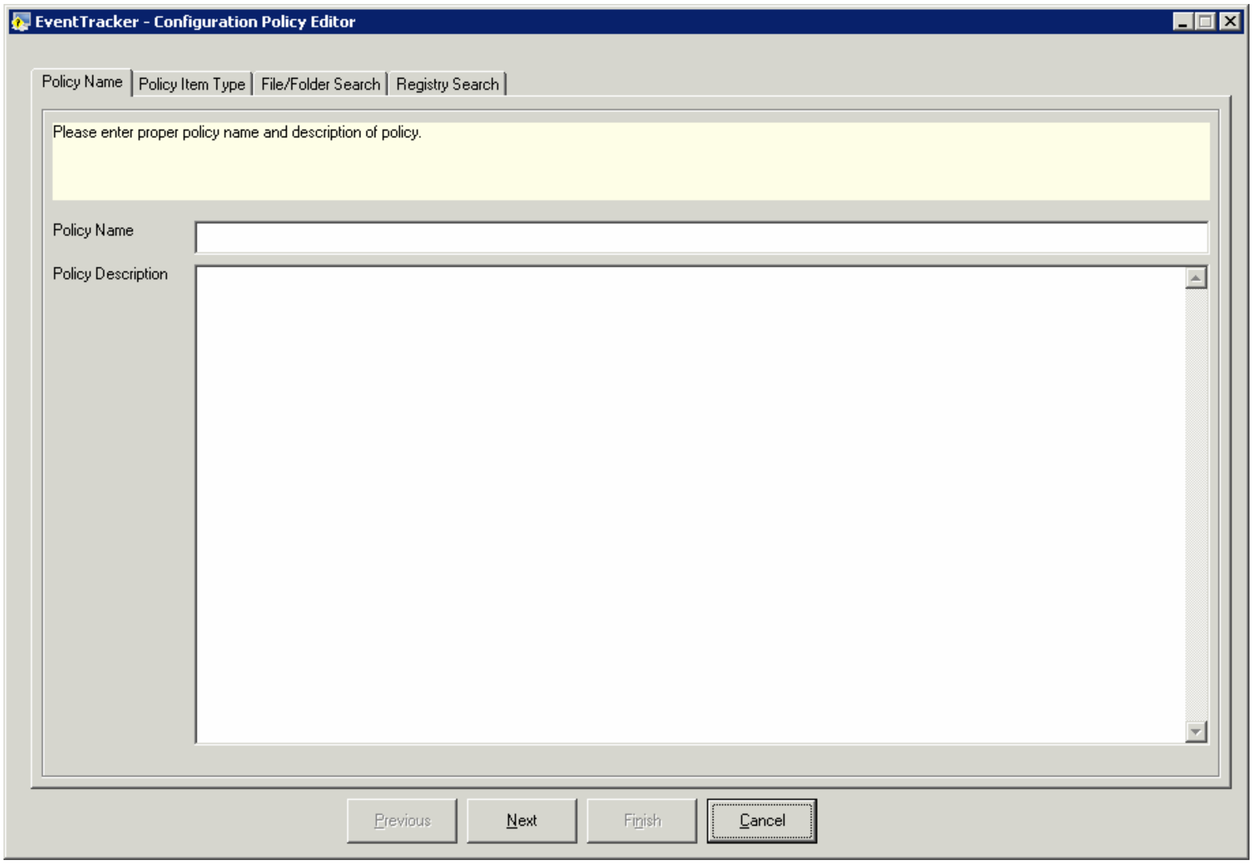
File	Description	Size	Version	Checksum
□ C:\WINDOWS\system32\find.exe	Found integrity ...	9216	5.1.2600.0	2329F2C682
□ C:\WINDOWS\system32\ftp.exe	Found integrity ...	42496	5.1.2600.5512	4112AA01C1
□ C:\WINDOWS\system32\notepad.exe	Found integrity ...	69120	5.1.2600.5512	7A90F8B051
□ C:\WINDOWS\system32\nslookup.exe	Found integrity ...	76800	5.1.2600.5512	D3E955813C
□ C:\WINDOWS\system32\print.exe	Found integrity ...	9216	5.1.2600.0	2F2AD17264
□ C:\WINDOWS\system32\regedt32.exe	Found integrity ...	3584	5.1.2600.0	DEB00B2DB
□ C:\WINDOWS\system32\route.exe	Found integrity ...	19968	5.1.2600.0	31282AD39F

Registry Key	Value	Description	Data

Figure 182

2. Click **Add Policy**.

   EventTracker - Change Audit displays the Policy Name tab.



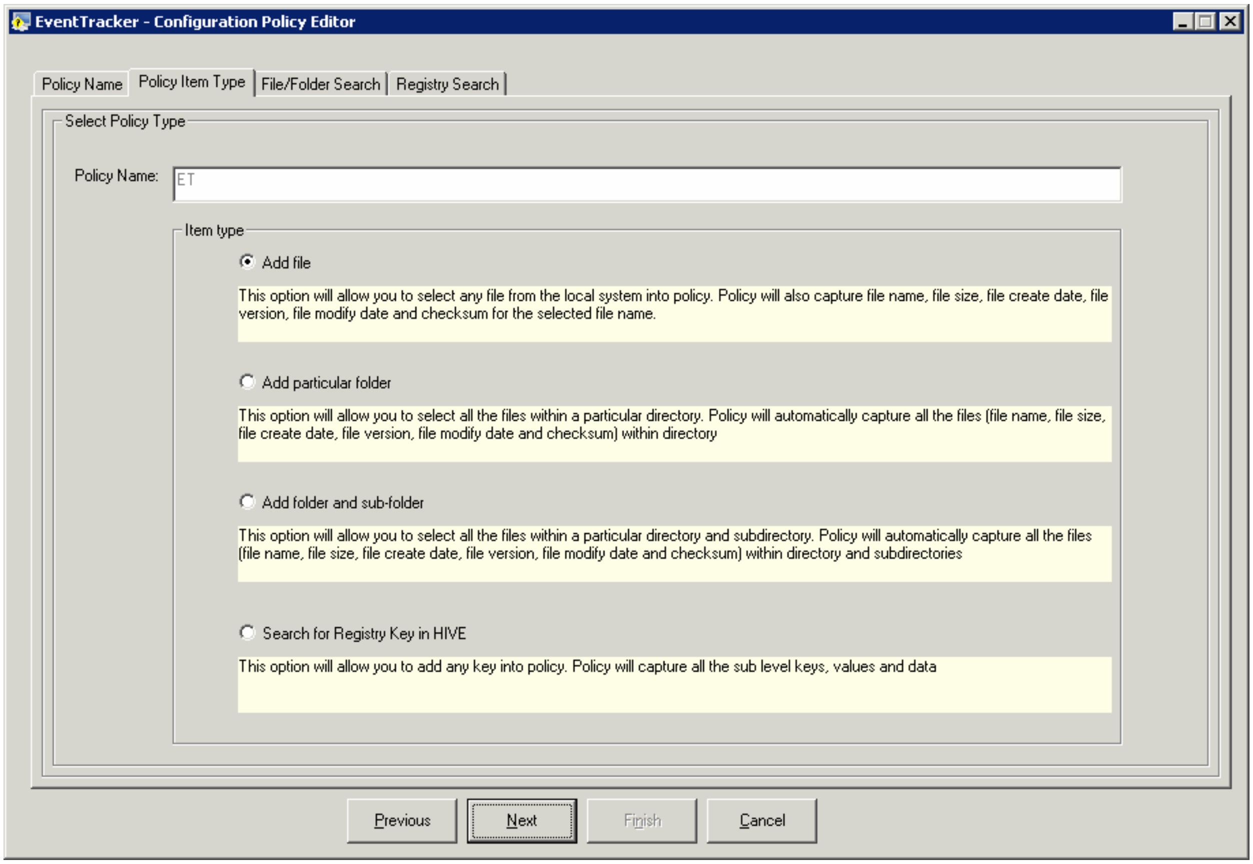
Please enter proper policy name and description of policy.

Figure 183

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.



Select Policy Type

Policy Name: ET

Item type

● Add file

This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.

○ Add particular folder

This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory

○ Add folder and sub-folder

This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories

○ Search for Registry Key in HIVE

This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

Figure 184

Field	Description
Item Type	
Add file	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.
Add particular folder	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.
	This option allows you to select all the files within a

Field	Description
Select folder and subfolder	particular folder and sub-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 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.

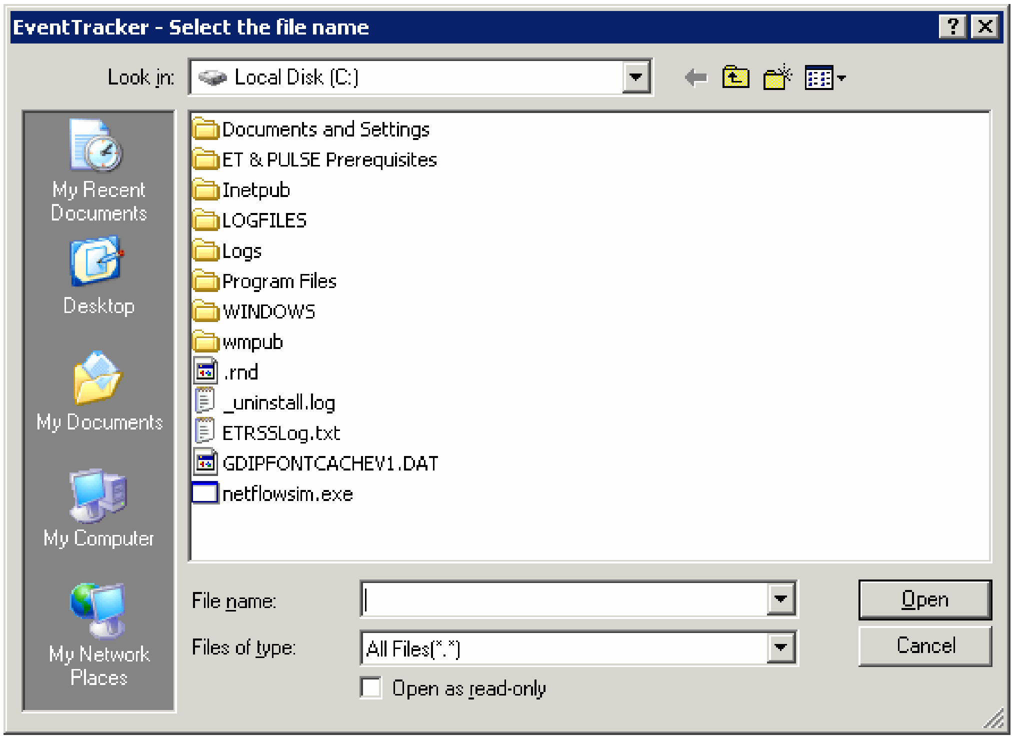
7.1.2 Searching a File

To search a File, follow the steps below:

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

Look in: Local Disk (C:)

Documents and Settings
ET & PULSE Prerequisites
Inetpub
LOGFILES
Logs
Program Files
WINDOWS
wmpub
.rnd
_uninstall.log
ETRSSLog.txt
GDIPFONTCACHEV1.DAT
netflowsim.exe

File name:

Files of type: All Files(*.*)

