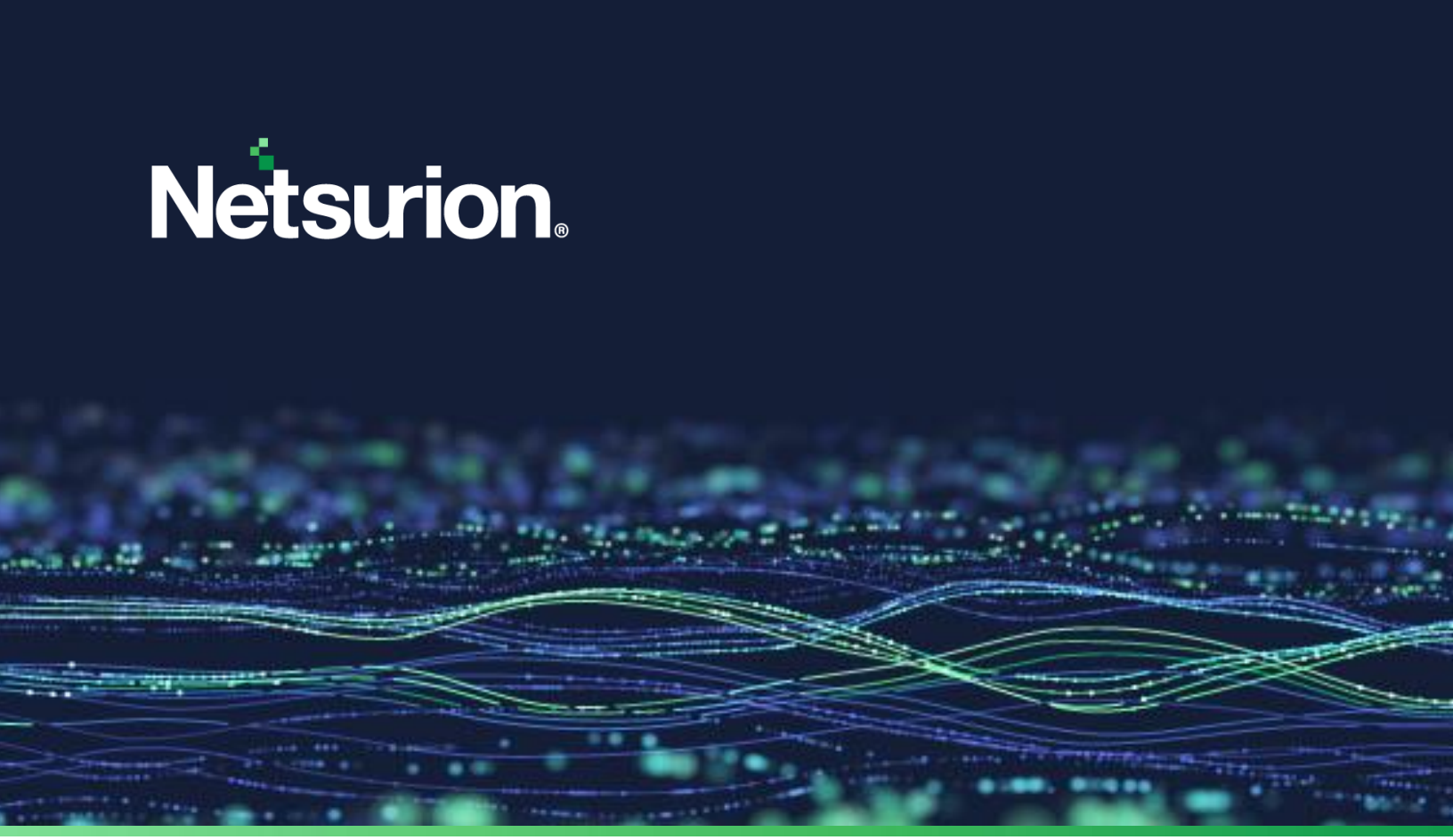


Feature Guide

Change Audit

Publication Date

March 25, 2024

Abstract

This document provides instructions for configuring Change Audit and the associated protocols in Netsurion Open XDR. Change Audit tracks changes covering file servers, folders, registry items, and other key services to enhance threat detection and threat prevention across your enterprise.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.x.

Audience

This guide is for the administrators and Operations personnel who are responsible for managing and investigating network security.

Table of Contents

1 Overview

Change Audit is a diagnostic tool that targets a broad area of Change Management. Change Management is a concept by which all the 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 with 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 Capabilities of Netsurion Open XDR – Change Audit

- Configuring Change Audit to log Snapshot results, as Change Audit logs the events locally (Windows Application logs).
- Configuration Policies Management (Configuration Policy Editor).
- Comparing systems based on Configuration Policies. It 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 secure the systems of new viruses before the Anti-Virus provider comes up with a solution.
- Capture and store system snapshots. Snapshots contain detailed information about the file system, registry, and system configuration.
- Track registry changes and restore “last known good configuration’ registry settings.
- Schedule or take Snapshots on demand.
- Edit Snapshots.
- Reinitialize Snapshots.
- Compare Snapshots. Unlike first-generation products, only differences are stored to maximize speed and minimize disk space usage.
- Configure **Filters** to filter out non-critical directories and registry hives. 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 and 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, and 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.
- **Insurance against change:** With Change Audit installed a user is confident about installing a new software or making major configuration changes as the user has information available that helps in reverting to a good configuration if any problem occurs.

1.2 Change Audit Architecture

Change Audit architecture is completely centralized and provides control to manage all the systems on the network from one console.
Change Audit consists of two main modules, namely the Manager and the Client. The Manager, in turn, include three components: Service, Console GUI, and a backend database that stores enterprise change data.
A typical deployment of Change Audit can include one console and multiple clients installed on each client machine.

1.3 Ports Used by Change Audit

Change Audit uses two TCP ports to communicate between Netsurion Open XDR - 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 the firewall on the Change Audit Manager adds ports 14502 and 14508 to the firewall exceptions list.

1.4 Change Audit Events

Name	Description	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 the 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.
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.
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 the 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 updating.	Take appropriate action.
3416	When the Change Audit engine executes the policy comparison request from the manager.	Take appropriate action.

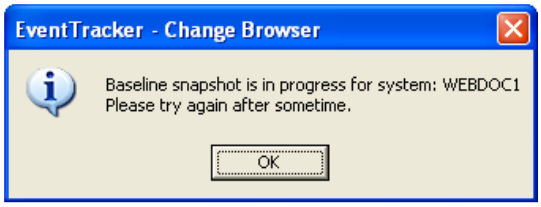
1.5 Starting Change Browser

This option helps to start Netsurion Open XDR– Change Browser from the Manager and the Client computers. Perform the following steps:

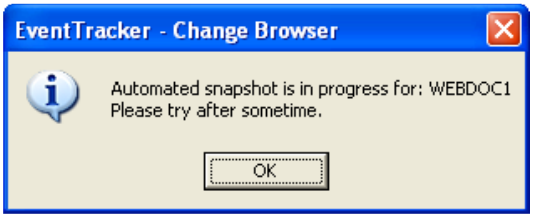
1 Select **Netsurion Open XDR Control Panel** > **Change Audit**, and then select the **Change Browser**.

(OR) Double-click **Change Audit** on the desktop Netsurion Open XDR Control Panel.

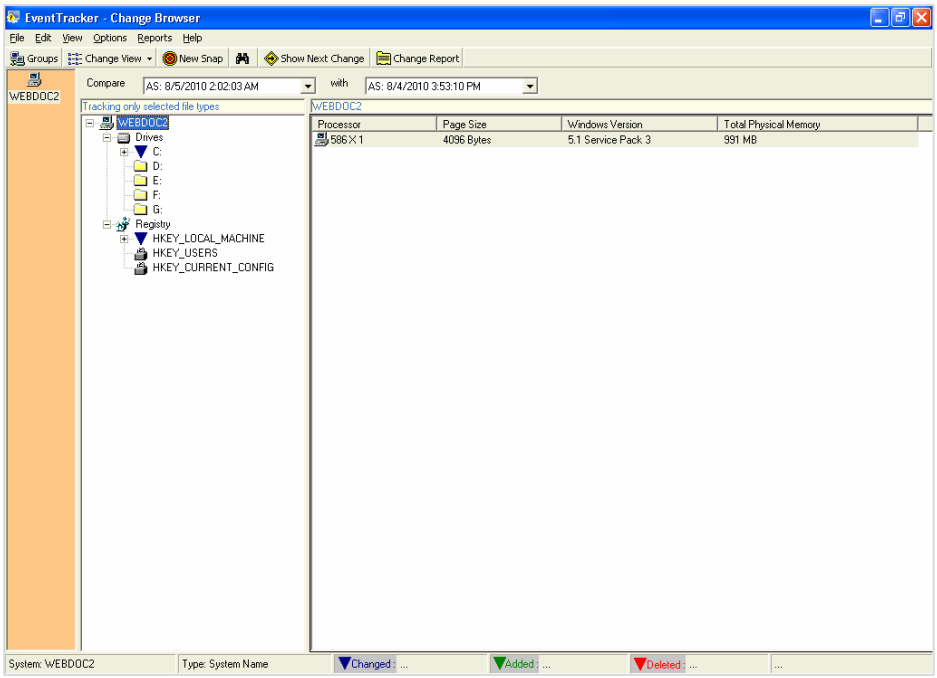
2. Netsurion Open XDR displays the **Results Summary Console**.
3. Click **Change Browser** on the toolbar.
4. Change Audit displays the **Change Browser** console indicating that the Baseline snapshot is in progress.



5. The following image indicates that the Automated snapshot is in progress.



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

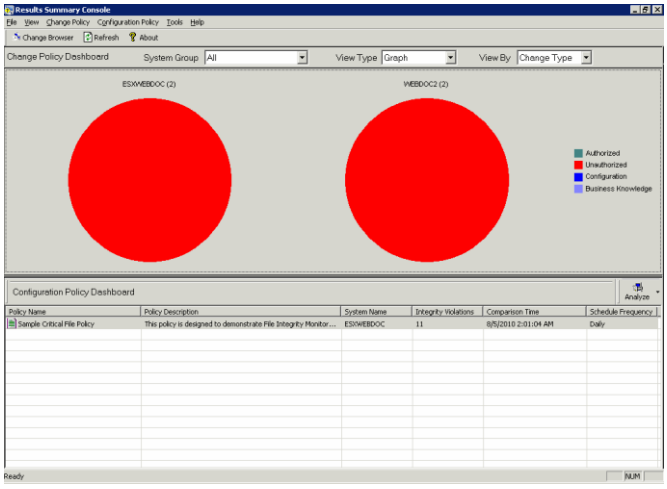


1.6 Starting Results Summary Console

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

To start the Results Summary Console, follow the below steps:

1. Double-click **Change Audit Results** on the desktop Control Panel.
2. Change Audit displays the Results Summary console with empty panes if the snapshot is in progress.
3. It is the graph view of the manager and the Netsurion Open XDR - Change Audit managed computers.



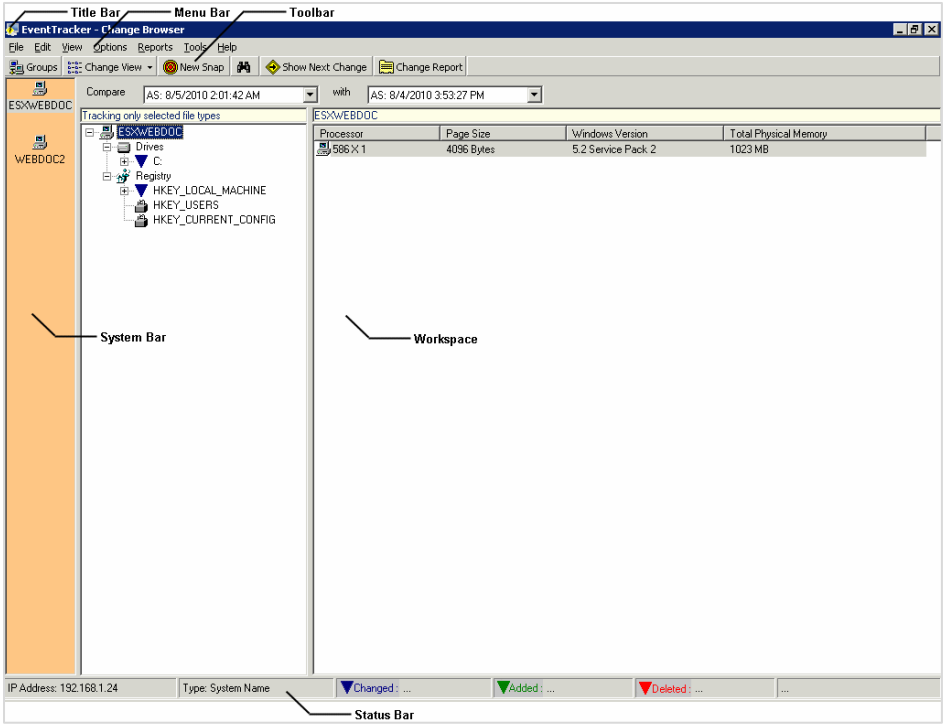
Field	Description	
System Group	This dropdown list displays all the system groups discovered by the Client Manager.	
View Type	Select an option to view chart or data on the console.	
Change Type	Authorized	Detected changes that can be matched to an approved change request.
	Unauthorized	Detected changes that cannot be matched to an approved change request.
	Configuration	Configuration audit helps to track all changes that are made to the computer configuration or to restore the configuration of that computer 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
	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 9.0 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 Netsurion Open XDR - Change Audit. This section helps us understand the Change Browser user interface. To work with Netsurion Open XDR - Change Audit effectively, a thorough understanding of its user interface is very important.



Title Bar

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

Menu Bar

The strip next to the Title Bar is the Menu Bar. The 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

The 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
Groups	Switch to Groups view.
Change View	Toggle between Full View and Change View.
New Snap	Take new Snapshots of the selected system.
	Search strings in the File System or Registry.
Show Next Change	View consecutive changes in the File System and Registry.

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 dropdown lists that list out Snapshots available for comparison. The right dropdown list contains all the available Snapshots, and the left one contains only the latest one.

By default, Netsurion Open XDR - 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, 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.

Change Audit displays the change details that include Addition, deletion, and modification of files, and folders, in this Change View. Change Audit displays mouse over ToolTip for all the items on both panes.

Status Bar
Change Audit displays the IP address of the selected system in the first section, the 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 Netsurion Open XDR- Change Audit Icons

The description of the Change Audit icons is given below:

Icon	Description
	Total count of all items added to the File System or Registry.
	Total count of all items modified in the File System or Registry.
	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 were found.
	Fresh item.
	Items accepted.
	Items ignored.
	Items rejected.

1.9 Change Audit Components

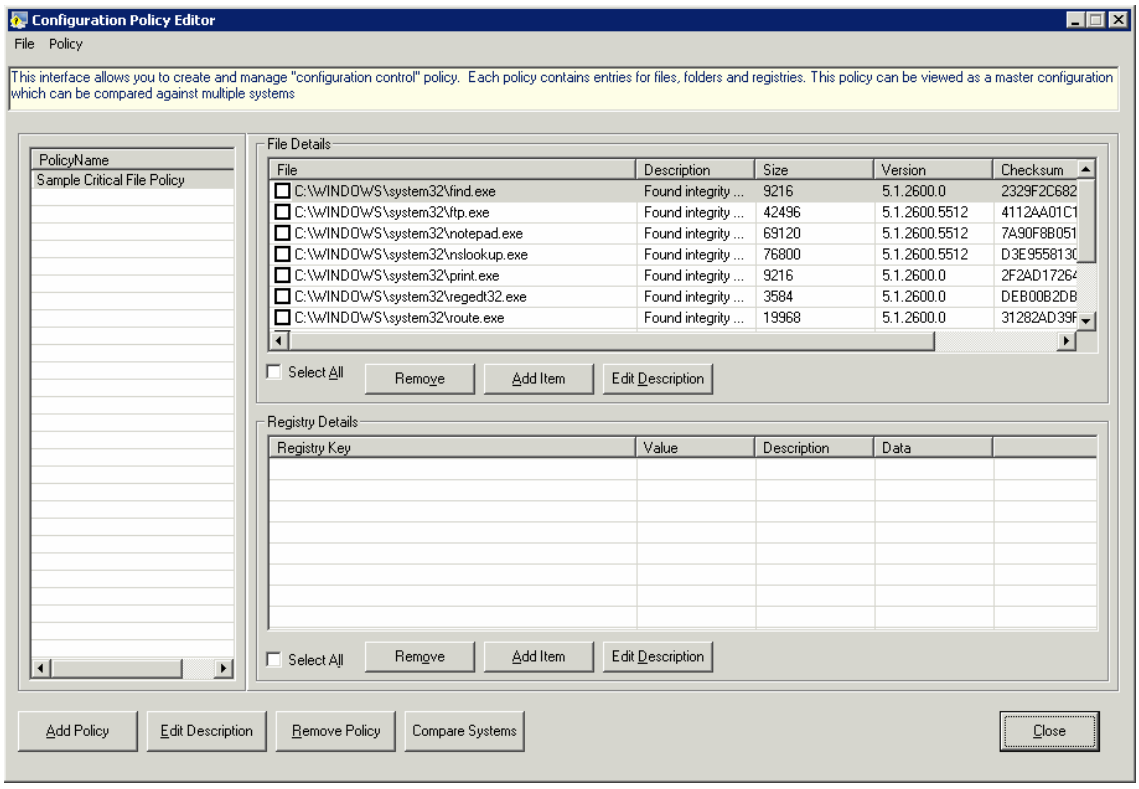
1.9.1 Change Browser

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 the **Configuration Policy Editor** option to open the **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 the 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 are 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.



Click	To
Add Policy	Create a new policy.
Edit Description	Edit the 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 the description of the selected item.
Select All	Select this check box to select all files.
Registry Details pane	
Remove	Remove the selected item from the Policy.
Add Item	Add an item to the Policy.
Edit Description	Edit the 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

The Change Policy Dashboard displays the summary of snapshot results.

The Configuration Policy Dashboard displays the most recent results of on-demand policy comparison done through the Compare Systems console and scheduled policy comparison done through Policy Comparison Scheduler.

Note

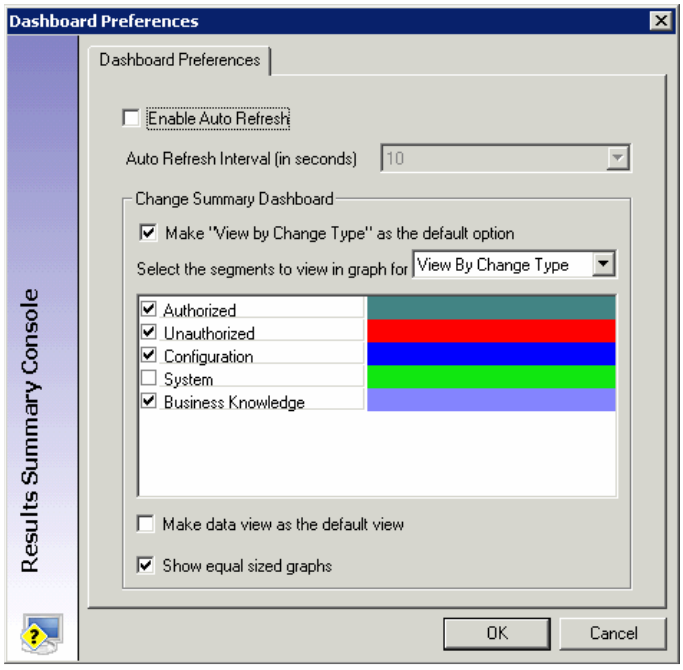
You can access the Results Summary Console from the Change Audit manager computer alone and not from the Netsurion Open XDR - Change Audit managed computers.

2.1 Setting Dashboard Preferences

This option helps to set preferences to view the change details. Preferences sets 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. The Results Summary Console displays the Dashboard Preferences window as shown below:



Field	Description
Enable Auto Refresh	Select this check box if you prefer Change Audit to refresh the Results Summary Console automatically. Change Audit enables the “Auto Refresh Interval [in seconds]” dropdown list. Set the interval to refresh the console.
Change Summary Dashboard	
Make “View by Change Type” as the default option	Change Audit selects this check box by default. Clear this check box if you prefer to view Object Type as the default view.
Select the segments to view in the graph for	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.
Make the data view as the default view.	Select this check box if you prefer to view “Data View” by default. Otherwise, Change Audit displays the “Graph View” as the default view.
Show equal-sized graphs.	Change Audit selects this check box by default. Clear this check box if you prefer to view unequal-sized graphs.

Note

To get data for Authorized, Configuration, and Business Knowledge, the user must add it manually by:

- Navigating to Netsurion Open XDR **Change Browser-> Options->Global Configuration->File Type.**
- Add the file types.

2. Set the preferences and then click **OK**.
3. To change the color of the preferred segment, click the color strip. Change Audit displays the browse button.
4. Click the browse button. Change Audit displays the color palette.

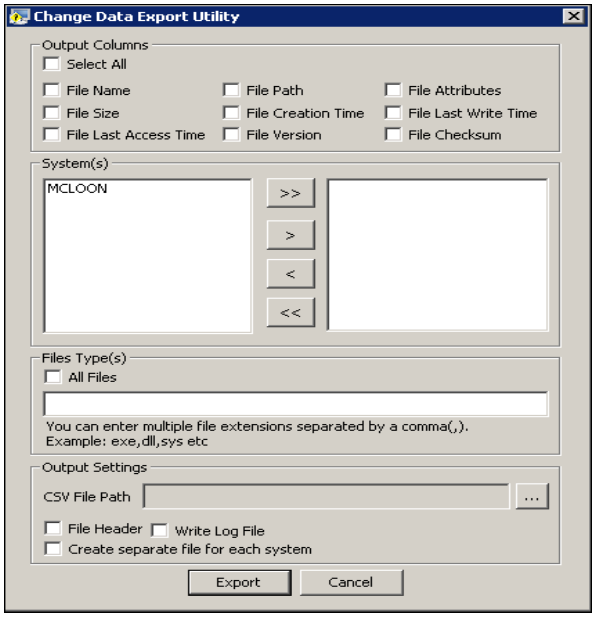
5. Select the color and then click **OK**.

2.2 Export Change Data

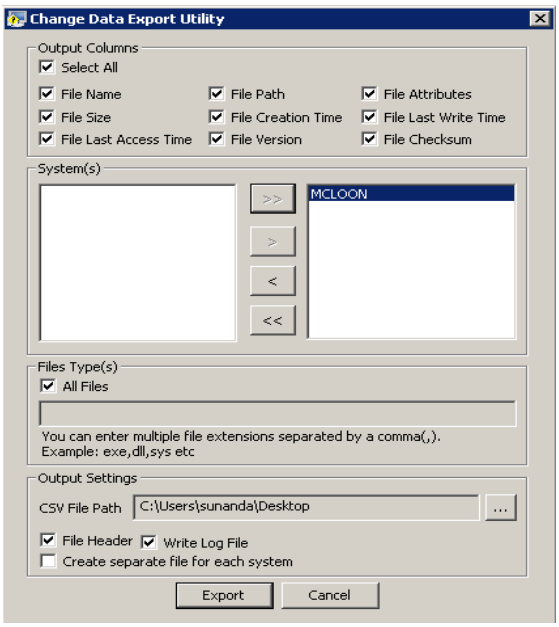
This option helps you to export the details about the files that are present on the system. Later, this list can be generated to track irrelevant files/processes.

To export Change Data, follow the below steps:

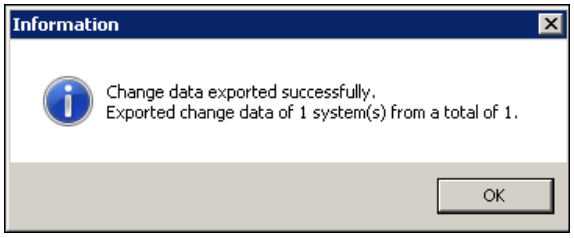
1. Click the **Tools** menu and then select **Export Change Data**. The **Change Data Export Utility** window will be displayed as shown below:



2. Select the required **Output Columns** or the **Select All** option.
3. In the **System(s)** pane, select the required systems.
4. In the **File Type(s)** pane, select the **All Files** option or enter the required file extensions separated by a comma.
5. In **the Output Settings** pane, browse the **CSV File Path**.
6. If required select **File Header, Write Log File, and Create a separate file for each system option**.



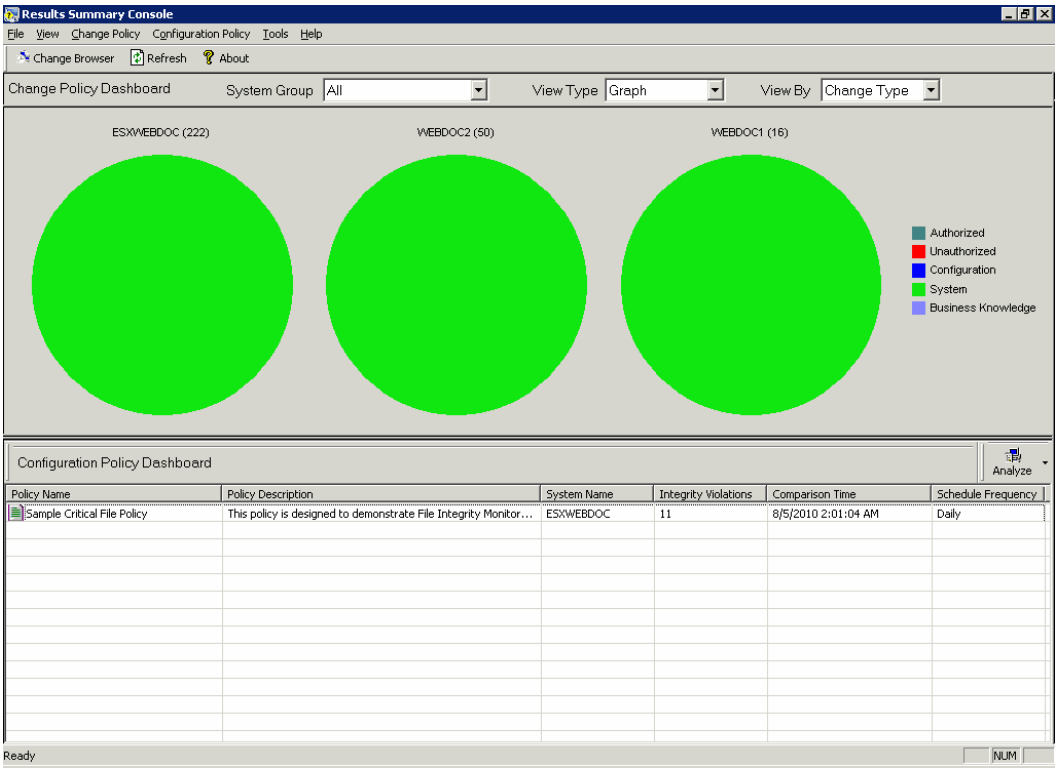
7. Select the **Export** button. A success message will be displayed as shown below:



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

2.3 Viewing the Summary of Change Details

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

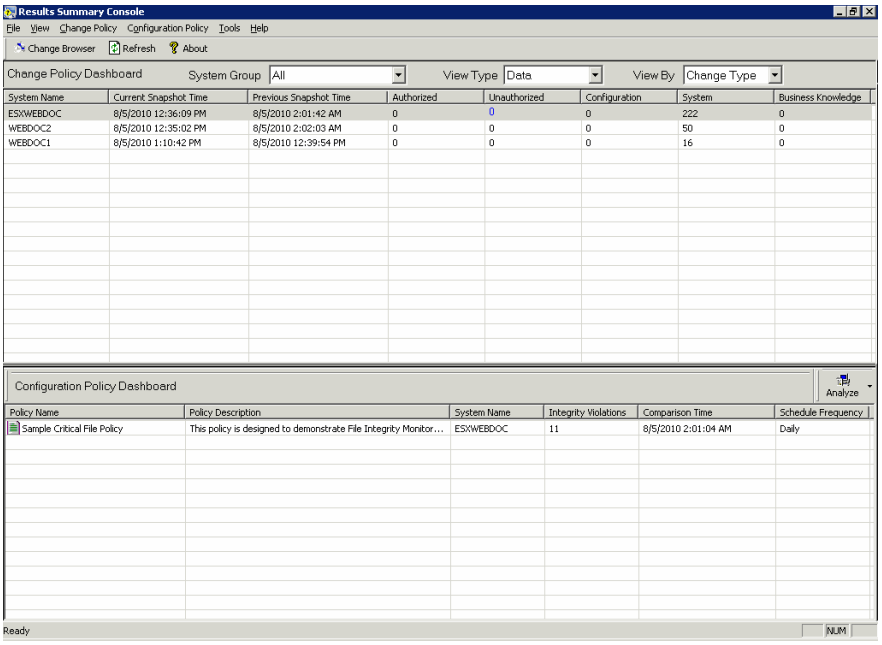


Note

Depending on the Configuration settings, the graph varies.

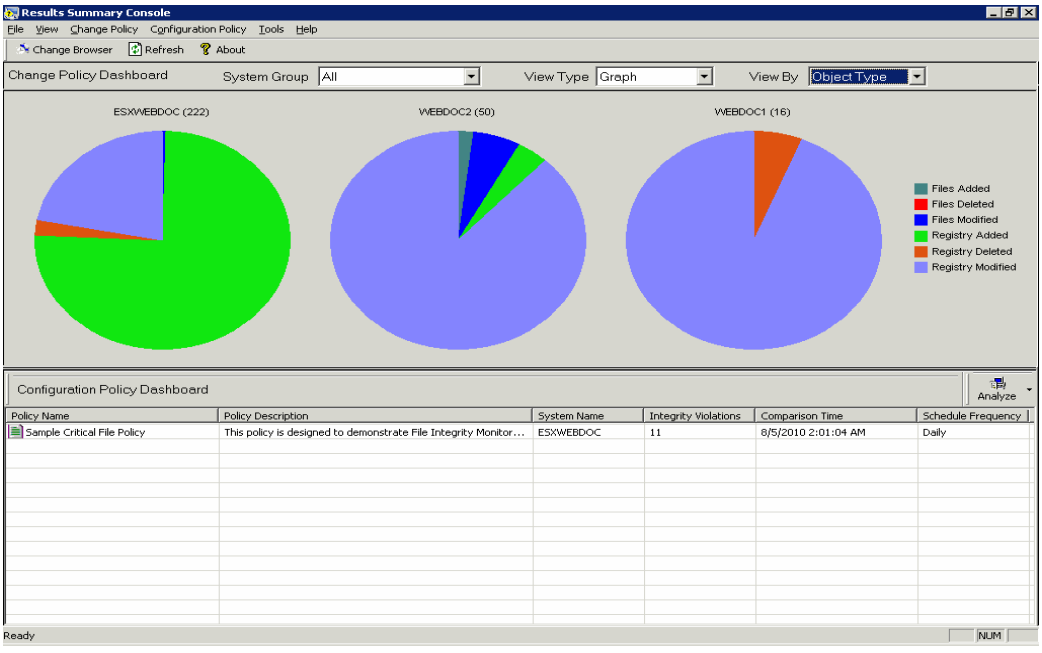
To view statistical data of Change Type, follow the below steps:

1. Select the **Data** option from the **View Type** dropdown list.
   (OR) Double-click the pie chart to view the data. The statistical data will be displayed as shown below:



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

1. Select the **Object Type** option from the **View By** dropdown list. The chart view summary of Object Type will be displayed as shown below:



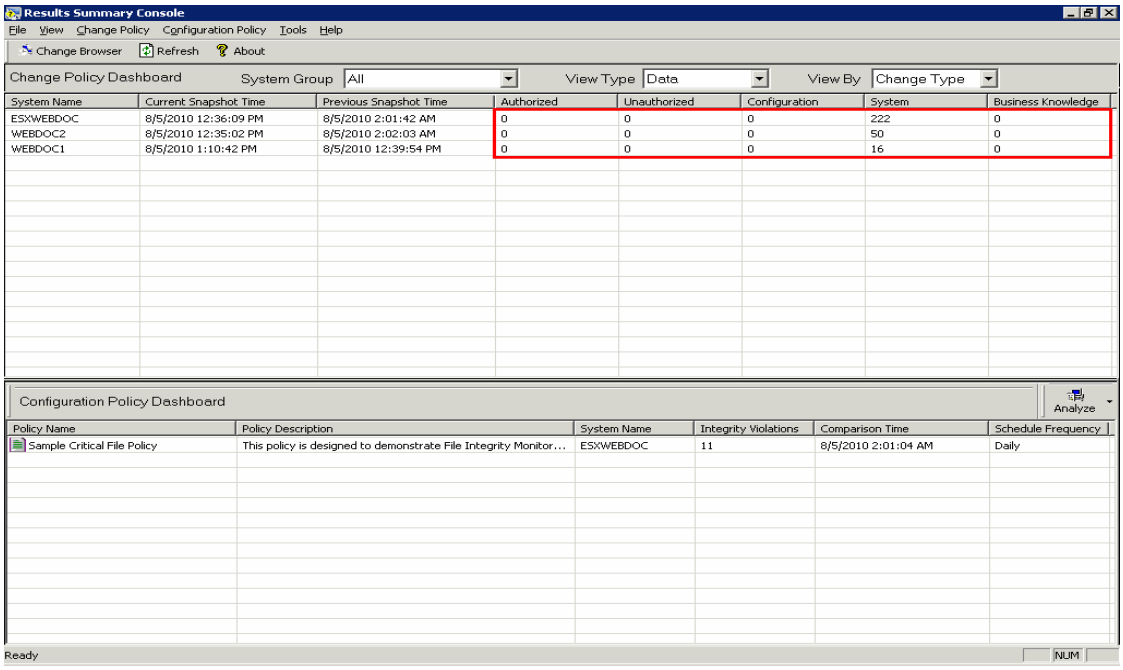
Note

Depending on the Configuration settings, the graph varies.

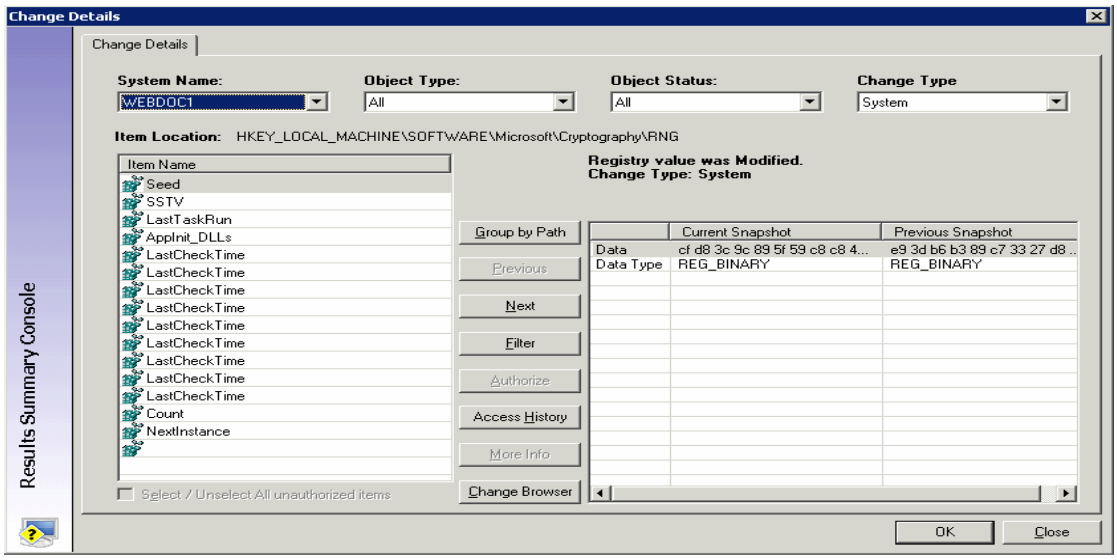
2.4 Viewing the Change Details Console

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

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



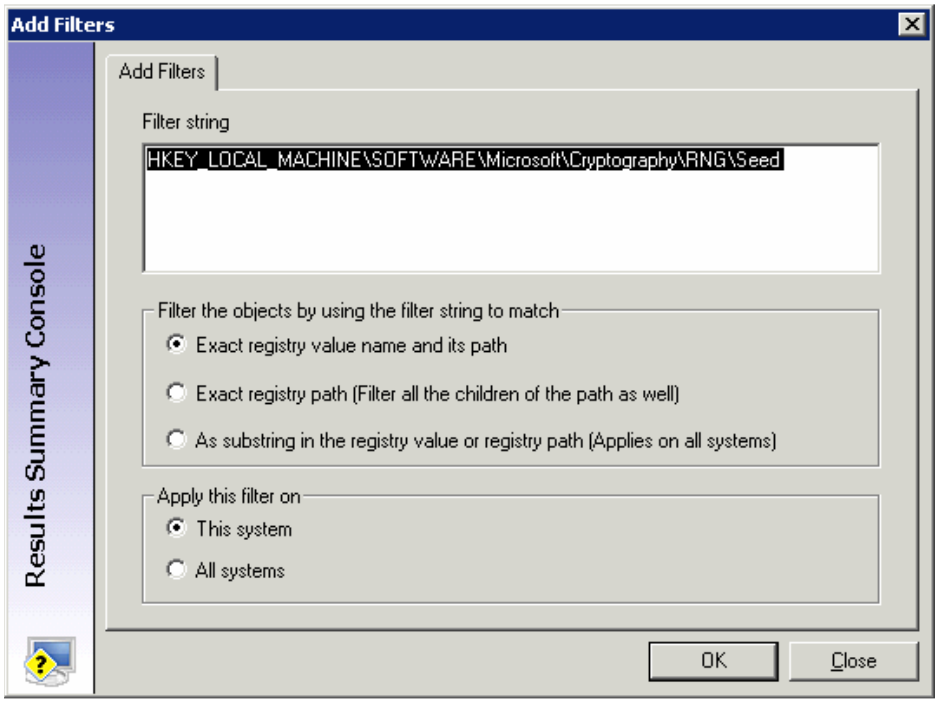
3. The **Results Summary Console** displays the Change Details,



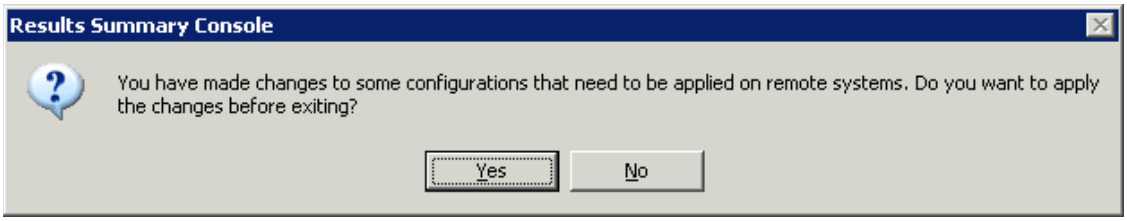
Note

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

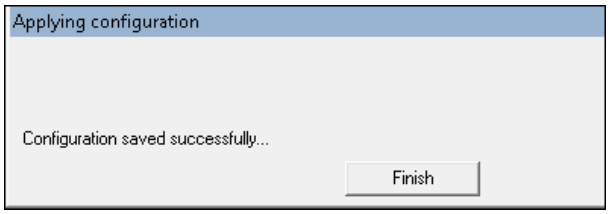
4. Select an item and then click **Filter** to add a new filter to System or Global Configuration.