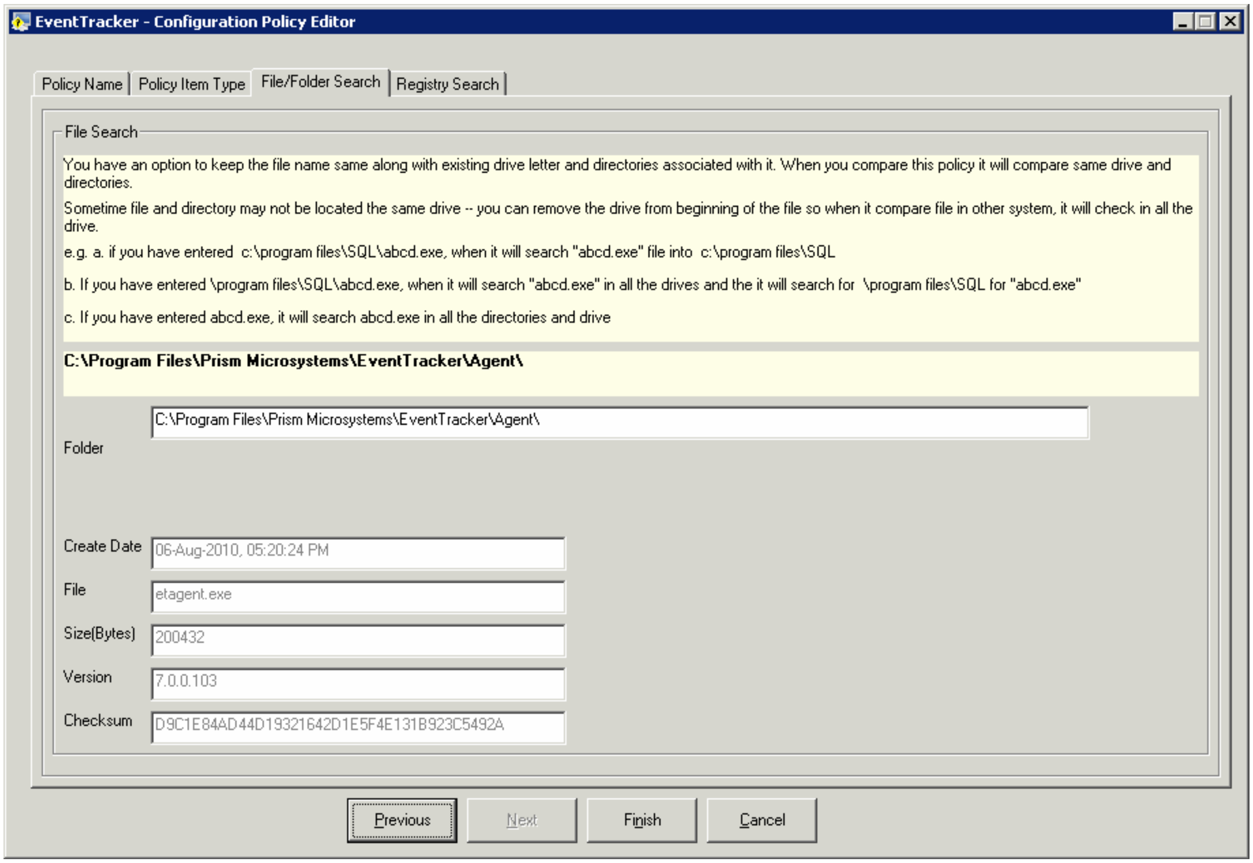
□ Open as read-only

Figure 185

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.



You have an option to keep the file name same along with existing drive letter and directories associated with it. When you compare this policy it will compare same drive and directories.

Sometime file and directory may not be located the same drive -- you can remove the drive from beginning of the file so when it compare file in other system, it will check in all the drive.

e.g. a. if you have entered c:\program files\SQL\abcd.exe, when it will search "abcd.exe" file into c:\program files\SQL

b. If you have entered \program files\SQL\abcd.exe, when it will search "abcd.exe" in all the drives and the it will search for \program files\SQL for "abcd.exe"

c. If you have entered abcd.exe, it will search abcd.exe in all the directories and drive

C:\Program Files\Prism Microsystems\EventTracker\Agent\

Folder: C:\Program Files\Prism Microsystems\EventTracker\Agent\

Create Date: 06-Aug-2010, 05:20:24 PM

File: etagent.exe

Size(Bytes): 200432

Version: 7.0.0.103

Checksum: D9C1E84AD44D19321642D1E5F4E131B923C5492A

Figure 186

NOTE:

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

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

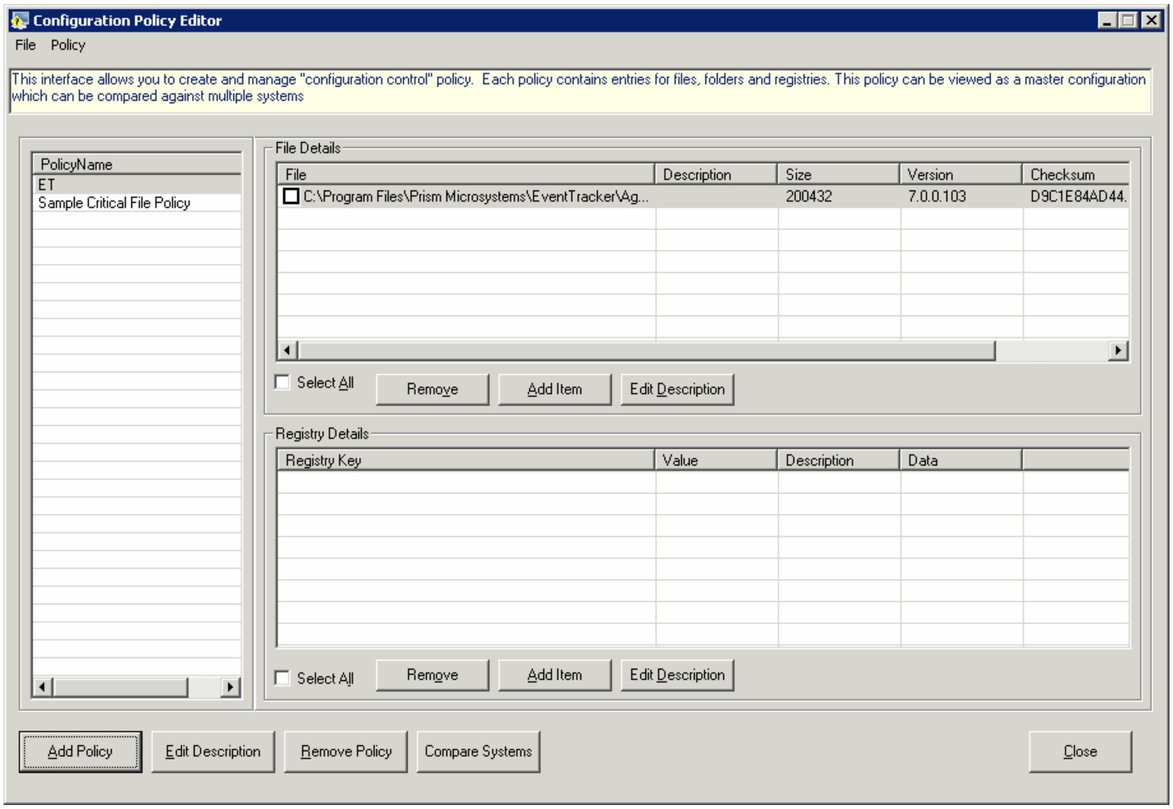
EventTracker - Change Audit searches the abcd.exe in C:\Program Files\SQL

Had you entered Program Files\SQL\abcd.exe, EventTracker - Change Audit searches the abcd.exe in Program Files\SQL

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

4. Click **Finish**.

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



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
ET
Sample Critical File Policy

File	Description	Size	Version	Checksum
□ C:\Program Files\Prism Microsystems\EventTracker\Ag...		200432	7.0.0.103	D9C1E84AD44.

Registry Key	Value	Description	Data

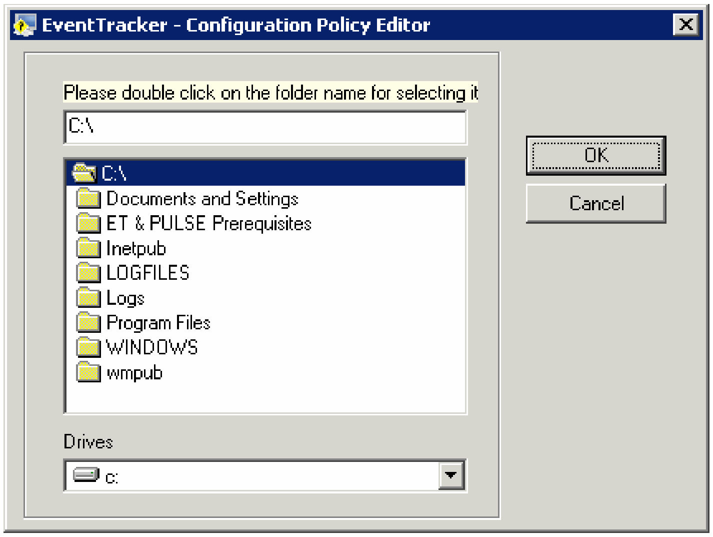
Figure 187

5. Click **Close**.

7.1.3 Search Folder option

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

   EventTracker - Change Audit displays the Configuration Policy Editor window.



Please double click on the folder name for selecting it

C:\

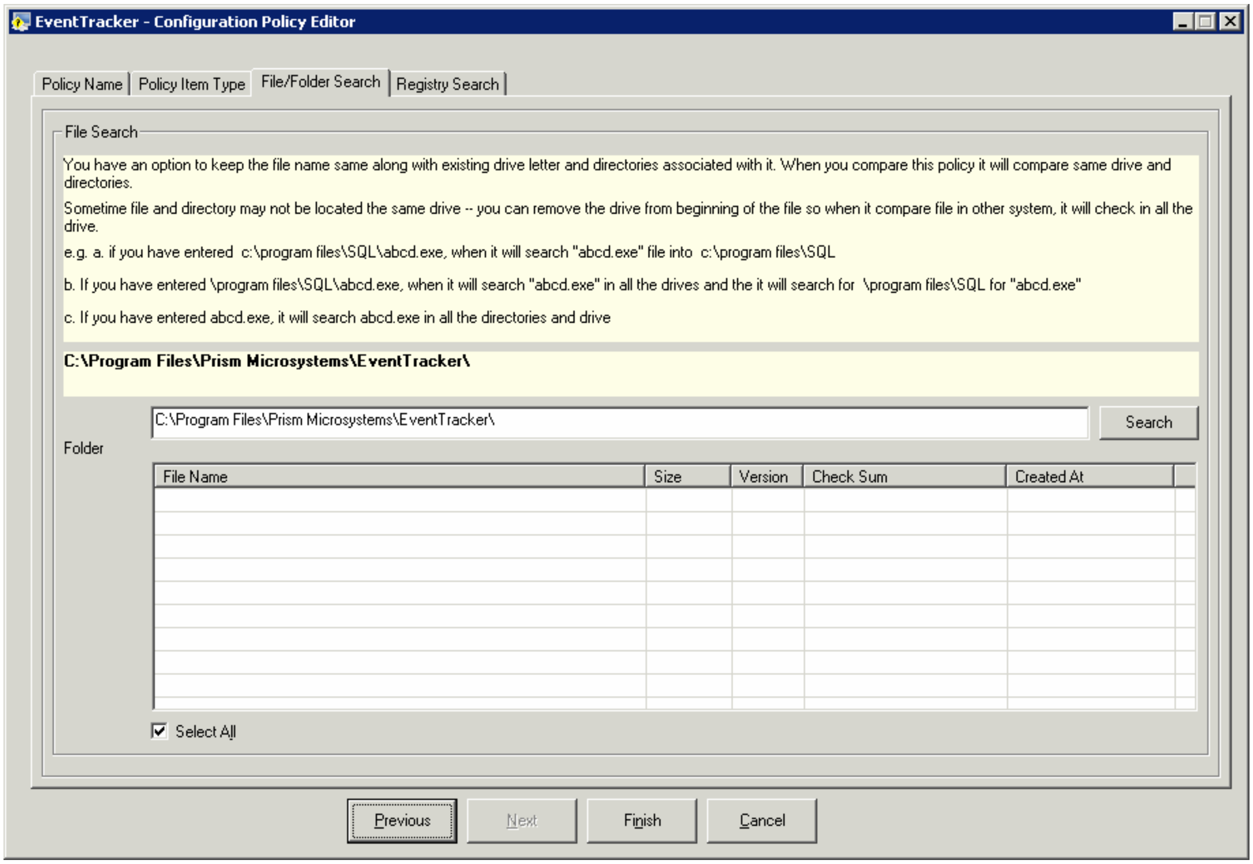
- C:\
- Documents and Settings
- ET & PULSE Prerequisites
- Inetpub
- LOGFILES
- Logs
- Program Files
- WINDOWS
- wmpub

Drives: c:

Figure 188

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

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



You have an option to keep the file name same along with existing drive letter and directories associated with it. When you compare this policy it will compare same drive and directories.

Sometime file and directory may not be located the same drive -- you can remove the drive from beginning of the file so when it compare file in other system, it will check in all the drive.

e.g. a. if you have entered c:\program files\SQL\abcd.exe, when it will search "abcd.exe" file into c:\program files\SQL

b. If you have entered \program files\SQL\abcd.exe, when it will search "abcd.exe" in all the drives and the it will search for \program files\SQL for "abcd.exe"

c. If you have entered abcd.exe, it will search abcd.exe in all the directories and drive

C:\Program Files\Prism Microsystems\EventTracker

Folder: C:\Program Files\Prism Microsystems\EventTracker\

File Name	Size	Version	Check Sum	Created At

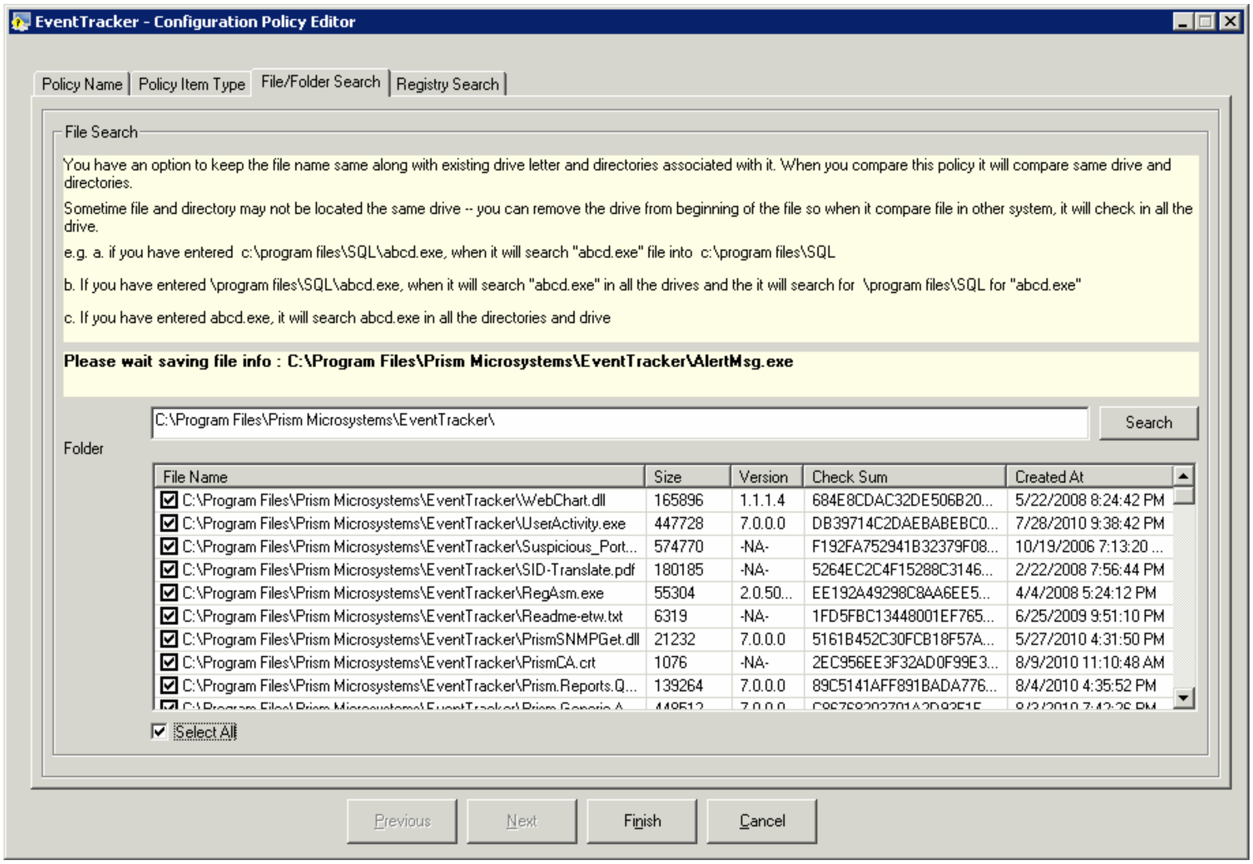
☑ Select All

Figure 189

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.



You have an option to keep the file name same along with existing drive letter and directories associated with it. When you compare this policy it will compare same drive and directories.

Sometime file and directory may not be located the same drive -- you can remove the drive from beginning of the file so when it compare file in other system, it will check in all the drive.

e.g. a. if you have entered c:\program files\SQL\abcd.exe, when it will search "abcd.exe" file into c:\program files\SQL

b. If you have entered \program files\SQL\abcd.exe, when it will search "abcd.exe" in all the drives and the it will search for \program files\SQL for "abcd.exe"

c. If you have entered abcd.exe, it will search abcd.exe in all the directories and drive

Please wait saving file info : C:\Program Files\Prism Microsystems\EventTracker\AlertMsg.exe

Folder: C:\Program Files\Prism Microsystems\EventTracker\

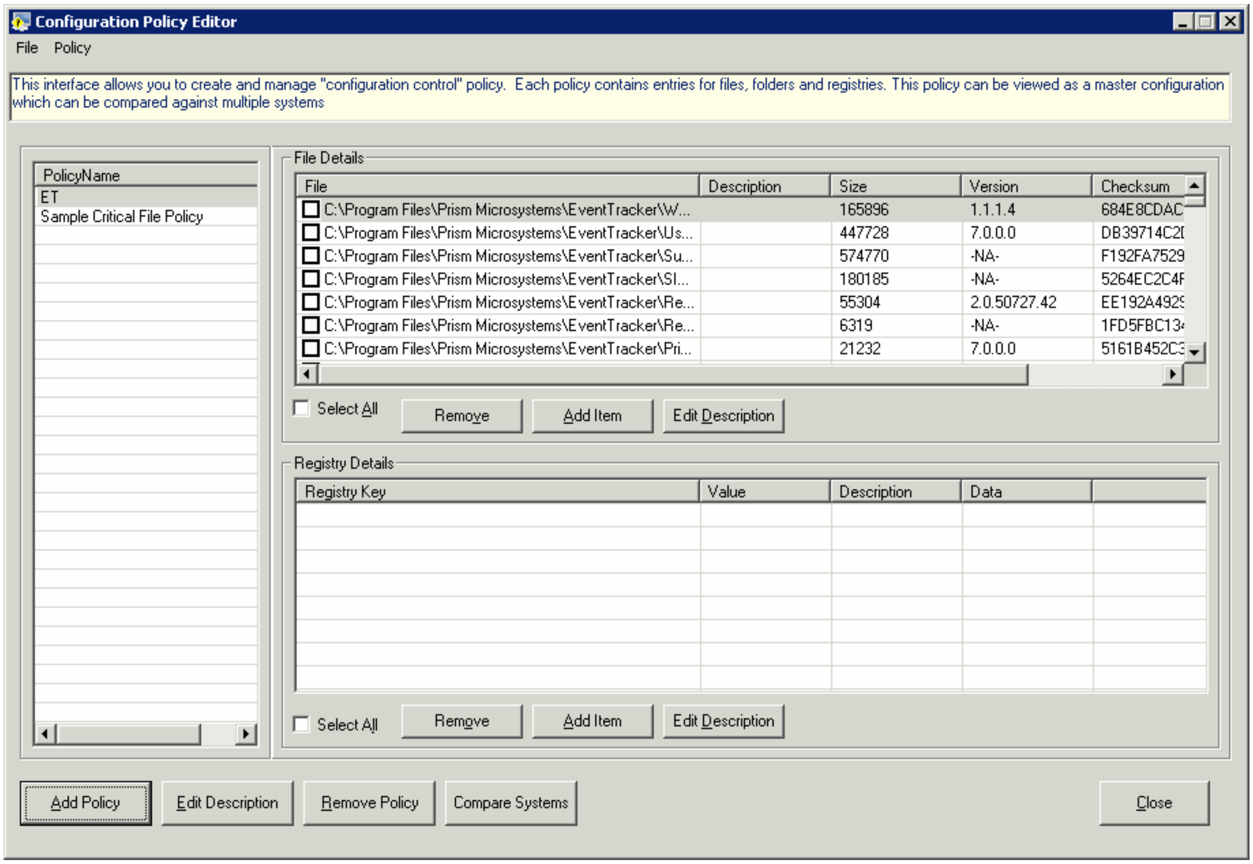
File Name	Size	Version	Check Sum	Created At
☑ C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll	165896	1.1.1.4	684E8CDAC32DE506B20...	5/22/2008 8:24:42 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\UserActivity.exe	447728	7.0.0.0	DB39714C2DAEBABEBC0...	7/28/2010 9:38:42 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\Suspicious_Port...	574770	-NA-	F192FA752941B32379F08...	10/19/2006 7:13:20 ...
☑ C:\Program Files\Prism Microsystems\EventTracker\SID-Translate.pdf	180185	-NA-	5264EC2C4F15288C3146...	2/22/2008 7:56:44 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\RegAsm.exe	55304	2.0.50...	EE192A49298C8AA6EE5...	4/4/2008 5:24:12 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\Readme-etw.txt	6319	-NA-	1FD5FBC13448001EF765...	6/25/2009 9:51:10 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\PrismSNMPGet.dll	21232	7.0.0.0	5161B452C30FCB18F57A...	5/27/2010 4:31:50 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\PrismCA.crt	1076	-NA-	2EC956EE3F32AD0F99E3...	8/9/2010 11:10:48 AM
☑ C:\Program Files\Prism Microsystems\EventTracker\Prism.Reports.Q...	139264	7.0.0.0	89C5141AFF891BADA776...	8/4/2010 4:35:52 PM
☑ C:\Program Files\Prism Microsystems\EventTracker\Prism.Generic.A...	449512	7.0.0.0	[illegible]	8/3/2010 7:42:26 PM

☑ Select All

Figure 190

6. Click **Finish**.

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



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
ET
Sample Critical File Policy

File	Description	Size	Version	Checksum
☐ C:\Program Files\Prism Microsystems\EventTracker\W...		165896	1.1.1.4	684E8CDAC
☐ C:\Program Files\Prism Microsystems\EventTracker\Us...		447728	7.0.0.0	DB39714C2I
☐ C:\Program Files\Prism Microsystems\EventTracker\Su...		574770	-NA-	F192FA7529
☐ C:\Program Files\Prism Microsystems\EventTracker\Sl...		180185	-NA-	5264EC2C4F
☐ C:\Program Files\Prism Microsystems\EventTracker\Re...		55304	2.0.50727.42	EE192A492S
☐ C:\Program Files\Prism Microsystems\EventTracker\Re...		6319	-NA-	1FD5FBC13
☐ C:\Program Files\Prism Microsystems\EventTracker\Pri...		21232	7.0.0.0	5161B452C3