5. Select an appropriate option under **Filter the objects by using the filter string to match**.
6. Select the **All systems** option under **Apply this filter** to add this filter to Global Configuration. Click **OK** on the Change Details console. A confirmation window will be displayed as shown below:

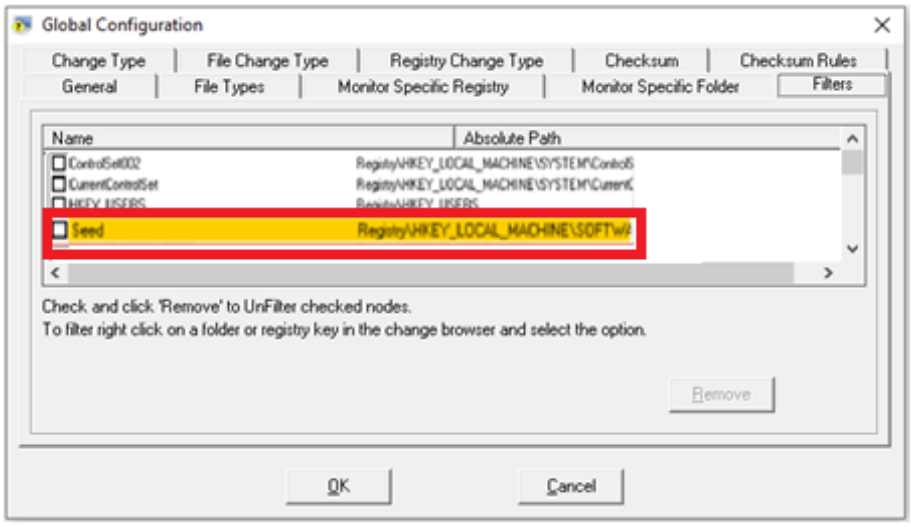


7. Click **Yes**. The Results Summary Console displays the **Applying Configuration** dialog box with the appropriate message.

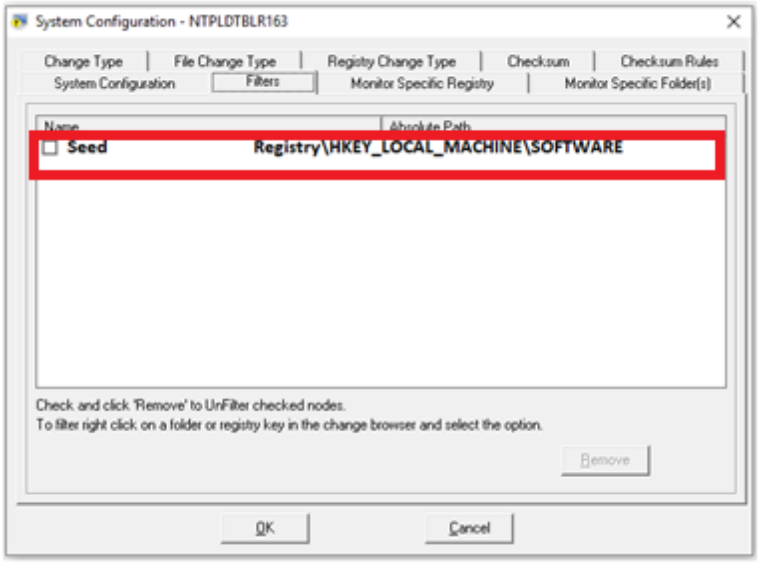


8. Click **Finish.**
9. Open the **Change Browser**.
10. Click the **Options** menu and select the **Global Configuration** option.

11. Click the **Filters** tab.



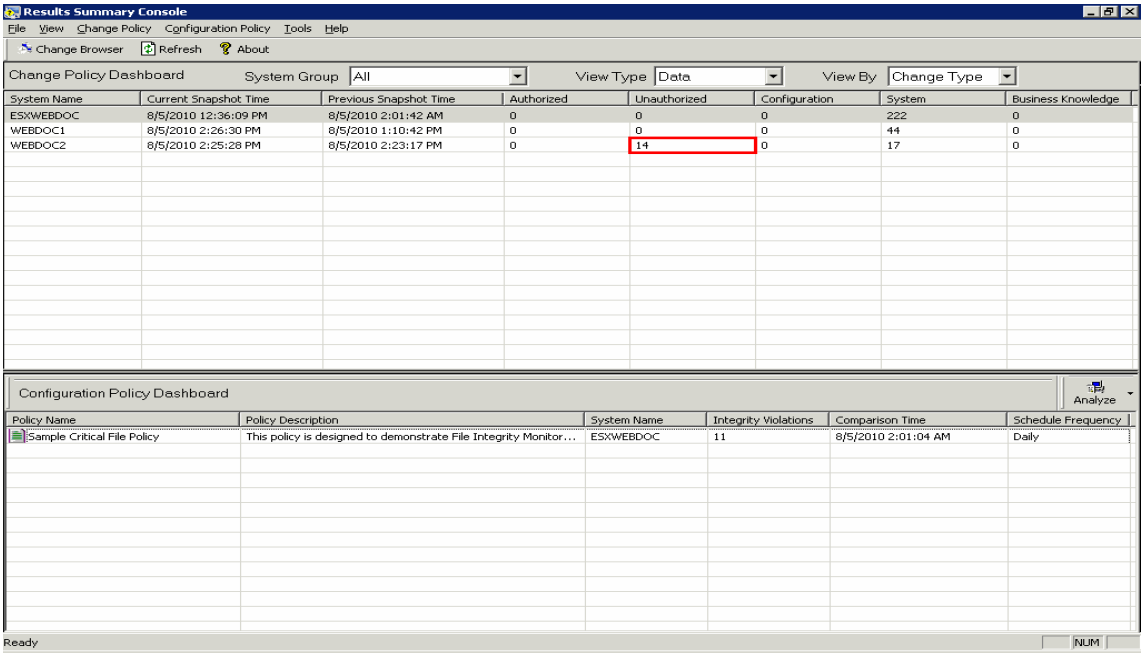
12. Select **This system** option under **Apply this filter** to add this filter to the System Configuration.
13. Open **Change Browser**.
14. Load the system that you want to view the newly added filter.
15. Click the **Options** menu and select the **System Configuration** option.
16. Click the **Filters** tab.



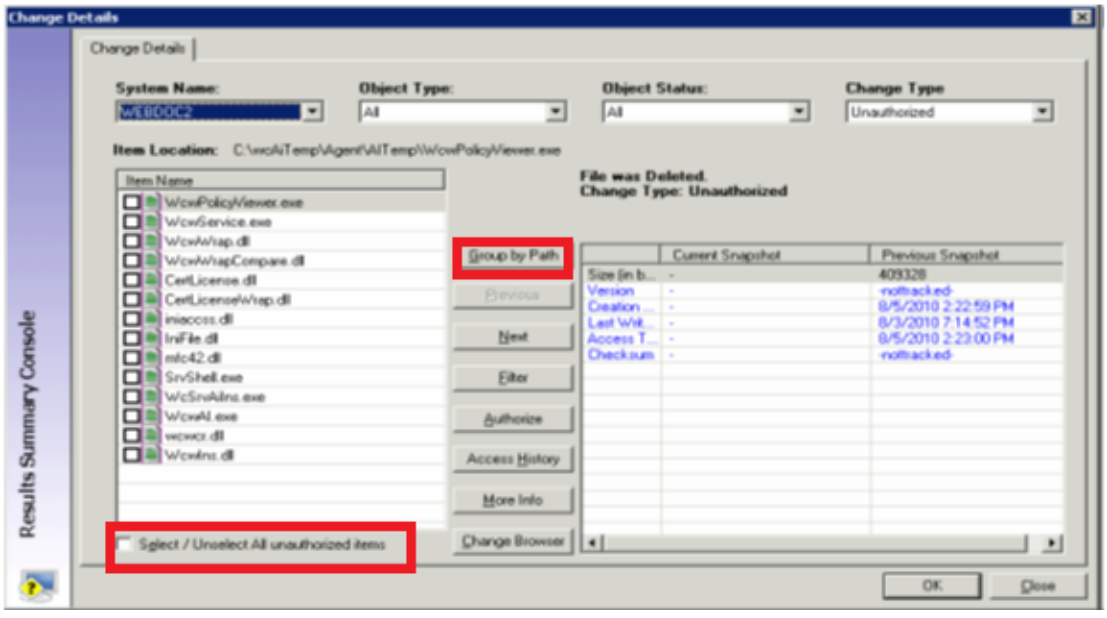
2.5 Authorizing Unauthorized Changes

To authorize unauthorized changes, follow the below steps:

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

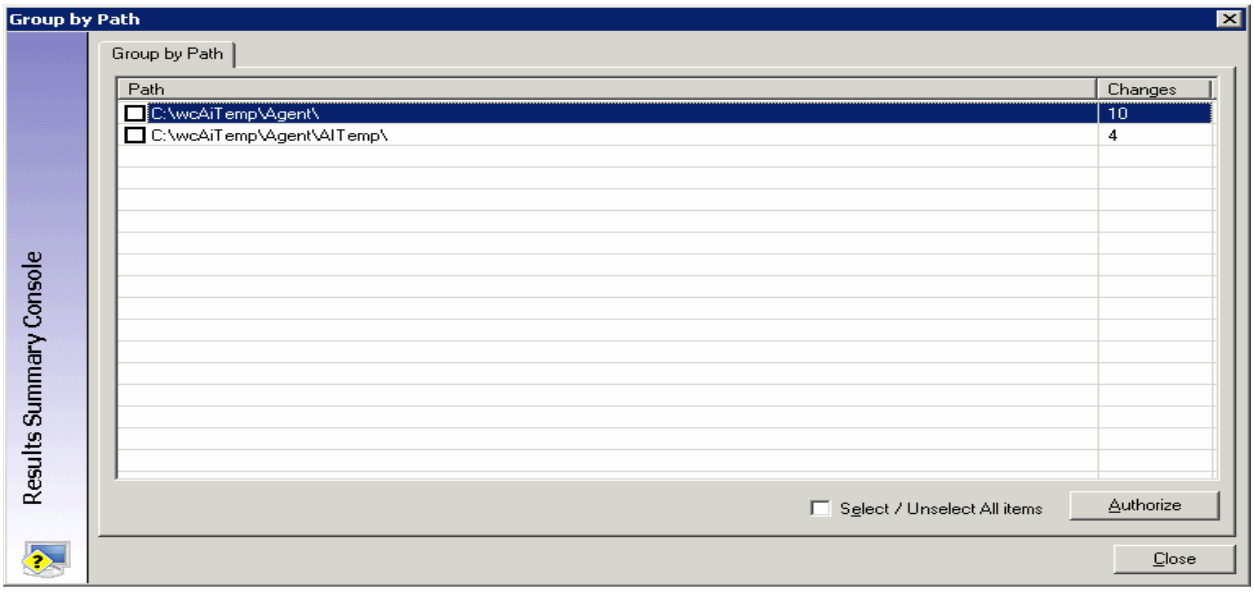


2. The Results Summary Console displays the Change Details page.



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)

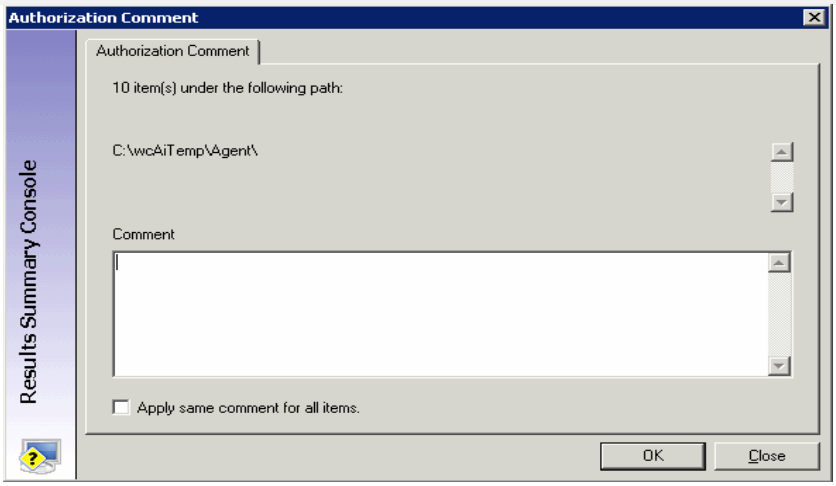
Click **Group by Path** to view all the unauthorized changes based on the location. The Results Summary Console displays the Group by Path window as shown below:



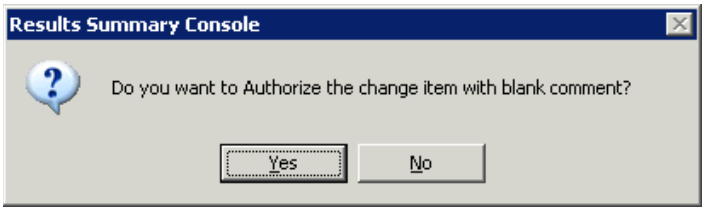
4. Select the items and then click **Authorize**.

Note

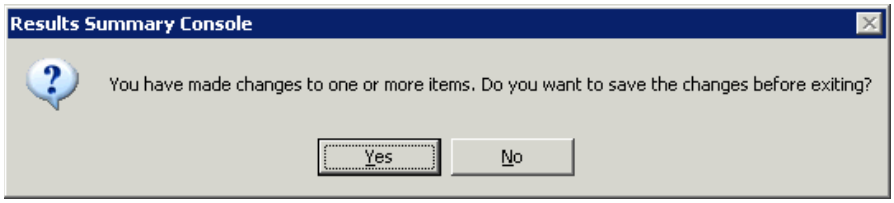
For the selected path, the Results Summary Console displays a separate **Authorization Comment** window.



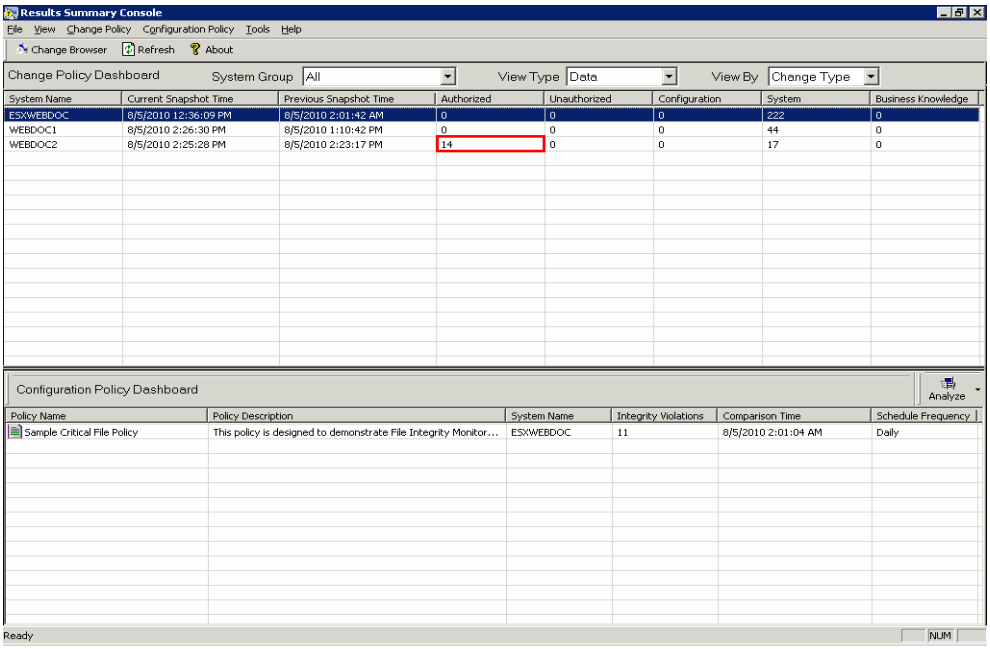
5. Type an appropriate comment.
6. Select the **Apply same comment for all items** check box if you wish to apply the comment for all items.
7. Click **OK**. If you leave the comment field empty, the Results Summary Console displays a confirmation message as shown below:



8. Click **Close** in the Group by Path window.
9. Click **OK** on the Change Details window.



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



2.6 Viewing the Change Details in the Change Browser

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

1. Click the hyperlink under the **System Name** column. The Change Audit loads the system in the Change Browser and displays the changes. The following are the alternative ways.
    a. Click the Change Policy menu and select the Change Browser option. Double-click the system that you want to view change details.
    b. Press **M** holding the **CTRL key** on your keyboard. Double-click the system that you want to view change details.

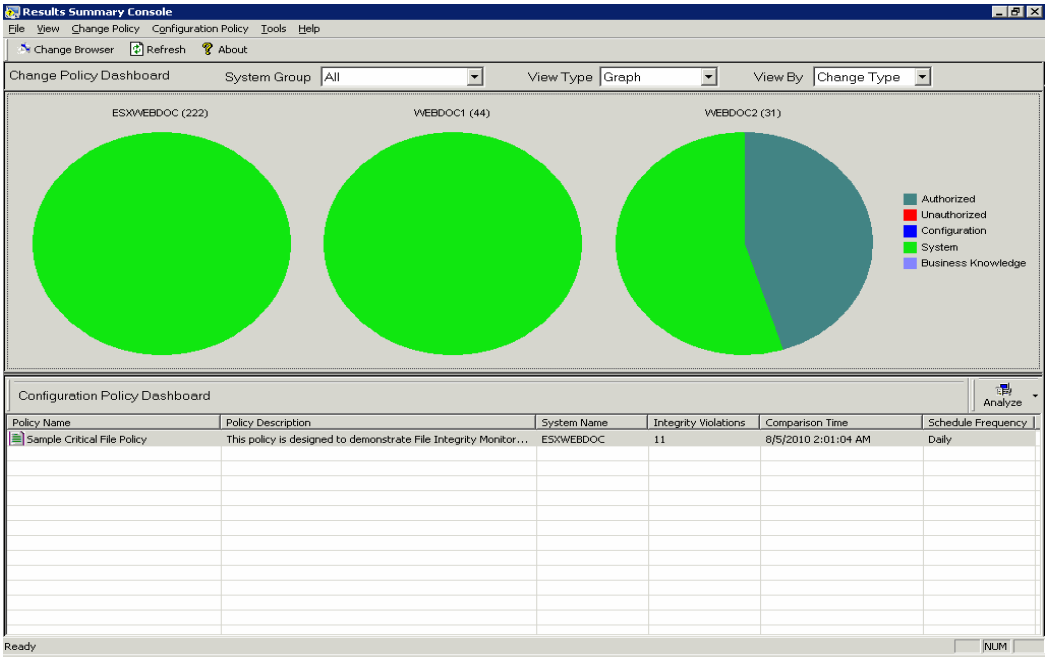
2.7 Viewing Change Report

To view the 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. The Results Summary Console displays the report.

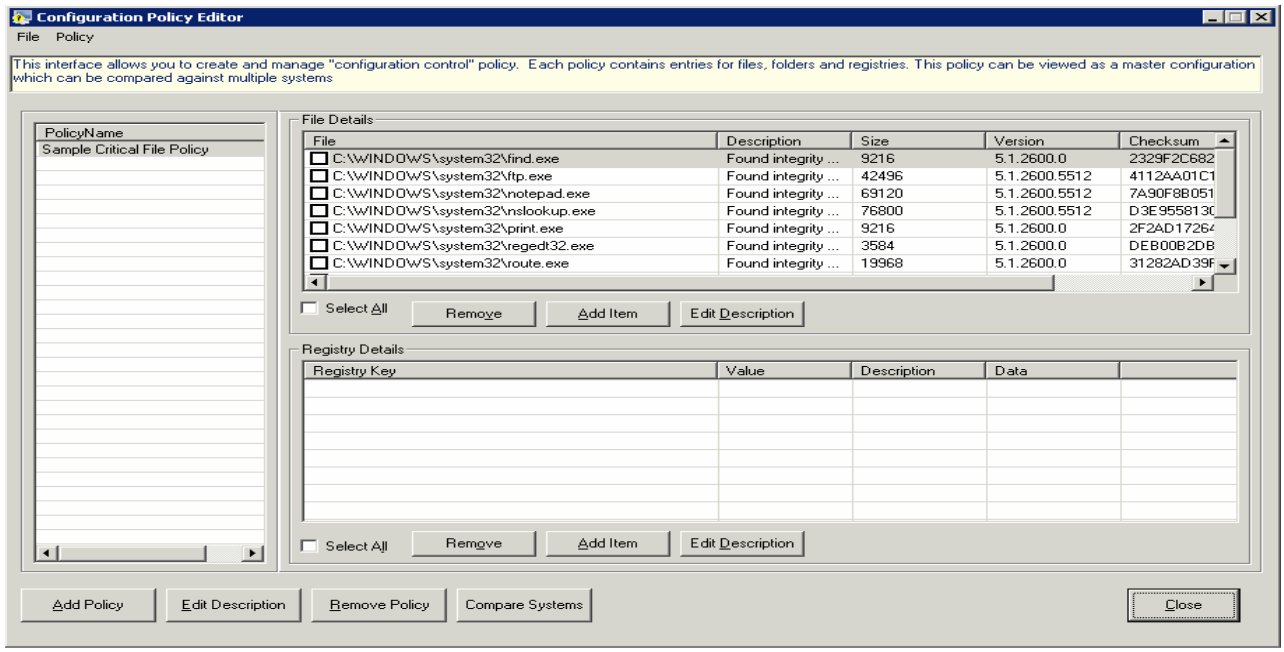
2.8 Configuration Policy Dashboard

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

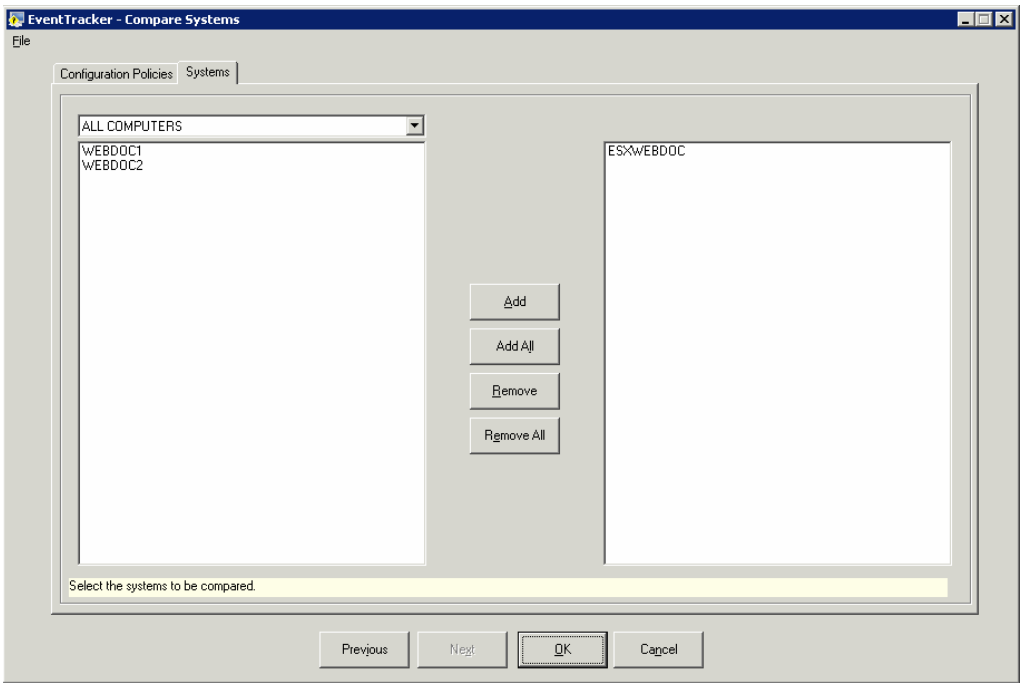


Icon	Description
	Snapshot in progress.
	No changes were found.
	File changes found.
	Registry changes found.
	File and registry changes found.

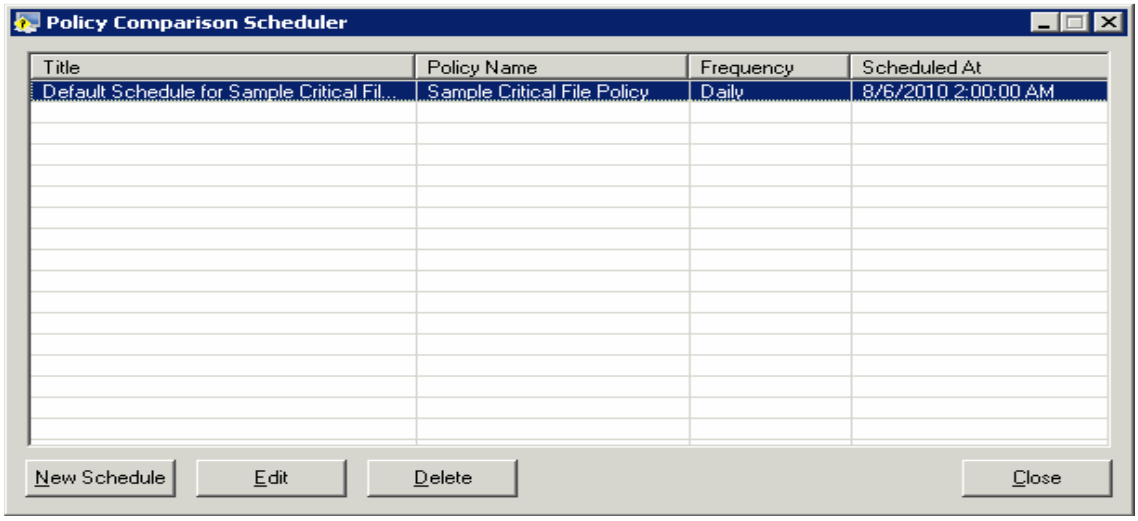
1. Click the name of the policy in the **Policy Name** column to view and edit policy details in the Configuration Policy Editor. The following are the alternative ways.
    a. Click the **Analyze** dropdown button. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Edit Policy**.
    b. Right-click a record. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Edit Policy**.



2. Click the name of the system in the **System Name** column to view and compare the system details. You can also compare policies on systems on demand. The following are the alternate ways.
    a. Click the **Analyze** dropdown button. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Run**.
    b. Right-click a record. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Run**.



3. Click the frequency of the schedule in the **Schedule Frequency** column to view and schedule policy comparison. The following are the alternate ways.
    a. Click the **Analyze** dropdown button. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Schedule**.
    b. Right-click a record. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Schedule**.



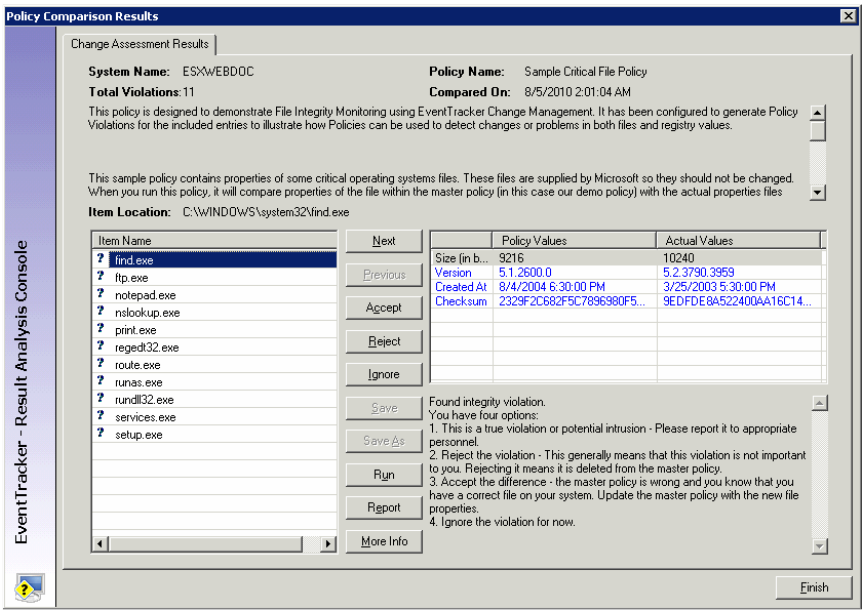
2.9 Analyzing the Policy Comparison Results

To analyze the policy comparison results, follow the below steps:

1. Click an item in the **Integrity Violations** column. (Configuration Policy Dashboard)**.**
2. Select an item and click the Analyze button. The Results Summary Console displays the shortcut menu.

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

3. The Results Summary Console displays the Policy Comparison Results window.



Field	Description
Top pane	
System Name	Name of the target system where the policy is compared.
Policy Name	Name of the policy compared to 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.
Actual Values	Actual Values of the policy item are 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
Tooltips are provided to understand the purpose of buttons. Hove the mouse 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 are 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 reports. **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.

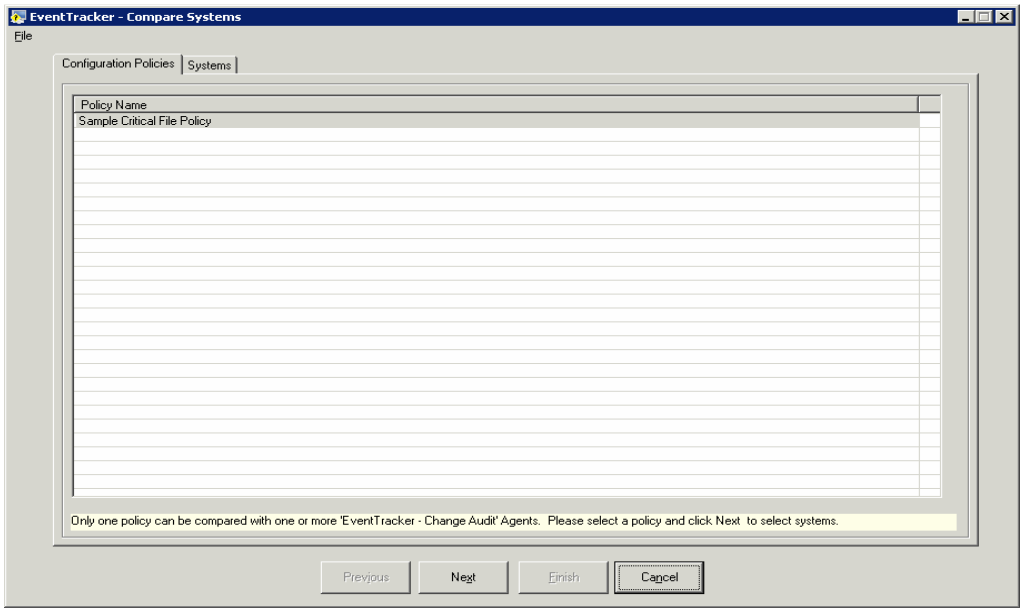
Icon	Represents
	No changes were found.
	Fresh item.
	Items accepted.
	Items ignored.
	Items rejected.

2.10 Compare Policies

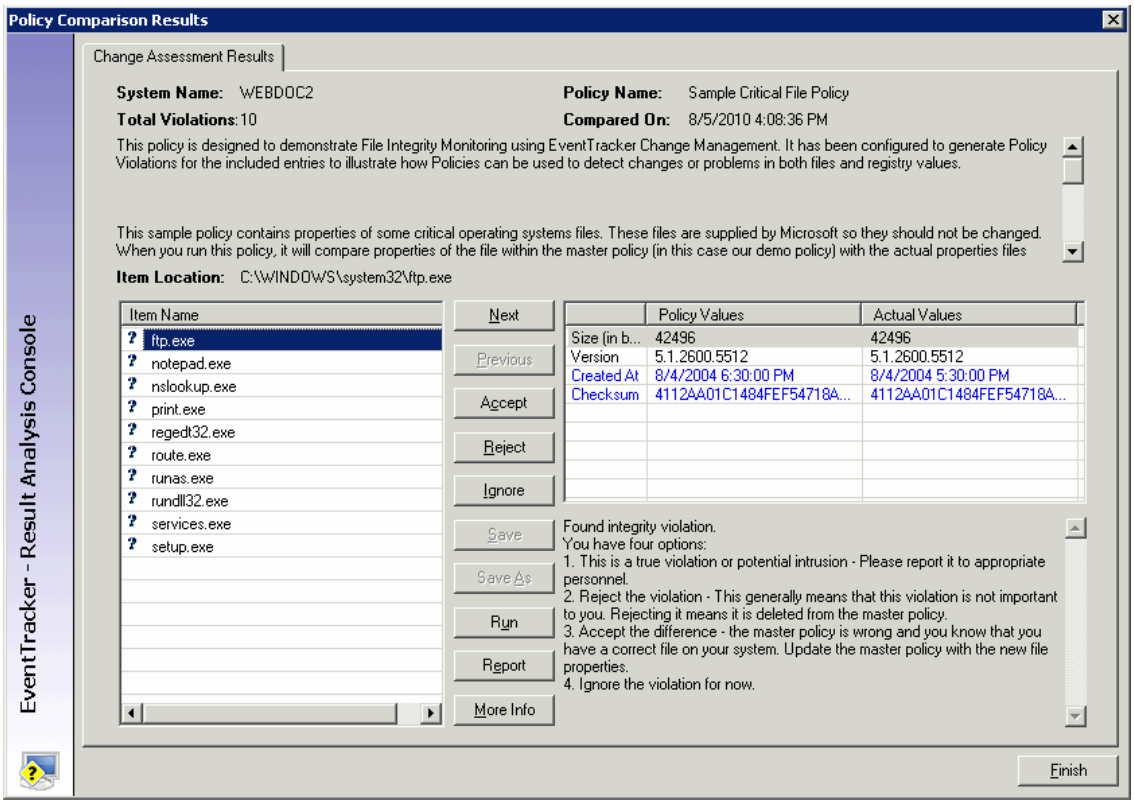
This option helps you compare policies on demand against managed systems.

To compare the 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. The Results Summary Console displays the Compare Systems window.



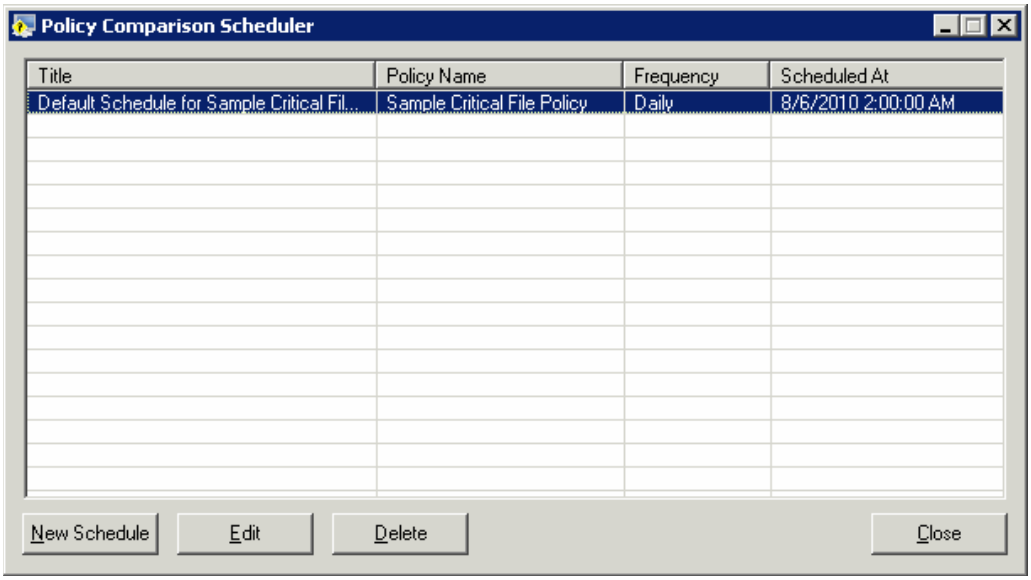
3. Select the policy that you want to compare and then click **Next**.
4. Select the domains/systems and then click **OK**. The Results Summary Console displays the result in the Policy Comparison Results window.



2.11 Scheduling the Policy Comparison

To schedule a policy comparison, follow the below steps:

1. Right-click a record. The Results Summary Console displays the shortcut menu. From the shortcut menu, choose **Schedule**. The following are the alternate ways.
    a. Click the **Analyze** button. The Results Summary Console displays the shortcut menu. From the shortcut menu, choose **Schedule**.
    b. Click the **Configuration Policy** menu and select the **Schedule Policy Comparison** option. The Results Summary Console displays the Policy Comparison Scheduler.



2. Set the schedule and then click **Close**. A red icon indicates policies that are scheduled for comparison.

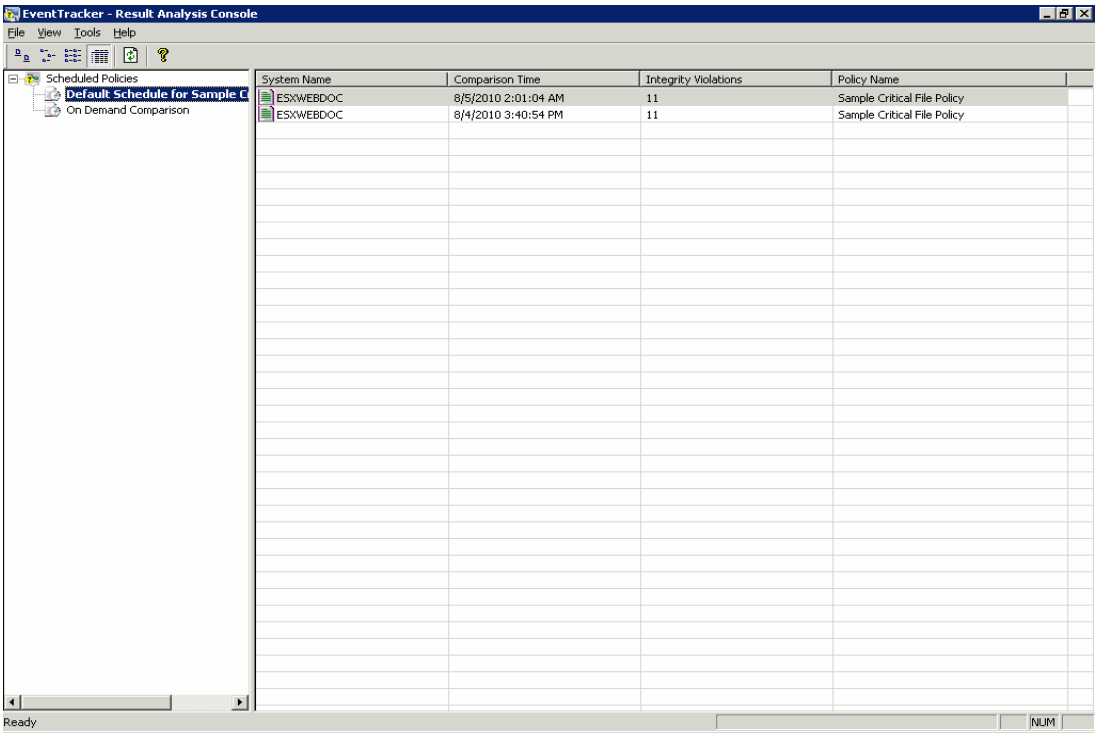
A red icon precedes the policy that is scheduled for comparison. The red icon appears only when the policy is scheduled for the first time. For the second and the consecutive executions, only the recent changes found are displayed with appropriate icons.

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 the 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.
3. Or, Double-click anywhere inside the Configuration Policy Dashboard. The Change Audit displays the Result Analysis Console.



The 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.

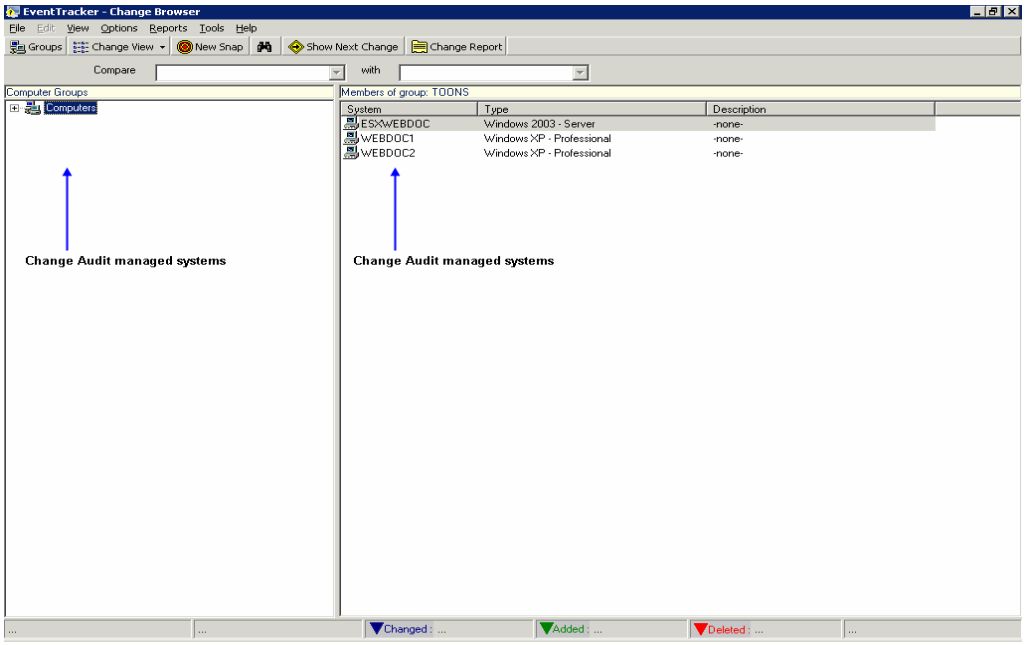
Follow the below steps, to Switch to the Groups view.

1. Open **Change Browser**.

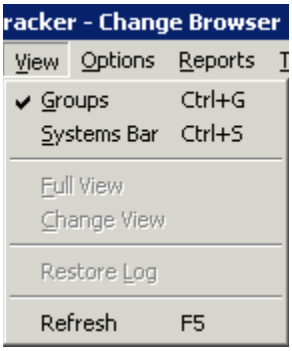
Note

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

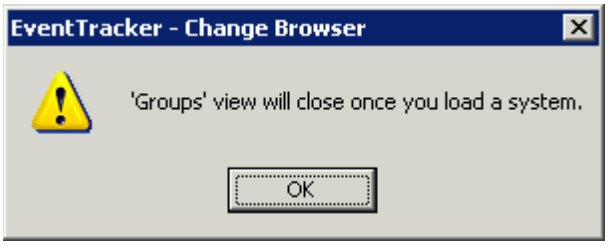
2. Click the **View** menu and select the **Groups** option. The alternate ways are given below:
    a. Press **G** holding the **Ctrl** key on the keyboard. The Change Audit displays the **Groups** view.
    b. Click **Groups** on the toolbar.



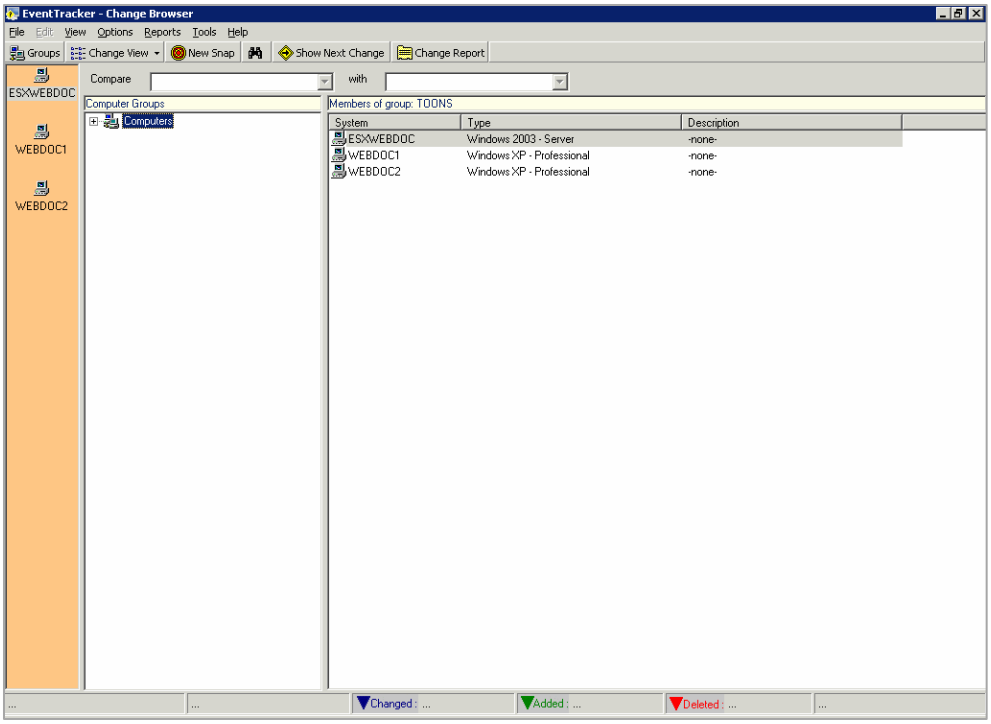
3. To view Groups, expand the **computers** node on the left pane.
4. Click a Group. The Change Audit displays the members of that Group alone on the Right pane. A check box appears before the Groups command in the **View** menu when Change Audit displays the Groups view.



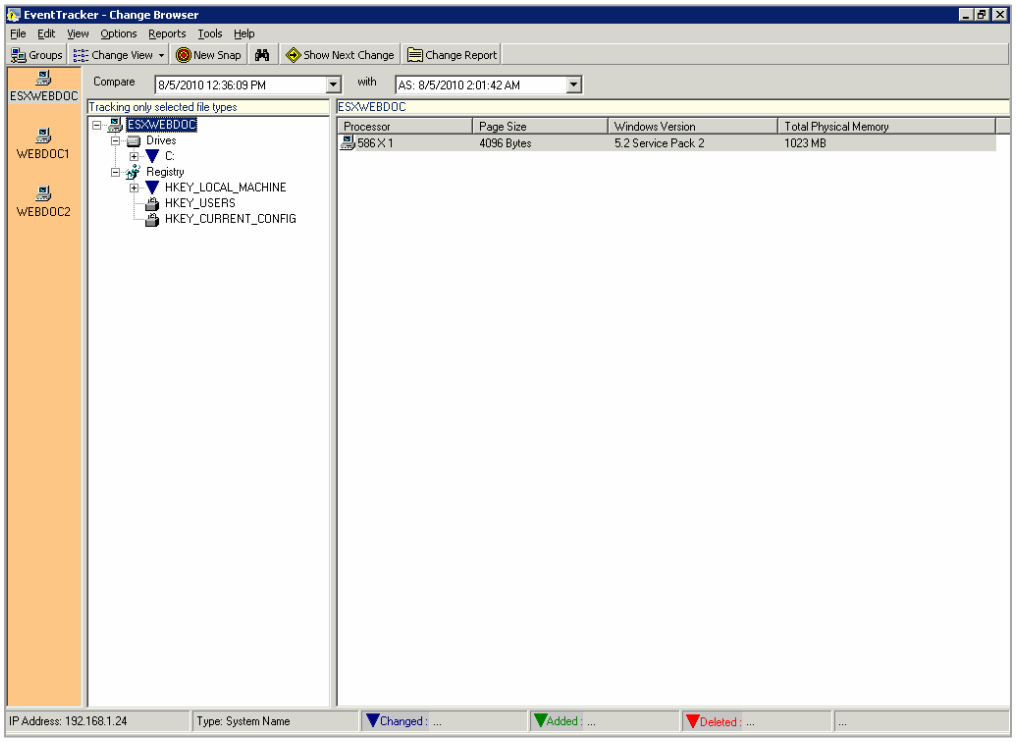
5. If you try to unselect the checkbox, Change Audit displays the Change Browser dialog box.



6. To access the System Bar, click the **View** menu and select the **System Bar** option. Or, Press **S** holding the **Ctrl** key on your keyboard. The Change Audit displays the System Bar.



7. Double-click a system on the System Bar or the right pane to view change details. The Change Audit loads the system and displays the change details.

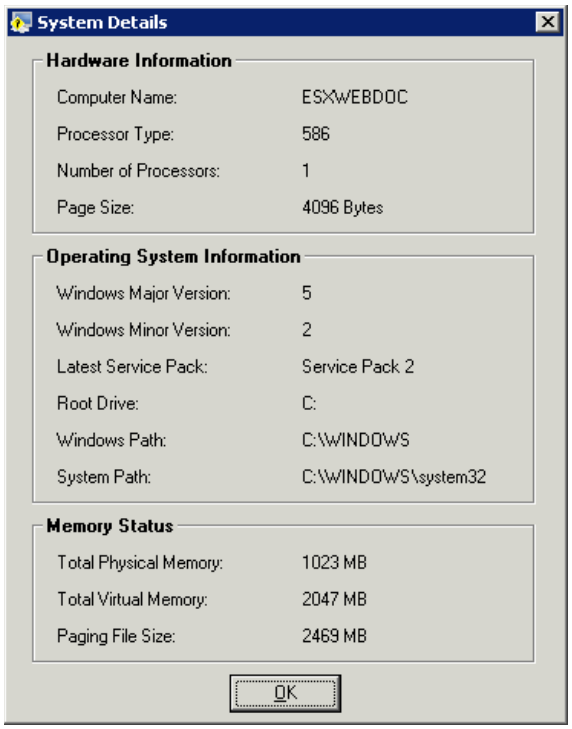


3.2 Viewing System Details

This option helps you view the 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. The Change Audit displays the shortcut menu. From the shortcut menu, choose Details. The Change Audit displays the System Details window.



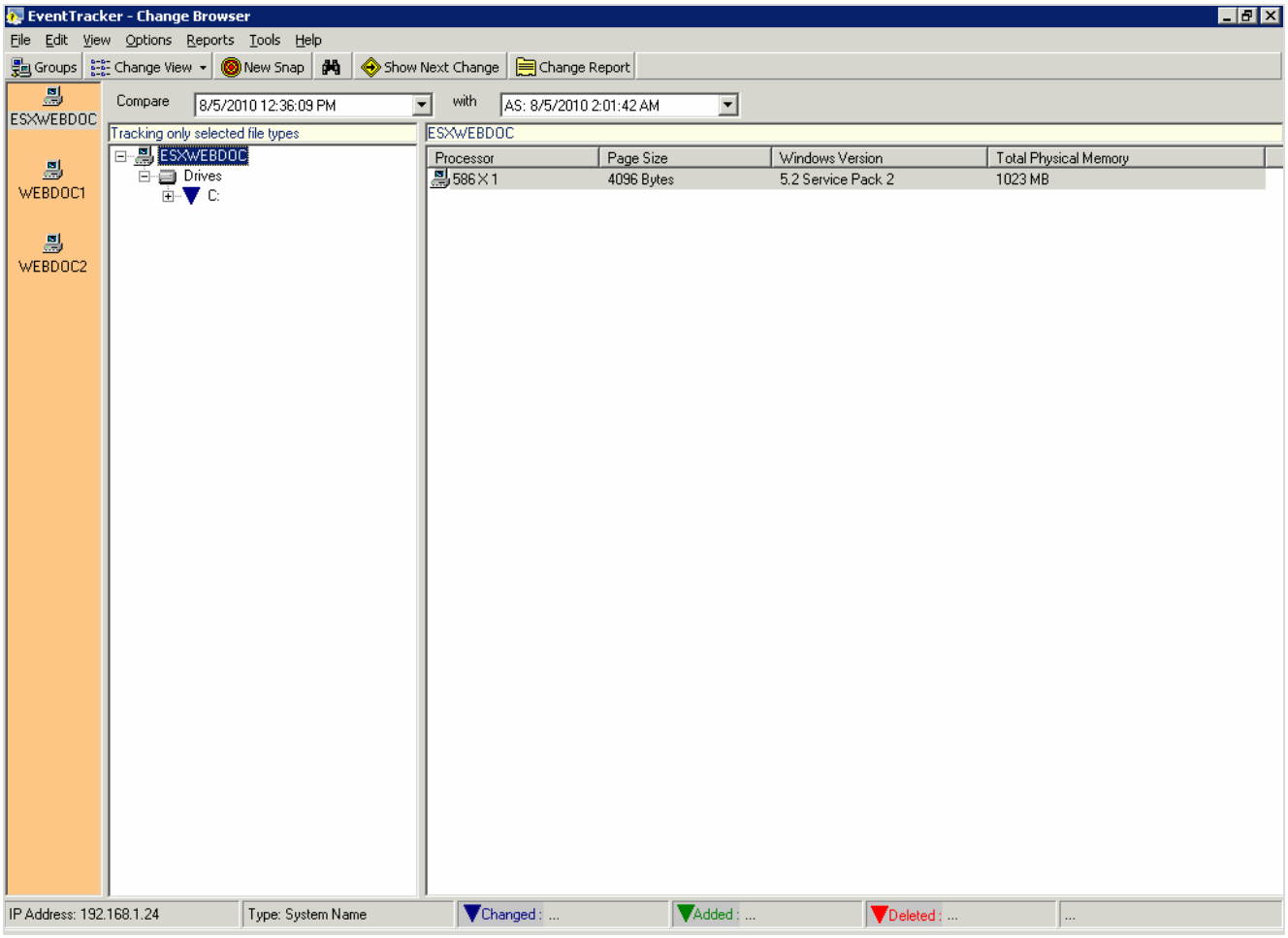
3. If there is no Snapshot for the selected system, then Change Audit displays the error message.

3.3 Viewing the File System Changes

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

To view 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. The Change Audit displays the shortcut menu.
3. From the shortcut menu, choose **File System**. The Change Audit loads and displays the File System details of the selected computer.

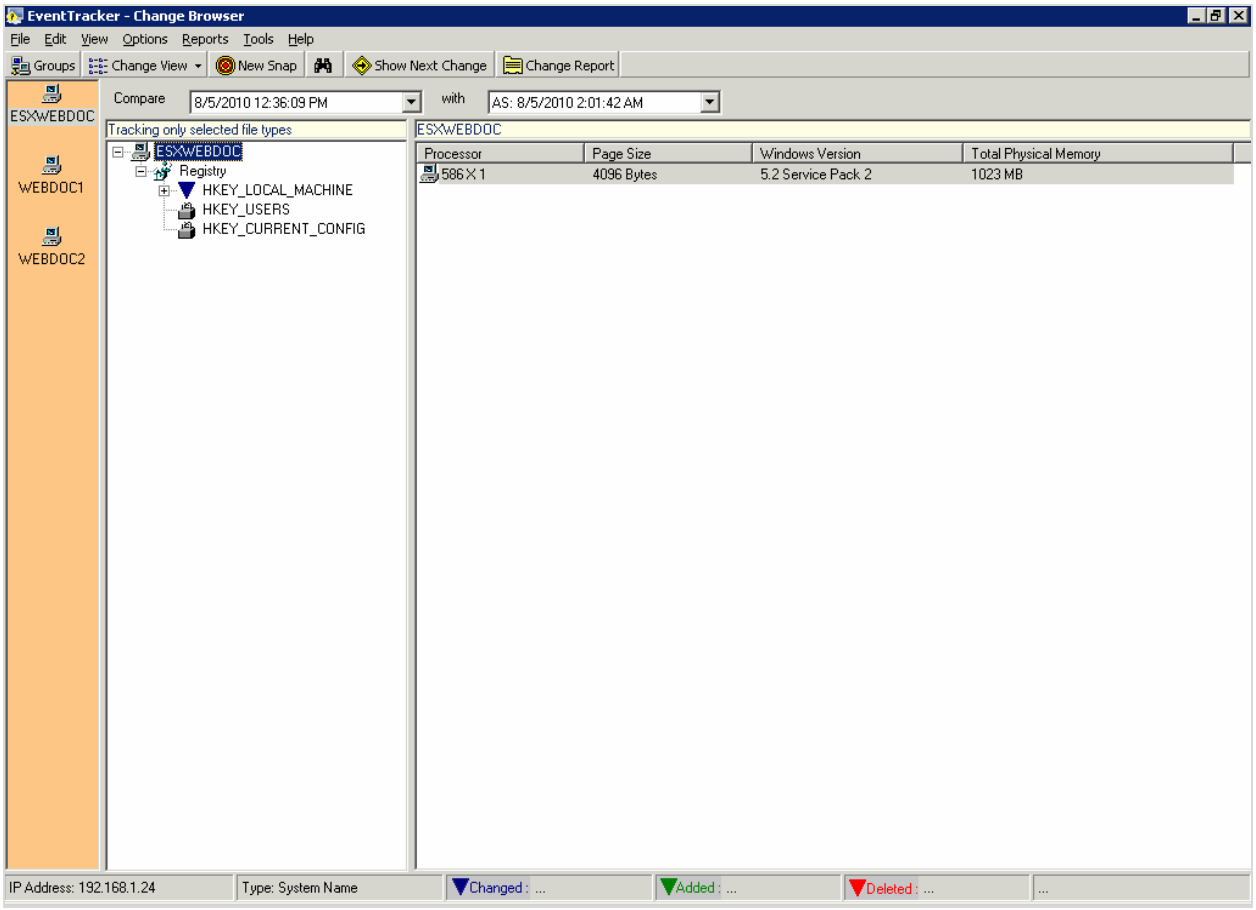


3.4 Viewing the Registry Changes

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. The Change Audit displays the shortcut menu.
3. From the shortcut menu, choose **Registry**. The Change Audit loads and displays the registry details of the selected computer.



3.5 Full View Option

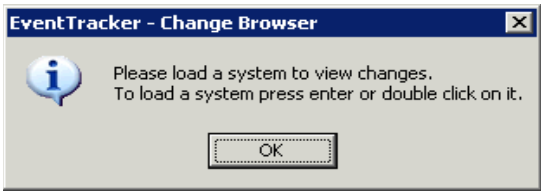
This option helps you fully/completely view the monitored computers. In Full View, Change Audit compares the two latest Snapshots and displays the difference in Snapshots that includes Addition, Deletion, or Modification of files, folders and registry keys, filtered items, and all other unaltered items.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

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

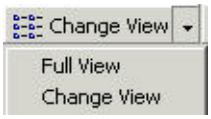
1. Double-click a system on the System Bar.

Note

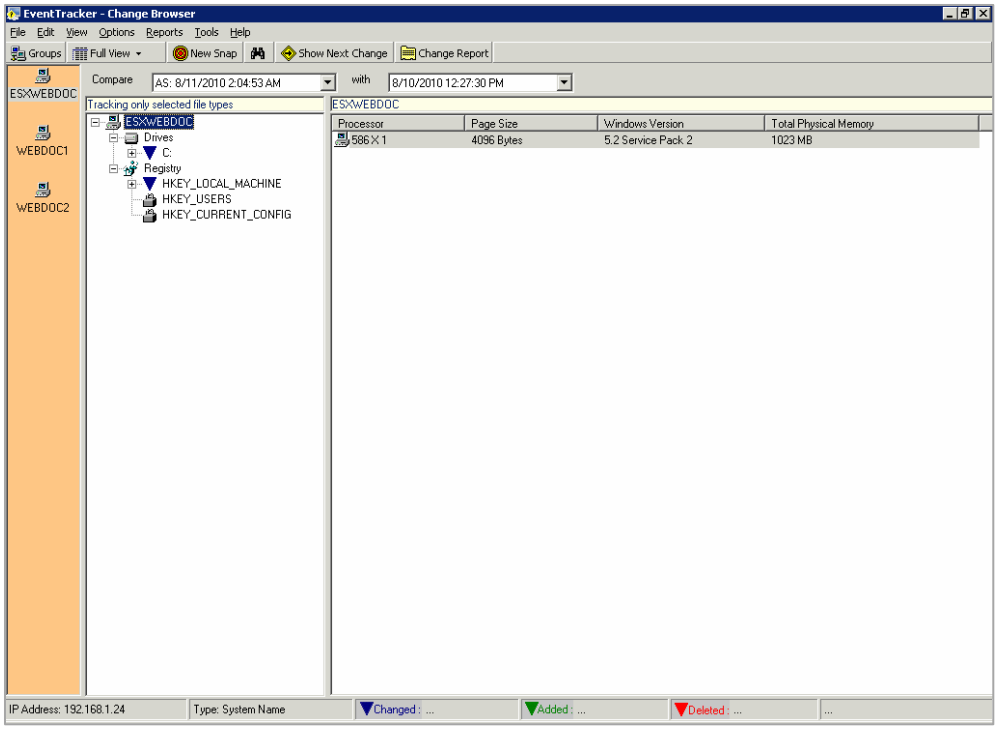
If you click the toggle button when Change Audit displays the Groups view, then Change Audit displays the dialog box to load the system as shown in the following figure.



2. Click the **View** menu and select the **Full View** option. Or, Click the toggle button on the toolbar. The Change Audit displays the shortcut menu.



3. From the shortcut menu, choose **Full View**.
4. Expand the Drives or Registry trees and click an item. The Change Audit displays the Full View.



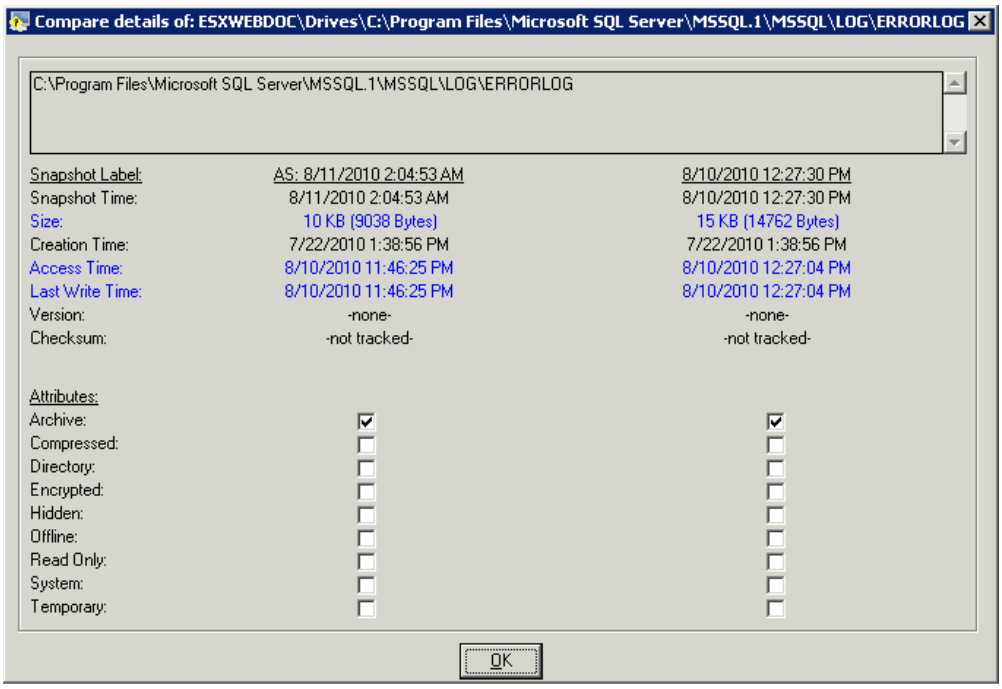
5. Hover the items on the left and right panes. The Change Audit displays the tooltip about the status of the item.

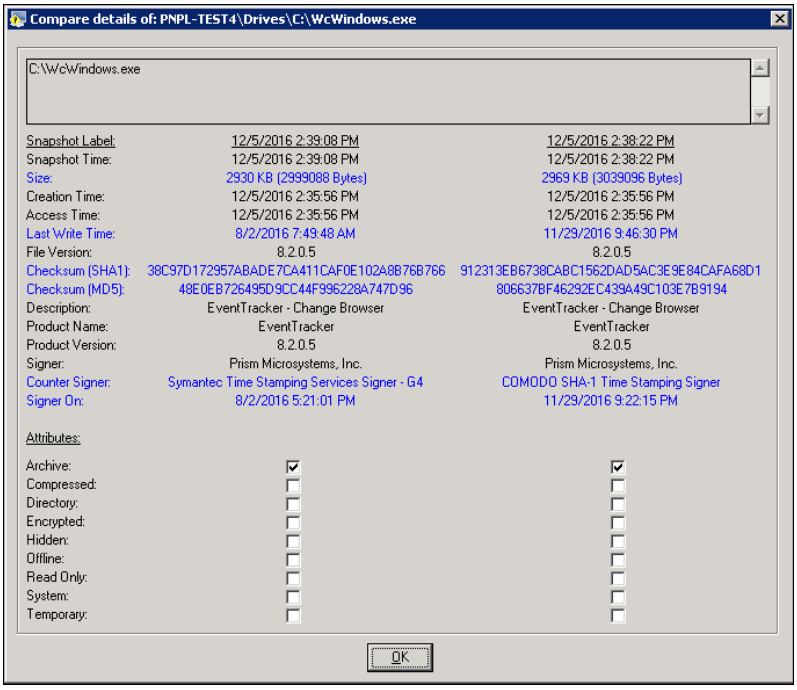
3.6 Viewing the Comparison Details

This option helps you view and compare the details of folders and files.

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

1. Expand the File system tree.
2. Click the folder on the left pane. Change Audit displays the sub-folder or files 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.
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. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Compare details**.





The Comparison details consist of the following:

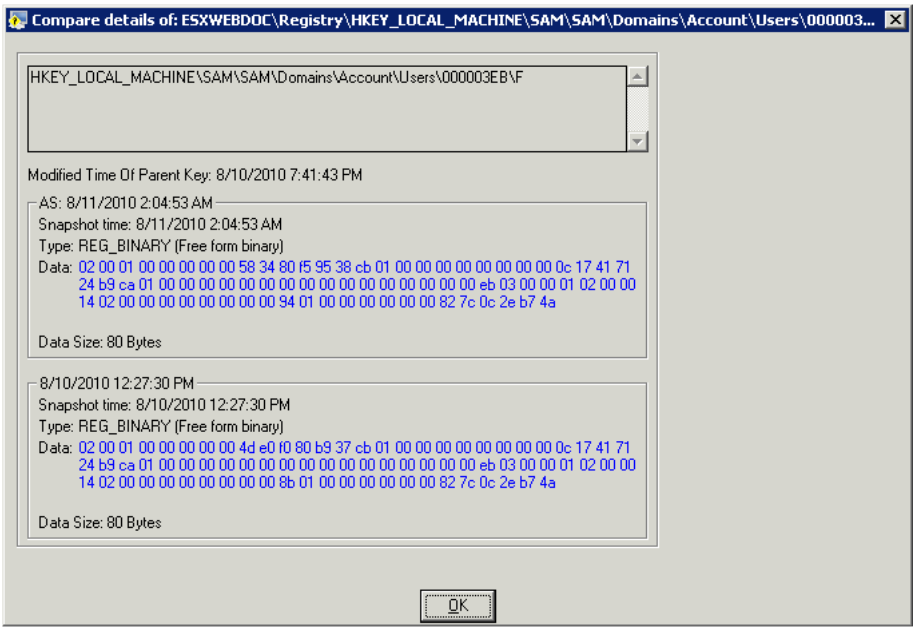
- MD5 Checksum
- File Description
- Product Name
- Product Version
- Signer
- Counter Signer
- Signed On

3.7 Comparing the Details of the Registry Items

This option helps you compare the details of the Registry items.

To compare the 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 or right-click an item on the right pane. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Compare details**.



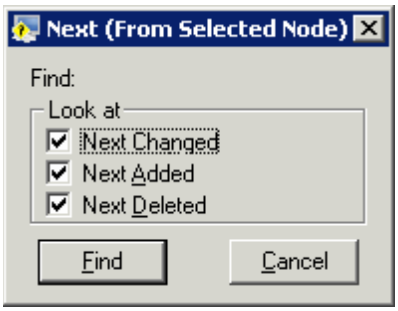
3.8 Change View

In Change View, Change Audit compares the 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 dropdown lists.

3.9 Find Changes Option

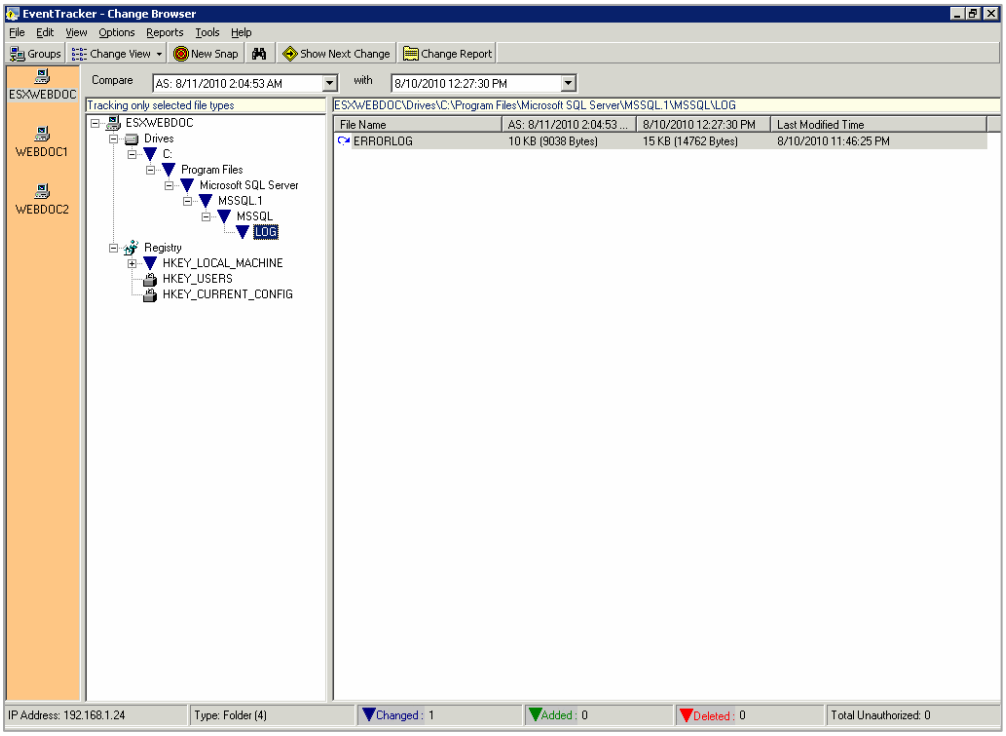
This option helps you find addition, deletion, and modification of folders, files, and values both in Full and Change Views.

1. Click the **Edit** menu and select the **Find Change** option. Or, press **N** holding the **Ctrl** key on the keyboard. The Change Audit displays the Next (From Selected Node) dialog box.



Field	Description
Next Changed	This check box is selected by default. This option enables you to view the modified items. Unselect this if you do not want to view the modified items.
Next Added	This check box is selected by default. This option enables you to view the added items. Unselect this if you do not want to view the Added items.
Next Deleted	This check box is selected by default. This option enables you to view the deleted items. Unselect this if you do not want to view the Deleted items.

2. Select the option appropriately and then click **Find**. The Change Audit displays the Change Browser with the change details.

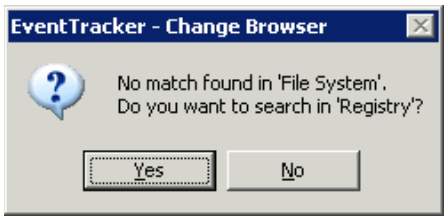


(OR)

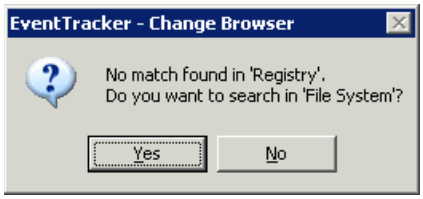
Click on the toolbar. This option is equivalent to selecting all the checkboxes in the Next (From Selected Node) dialog box.