Registry Key	Value	Description	Data

Figure 191

7.1.4 Searching a Folder and Sub-folder

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

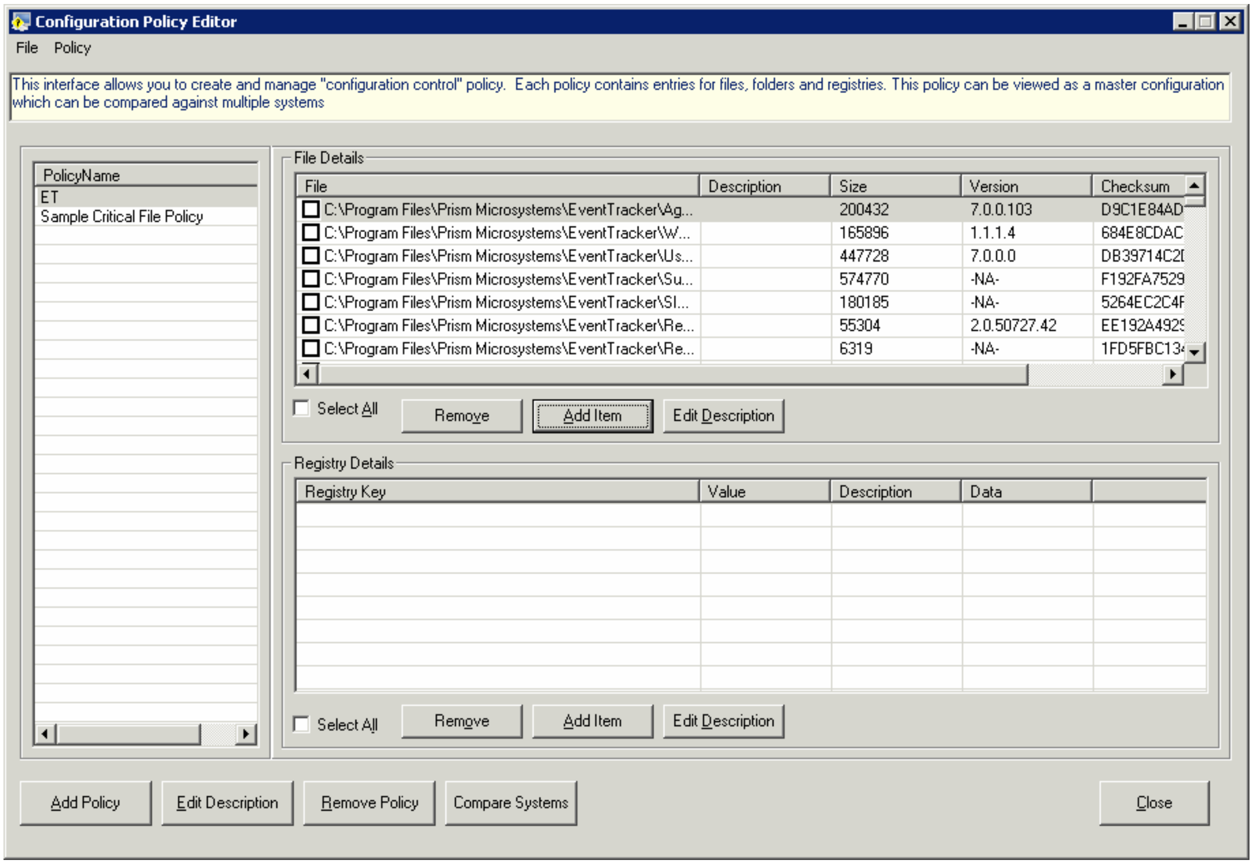
   EventTracker - Change Audit displays the File/Folder Search tab.

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.



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
ET
Sample Critical File Policy

File Details

File	Description	Size	Version	Checksum
□ C:\Program Files\Prism Microsystems\EventTracker\Ag...		200432	7.0.0.103	D9C1E84AD
□ C:\Program Files\Prism Microsystems\EventTracker\W...		165896	1.1.1.4	684E8CDAC
□ C:\Program Files\Prism Microsystems\EventTracker\Us...		447728	7.0.0.0	DB39714C2
□ C:\Program Files\Prism Microsystems\EventTracker\Su...		574770	-NA-	F192FA7529
□ C:\Program Files\Prism Microsystems\EventTracker\Sl...		180185	-NA-	5264EC2C4
□ C:\Program Files\Prism Microsystems\EventTracker\Re...		55304	2.0.50727.42	EE192A492
□ C:\Program Files\Prism Microsystems\EventTracker\Re...		6319	-NA-	1FD5FBC13

Registry Details

Registry Key	Value	Description	Data

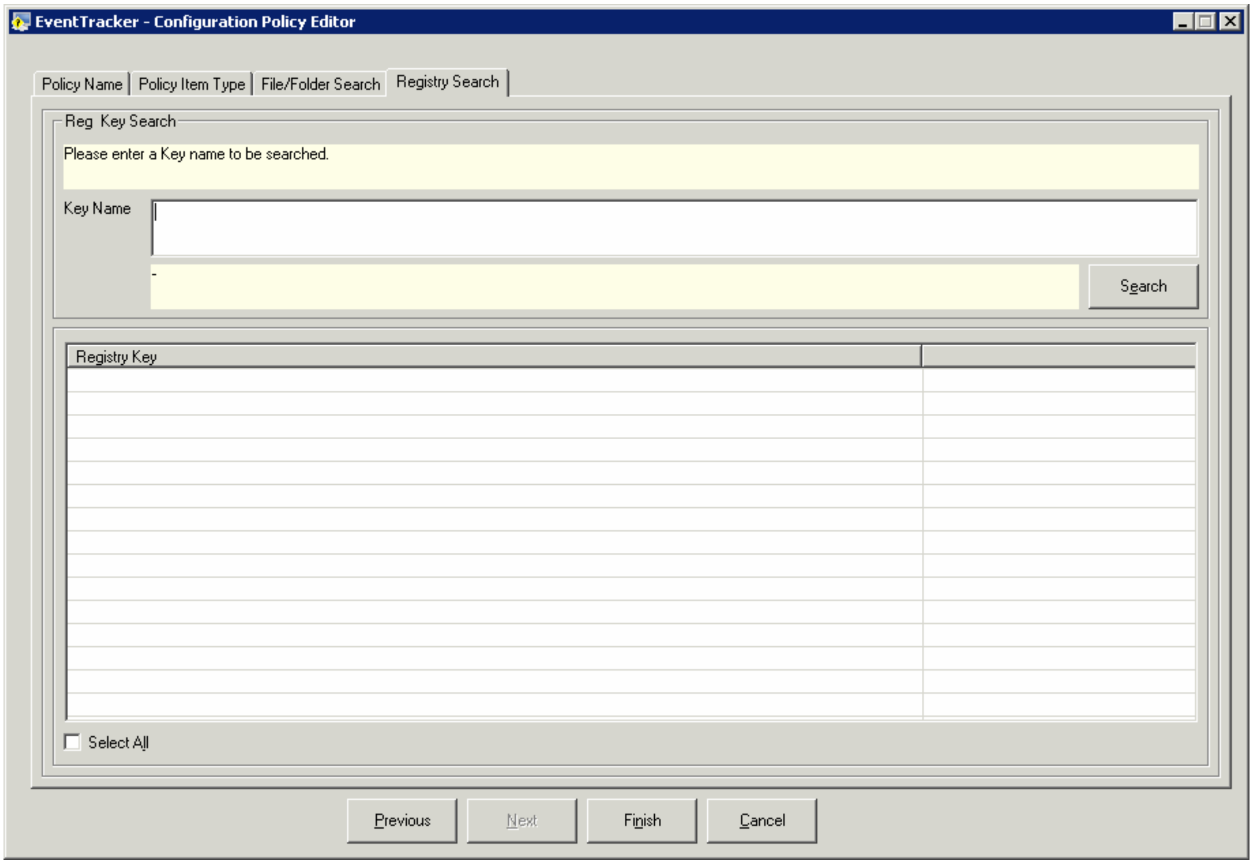
Figure 192

7.1.5 Searching Registry Key in Hive

To Search Registry Key in Hive

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

EventTracker - Change Audit displays the Registry Search tab.



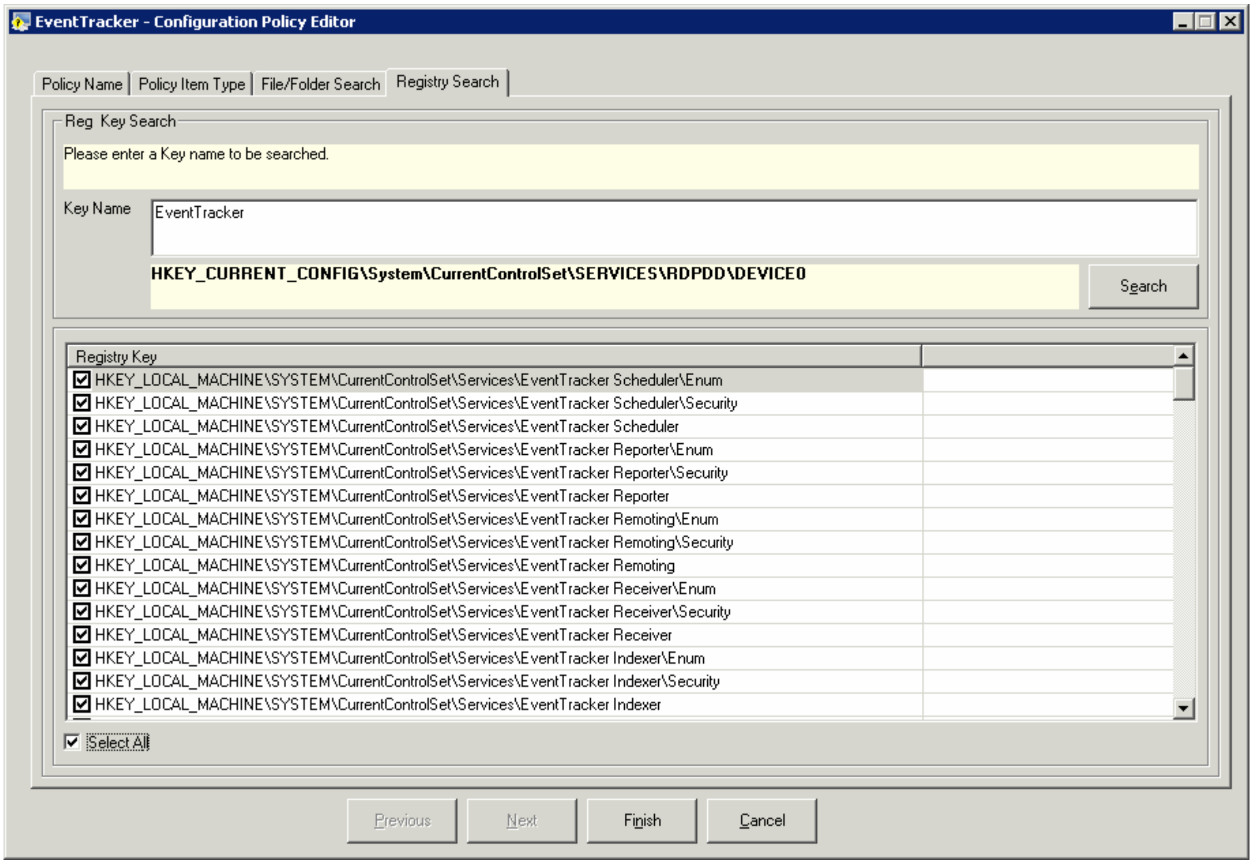
Please enter a Key name to be searched.

Figure 193

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 the search.

   EventTracker - Change Audit displays the Registry Search tab with the list of hives.



Reg Key Search

Please enter a Key name to be searched.