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.

3. Change Audit displays the next change.
4. If there is no change in the File System to display, the Change Audit displays the following message.



5. If there is no change in the Registry to display, the Change Audit displays the following message.

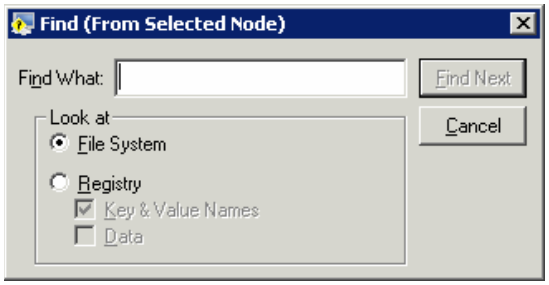


3.10 Search Strings

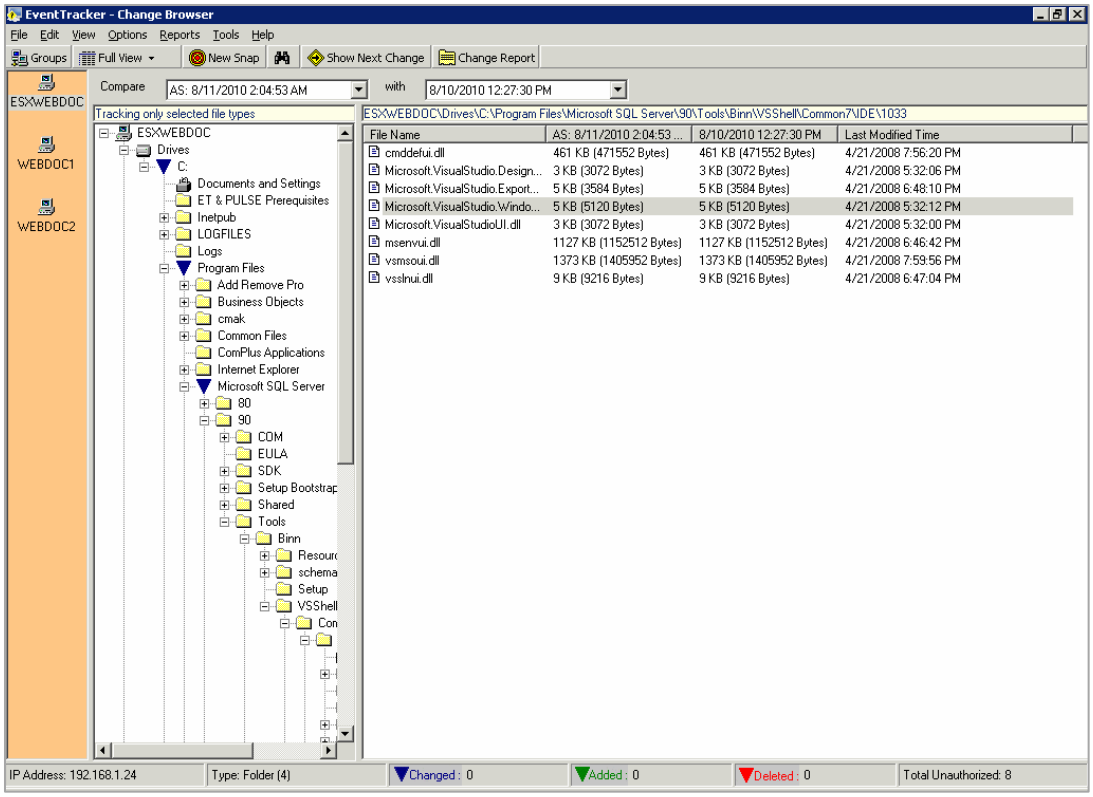
This option helps you search strings both in Full and Change Views.

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

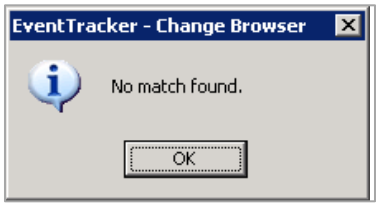
1. Open the Change Browser.
2. Click the **Edit** menu and select the **Find** option. The following are the alternate ways.
    a. Press F holding the Ctrl key on the keyboard.
    b. Click the toolbar. Change Audit displays the Find (From Selected Node) dialog box.



3. Enter the string in the **Find What** field.
   Example: Windows.
4. Click **Find Next**. The Change Audit displays the search result.



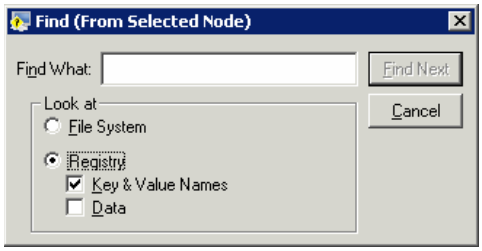
If there are no matches found, then Change Audit displays a No Match Found message.



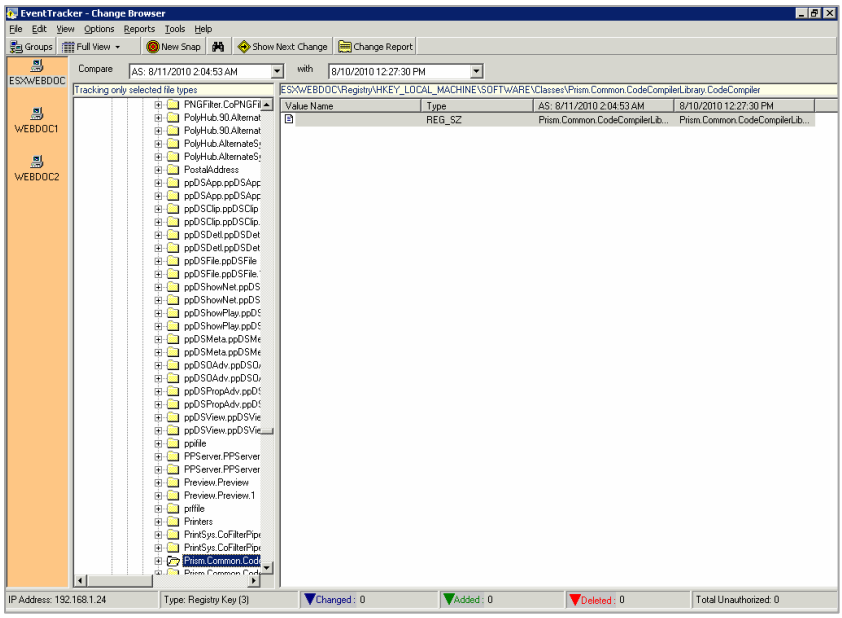
5. To find the consecutive occurrence of the string searched for, click the **Edit** menu, select the **Find Next** option, or press F3 on your keyboard.

3.11 Searching the Strings in the Registry

1. Open the Change Browser.
2. Click the **Edit** menu and select the **Find** option. The following are the alternate ways.
    a. Press F holding the Ctrl key on your keyboard.
    b. Click on the toolbar. The Change Audit displays the Find (From Selected Node) dialog box.
3. Select the **Registry** option.



4. Type the string in **Find What** field.
   Example: Prism.
5. Click **Find Next**. The Change Audit displays the search result.



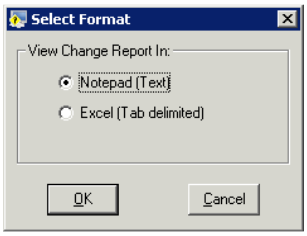
6. To find the consecutive occurrence of the string searched for, click the **Edit** menu, select the **Find Next** option, or press F3 on your keyboard.

3.12 Generating the Change Report

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

To Generate a Change report, follow the steps below:

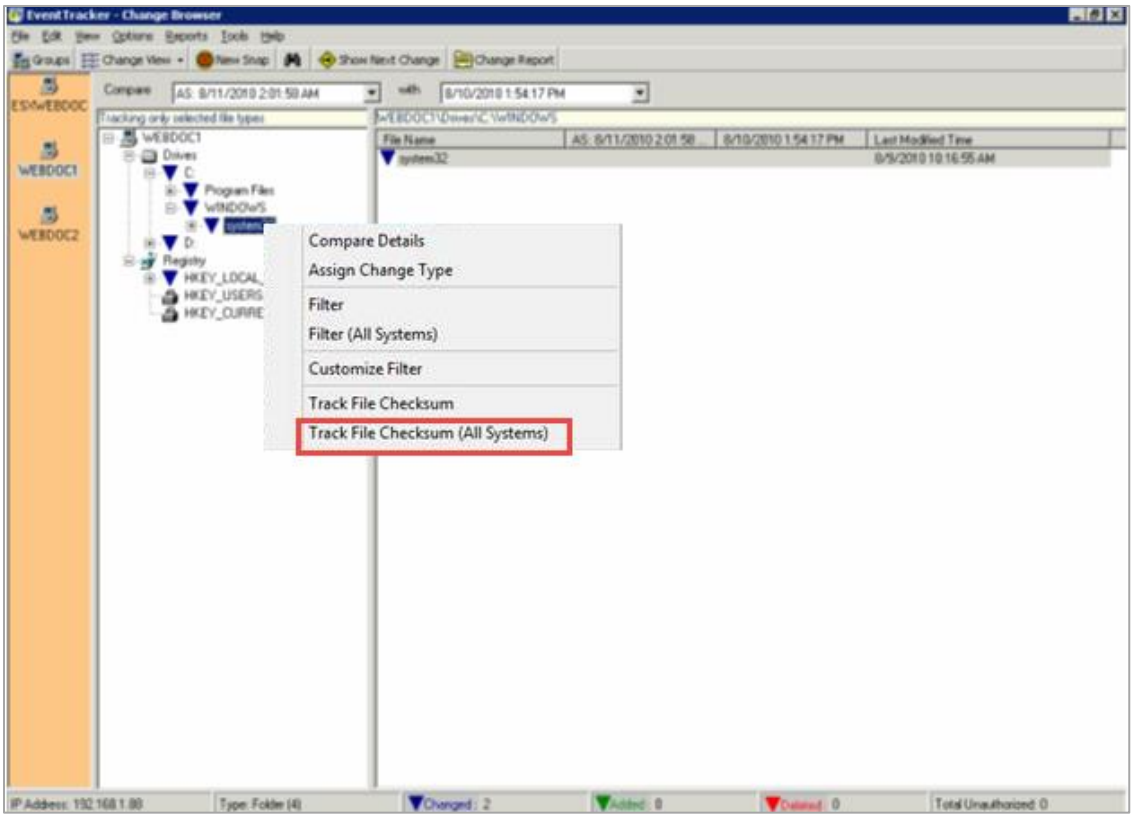
1. Open the Change Browser.
2. On the System Bar, double-click the system for which you want to generate a change report.
3. Select the Snapshots from the dropdown lists.
4. Click the **Reports** menu and select the **View Reports** option or click on the toolbar.
   The Change Audit displays the Select Format window.



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**. The Change Audit generates and displays the change report.

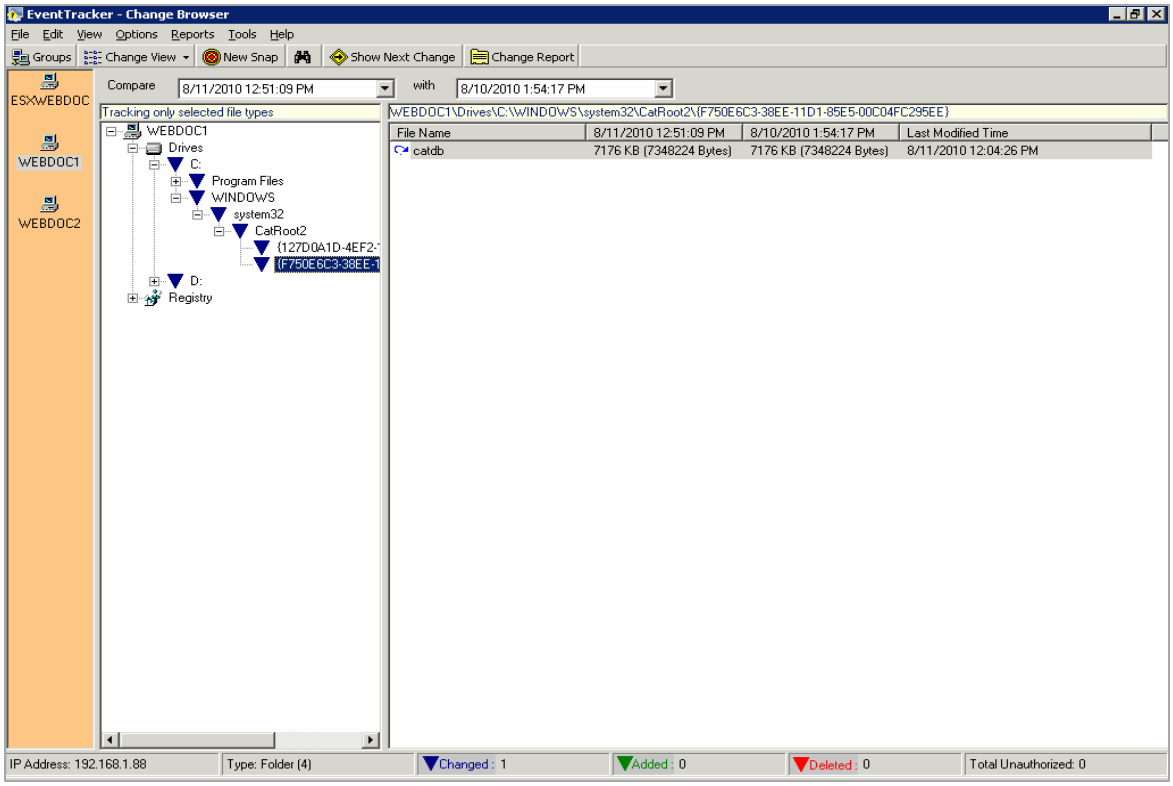
3.13 Track File Checksum Feature

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

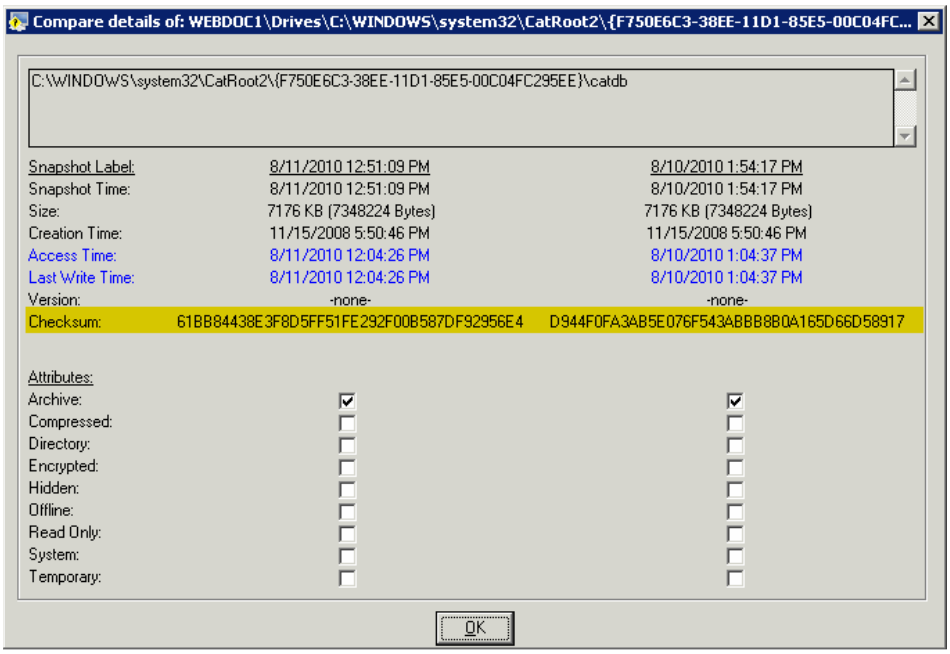


To view the file checksum, follow the steps below:

1. Open the Change Browser.
2. Double-click the system to load.
3. Select **Full View** or **Change View**.
4. Expand the **Drives** tree and click **system32**. The Change Audit displays the sub-folders and the files associated with the selected folder.



5. Double-click an item in the right pane. The Change Audit displays the Compare Details window with checksum details.



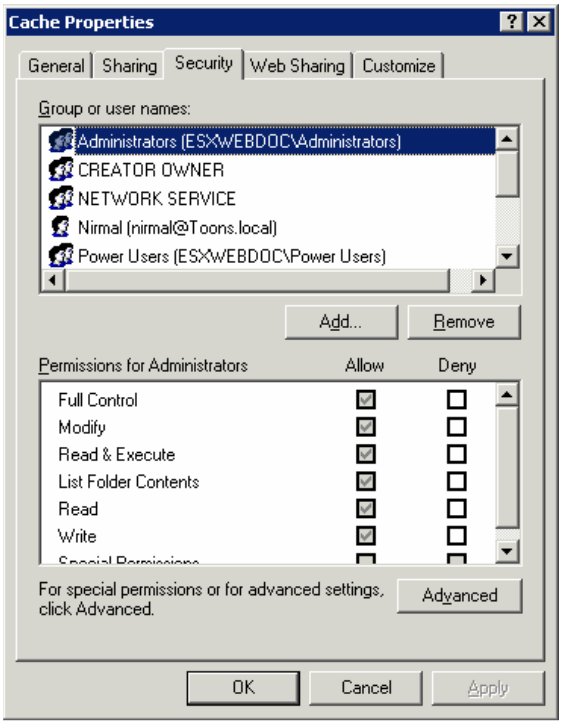
3.13.1 Enabling File Checksum Tracking

1. Open the Change Browser.
2. Double-click the system to load.
3. Select **Full View** or **Change View**.

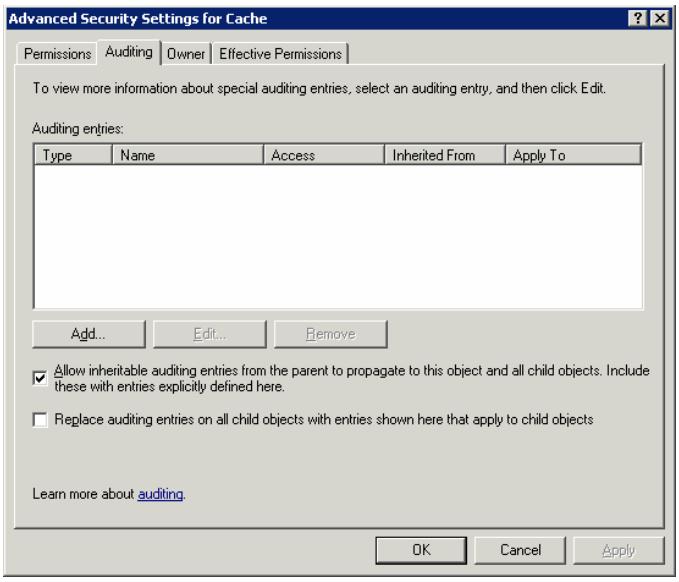
4. Expand the **Drives** tree and right-click a folder. The Change Audit displays the shortcut menu. From the shortcut menu, choose **Track File Checksum** to track file checksum for the local system.
5. Or, choose **Track File Checksum (All Systems)** to track file checksum for all monitored systems.

3.13.2 Enabling the O/S Audit on Files and Folders

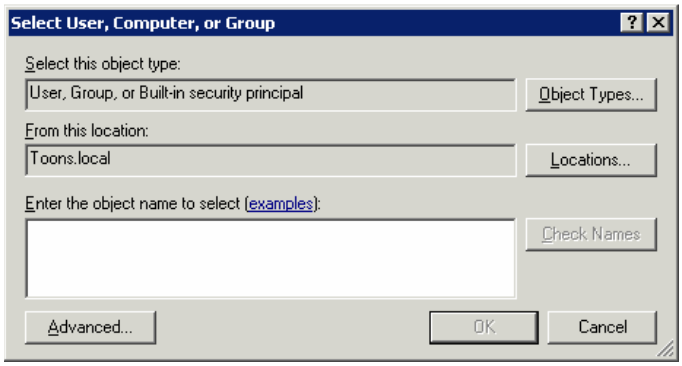
1. Right-click the folder you want to enable auditing.
   Example: \\<systemname>\Program Files\Prism Microsystems\Netsurion Open XDR\Cache.
2. From the shortcut menu, choose **Properties**.
3. Click the **Security** tab on the Properties window.



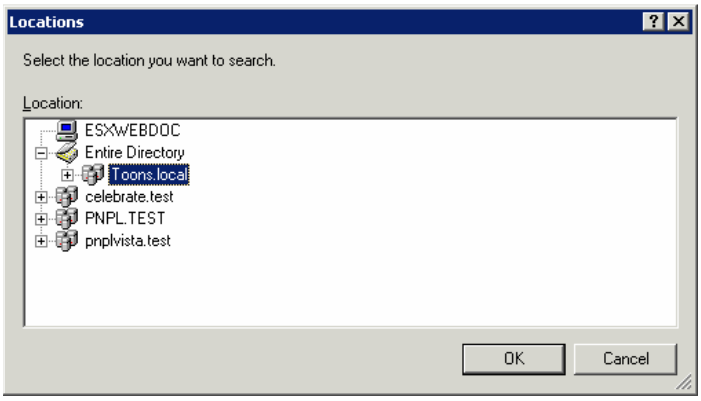
4. Click **Advanced**.
5. Click the **Auditing** tab on the Advanced Security Settings window.



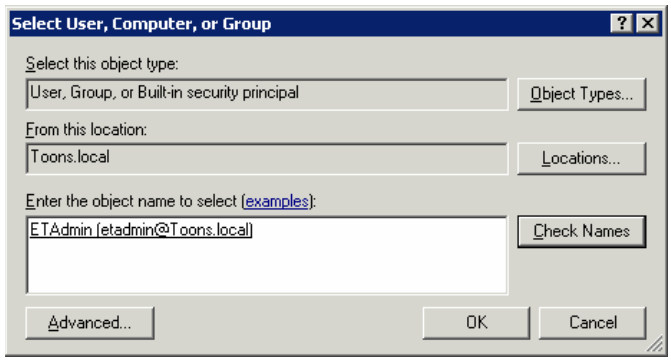
6. Click **Add**. Select User, Computer, or Group window will be displayed.

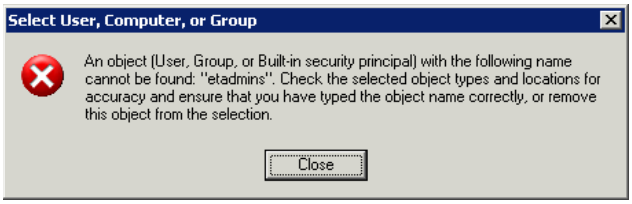


7. Click **Locations**, to select the location from where you want to pick users.

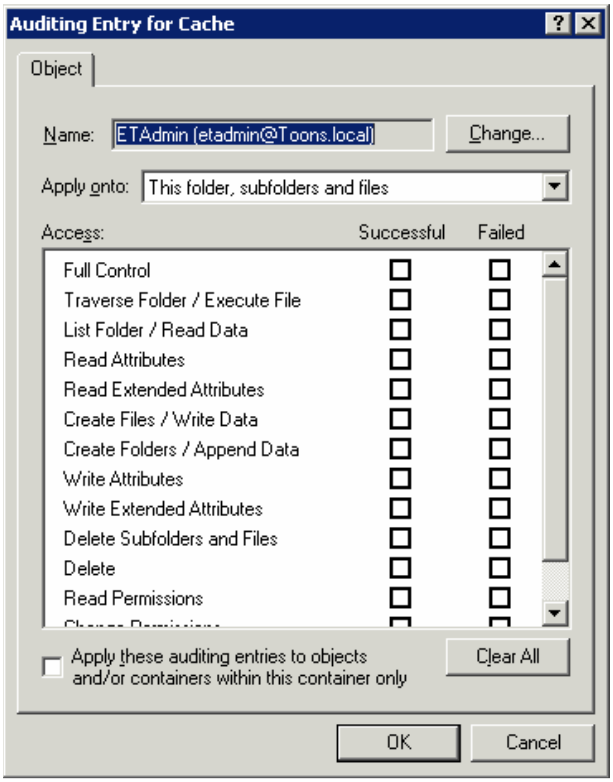


8. Select the **Location** from the Locations window and then click **OK**.
9. Enter the username in the **Enter the object name to select** field.
   Example: ETAdmin
10. Click **Check Names**. If the username is valid, the user name is displayed in the **Enter the object name** to select field. Otherwise, an error message is displayed.

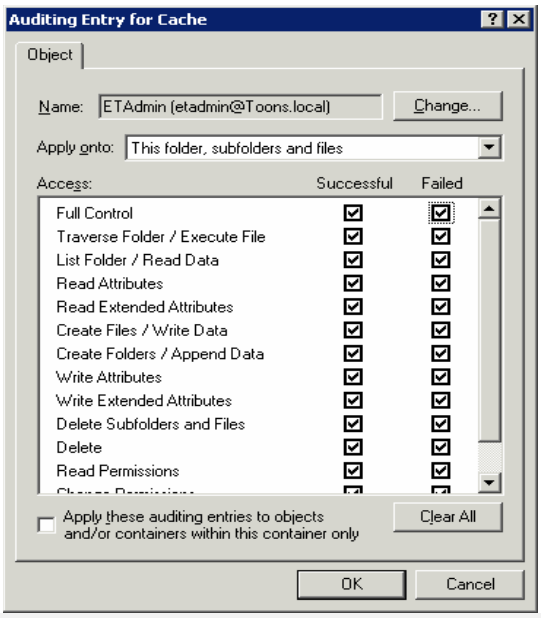




11. Click **OK**. The Auditing Entry for Cache window will be displayed as shown below:

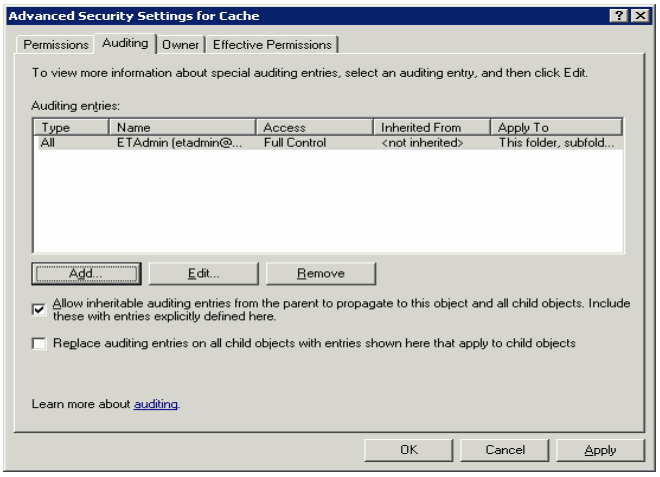


12. Select **Full Control** under **Successful** and **Failed**. All other check boxes are also selected automatically when you select the **Full Control** check box.



Note
You do not need to select the Full Control check box. Select the options as per the requirement.

13. Click **OK**. The Advanced Security Settings window is displayed with the newly added user.



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

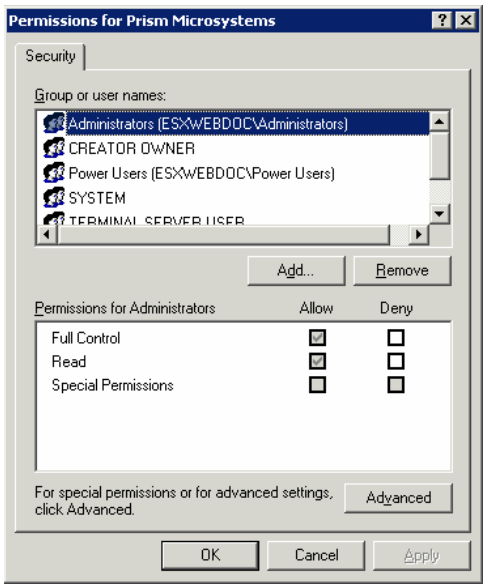
Note
Similarly, enable auditing for file or registry keys.

3.13.3 Enabling the O/S Audit on the Registry Keys

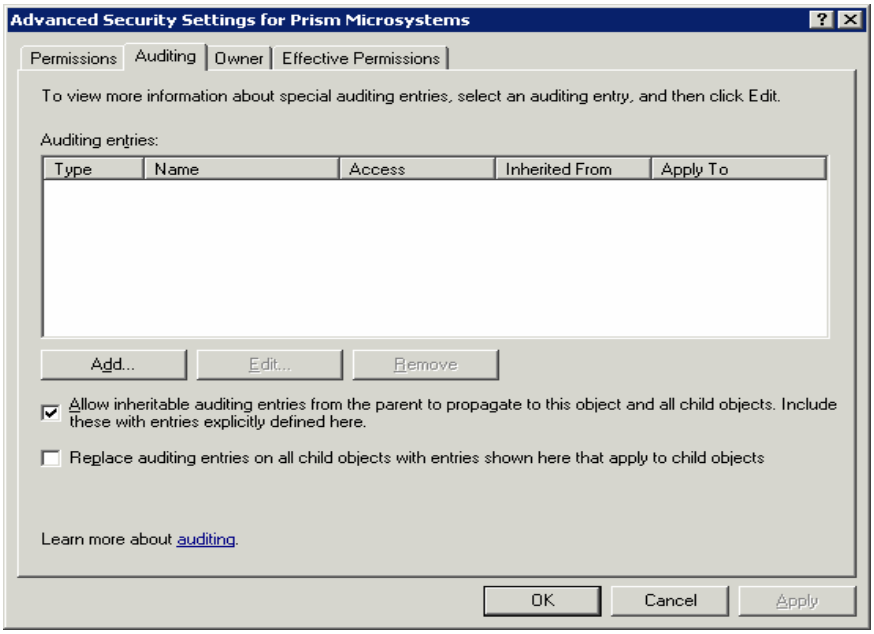
To enable O/S audit on registry keys, follow the steps below:

1. Open the Registry Editor.
2. Right-click the key that you want to audit.

3. From the shortcut menu, choose **Permissions**.



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



6. Add users as explained in the previous section.

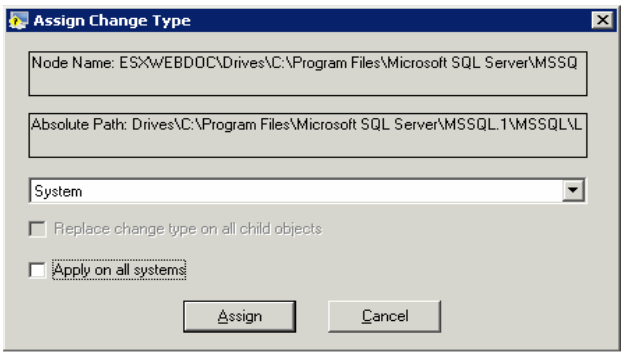
3.14 Assign Change Type

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

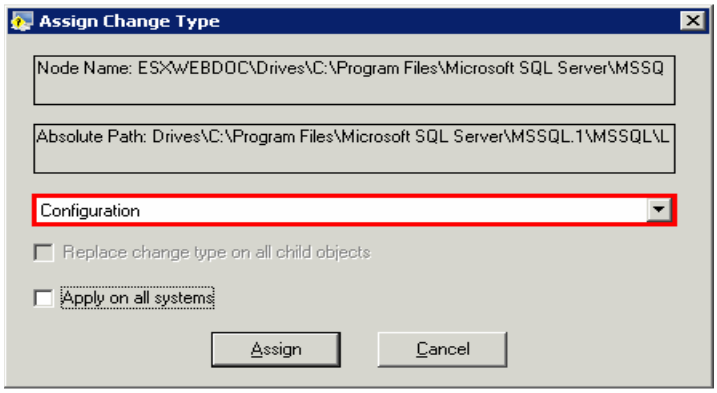
To modify the Change Type, follow the steps below:

1. Open the Change Browser.

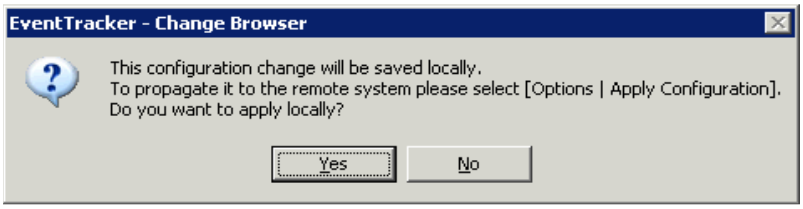
2. Select **Full View** or **Change View**.
3. Expand the File System node or Registry node.
4. Right-click an item (folder/file/registry key) on the left or right pane. The change Audit displays the shortcut menu.
5. From the shortcut menu, select the **Assign Change Type**. The Change Audit displays the Assign Change Type window.



6. Select a **Change Type** from the dropdown list.
7. Select the **Apply on all systems** check box if you wish to apply the settings to all monitored computers.
8. Click **Assign**. The Change Audit refreshes the Change Browser.
9. Right-click the key that you have modified the Change Type.



10. Load the monitored system.
11. Right-click a key and choose **Assign Change Type** from the shortcut menu. The Change Audit displays the confirmation dialog box.



4 Snapshots

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

After successful installation, Change Audit takes a baseline Snapshot. It takes one or more Snapshots immediately following the baseline Snapshot after a specific time interval. By default, Change Audit automatically takes Snapshots Daily at 2 A.M. It preserves up to 64 Snapshots for comparison. When the maximum limit exceeds, 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, Change Audit preserves the baseline and the latest Snapshots forever. You can also modify these settings through Edit Snapshot settings.

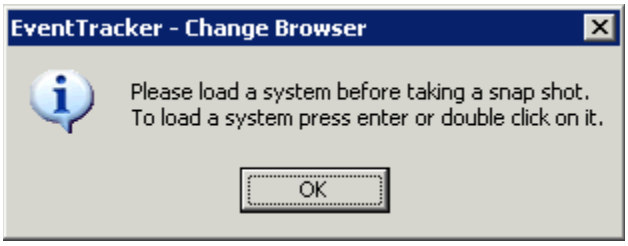
If you have configured the maximum number as 30 and have chosen to retain all the 30 Snapshots and trying to take a new Snapshot, in this scenario, Change Audit will not delete any of the earlier Snapshots and will not attempt to take the new Snapshot.

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:

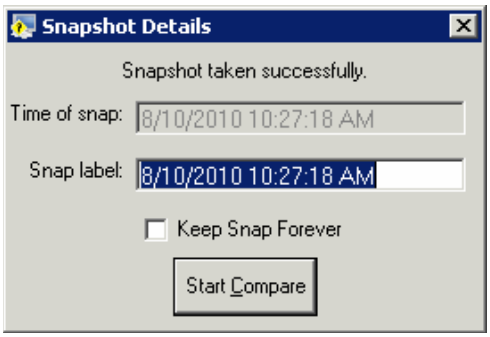
1. Open the **Change Browser**.
2. On the System Bar, double-click the computer for which you want to take Snapshot. If you try to take Snapshots in Groups view, Change Audit displays the dialog box asking you to load the system before taking the Snapshots.



   Change Audit loads the details of the selected system.

3. Click the **Options** menu and select the **Take Snapshot** option or click on the toolbar.
   The Snapshot progress will be displayed as shown below.

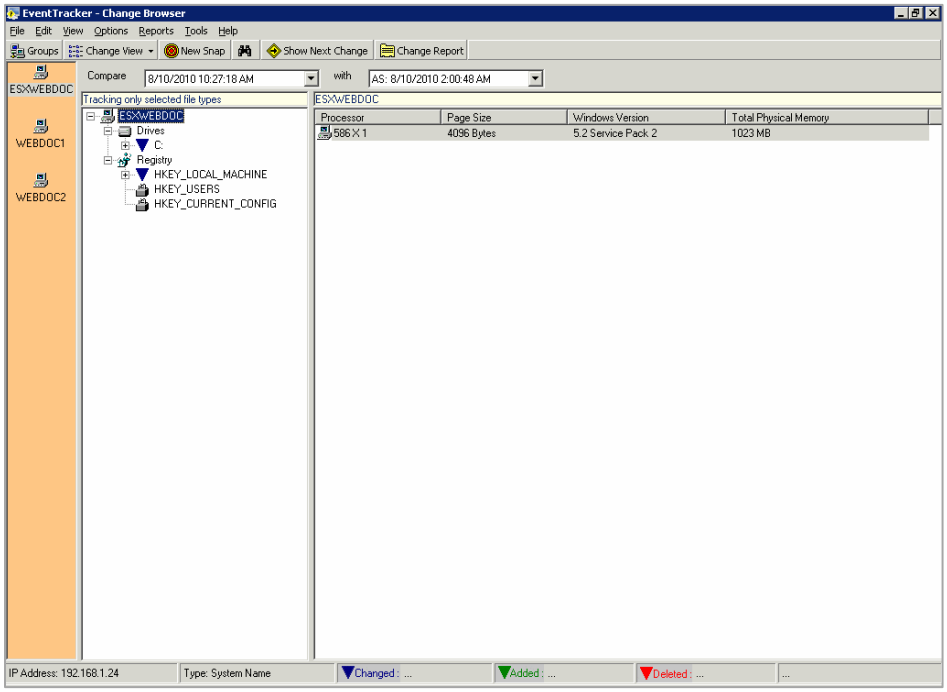
4. After completion of taking the Snapshot, Change Audit displays the Snapshot Details dialog box.



Field	Description
Time of snap	Displays the date and time when the Snapshot was taken.
Snap label	Displays the 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 to Compare	Click this button for the Change Audit to start comparing with the immediate previous Snapshot.

5. Type an appropriate name for the new Snapshot in the **Snap label** field.
6. Select the **Keep Snap Forever** checkbox if you want to preserve the Snapshot for future comparison.
7. Click **Start Compare**.

Change Audit compares the new Snapshot with the immediate previous Snapshot and displays the changes in the Change Browser.



4.2 Edit Snapshots

This option helps you edit the Snapshots.

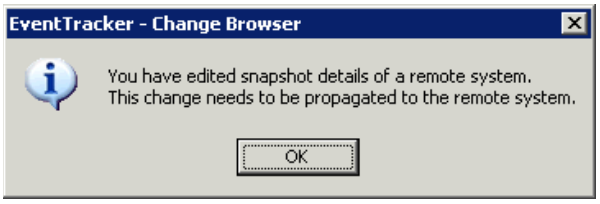
To edit the Snapshots, follow the steps below:

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

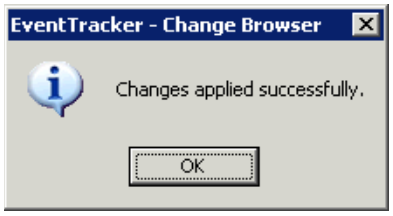
Field	Description
List of snapshots for the current system	Displays the list of Snapshots taken for the selected Computer.
Time of snap	Displays the date and time when the Snapshot was taken.
Snap label	Displays the name of the selected Snapshot.
Keep Snap Forever	Change Audit selects this check box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

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

5. Click **OK**, and then click **Close.** Change Audit displays the dialog box if the update is done for the remote system.



6. Click **OK**.

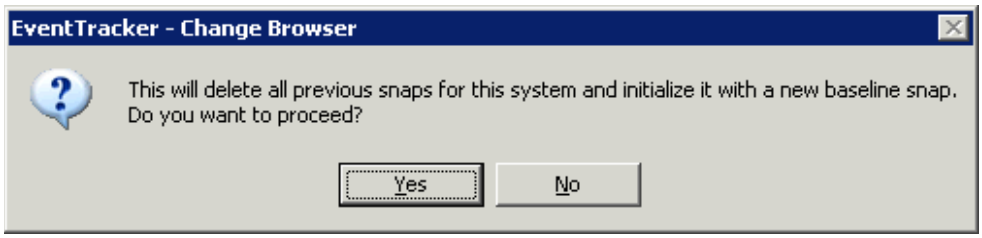


4.3 Reinitialize Snapshots

This option helps you delete all the previous Snapshots for the selected Computer. After deleting all the Snapshots, Change Audit takes a new baseline Snapshot.

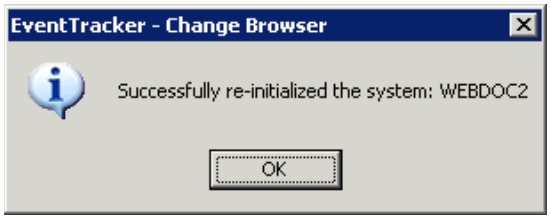
To re-initialize Snapshots, follow the steps below:

1. Open the Change Browser.
2. Double-click the computer on the System Bar.
3. Click the **Options** menu and select the **Re-initialize Snaps** option. The confirmation window will be displayed as shown below:

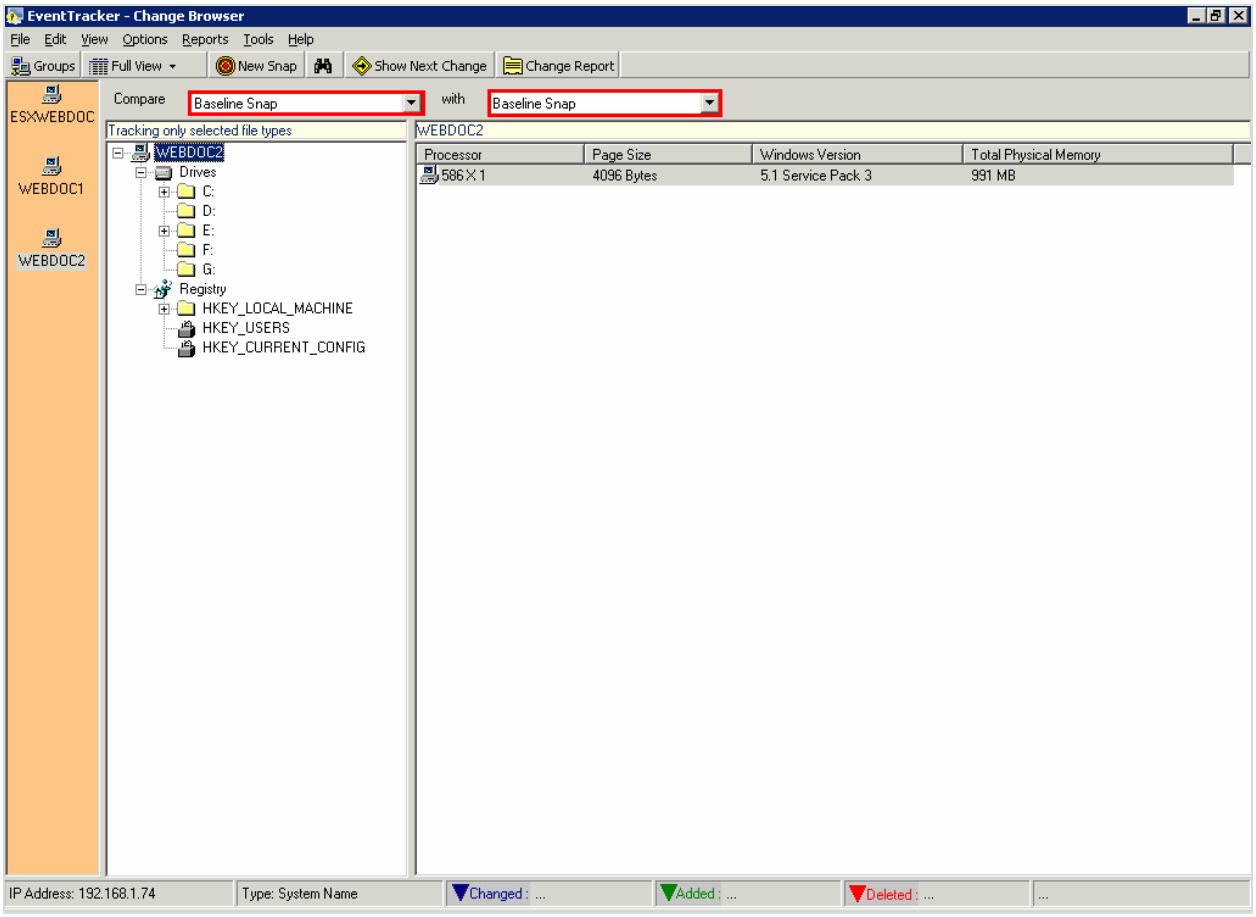


4. Click **Yes** to proceed.

After successfully re-initializing the Snapshots, the success message will be displayed as shown below.



5. Click **OK**. Change Audit displays the Change Browser.



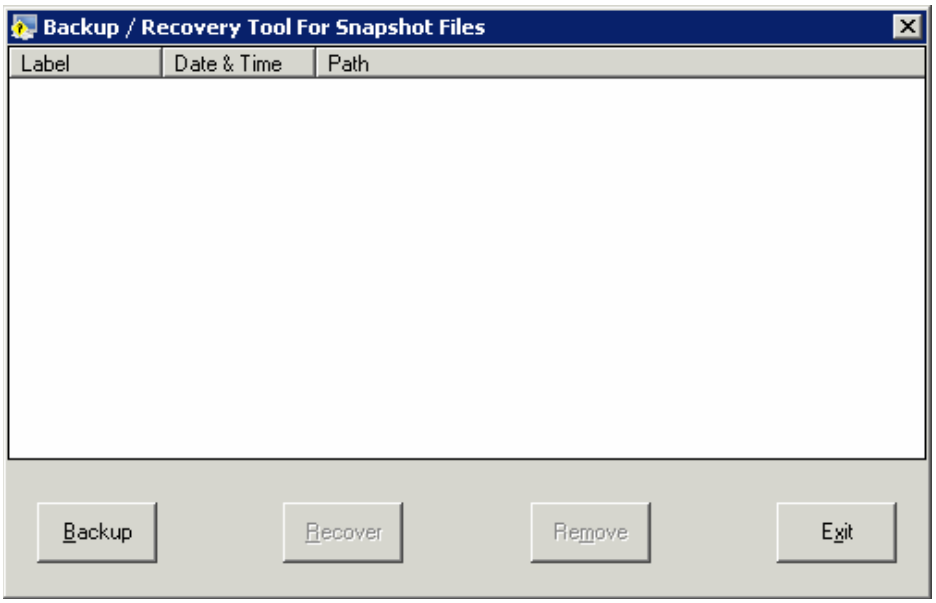
If Change Audit has deleted all the previous Snapshots including the baseline and has created a new baseline Snapshot, it compares the **Baseline Snapshot** with the **Baseline Snapshot** since no other Snapshots exist.

4.4 Back up the Snapshots

This option helps you to back up the Snapshots.

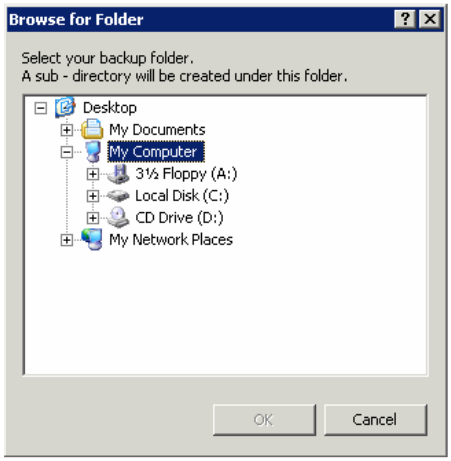
To back up Snapshots, follow the steps below:

1. Open the Change Browser.
2. Click the **Options** menu and select the **Backup / Recovery (Snapshots)** option. The confirmation message will be displayed.
3. Click **Yes** to proceed.
4. Change Audit displays the Backup / Recovery Tool.

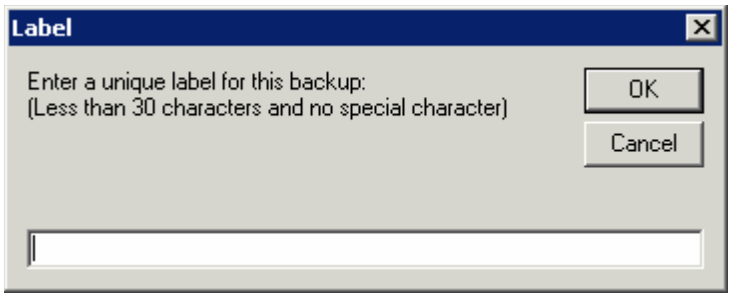


Button	Description
Backup	Back up the Snapshots of the current system.
Recover	Select the backup file from the list and then click to recover the Snapshots.
Remove	Select the backup file from the list and then click to delete the file.
Exit	Exit Backup / Recovery Tool.

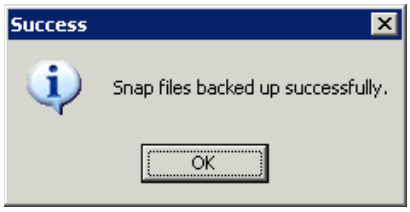
5. Click **Backup** and browse the folder.



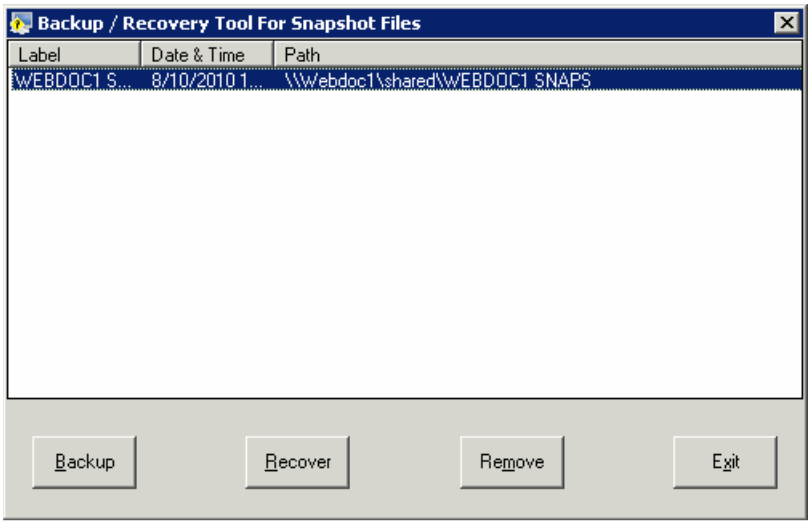
6. Select the appropriate folder and then click **OK**. The Label window will be displayed as shown below:



7. Type a unique label in the text box and then click **OK.** After successfully backing up the Snapshots, the success message will be displayed as shown below:



8. Click **OK**. The Backup / Recovery Tool with the backup will be displayed.



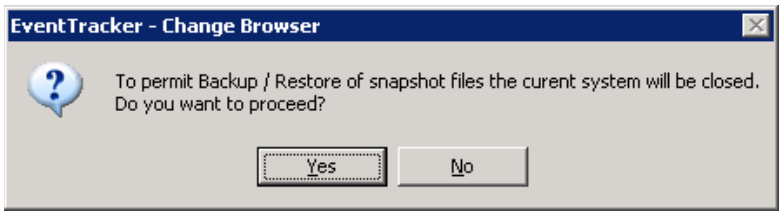
9. Click **Exit**.

4.5 Recover Snapshots

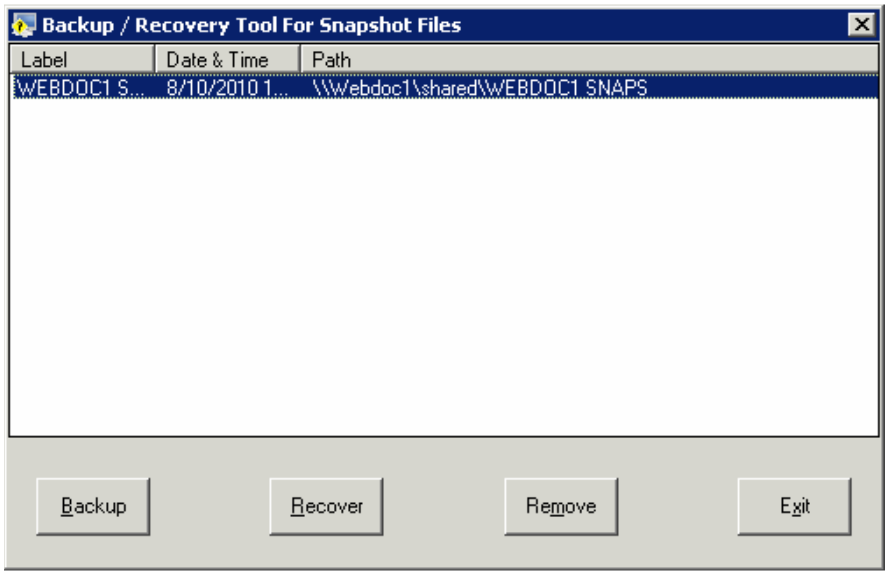
This option helps you recover the Snapshots.

To recover Snapshots, follow the steps below:

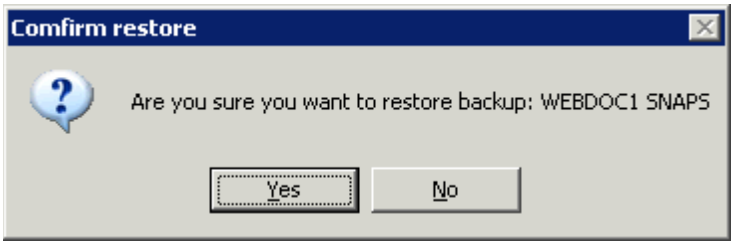
1. Open the Change Browser.
2. Click the **Options** menu and select the **Backup / Recovery (Snapshots)** option. The confirmation message will be displayed as shown below.



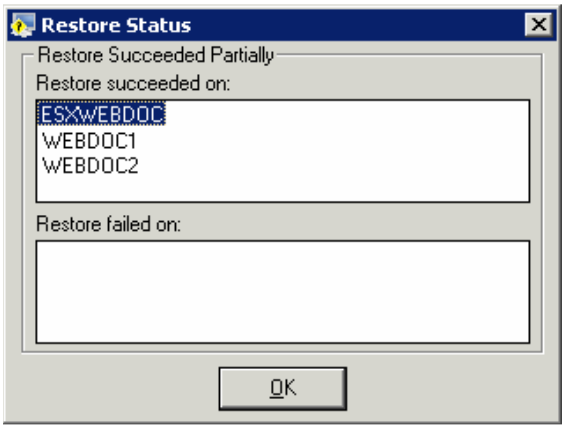
3. Click **Yes** to proceed. Change Audit displays the Backup / Recovery Tool.



4. Select the file from the list and then click **Recover**. The Confirm Restore dialog box will be displayed as shown below:



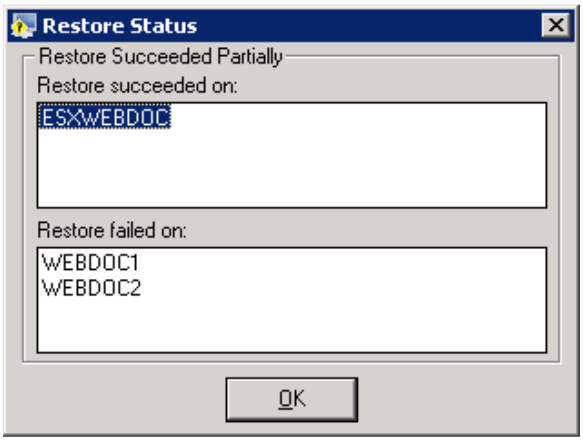
5. Click **Yes** to proceed.



6. Click **OK**.

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

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



5 Configuration

Administrators 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 aims at performance and efficiency enhancement.

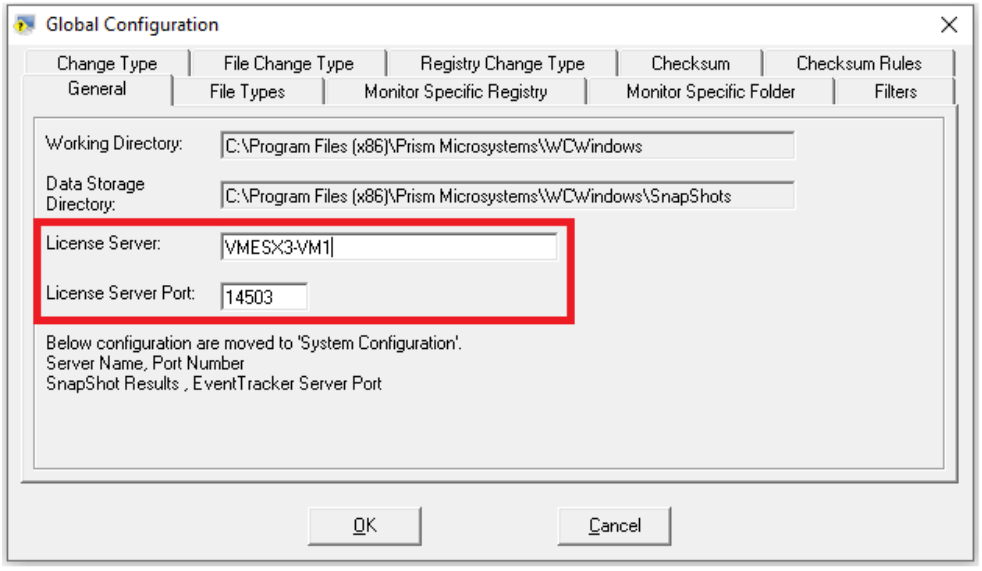
5.1 Global Configuration

This option helps to set the Global Configuration.

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

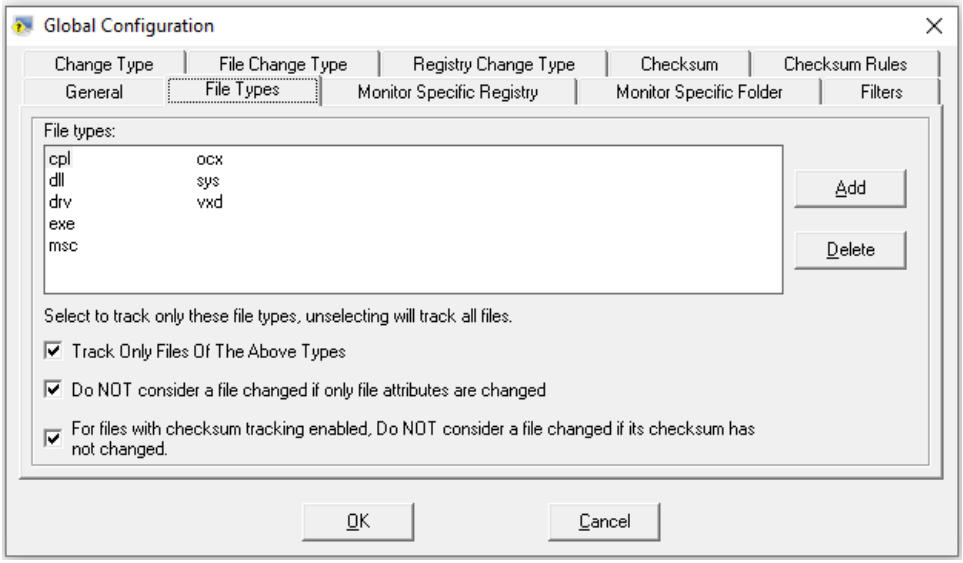
To set up Global Configuration, follow the steps below:

1. Open the Change Browser.
2. Click the **Options** menu and select the **Global Configuration** option. The Global Configuration window will be displayed as shown below:



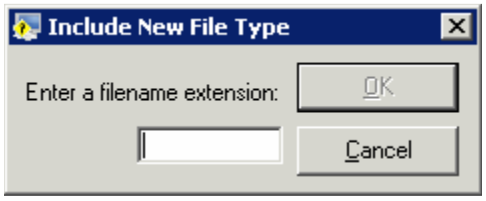
Field	Description
General	General Change Audit selects this tab by default and displays information about the Working Directory path, and Data Store directory path.

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

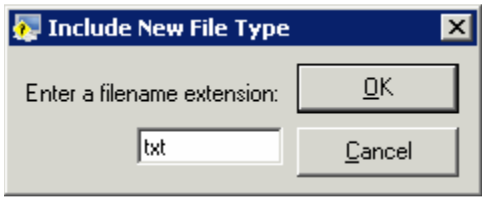


Field	Description
File Types	Click this tab to view the file types being tracked by Change Audit. By default, Change Audit tracks the file types listed in the File Types list. You can add or remove file types for tracking of your choice from the list. Change Audit selects the **Track Only** files by default. Unselect this checkbox if you want to track all file types.
Track Only Files of The Above Types	Unselect this check box if you wish to track all file types.
Do not consider a file changed if only file attributes are changed	Unselect 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 changed	Unselect this check box to exclude checksum tracking enabled files if the checksum has not changed.

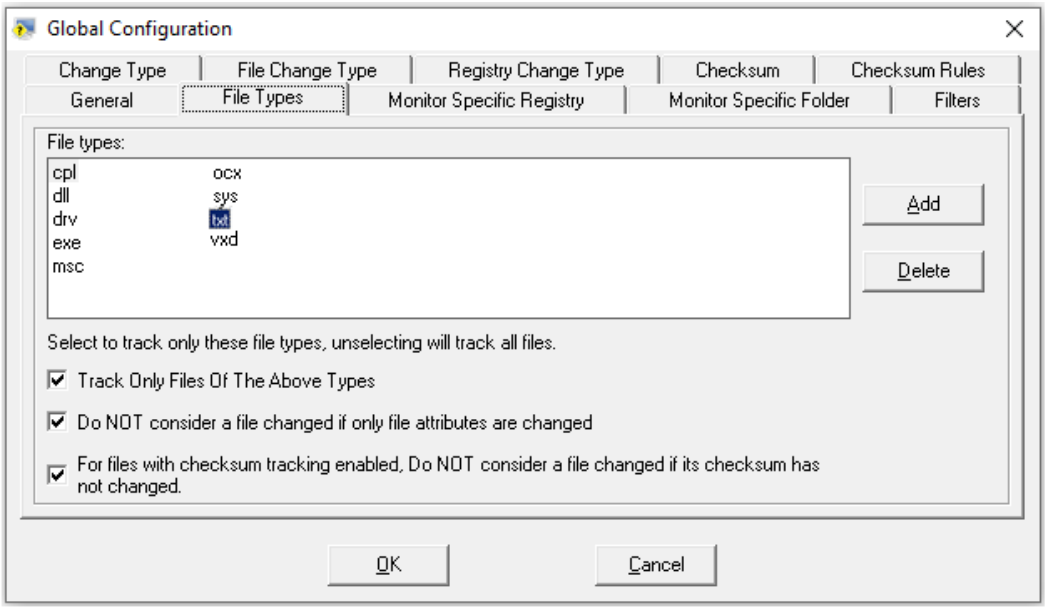
4. Click **Add** to add a new file type. Change Audit displays the **Include New File Type** dialog box.



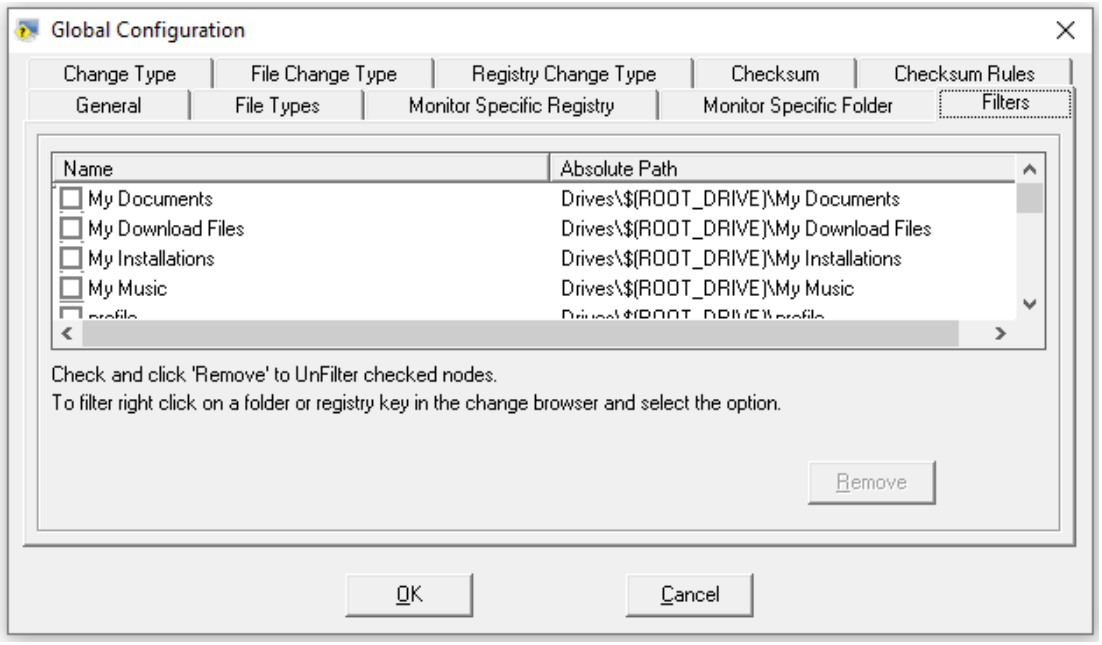
5. Type the filename extension and then click **OK**.



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

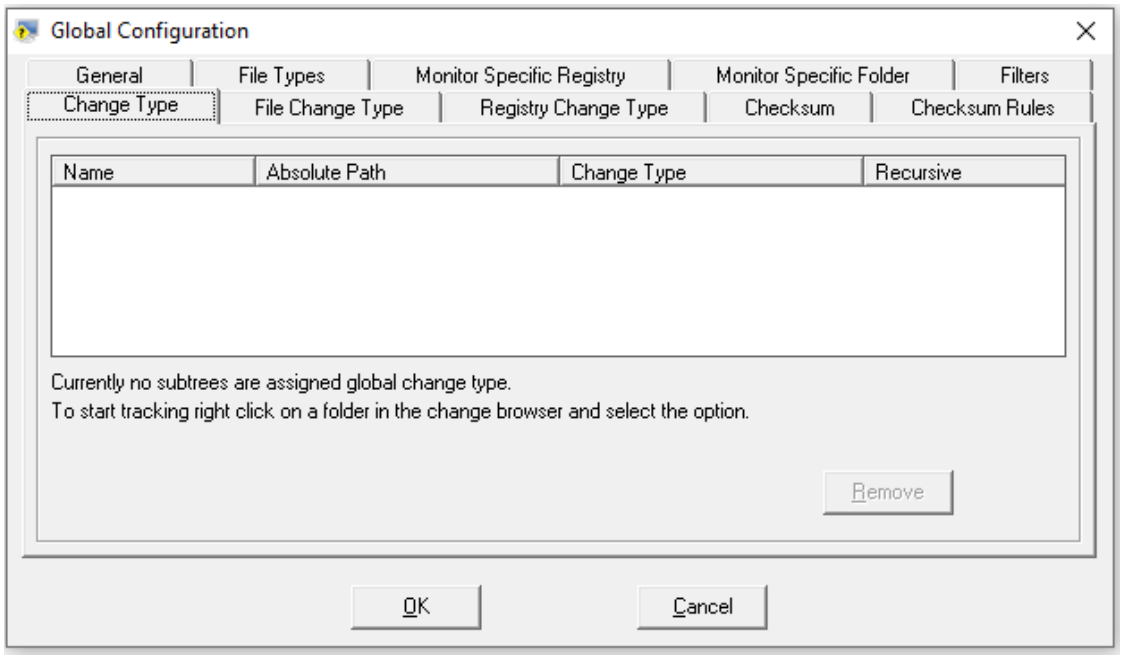


7. To delete a certain file type, select it from the list and then click **Delete**. Change Audit removes the selected file type from tracking.
8. Click the **Filters** tab. Change Audit displays the Filters tab with the preset filter items.



Field	Description
Filters	Click this tab to view files, folders, registry hives, and keys filtered by 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 here.

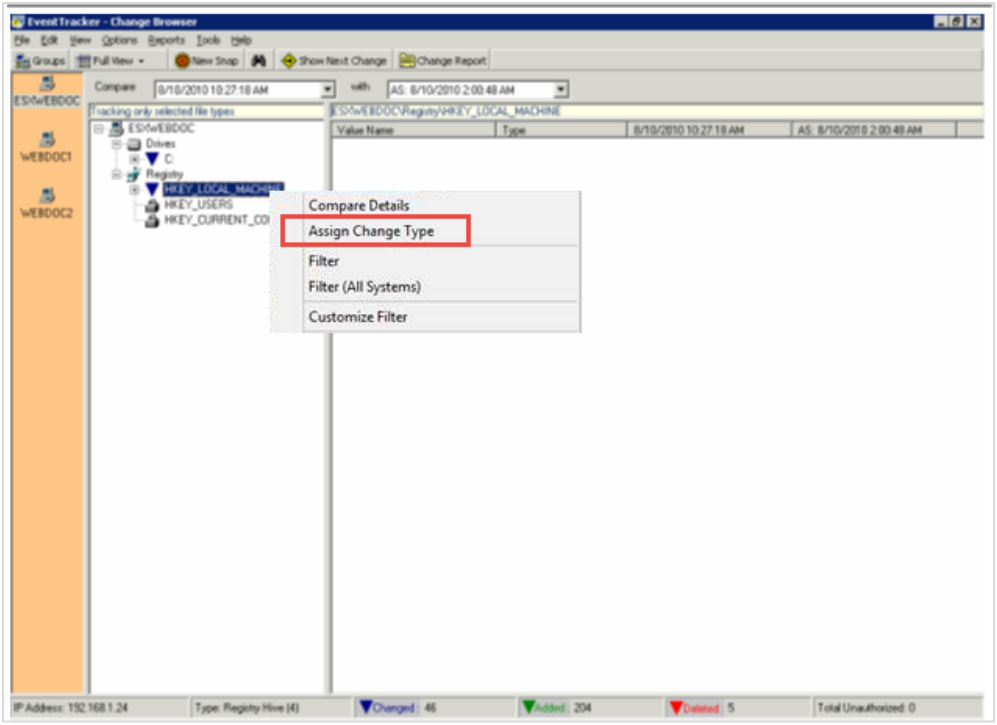
9. Select the check box against the item that you wish to remove from the filter list and then click **Remove**. Change Audit removes the selected item from the filter list.
10. Click the **Change Type** tab. Change Audit displays the Change Type tab.



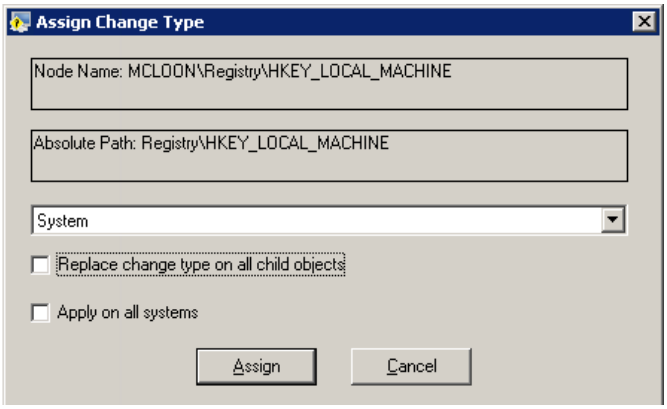
Field	Description
Change Type	**Authorized**: Detected changes that can be matched with an approved change request. **Unauthorized**: Detected changes that cannot be matched to an approved change request. **Configuration**: Configuration audit helps to track all changes that are made to the computer configuration or to be able to restore the configuration of that computer 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 the Change Type

1. Right-click a folder, file, registry hive, or registry key. Change Audit displays the shortcut menu.



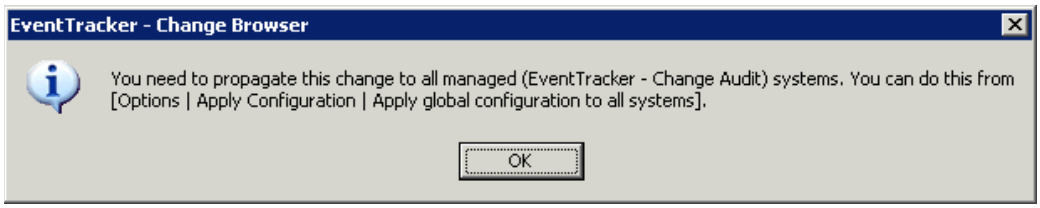
2. From the shortcut menu, choose **Assign Change Type**. Change Audit displays the Assign Change Type window.



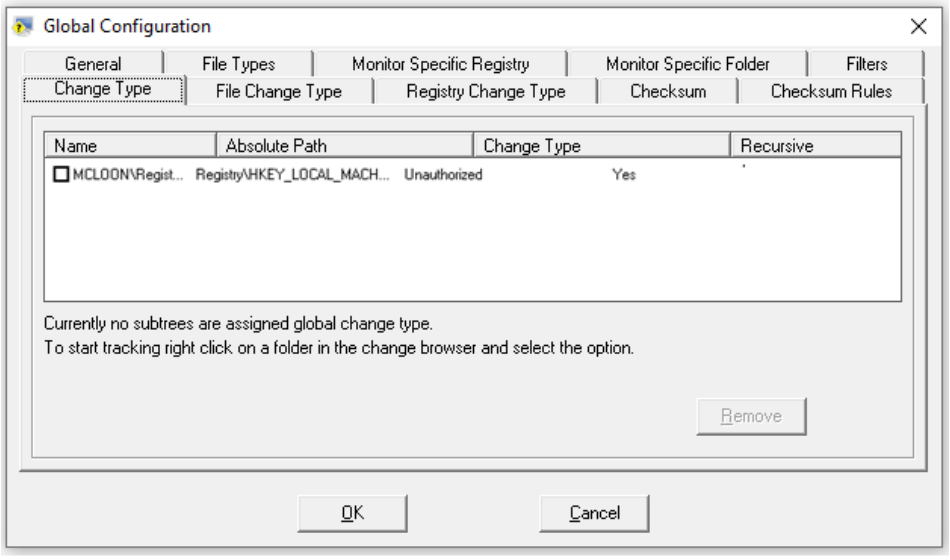
Field	Description
Change Type	For the following classification of Change Type, Change Audit considers all as the System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc, *.xlsx, *.docx,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

	Select an appropriate change type from this dropdown list.
Replace the change type on all child objects	Select this checkbox 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.