Key Name: EventTracker

HKEY_CURRENT_CONFIG\System\CurrentControlSet\SERVICES\RDPDD\DEVICE0

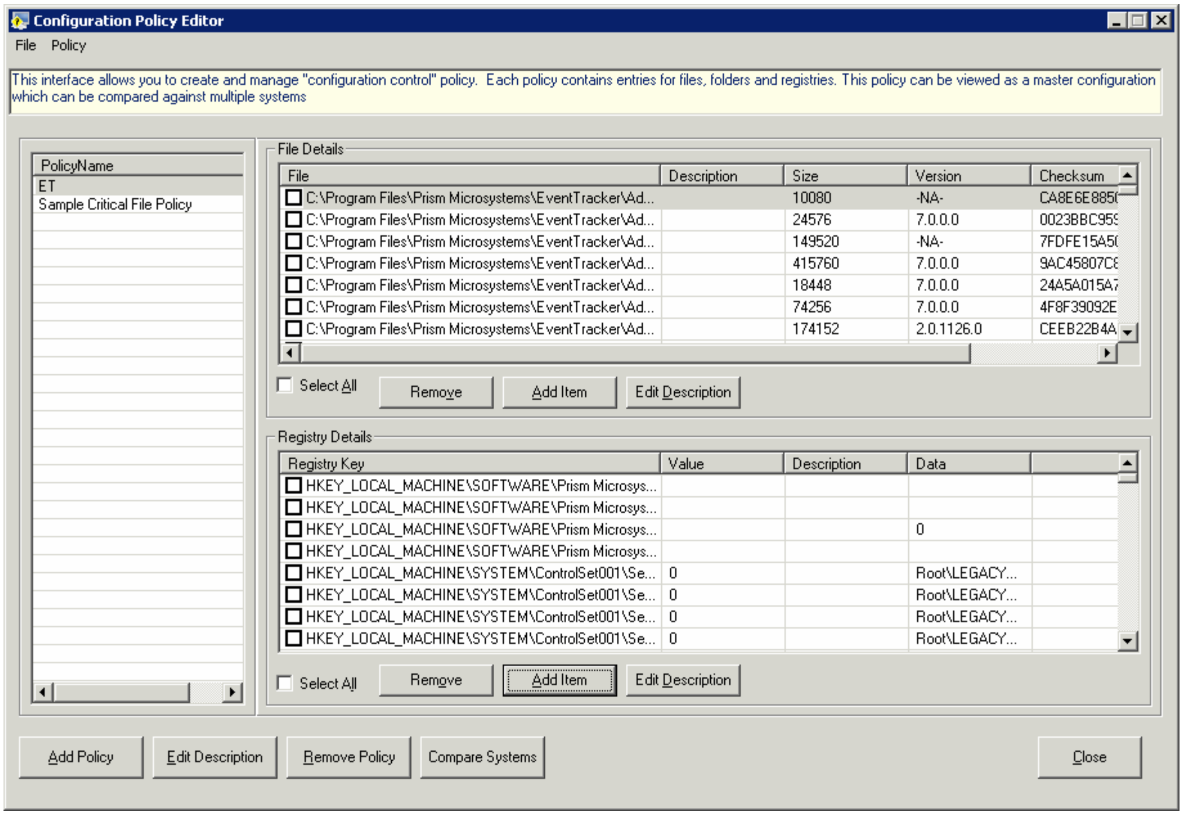
Registry Key	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler\Enum	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler\Security	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter\Enum	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter\Security	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting\Enum	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting\Security	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Receiver\Enum	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Receiver\Security	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Receiver	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Indexer\Enum	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Indexer\Security	
☑ HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Indexer	

☑ Select All

Figure 194

5. Select the keys and then Finish.

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



This interface allows you to create and manage "configuration control" policy. Each policy contains entries for files, folders and registries. This policy can be viewed as a master configuration which can be compared against multiple systems

PolicyName
ET
Sample Critical File Policy

File Details

File	Description	Size	Version	Checksum
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		10080	-NA-	CA8E6E885
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		24576	7.0.0.0	0023BBC95
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		149520	-NA-	7FDFE15A5
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		415760	7.0.0.0	9AC45807C
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		18448	7.0.0.0	24A5A015A
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		74256	7.0.0.0	4F8F39092E
□ C:\Program Files\Prism Microsystems\EventTracker\Ad...		174152	2.0.1126.0	CEEB22B4A

Registry Details

Registry Key	Value	Description	Data
□ HKEY_LOCAL_MACHINE\SOFTWARE\Prism Microsys...			
□ HKEY_LOCAL_MACHINE\SOFTWARE\Prism Microsys...			
□ HKEY_LOCAL_MACHINE\SOFTWARE\Prism Microsys...			0
□ HKEY_LOCAL_MACHINE\SOFTWARE\Prism Microsys...			
□ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Se...	0		Root\LEGACY...
□ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Se...	0		Root\LEGACY...
□ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Se...	0		Root\LEGACY...
□ HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Se...	0		Root\LEGACY...

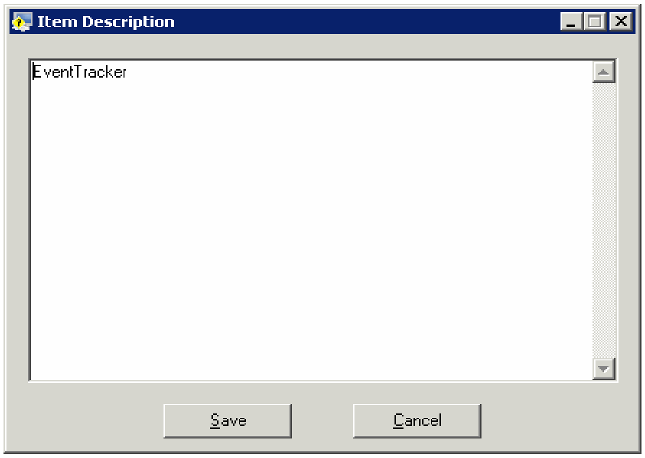
Figure 195

7.2 Edit Policy Description

To Edit Policy Description, follow the steps below:

1. Open the **Configuration Policy Editor**.
2. Select a Policy.
3. Click **Edit Description**.

   EventTracker - Change Audit displays Item Description window.



EventTracker

Figure 196

4. Edit the description and then click **Save**.
5. Click **Close**.

7.3 Edit File/Registry Key Description

To Edit file/Registry key, follow the steps below:

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**.

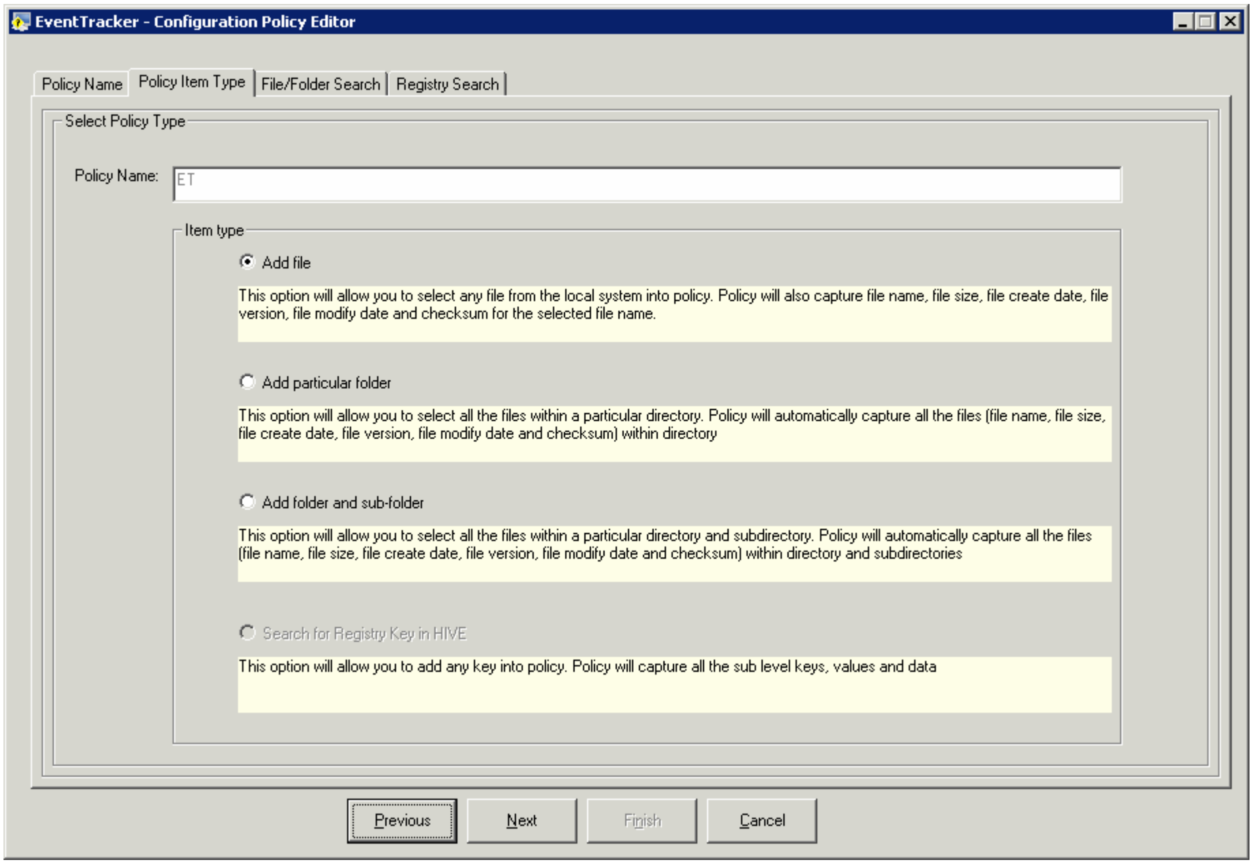
7.4 Add Policy Items option

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

To add policy items, follow the steps below:

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

   EventTracker displays the Configuration Policy Editor window.



Select Policy Type

Policy Name: ET

Item type

● Add file

This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.

○ Add particular folder

This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory

○ Add folder and sub-folder

This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories

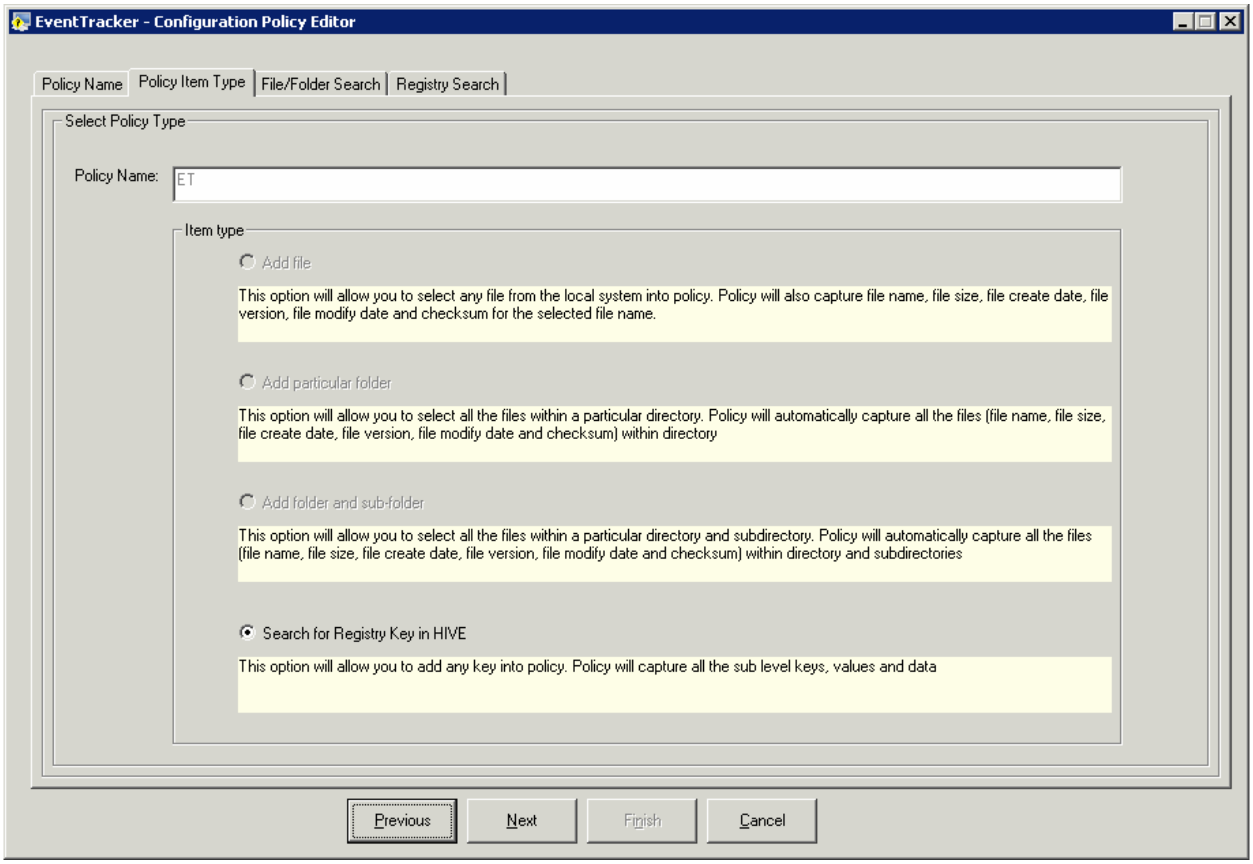
○ Search for Registry Key in HIVE

This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

Figure 197

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.



Policy Name: ET

○ Add file

This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.

○ Add particular folder

This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory

○ Add folder and sub-folder

This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories

● Search for Registry Key in HIVE

This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

Figure 198

7.5 Compare Systems option

This option helps you compare Policies between monitored computers.

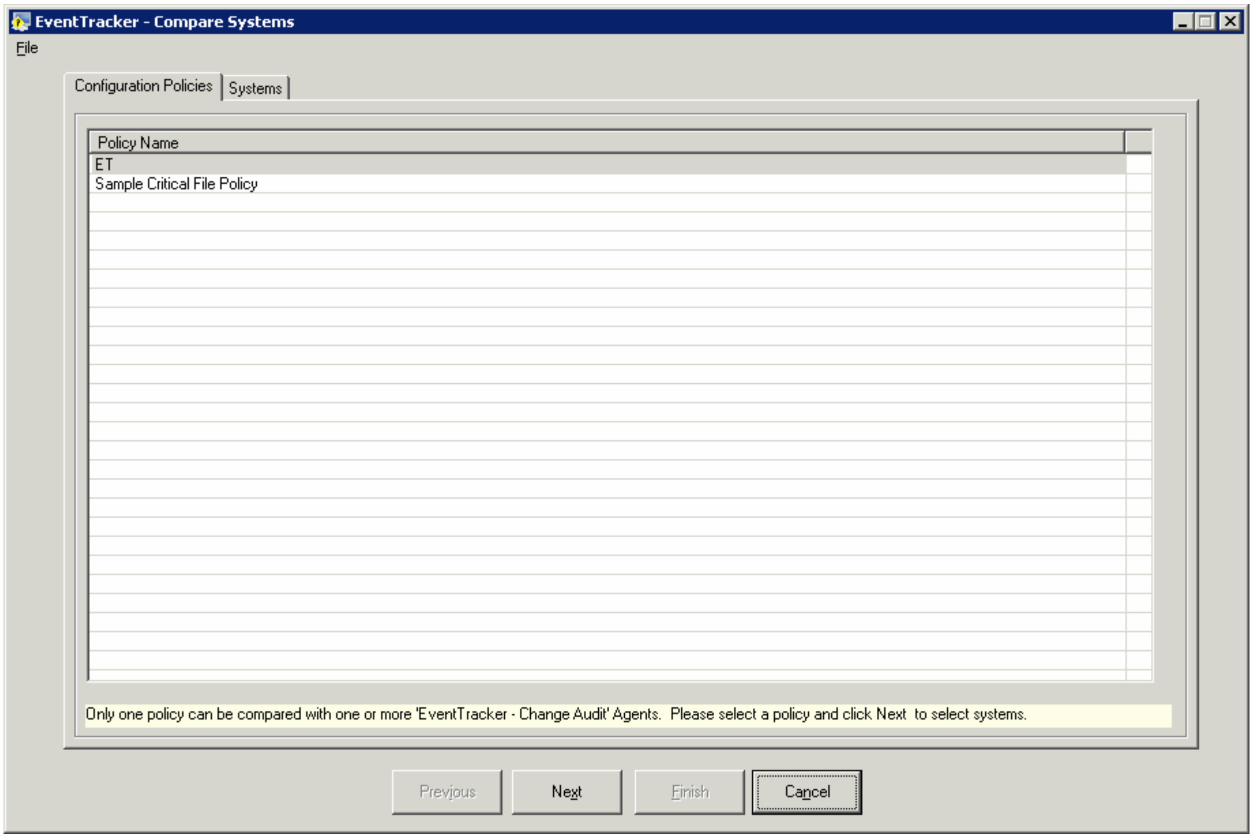
To compare systems, follow the steps below:

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.



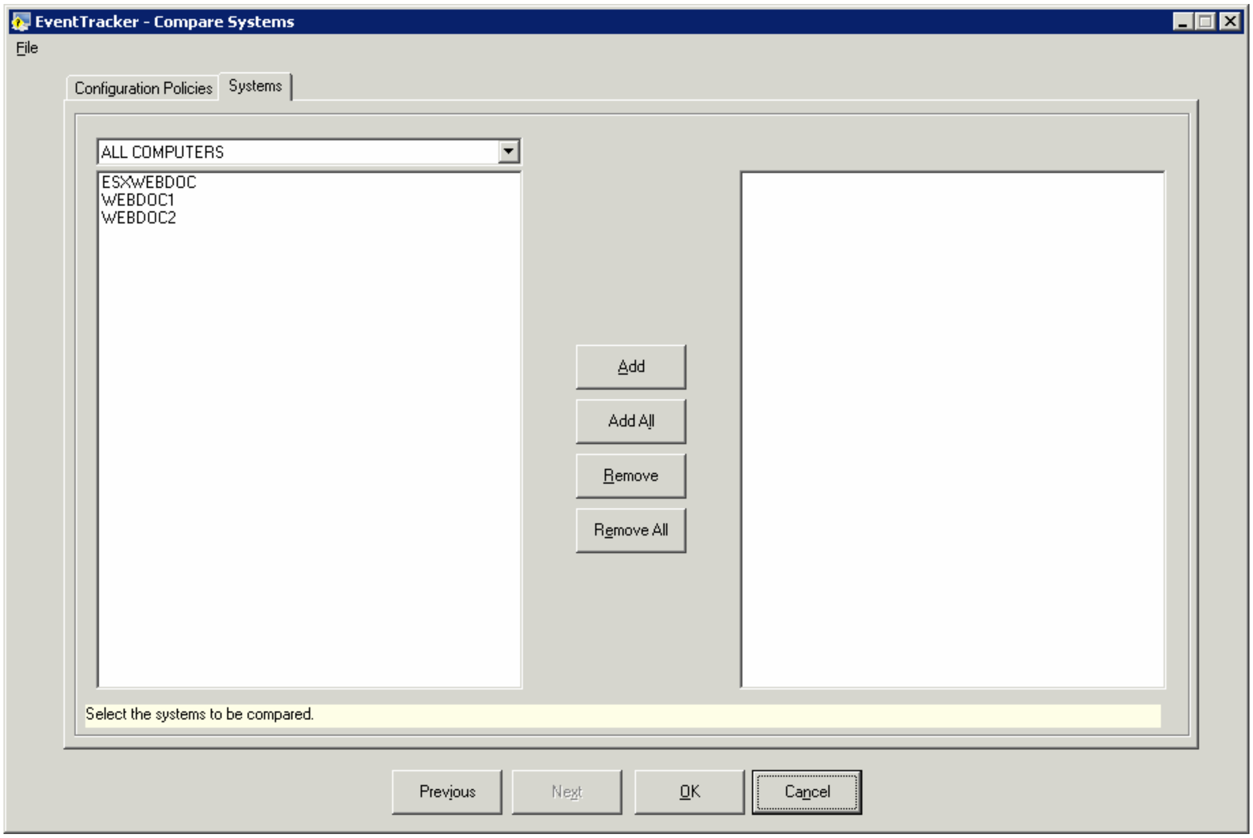
Only one policy can be compared with one or more 'EventTracker - Change Audit' Agents. Please select a policy and click Next to select systems.

Figure 199

3. Select a Policy and then click Next.

   NOTE: You can select only one Policy for comparison.

   EventTracker - Change Audit displays the Systems tab.



Select the systems to be compared.

Figure 200

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.

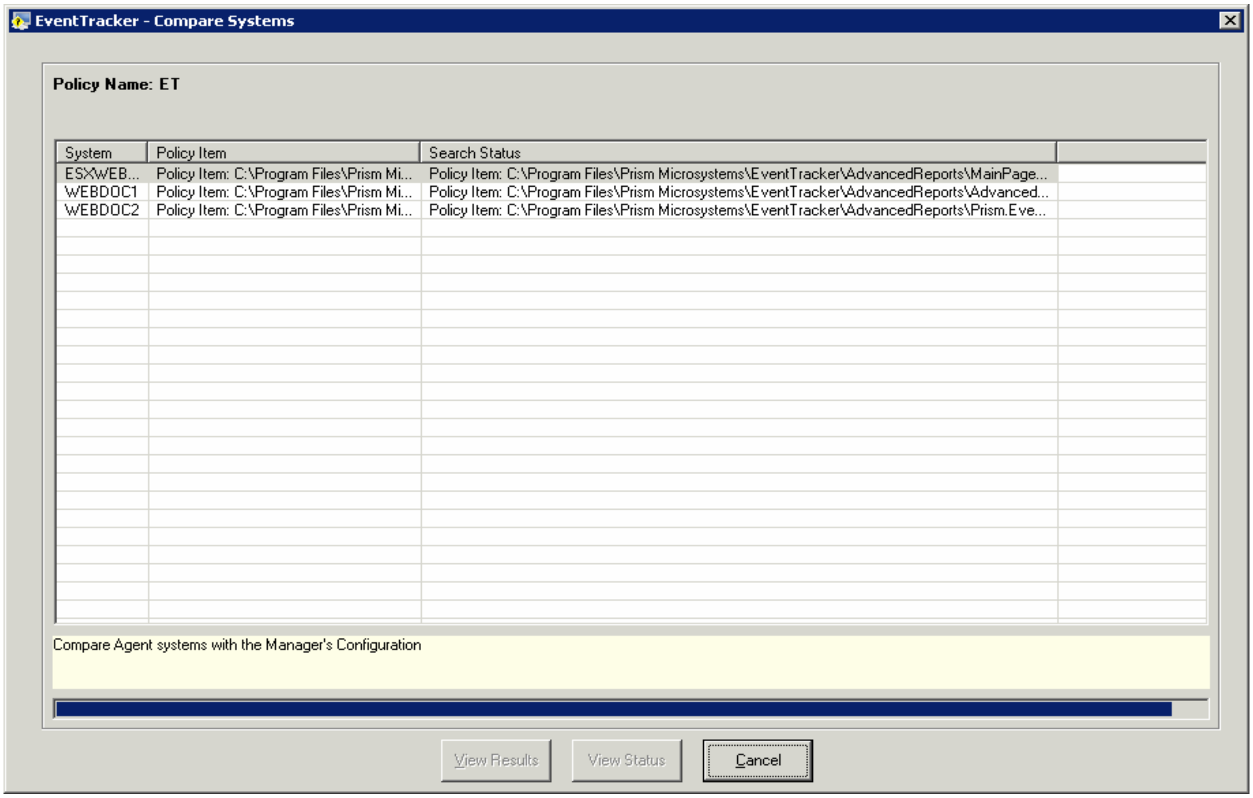
   (OR)

   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.