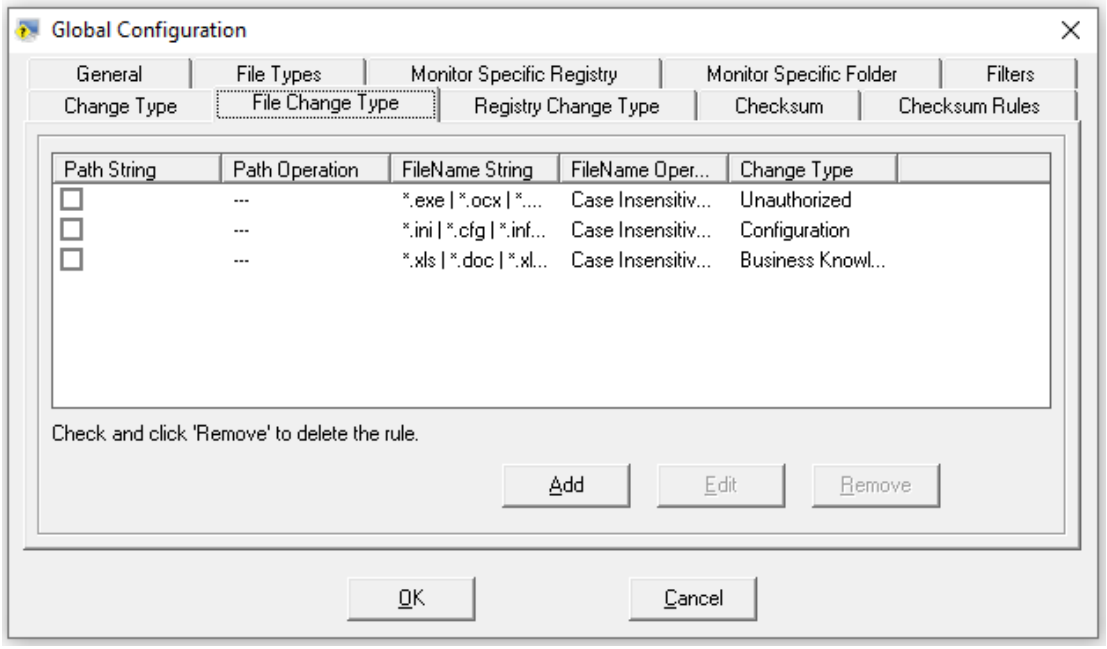
3. Select the appropriate options and then click **Assign**. If **Apply** is selected on all the systems check boxes, Change Audit displays the confirmation dialog box.



4. Click **OK** to continue. Change Audit applies the change to the local system alone. To apply globally to all monitored computers, do as advised in the dialog box.
5. Open the Global Configuration window and then click the **Change Type** tab. Change Audit displays the objects that have modified Change Type.



6. Select an object and then click **Remove**. Change Audit removes the selected object and propagates the changes to all systems.
7. Click the **File Change Type** tab. Change Audit displays the File change Type tab with the preconfigured FileName strings.



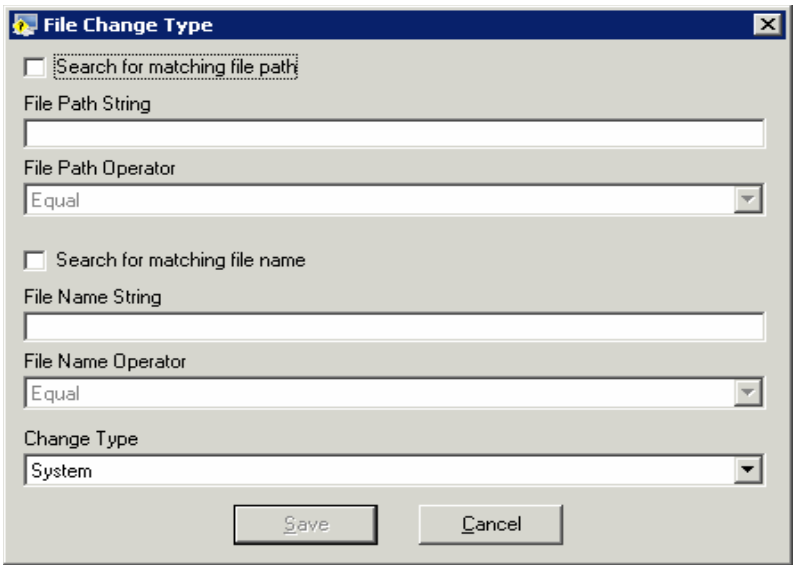
Field	Description
File Change Type	For the following classification of Change Type, Change Audit considers all as System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc, *.xlsx,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

8. Select an item and then click **Remove**. Change Audit removes the selected item.

5.1.1 Adding/Editing File Change Type

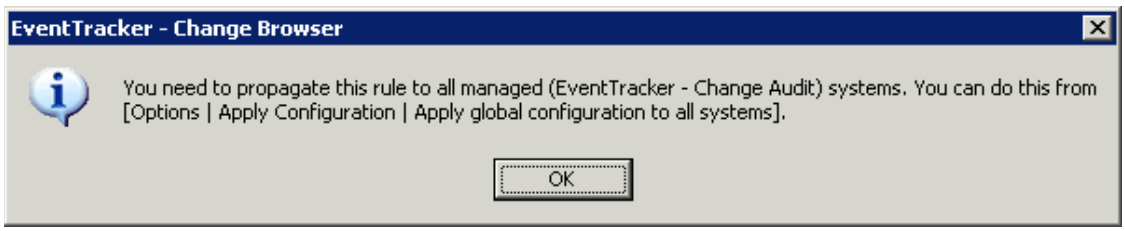
To add/edit File Change Type, follow the steps below:

1. Click **Add/Edit** to add a new File Name String. Change Audit displays the **File Change Type** window.



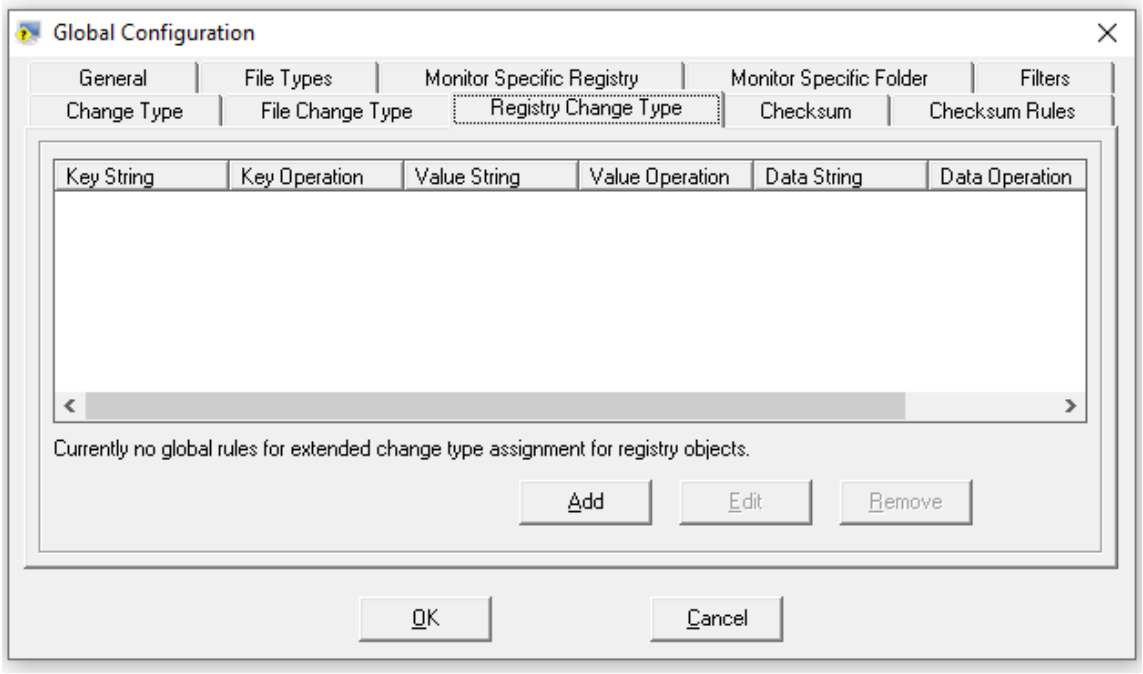
Field	Description
Search for a matching file path	Select this check box. Change Audit enables File Path String and File Path Operator fields.
File Path String	Type the location of the file.
File Path Operator	Select an operator from this dropdown list.
Search for a matching file name	Select this check box. 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 dropdown list.
Change Type	Select a change type from this dropdown list.

2. Enter/select the appropriate options.
3. Click **Save** to save changes. Change Audit displays the following message.



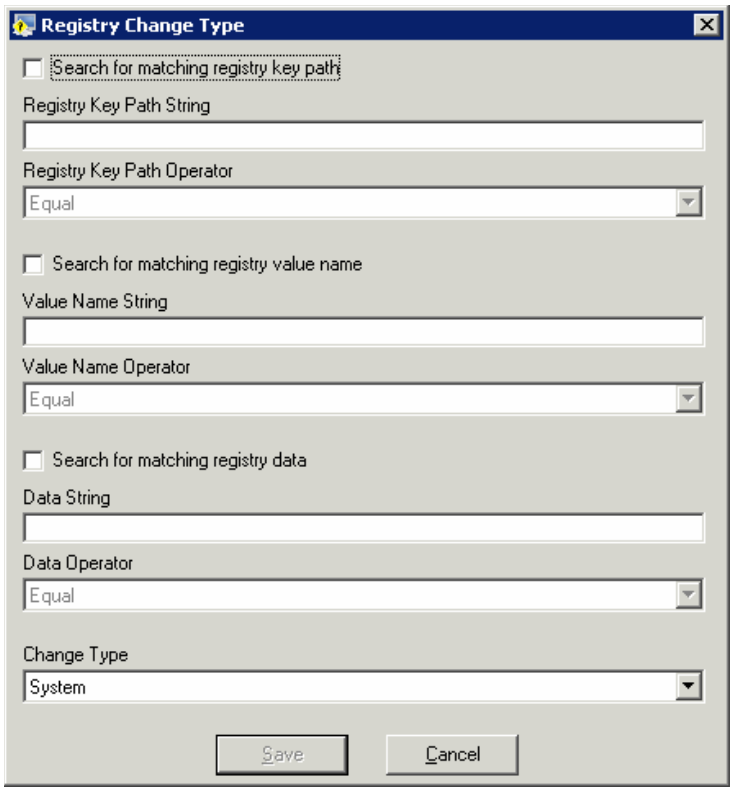
4. Click **OK** and follow the message on the message to propagate the changes to all monitored computers.

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



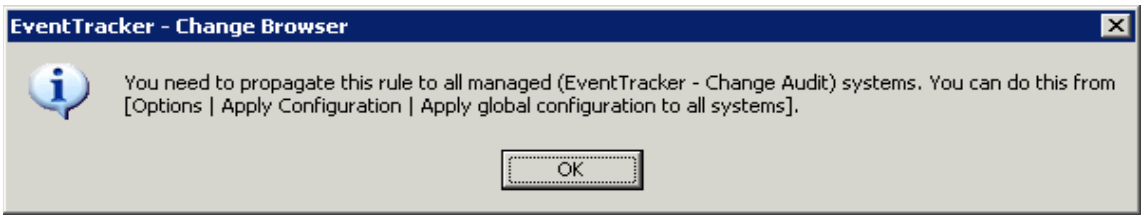
Field	Description
Registry Change Type	But for the following classification of Change Type, Change Audit considers all as System Change Type. **Unauthorized** - *.exe, *.ocx, *.dll, *.sys, *.drv, *.msc, *.cpl, *.vxd **Configuration** - *.ini, *.cfg, *.inf, *.nt **Business Knowledge** - *.xls, *.doc,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

6. Click **Add/Edit** to add the new registry keys or update existing registry keys. Change Audit displays the Registry Change Type window.

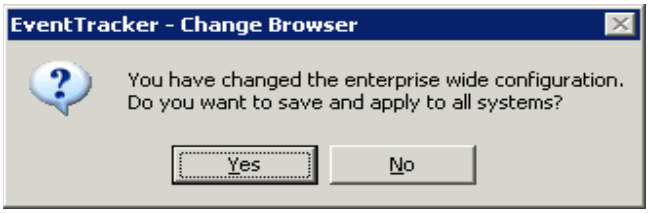


Field	Description
Search for a matching registry key path	Select this check box. Change Audit enables Registry Key Path String and Registry Key Path Operator fields.
Registry Key Path String	Select an operator from this dropdown list.
Search for matching registry value name	Select this check box. Change 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 dropdown list.
Search for matching registry data	Select this check box. Change Audit enables Data String and Data Operator fields.
Data String	Type the data string.
Data Operator	Select an operator from this dropdown list.
Change Type	Select a change type from this dropdown list.

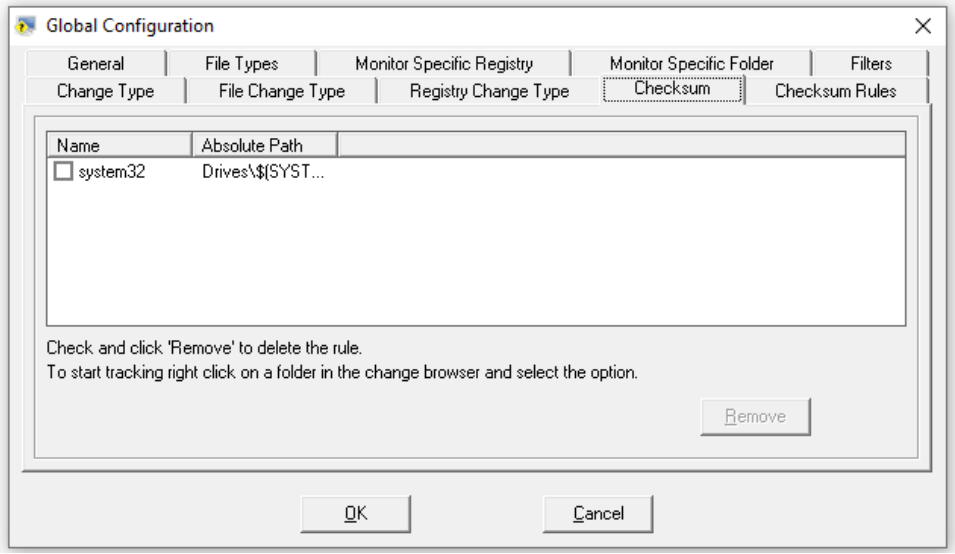
7. Enter/select appropriate options.
8. Click **Save** to save changes. Change Audit displays the message as shown below:



9. Click **OK** and propagate the changes to all the monitored systems. Change Audit displays the confirmation dialog box.

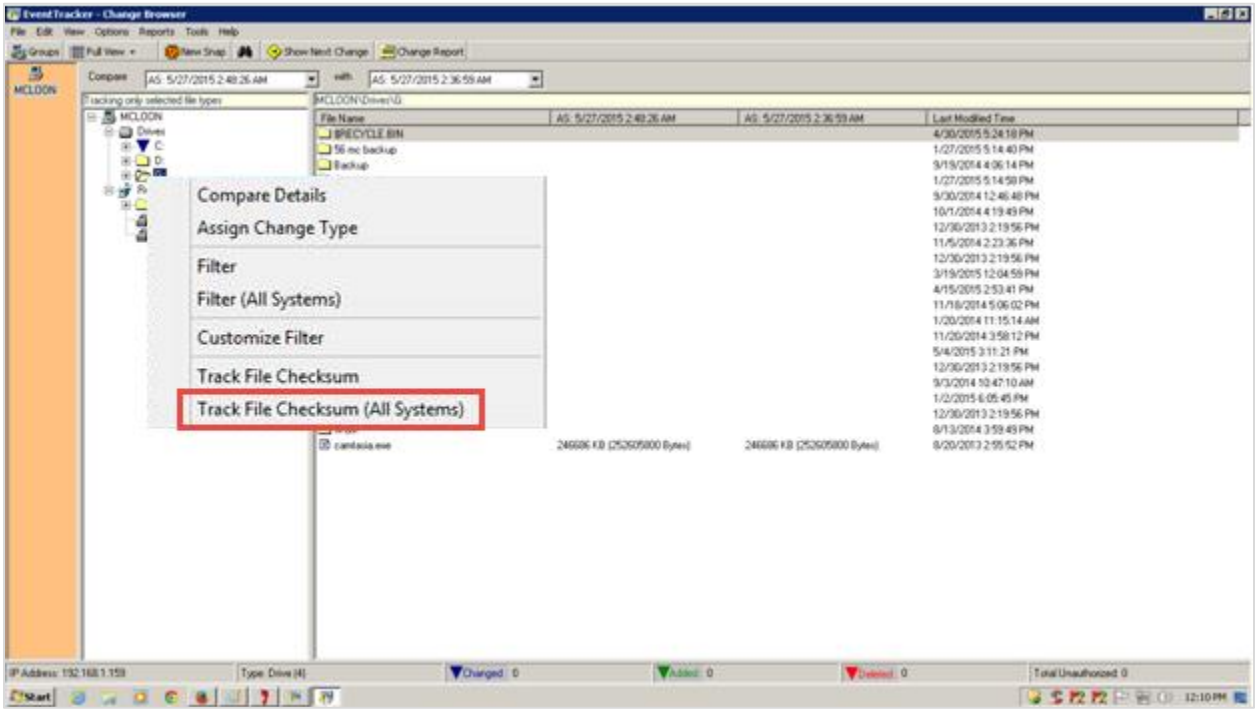


10. Click **Yes** to apply to all the systems. Change Audit applies the settings and displays the Configuration Status window.

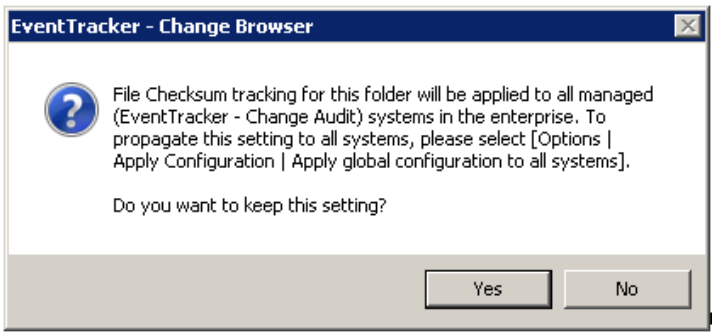


5.1.2 Configuring the Change Type

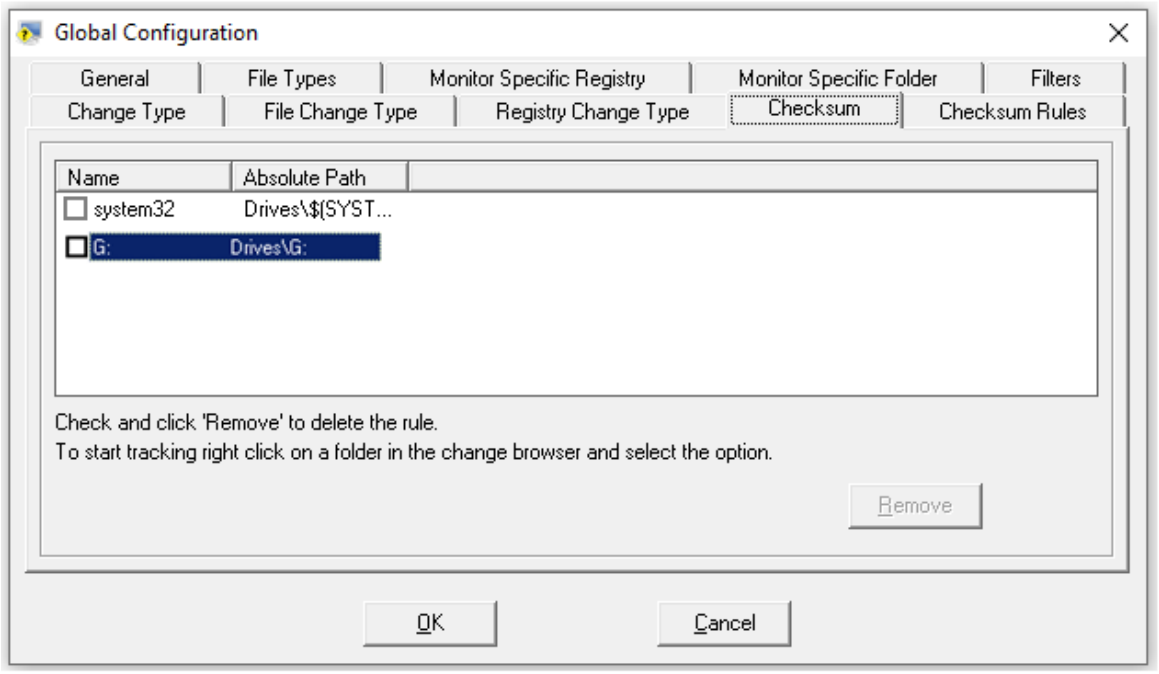
1. Right-click the folder or file. Change Audit displays the shortcut menu.



2. From the shortcut menu, choose **Track File Checksum (All Systems)**. Change Audit displays a dialog box as shown below:



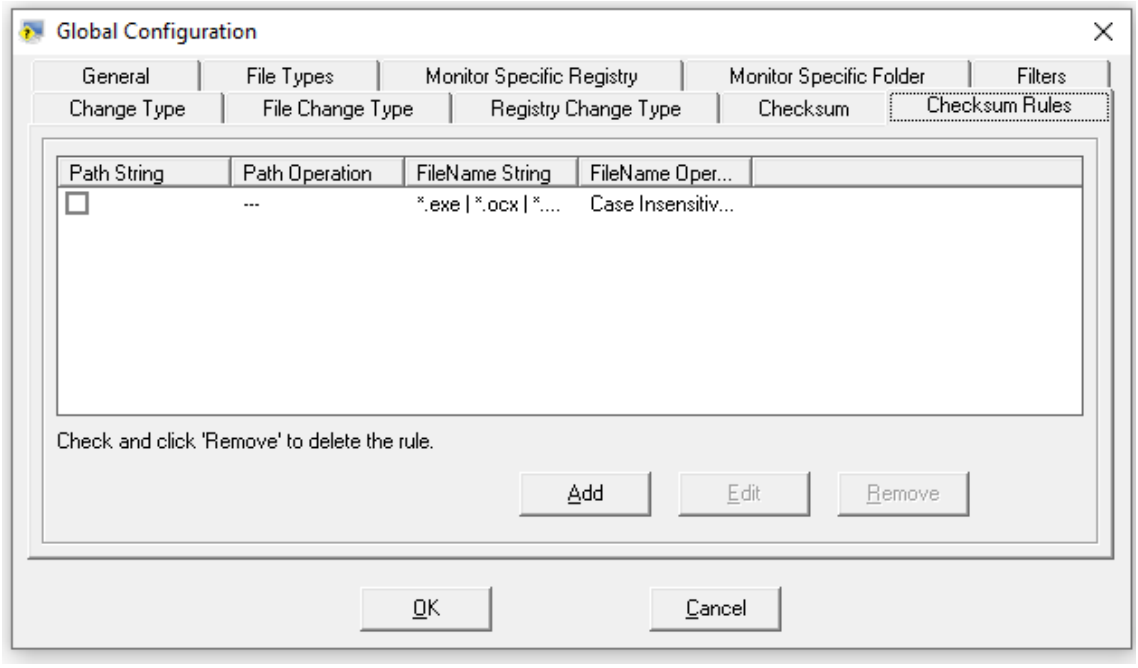
3. Click **Yes** to apply the configuration.
4. In the checksum tab, select the system by selecting the checkbox.



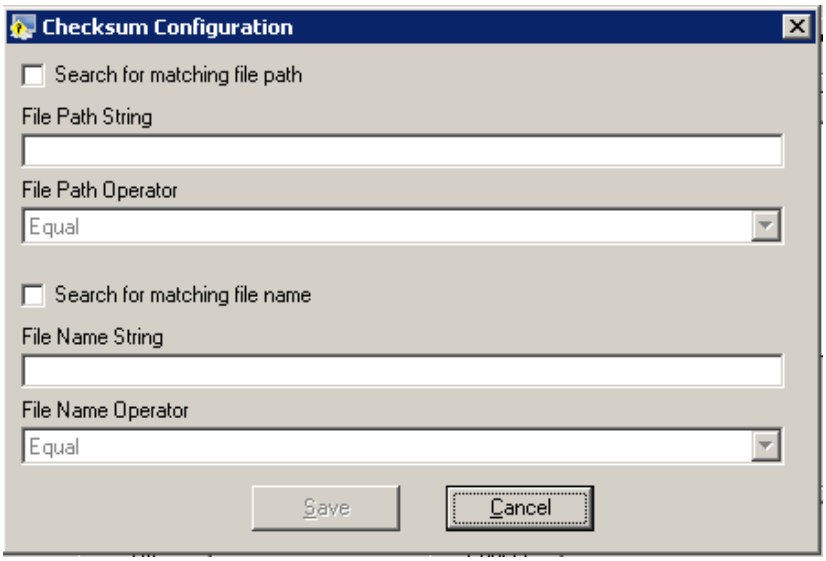
5. To remove it, click the **Remove** button.

5.1.3 Checksum Rules tab

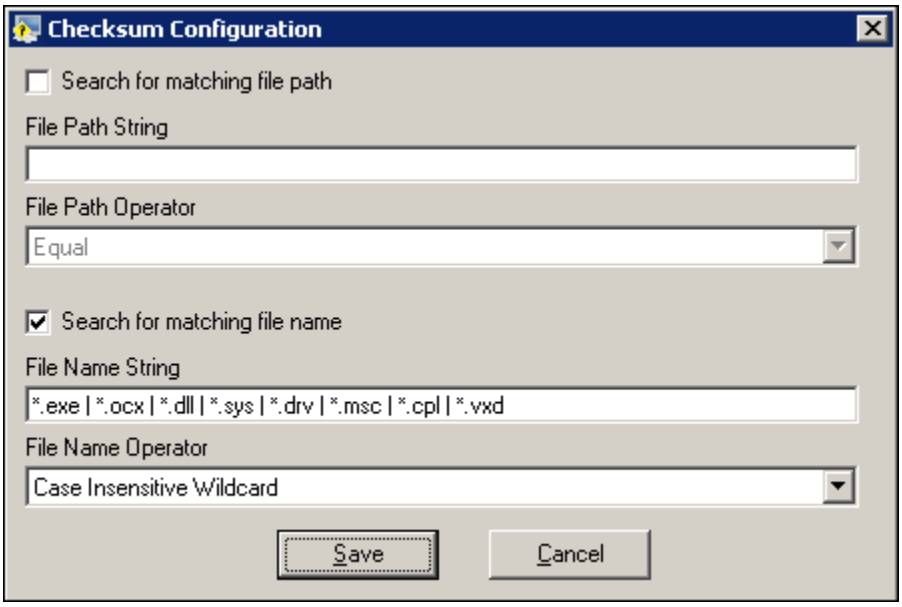
1. The Checksum tracking is enabled by default for all the executable files (*.exe, *.dll, etc.).



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



3. Enter the configuration details and click the **Save** button.
   Similarly, for editing,
4. Click the **Edit** button and make changes to the existing configuration.



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

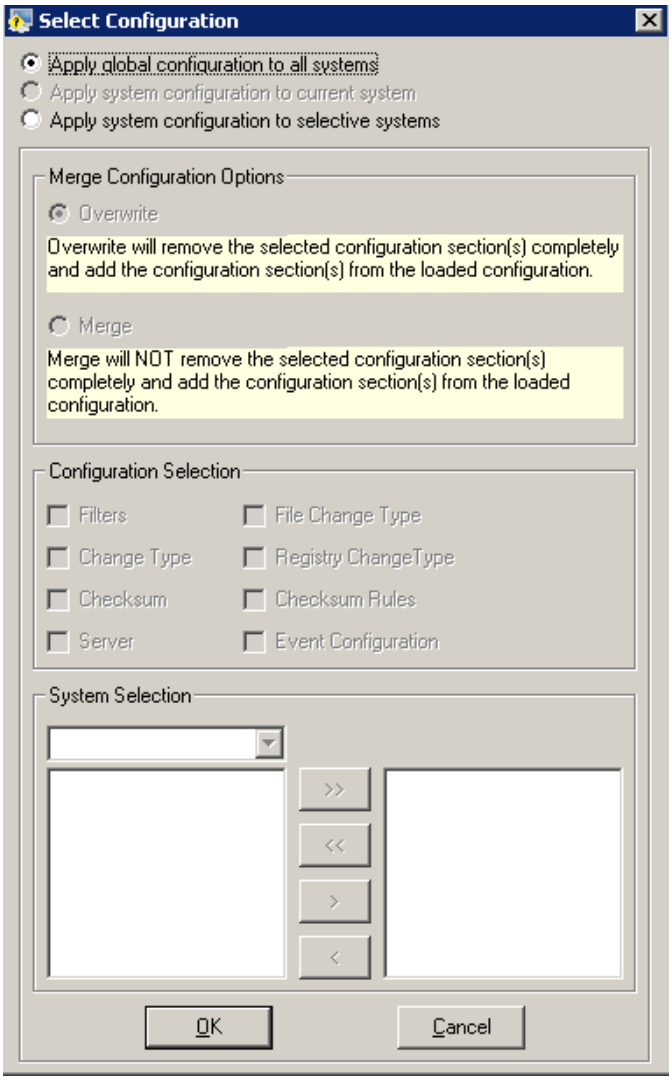
5.2 Apply Global Configuration

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

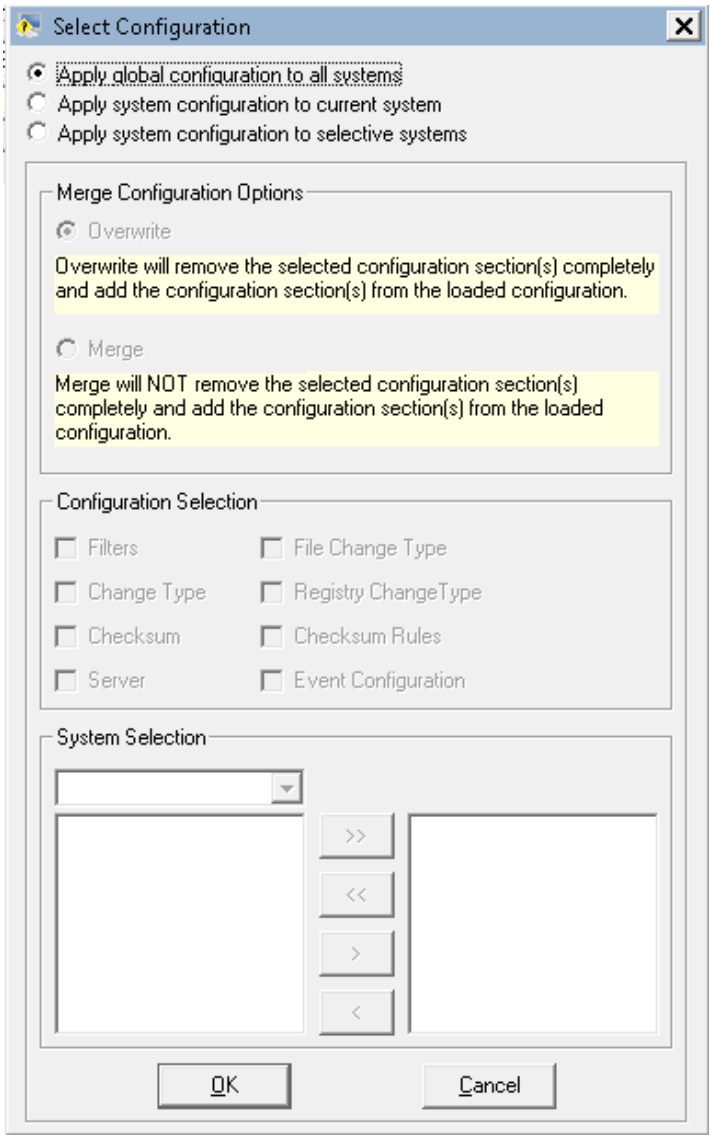
To apply Global Configuration, follow the steps below:

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 Change Audit displays the **Select Configuration** window with the option to apply global configuration alone.



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



3. Select the **Apply global configuration to all systems** option and then click **OK**. If you select the **Apply system configuration to the current system** option, then Change Audit is applied to the system configuration to the current system.
4. **Apply system configuration to selected systems** allows the user to apply the selected configuration on a group of systems. The **'Merge Configuration Options'** allows 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. **The system Selection** group provides system groups and a system list that the user can select and apply the configuration.
   Change Audit applies the global configuration to all the monitored systems.

5.3 System Configuration

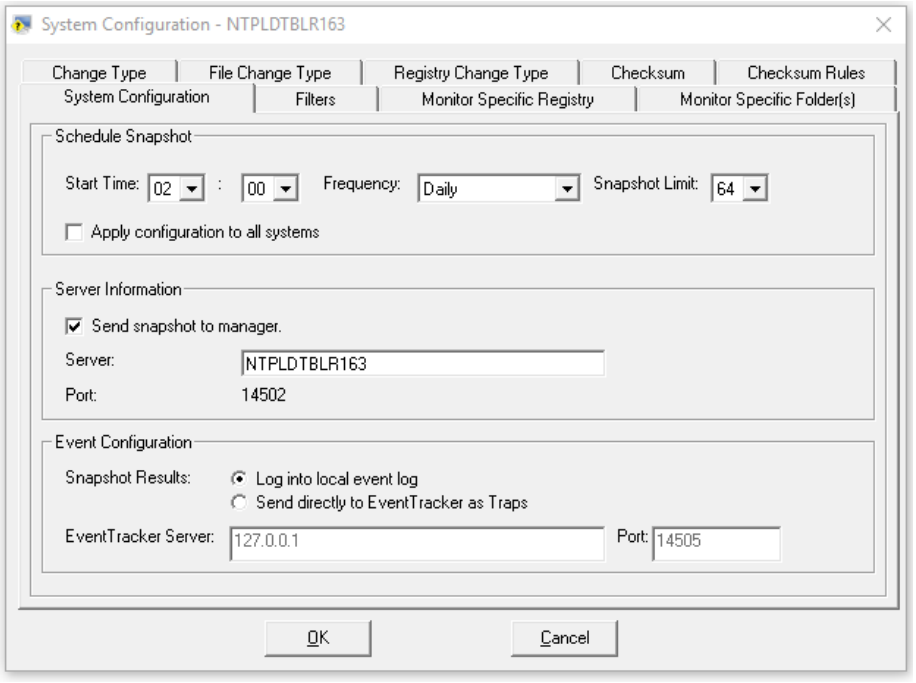
This option helps you set the System Configuration.

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, 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 the configuration. Change Audit loads the system details.
3. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.



Field	Description
System Configuration	
Start Time	By default, Change Audit selects 2 A.M. You can modify the time by selecting from the dropdown list.
Frequency	By default, Change Audit selects Daily as the frequency. You can modify the frequency by selecting from the dropdown list.
Snapshot Limit	By default, Change Audit selects the maximum limit as 30. You can modify this limit by selecting from the dropdown list.
Apply configuration to all systems	Select this checkbox 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 a backup of a snapshot on a manager system.
Server	Provide the server's name on which backup of snapshots should be taken.
Snapshot Result	Change Audit client logs the Snapshot Results as events with the source set to "Change Audit' to local log (Windows Application logs) or forward Snapshot Results as Traps to Netsurion Open XDR with source set to "Change Audit'.
Log into the local event log	Select this option if 1. Netsurion Open XDR Manager and Change Audit are installed on different systems. Netsurion Open XDR Manager can fetch those events through Agent-less monitoring available in Netsurion Open XDR System Manager. 2. Netsurion Open XDR Agent and Change Audit are installed on the same system. 3. You need guaranteed delivery of events. The transport mode can be set to TCP via Netsurion Open XDR Agent. 4. You need permanent entries in the event log. 5. You wish to make Change Audit events available to third-party tools.

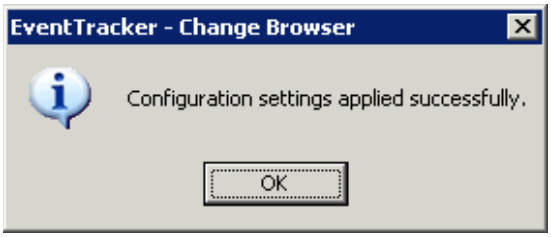
Send directly to Netsurion Open XDR as Traps	Select this option if Change Audit and Netsurion Open XDR Manager are installed on the same system. Delivery of Traps is not guaranteed since the transport mode is UDP. Type the IP address of the Netsurion Open XDR Server. Type the port number if you wish to send Traps through a different port.