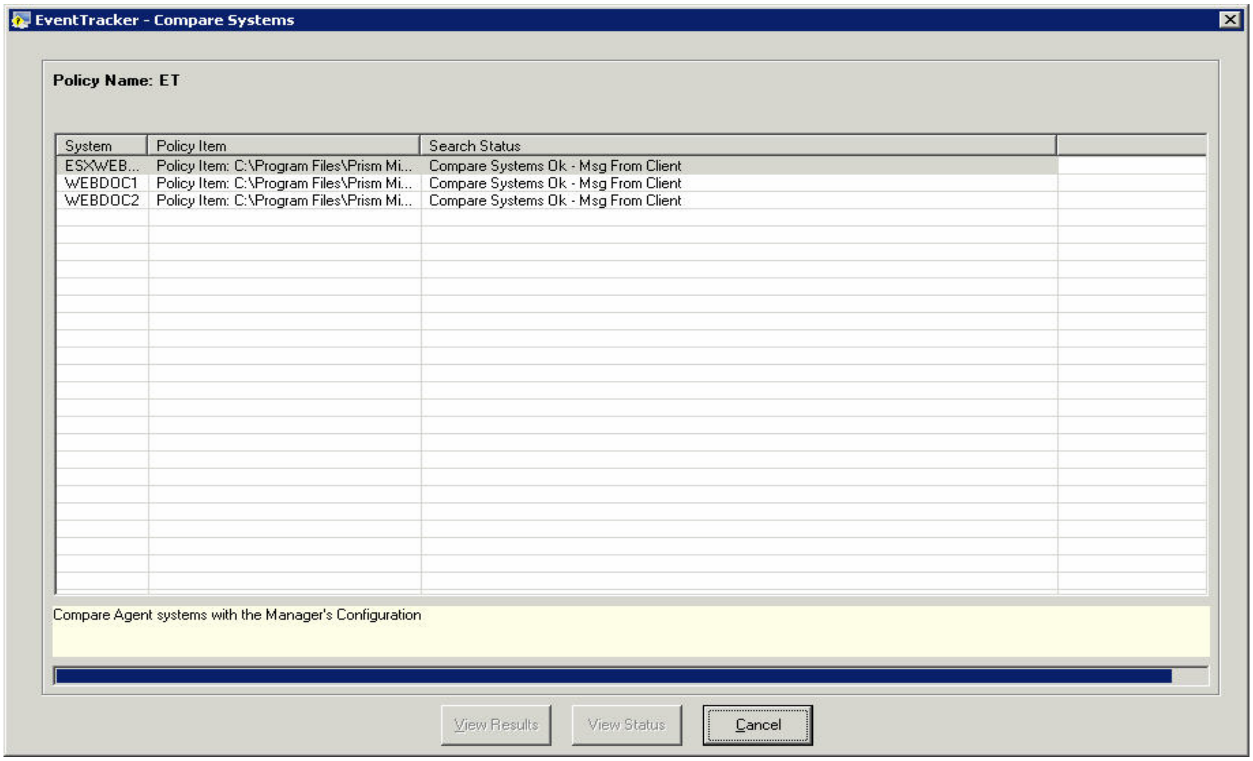
EventTracker - Compare Systems

Policy Name: ET

System	Policy Item	Search Status
ESXWEB...	Policy Item: C:\Program Files\Prism Mi...	Policy Item: C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports\MainPage...
WEBDOC1	Policy Item: C:\Program Files\Prism Mi...	Policy Item: C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Advanced...
WEBDOC2	Policy Item: C:\Program Files\Prism Mi...	Policy Item: C:\Program Files\Prism Microsystems\EventTracker\AdvancedReports\Prism.Eve...

Compare Agent systems with the Manager's Configuration

Figure 201



EventTracker - Compare Systems

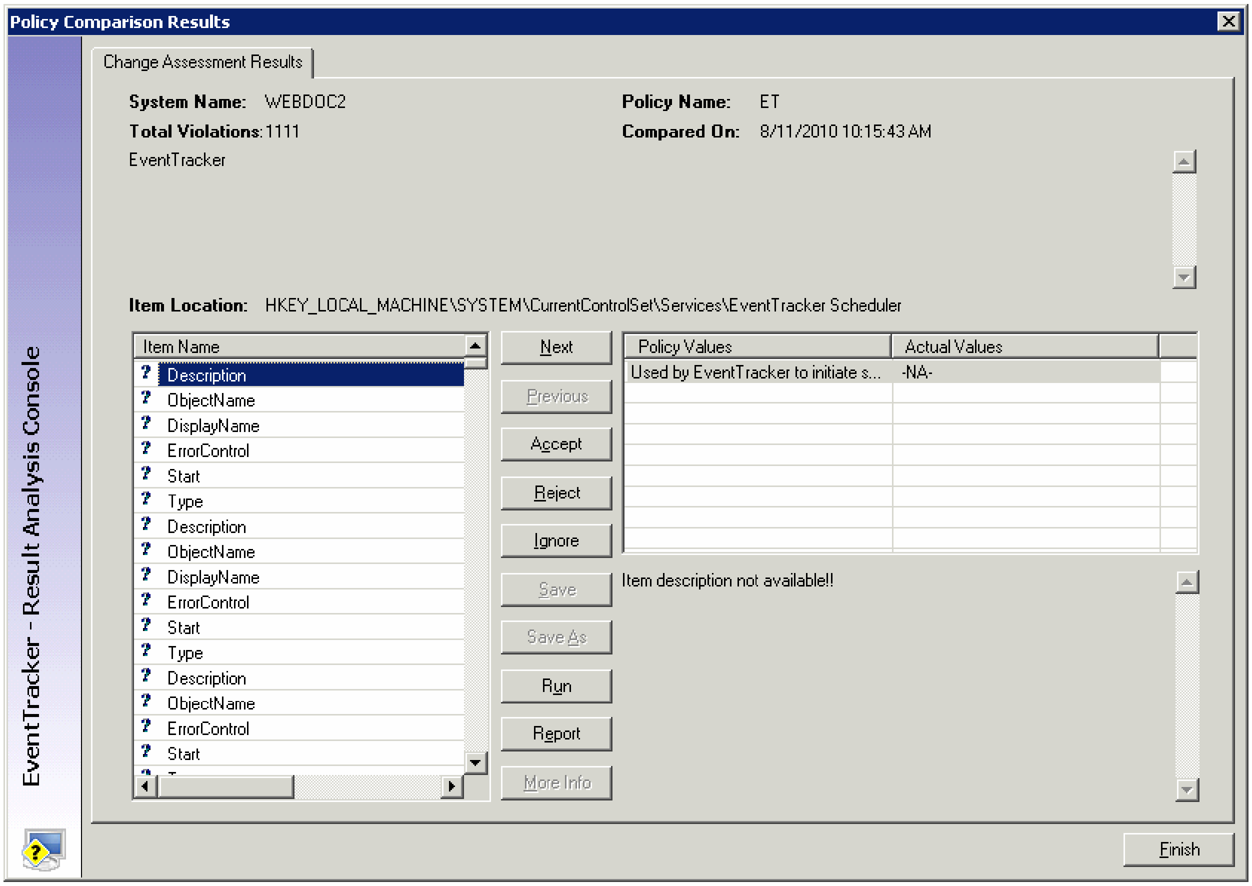
Policy Name: ET

System	Policy Item	Search Status
ESXWEB...	Policy Item: C:\Program Files\Prism Mi...	Compare Systems Ok - Msg From Client
WEBDOC1	Policy Item: C:\Program Files\Prism Mi...	Compare Systems Ok - Msg From Client
WEBDOC2	Policy Item: C:\Program Files\Prism Mi...	Compare Systems Ok - Msg From Client

Compare Agent systems with the Manager's Configuration

Figure 202

After comparing, EventTracker - Change Audit displays the result in the Policy Comparison Results window.


Policy Comparison Results
Change Assessment Results
EventTracker - Result Analysis Console
Next
Previous
Accept
Reject
Ignore
Save
Save As
Run
Report
More Info
Finish

System Name: WEBDOC2

Policy Name: ET

Total Violations: 1111

Compared On: 8/11/2010 10:15:43 AM

EventTracker

Item Location: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler

Item Name

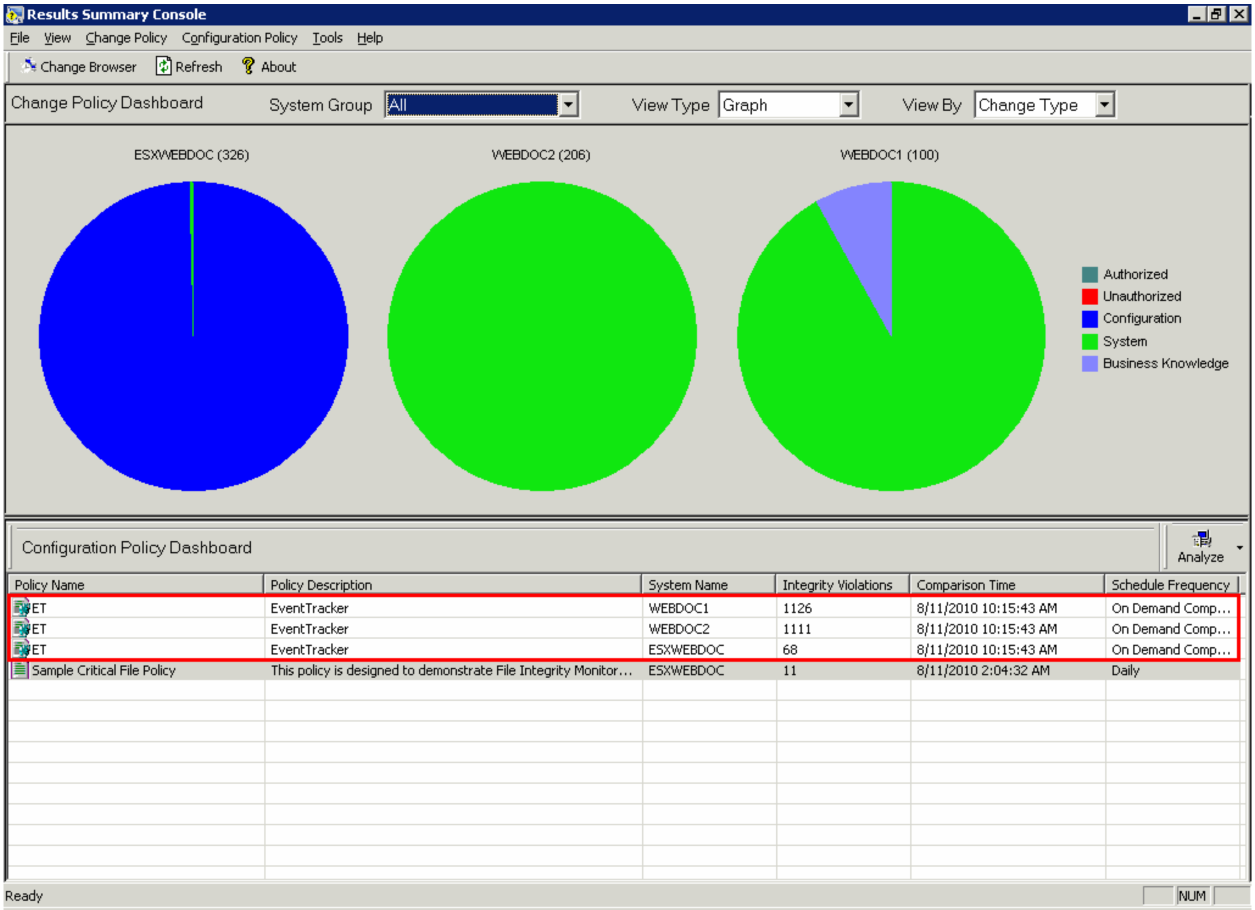
- Description
- ObjectName
- DisplayName
- ErrorControl
- Start
- Type
- Description
- ObjectName
- DisplayName
- ErrorControl
- Start
- Type
- Description
- ObjectName
- ErrorControl
- Start

Policy Values	Actual Values
Used by EventTracker to initiate s...	-NA-

Item description not available!!