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. 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**. Change Audit applies the changes and displays the Change Audit dialog box.



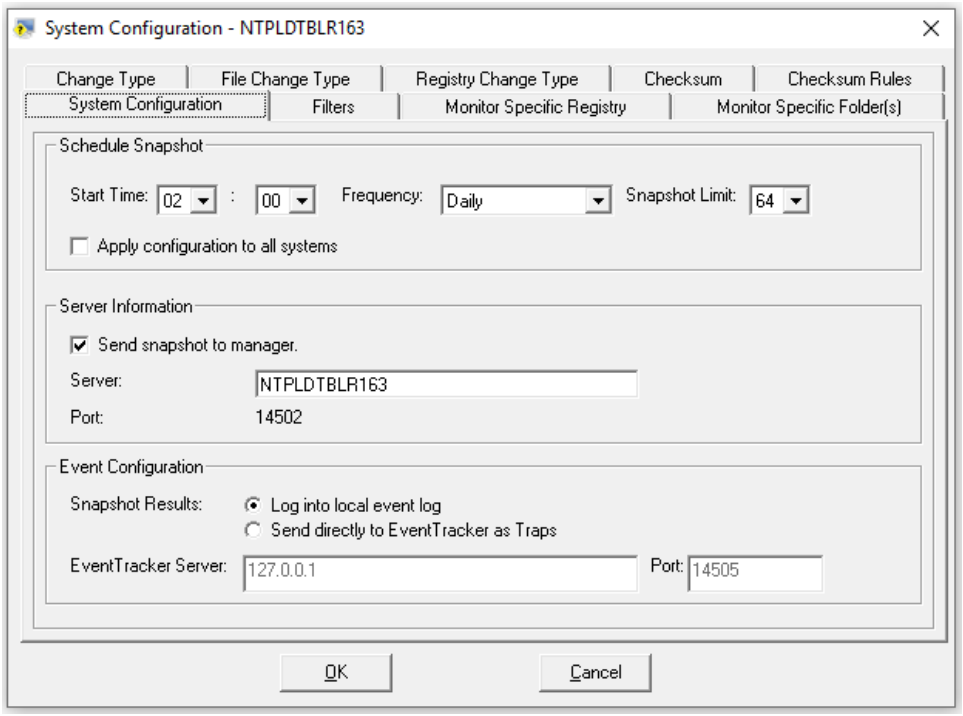
5. Click **OK**.

5.3.2 Apply System Configuration – Remote Systems

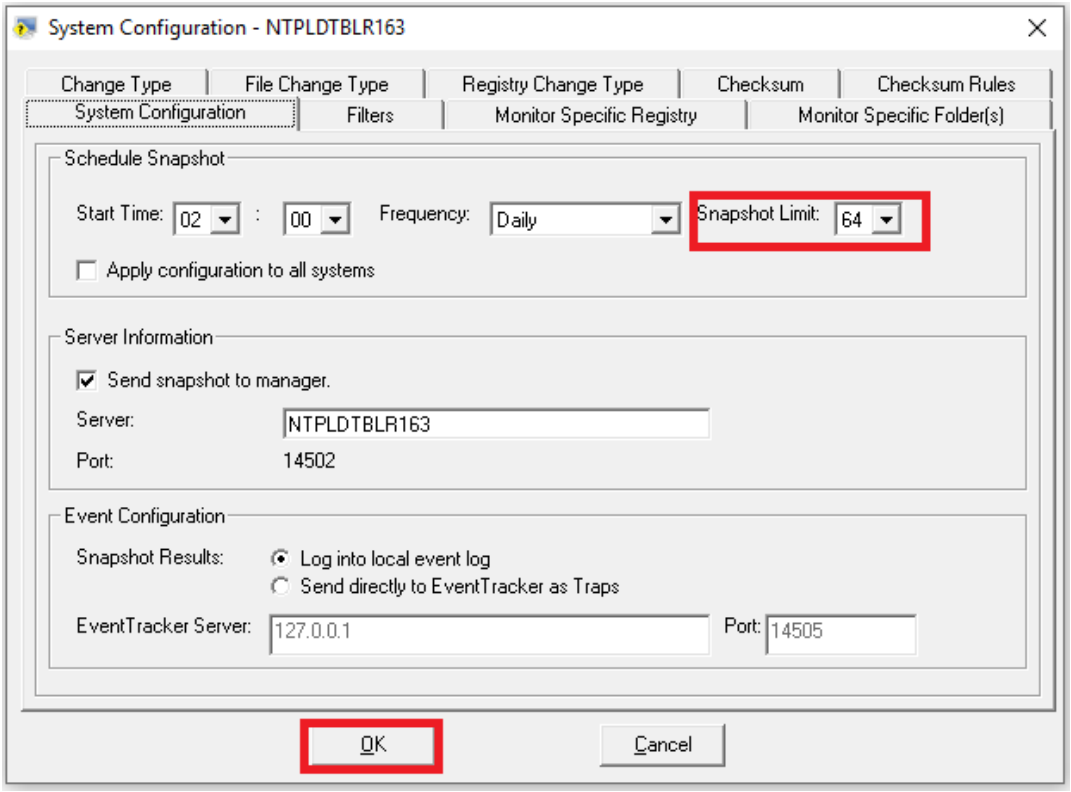
This option helps to apply Snapshot and Filter settings to remote systems.

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

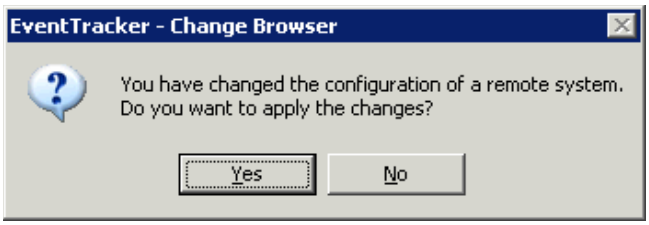
1. Open the Change Browser.
2. On the System Bar, double-click the remote computer for which you want to apply the configuration.
3. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.



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



Change Audit displays the dialog box as shown below:



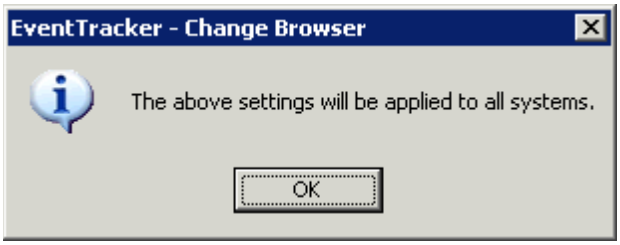
5. Click **Yes** to proceed. Change Audit applies changes to the selected computer.

5.3.3 Apply System Configuration – All Systems

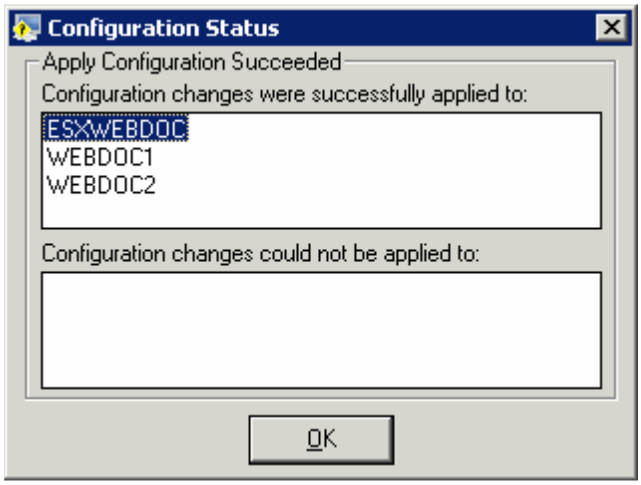
This option helps you apply Snapshot settings to all systems.

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. Change Audit displays the System Configuration window.
4. Modify the Snapshot Automation settings.
5. Select the **Apply configuration to all systems** checkbox. Change Audit displays the following dialog box.



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



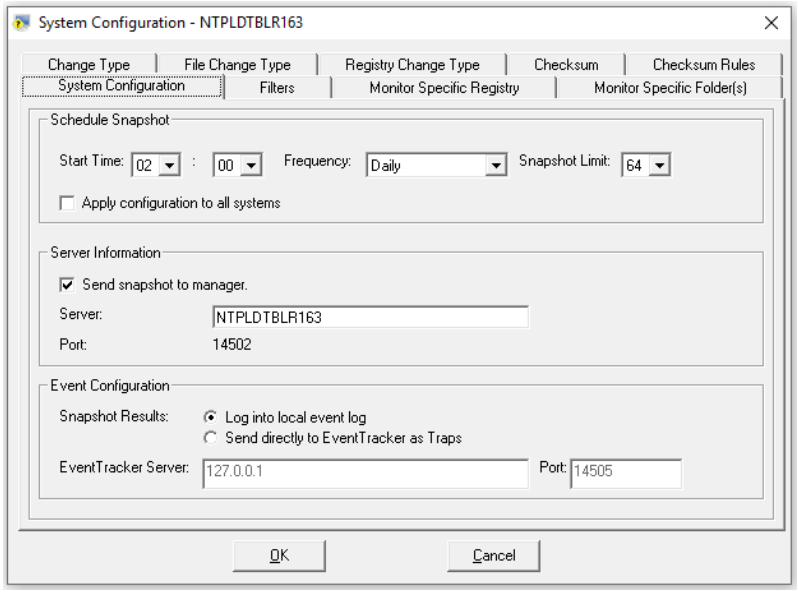
8. Click **OK**.

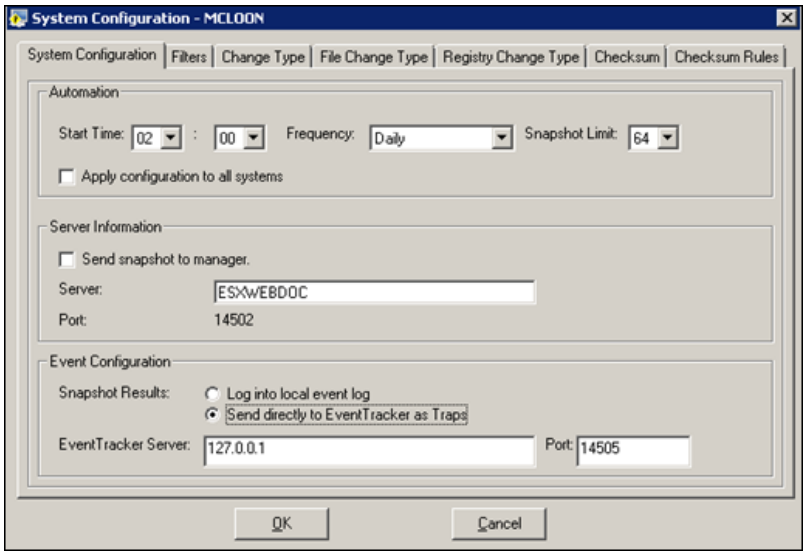
5.4 Search the Change Events (Netsurion Open XDR Search Interface)

5.4.1 Option to Log / Forward Snapshot Results to Netsurion Open XDR

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

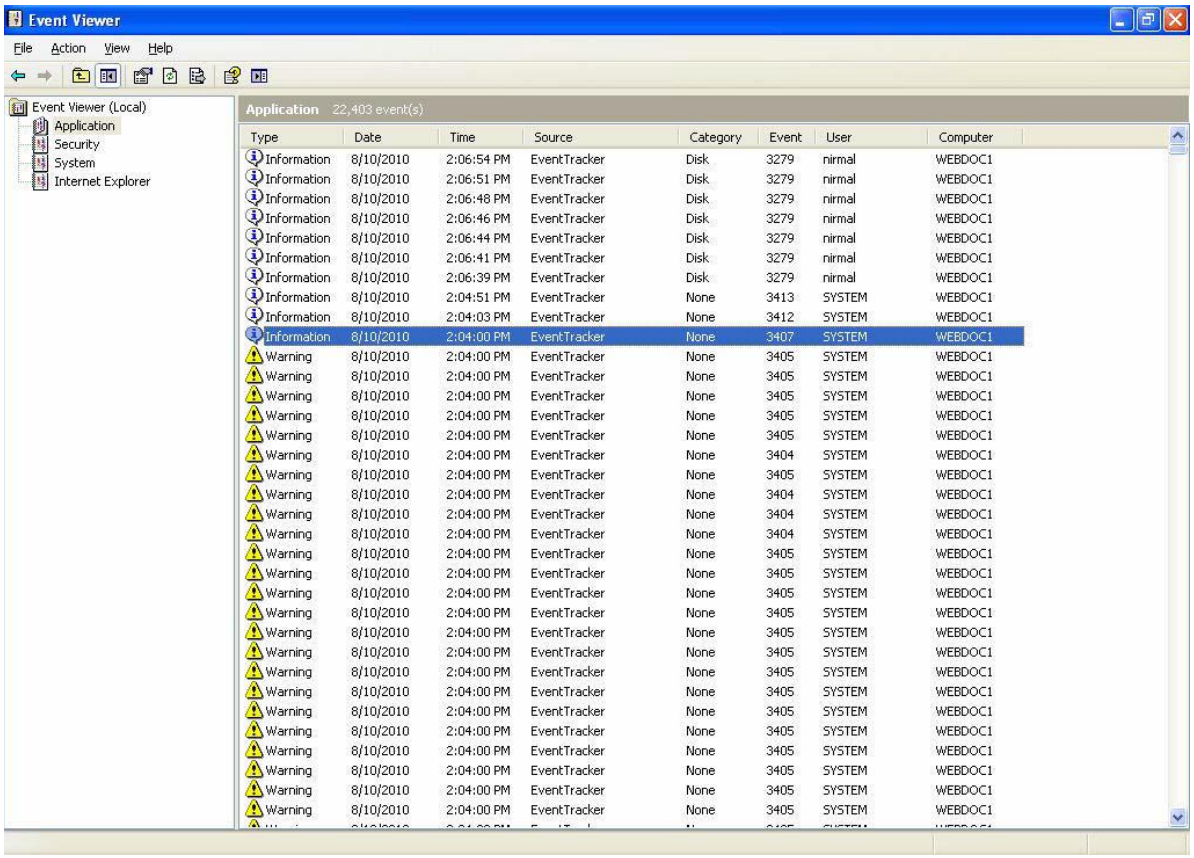
1. Open the Change Browser.
2. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.



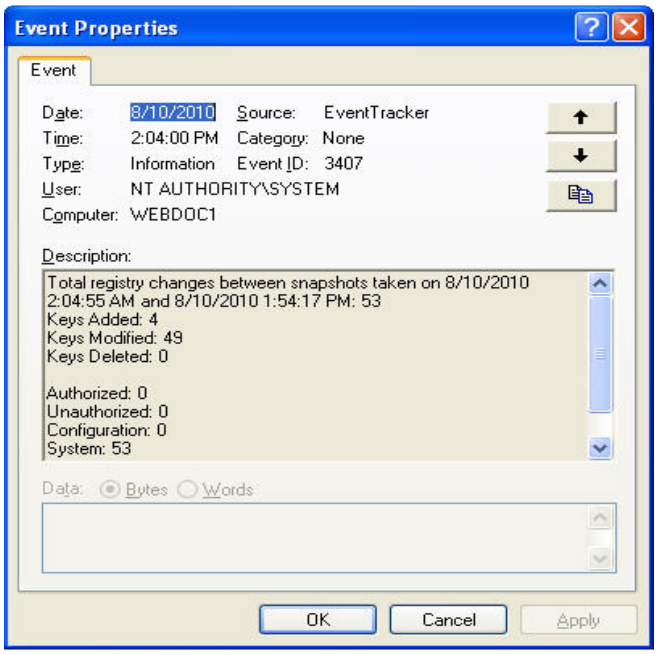


Field	Description
Snapshot Results: Change Audit client logs the Snapshot Results as events with source set to “Change Audit’ to local log (Windows Application logs) or forward Snapshot Results as Traps to Netsurion Open XDR with source set to “Change Audit’.	
Log into the local event log	Select this option if 1. Netsurion Open XDR Manager and Change Audit are installed on different systems. Netsurion Open XDR Manager can fetch those events through Agent-less monitoring available in Netsurion Open XDR System Manager. 2. Netsurion Open XDR Agent and Change Audit are installed on the same system. 3. You need guaranteed delivery of events. The transport mode can be set to TCP via Netsurion Open XDR Agent. 4. You need permanent entries in the event log. 5. You wish to make Change Audit events available to third-party tools.
Send directly to Netsurion Open XDR as Traps	Select this option if Change Audit and Netsurion Open XDR Manager are installed on the 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.



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



6. Select the **Send directly to Netsurion Open XDR as Traps** option and take new snapshots of the monitored computers. Change Audit forwards the snapshot results to Netsurion Open XDR.

5.5 Generating Reports against Change Audit Category

1. Log in to Netsurion Open XDR.
2. Click the **Tools** dropdown 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**. Netsurion Open XDR 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 the Report cost details.
13. Crosscheck the Report details and then click **Generate Report**.

6 Filters

Filters are configured to avoid Change Audit taking snapshots of frequently changing non-critical directories (such as the browser cache, temp directories) or registry entries. By default, Change Audit uses its 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 are 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 the file or registry system is known.
Adding a normal filter does not remove the filtered node from the snapshots i.e. the changes detected so far are retained; it only stops monitoring any changes in the object from the time it is filtered.	When we declare a customized filter, it means we do not want to monitor any changes to the object and we do not want to retain any previous changes detected to the object also.
The change history of the filtered object is retained.	The change history of the filtered object is NOT retained.
When the object is unfiltered again, because the 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 the size of the snapshot file.	Adding a customized filter may decrease the 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’.

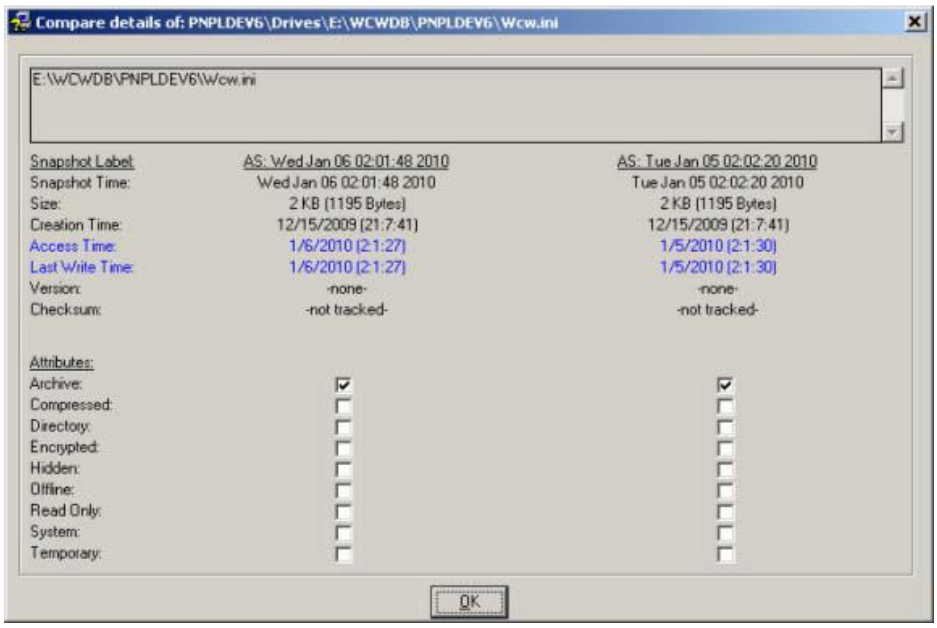
Note

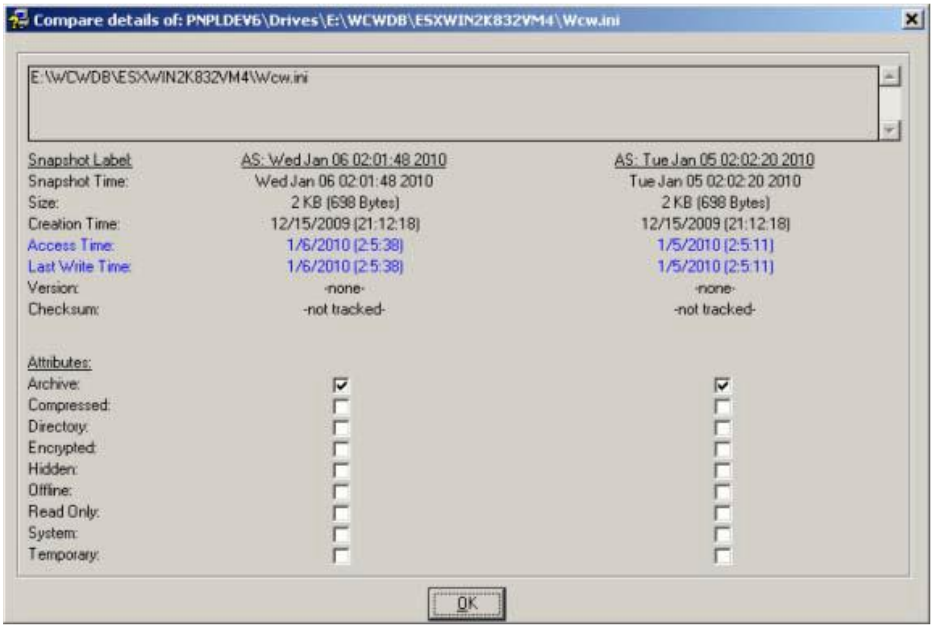
Both the files are currently being monitored.

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

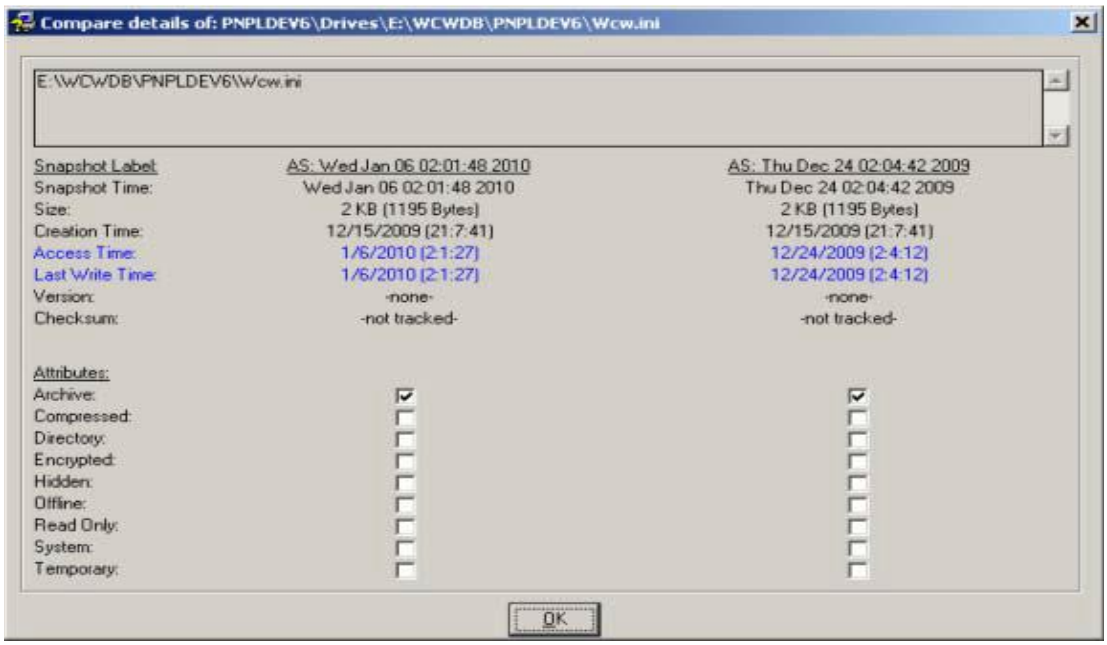


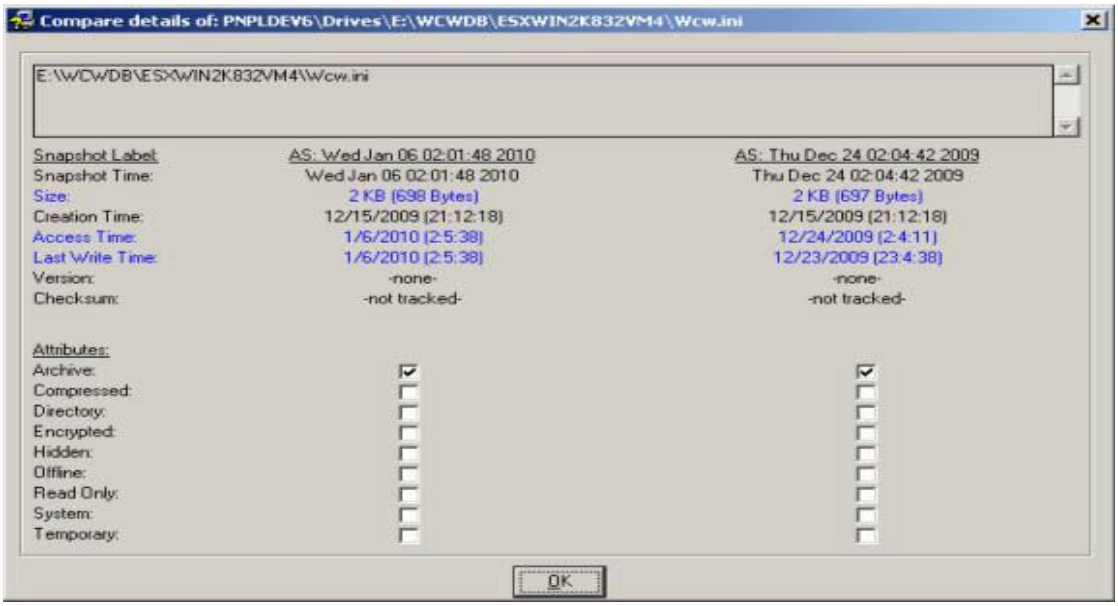


The following screenshots display the properties (concerning baseline snapshot) of 2 files E:\WCWDB\PNPLDEV6\wcw.in" and "E:\WCWDB\ESXWIN2k832VM4\wcw.ini" before adding the filters.

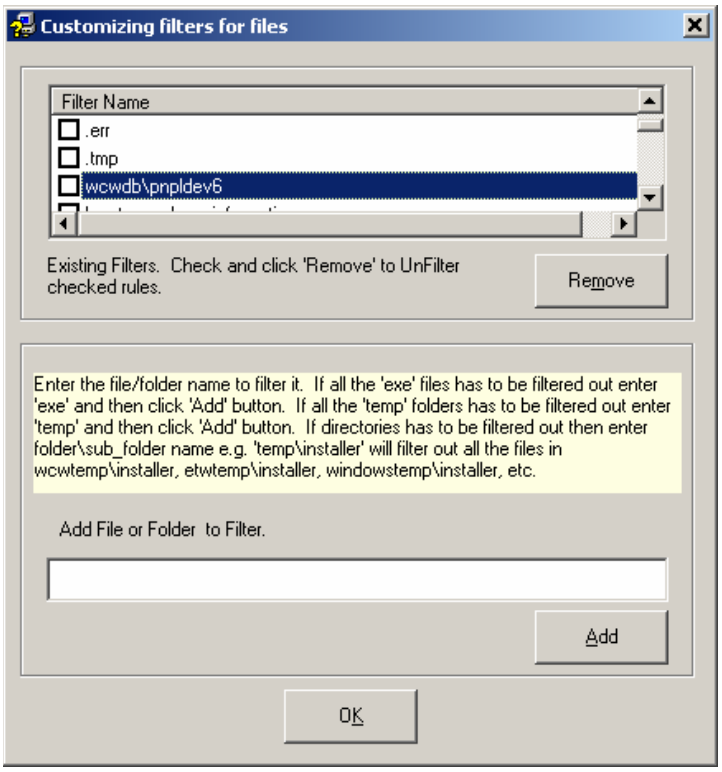
Current Snapshot: 2010-01-06T02:01:48

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

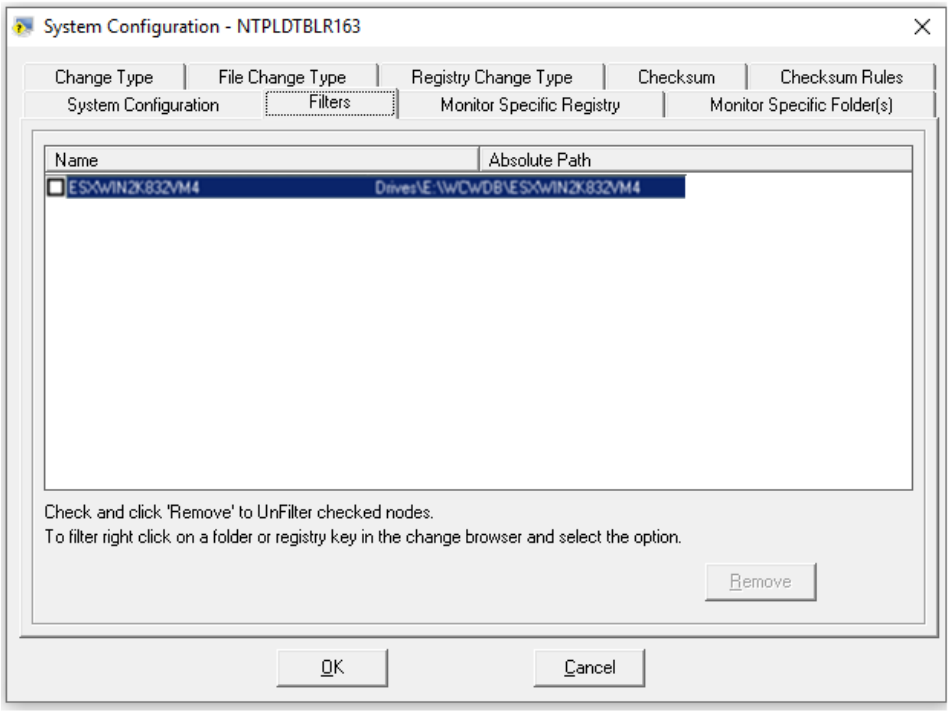




3. Add a customized filter to the folder “wcwdb\pnpldev6’.

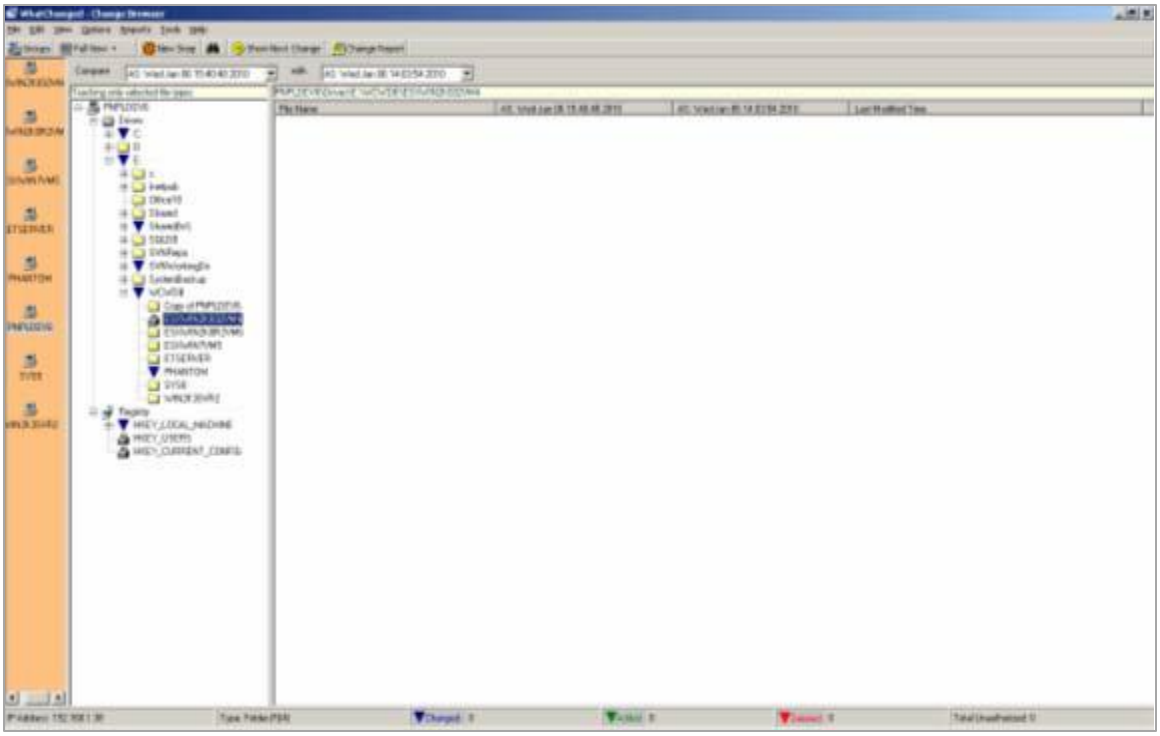


4. Add a normal filter to filter the folder “E:\WCWDB\ESXWIN2k832VM4\’.



5. Make changes to the two files and take a new snapshot after adding the two filters. Neither of the files is reported as changed.

   The folder “E:\WCWDB\ESXWIN2K832VM4’ is displayed as filtered, while the folder “E:\WCWDB\PNPLDEV6’ is not at all displayed because it has been completely removed from snapshots.



6. Remove both the filters and take a new snapshot.
   The following screenshots display the properties of both files after taking the snapshot without the filters.

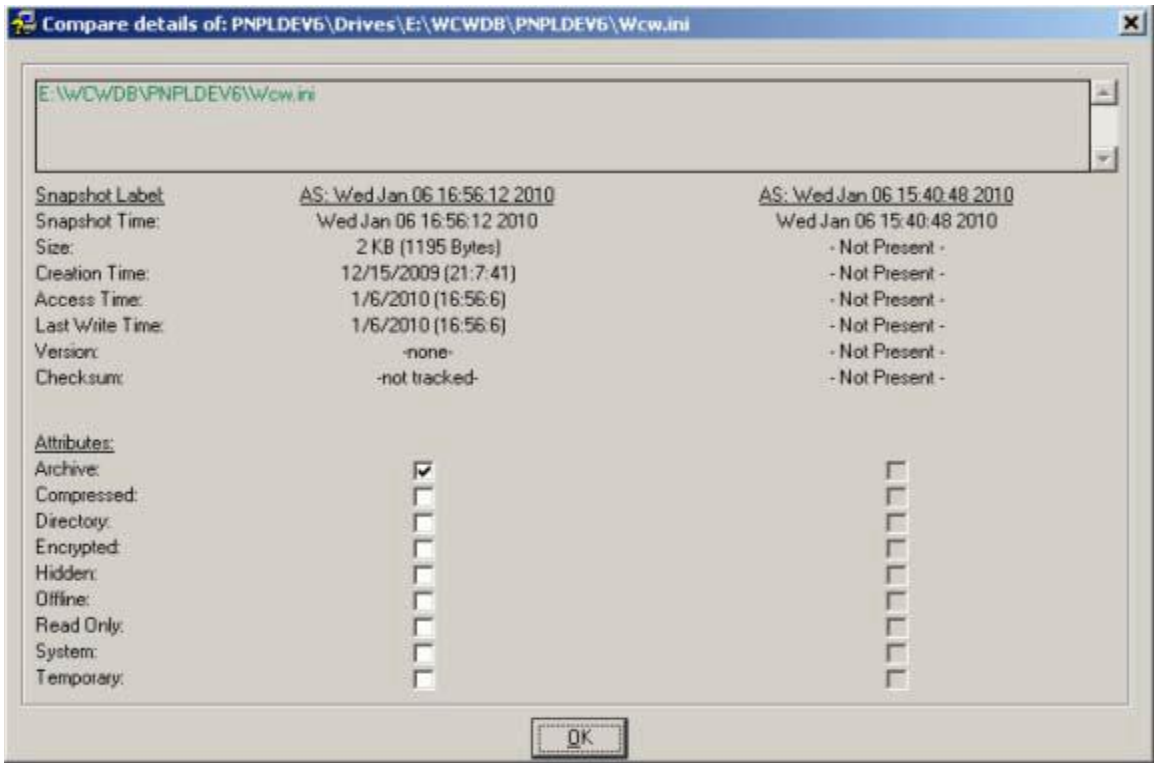
Note

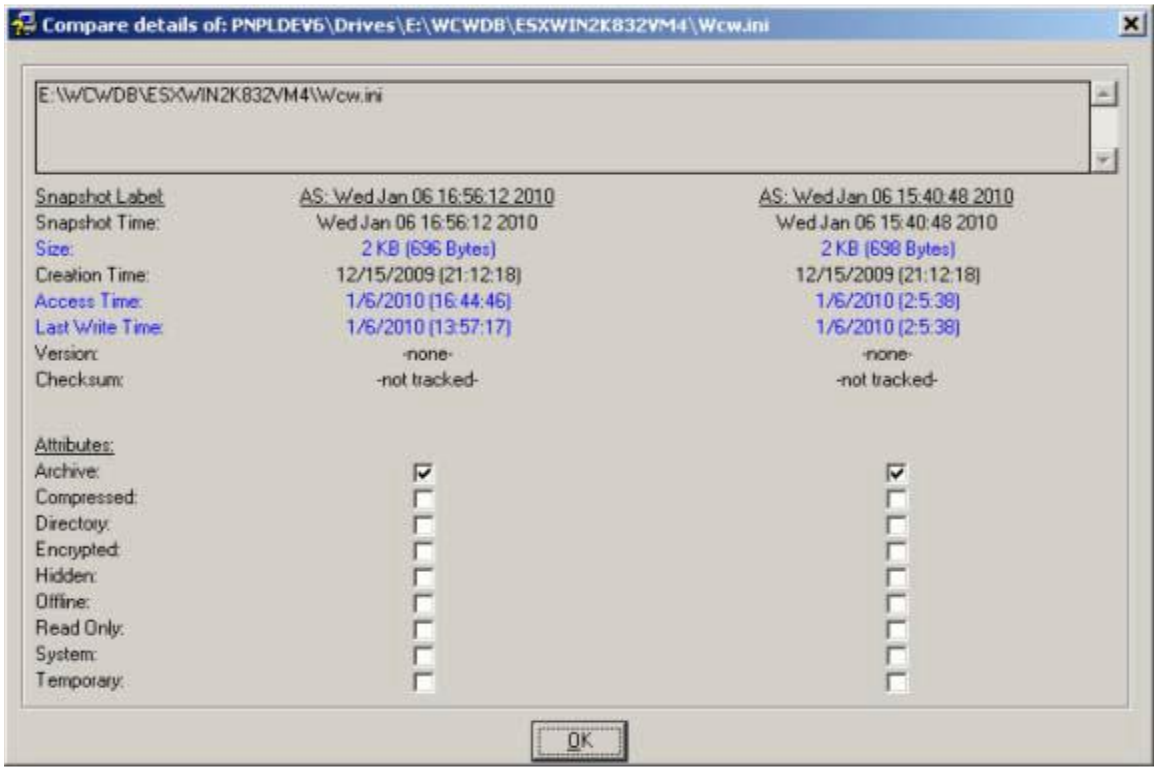
The file “E:\WCWDB\PNPLDEV6\wcw.ini’ is displayed in green color which means it is reported as a new file added to the snapshot because no change history for this file is available.