Figure 203

Open the Results Summary Console to view configuration policy comparison results.



Change Policy Dashboard

System Group: All

View Type: Graph

View By: Change Type

Configuration Policy Dashboard

Policy Name	Policy Description	System Name	Integrity Violations	Comparison Time	Schedule Frequency
ET	EventTracker	WEBDOC1	1126	8/11/2010 10:15:43 AM	On Demand Comp…
ET	EventTracker	WEBDOC2	1111	8/11/2010 10:15:43 AM	On Demand Comp…
ET	EventTracker	ESXWEBDOC	68	8/11/2010 10:15:43 AM	On Demand Comp…
Sample Critical File Policy	This policy is designed to demonstrate File Integrity Monitor…	ESXWEBDOC	11	8/11/2010 2:04:32 AM	Daily

Figure 204

7.6 Schedule Policy Comparison

This option helps you schedule Policy comparison.

To schedule Policy comparison, follow the steps below:

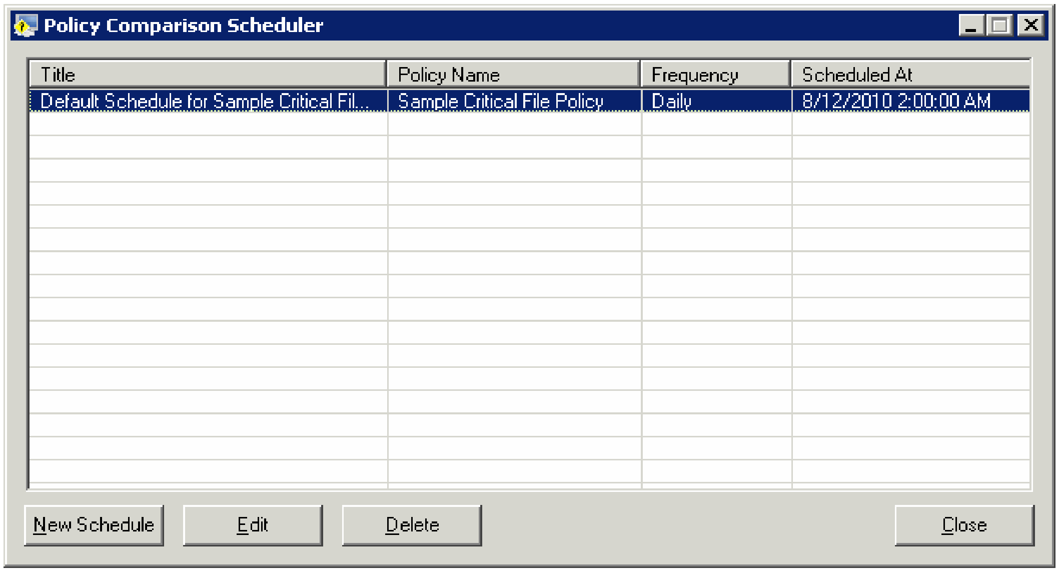
1. Open the Change Browser.
2. Click the **Tools** menu and select the **Schedule Policy Comparison** option.

   (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.



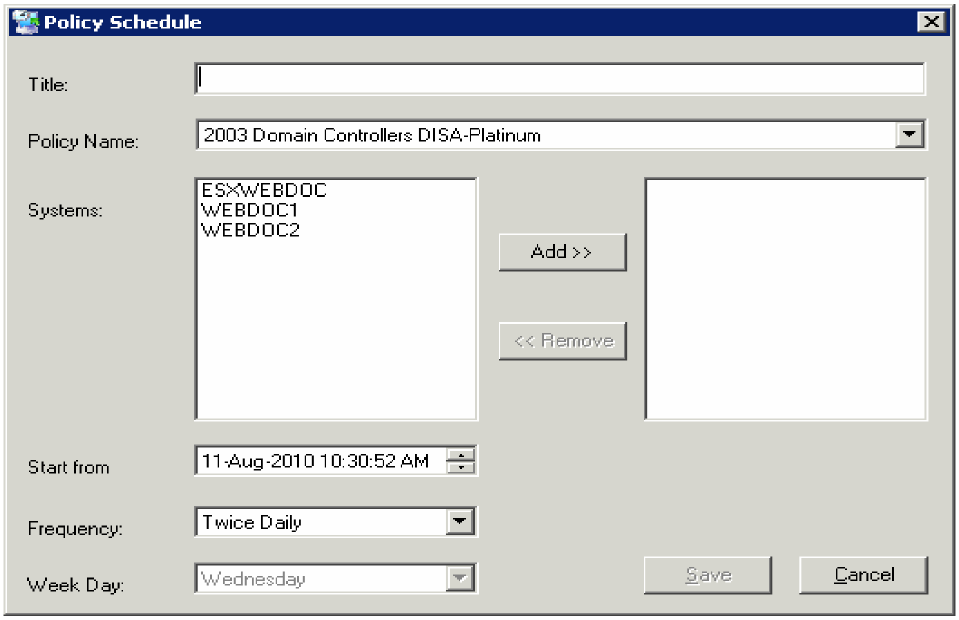
Policy Comparison Scheduler

Title	Policy Name	Frequency	Scheduled At
Default Schedule for Sample Critical Fil...	Sample Critical File Policy	Daily	8/12/2010 2:00:00 AM

Figure 205

3. Click **New Schedule**.

   EventTracker - Change Audit displays the Policy Schedule window.



Policy Schedule

Title:

Policy Name: 2003 Domain Controllers DISA-Platinum

Systems: ESXWEBDOC
WEBDOC1
WEBDOC2

Start from 11-Aug-2010 10:30:52 AM

Frequency: Twice Daily

Week Day: Wednesday

Figure 206

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.

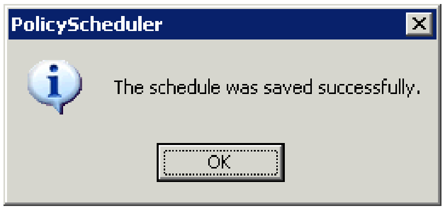
6. Select **Systems**.

7. Select the start date and time from the **Start from** the spin box.
8. Select how often you want the report to be generated from the Frequency drop-down list.

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

9. Click **Save**.

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



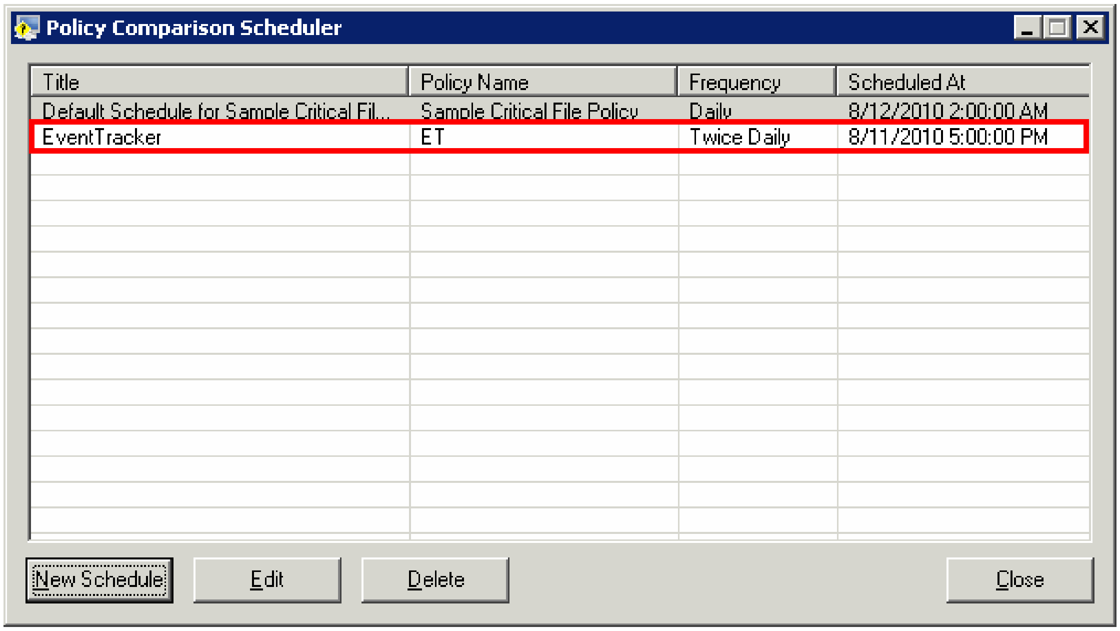
PolicyScheduler

The schedule was saved successfully.

Figure 207

10. Click **OK**.

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



Policy Comparison Scheduler

Title	Policy Name	Frequency	Scheduled At
Default Schedule for Sample Critical Fil...	Sample Critical File Policy	Daily	8/12/2010 2:00:00 AM
EventTracker	ET	Twice Daily	8/11/2010 5:00:00 PM

Figure 208

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.

7.7 Export Configuration Policies

This option helps you export configuration Policies to the desired location.

To export configuration Policies, follow the steps below:

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.

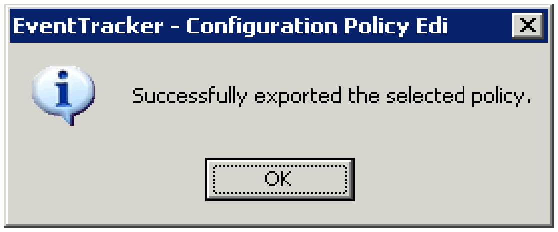
4. Select a Policy and then click **Export**.

   EventTracker - Change Audit displays the Select Export File window.

5. Go to the appropriate folder, enter the name in the File name field and then click **Save**.

   NOTE: Valid export file format is .ispol.

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



EventTracker - Configuration Policy Edi

Successfully exported the selected policy.

Figure 209

7.8 Import Configuration Policies

This option helps you import configuration Policies to monitored computers.

To import configuration Policies, follow the steps below:

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

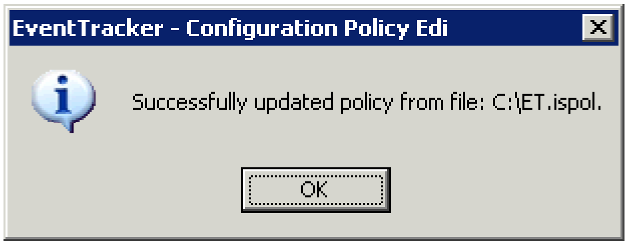
   EventTracker - Change Audit displays the Configuration Policy Editor.

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

   EventTracker - Change Audit displays the Select Import File window.

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

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



EventTracker - Configuration Policy Edi

Successfully updated policy from file: C:\ET.ispol.

Figure 210

Glossary

Term	Description
Change Management	The practice of administering changes with the help of tested methods and techniques to avoid new errors and minimize the impact of changes.
Change View	EventTracker - Change Audit displays the items that are added, modified and deleted in File System and Registry.
Client	Tiny footprint installed in monitored systems to track changes.
Computer Logical Groups	User-defined groups. These groups are logical in the sense you can group computers in different domains of your interest for easy management.
Edit Snapshots	It helps to keep the selected Snapshot forever or delete when the Snapshot limit exceeds.
File System	A system for organizing directories and files, generally in terms of how it is implemented in the disk operating system.

Term	Description
Filters	Filters are set to exclude folders and files from tracking.
Full View	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.
Global Configuration	Configure and apply folders/files to track and apply filters to all the monitored computers from the Manager console.
Policy	Helps to group and track registry hives and directories of an application.
Reinitialize Snapshots	EventTracker - Change Audit removes all the Snapshots including the Snapshots selected to keep forever and takes a new baseline Snapshot.
Removing Client Components	Helps to clean-up database entries and other components when clients are removed manually from the remote computers.
Snapshot	Snapshot is an image of the File System and Registry.

Term	Description
System Configuration	Configure Snapshot automation, Snapshot limit and filters to the current system. System Configuration can also be propagated to all other the system in the network.