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

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

Previous Snapshot: 2010-01-06T15:40:48





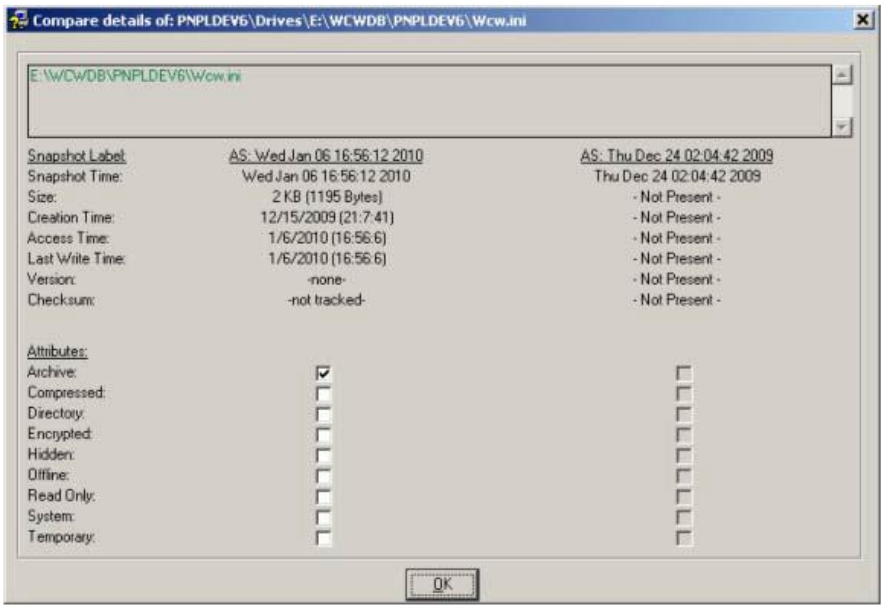
The following screenshots display the properties (concerning baseline snapshot) of 2 files “E:\WCWDB\PNPLDEV6\wcw.in’ and “E:\WCWDB\ESXWIN2k832VM4\wcw.ini’ after removing both the filters.

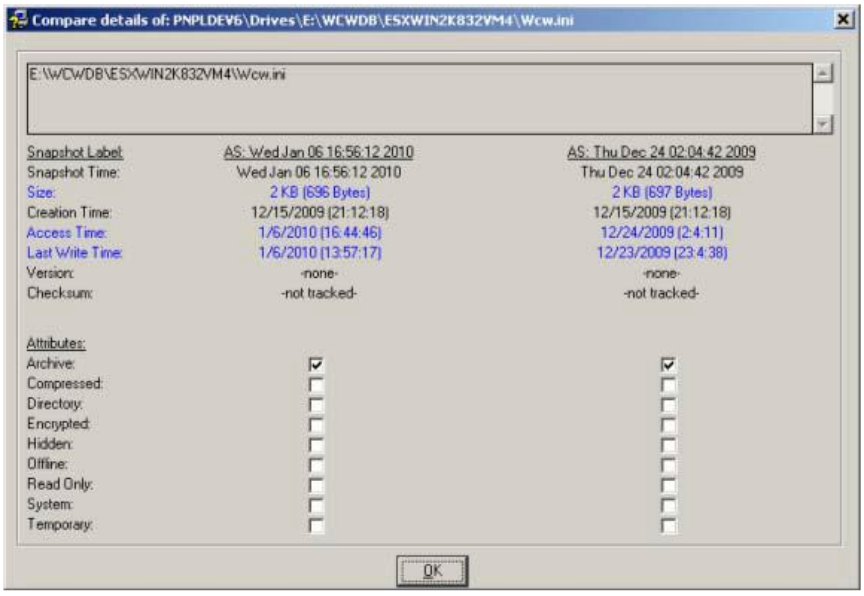
Note

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



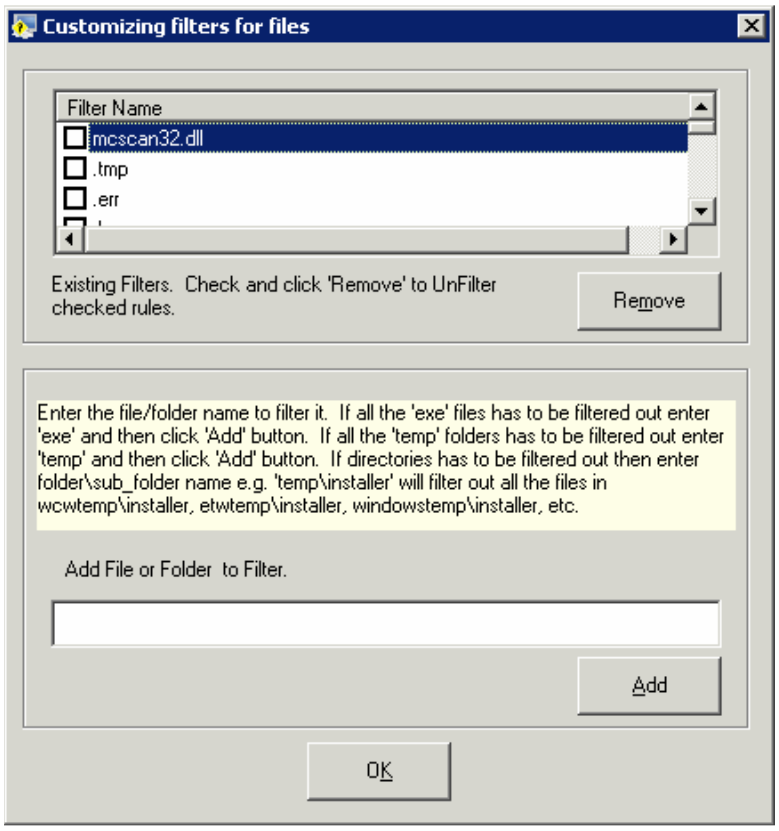


6.3.2 Customize Filters

This option helps you customize the filters.

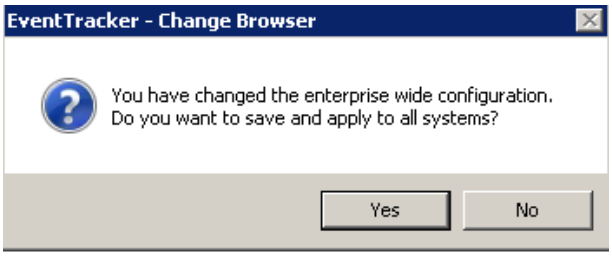
To customize filters, follow the steps below:

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.
4. Change Audit displays the shortcut menu. From the shortcut menu, choose **Customize Filter**. Change Audit displays the Customizing filters for the files window.



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

5. Select the check box against the filter name that you want to include in the Snapshot and then click **Remove**. Change Audit removes the selected file.
6. Click **OK**.
7. To add a file or folder to the filter, type the name of the file or folder in the **Add File or Folder to Filter** field.
8. Click **Add**. Change Audit adds the file to the Filter.
9. Click **OK**.



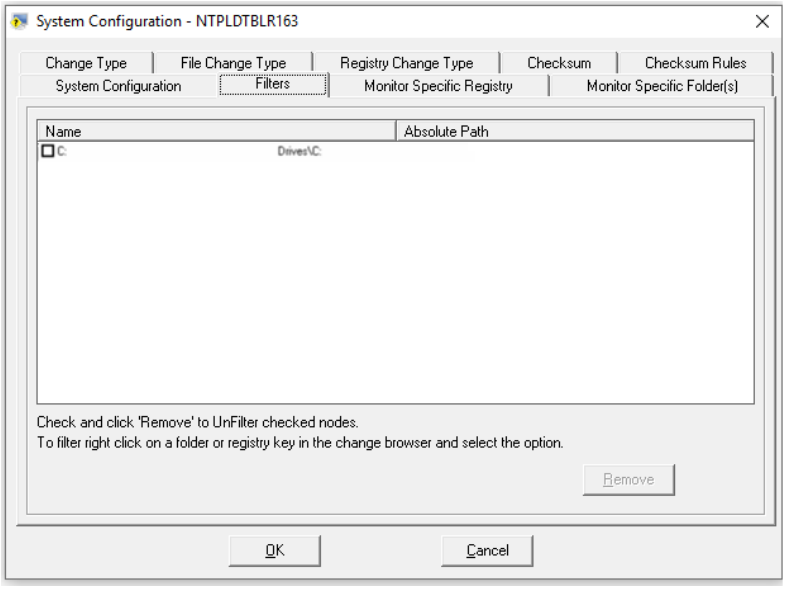
10. Click **Yes**.

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:** Change Audit displays the shortcut menu. From the shortcut menu, choose **Filter**. Change Audit filters the selected drive.
4. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.
5. Click the **Filters** tab. Change Audit displays the Filters tab with the newly added filter.



6.5 Apply Filters Option – Remote Systems

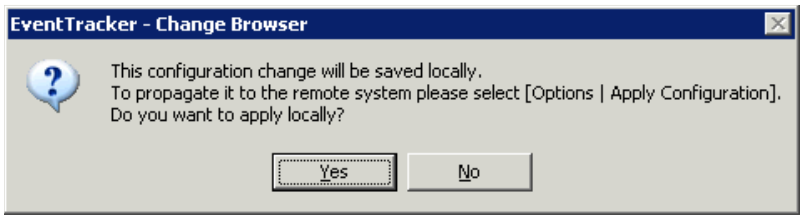
This option helps you apply filters to the remote system.

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

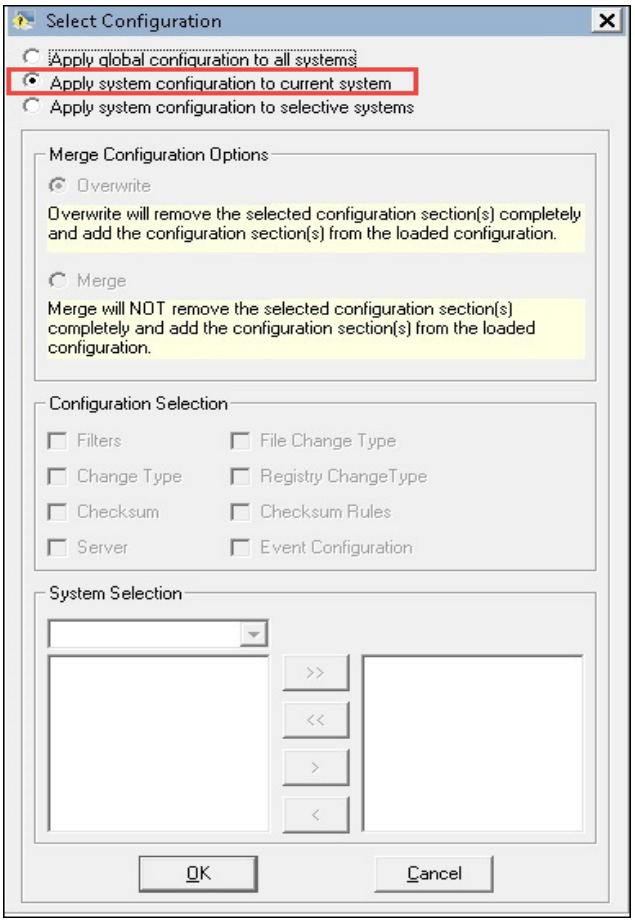
1. Open the Change Browser.

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:.

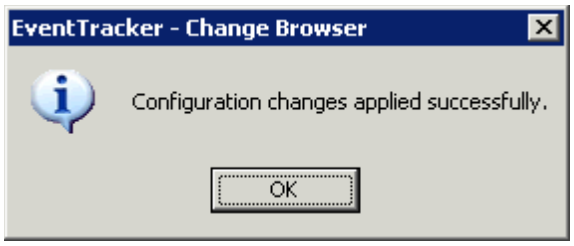
   Change Audit displays the shortcut menu. From the shortcut menu, choose **Filter**. A dialog box will be displayed as shown below:



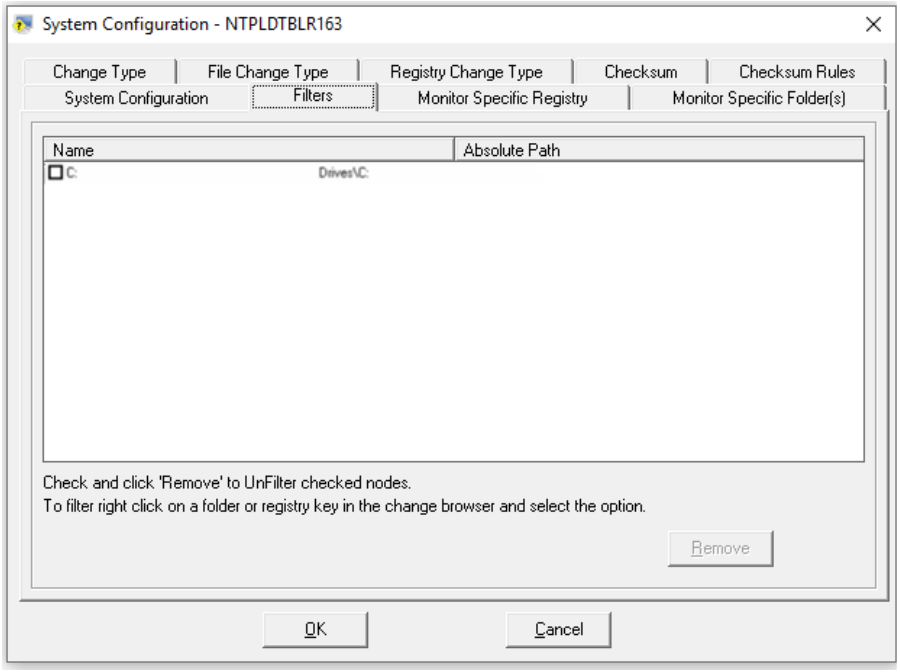
4. Click **Yes**. Change Audit filters the selected drive.
5. Click the **Options** menu and select the **Apply Configuration** option. Change Audit displays the **Select Configuration** window.



6. Select the **Apply system configuration to the current system** option and then click **OK**. Change Audit displays the Change Audit dialog box.



7. Click **OK**.
8. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.
9. Click the **Filters** tab. Change Audit displays the Filters tab with the newly added filter.

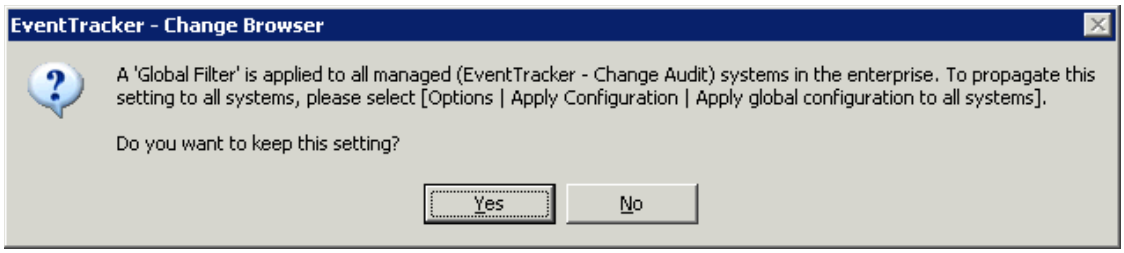


6.6 Apply Filters Option – All Systems

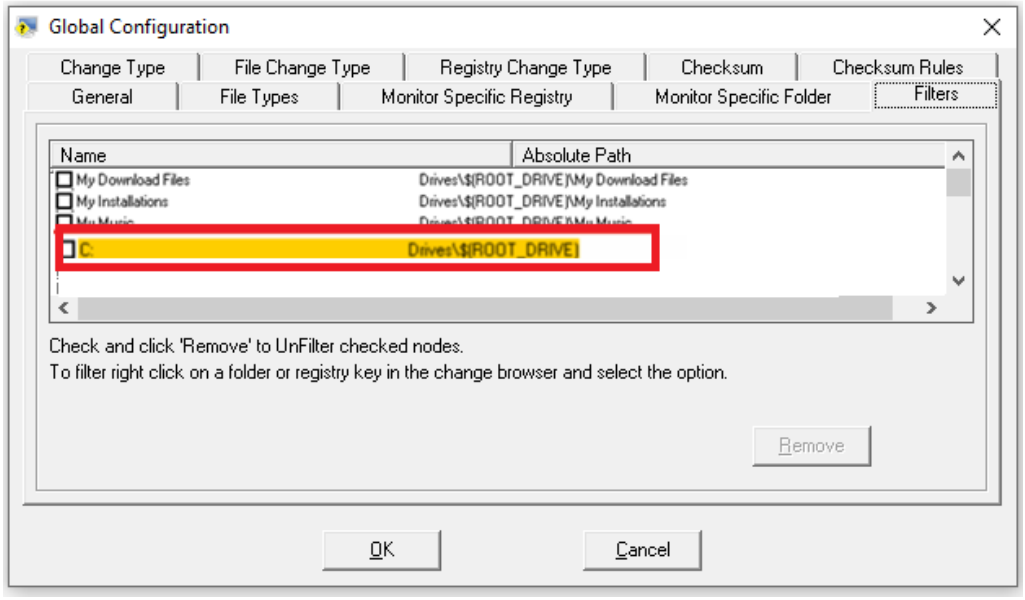
This option helps you apply filters to all systems.

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

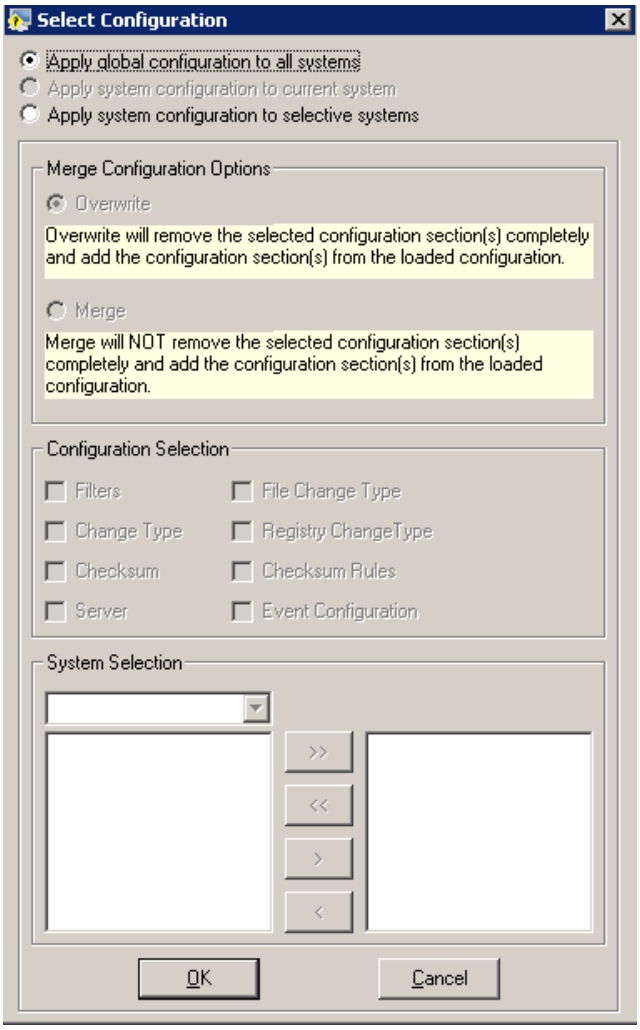
1. Open the Change Browser.
2. Double-click any Computer on the System Bar.
3. Right-click any item under Drives or Registry trees, for example, C:
   Change Audit displays the shortcut menu. From the shortcut menu, choose **Filter (All Systems)**.



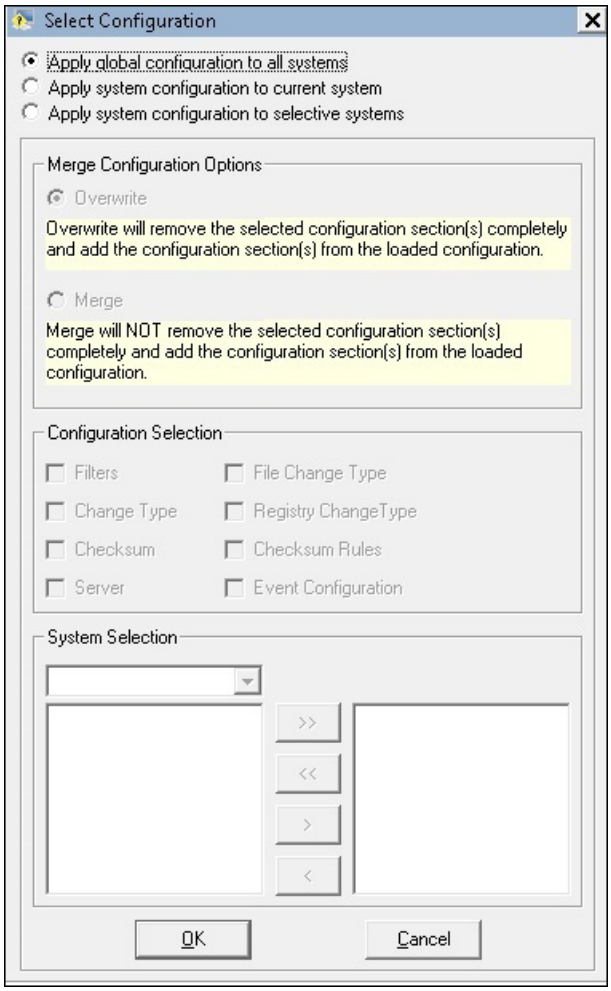
4. Click **Yes** to proceed.
5. Click the **Options** menu and select the **Global Configuration** option. Change Audit displays the Global Configuration window.
6. Click the **Filters** tab. Change Audit displays the Filters tab with the filtered drive.



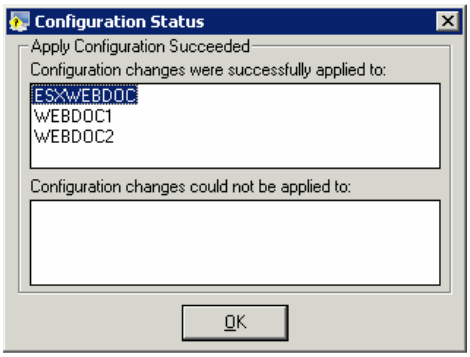
7. Click the **Options** menu and select the **Apply Configuration** option. If the selected system is a local system, then Change Audit displays the Select Configuration window.



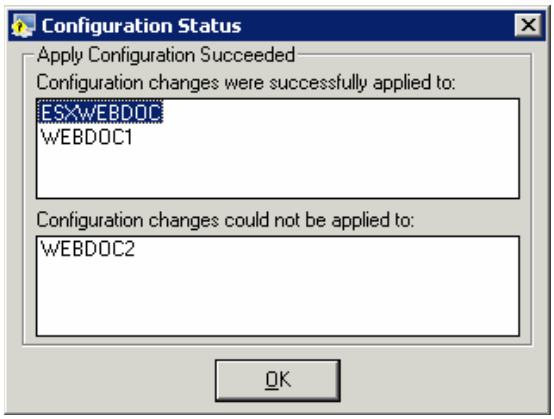
If the selected system is remote, then Change Audit displays the Select Configuration window.



8. Select the **Apply global configuration to all systems** options and then click **OK**. Change Audit applies the global configuration settings and displays the Configuration Status window.



9. Click **OK**.
   If the application of global configuration fails, then Change Audit displays the Configuration Status window with an appropriate message.



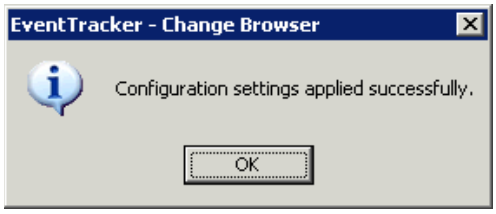
10. Double-click the remote system on the System Bar. Change Audit displays the remote system with the filtered drive.

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 in the Drives tree which was filtered earlier.
4. Change Audit displays the shortcut menu.
5. From the shortcut menu, choose **Filter** and unselect the checkbox. Change Audit un-filters the selected drive.
   (OR)
6. Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.
7. Click the **Filters** tab. Change Audit displays the Filters tab with the filtered drive.
8. Select the check box against the drive and then click **Remove**.
9. Click **OK**. Change Audit un-filters and displays the success dialog box.



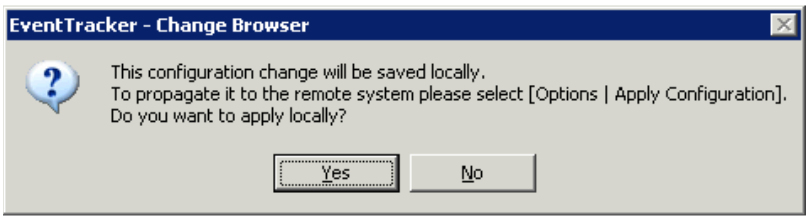
10. Click **OK**.

6.8 Remove Filters – Remote Systems

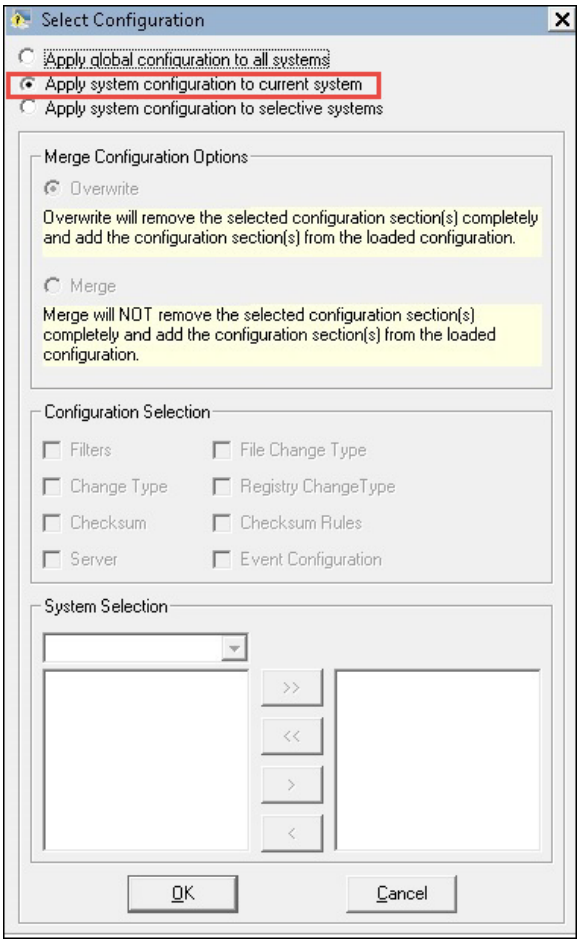
This option helps you remove filters from remote systems.

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

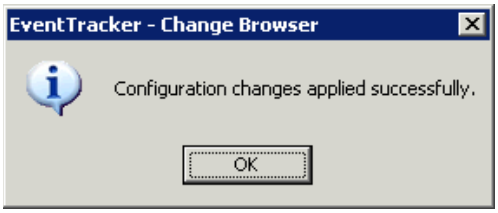
1. Open the Change Browser.
2. Double-click the remote computer on the System Bar for which you want to remove filters.
3. Right-click the drive.
   Example C: in the Drives tree, which was filtered earlier.
4. Change Audit displays the shortcut menu. From the shortcut menu, choose **Filter** and unselect the checkbox.
5. Change Audit displays the confirmation dialog box.



6. Click **Yes**.
7. Click the **Options** menu and select the **Apply Configuration** option. Change Audit displays the Select Configuration window.

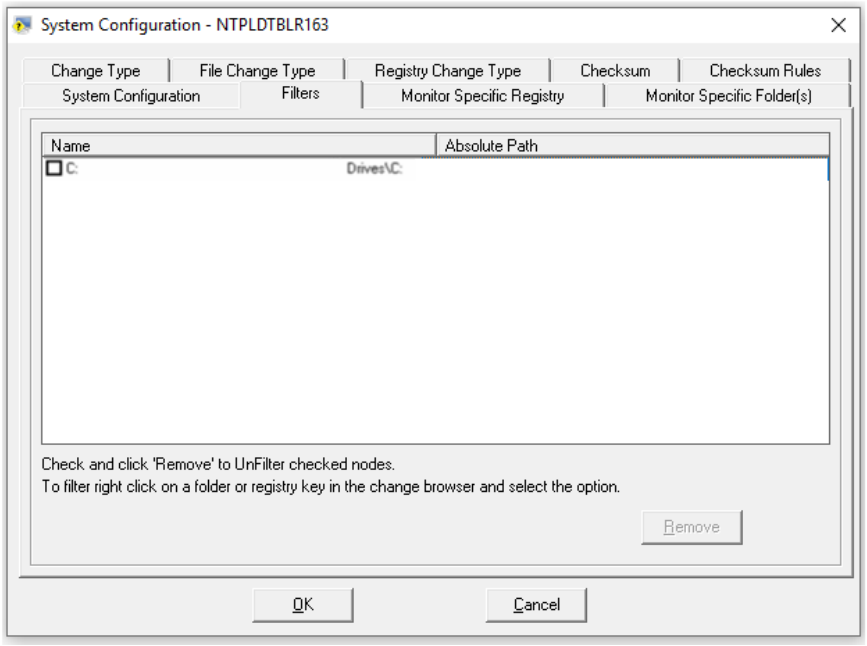


8. Select the **Apply system configuration to the current system** option and then click **OK**. Change Audit displays the dialog box.

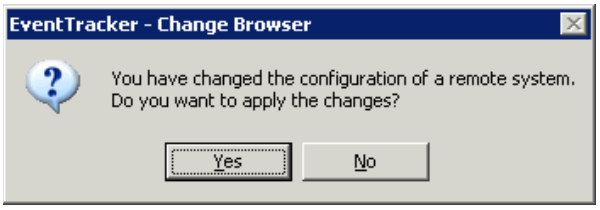


9. Click **OK**. Change Audit un-filters the selected drive.
   (OR)

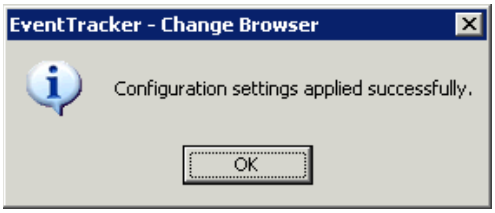
   Click the **Options** menu and select the **System Configuration** option. Change Audit displays the System Configuration window.
10. Click the **Filters** tab. Change Audit displays the Filters tab with the filtered drive.



11. Select the check box against the drive and then click **Remove**.
12. Click **OK**. Change Audit displays the dialog box as shown in the below image.



13. Click **Yes**.



14. Click **OK**. Change Audit un-filters the selected drive.

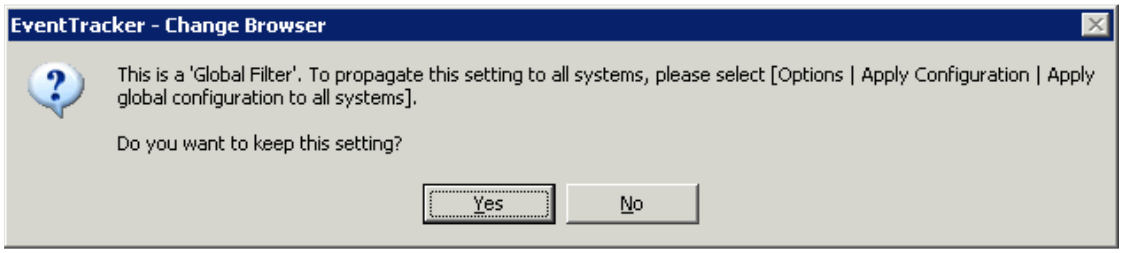
6.9 Remove Filters – All Systems

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.

4. Change Audit displays the shortcut menu. From the shortcut menu, choose **Filter (All Systems)** and then clear the tick mark. A dialog box will be displayed as shown below.



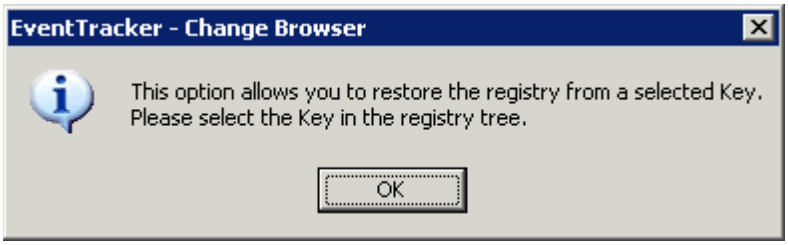
5. Click **Yes**. Change Audit un-filters the selected drive in all the local and remote computers.

6.10 Restore Registry Sub-tree

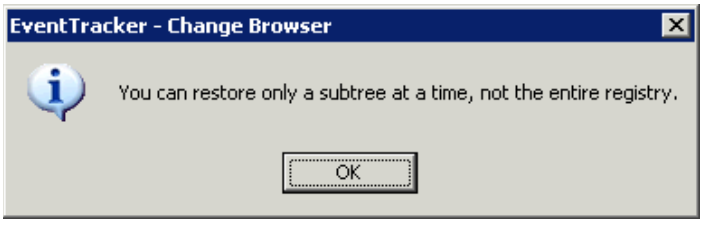
This feature helps you select a previously taken Snapshot of your system and return your system to that (registry) configuration. You can restore a selected registry key from the previous Snapshot. The key value is restored to its previous contents. Only users with Admin privileges may perform this operation.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

To restore the registry sub-tree, follow the steps below:

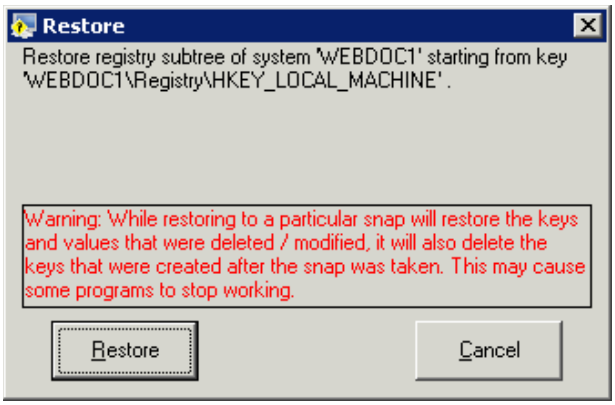
1. Open the Change Browser.
2. On the System Bar, double-click the computer for which you want to restore the registry sub-tree.
3. Select the Snapshots from the dropdown lists. A dialog box will be displayed as shown below.



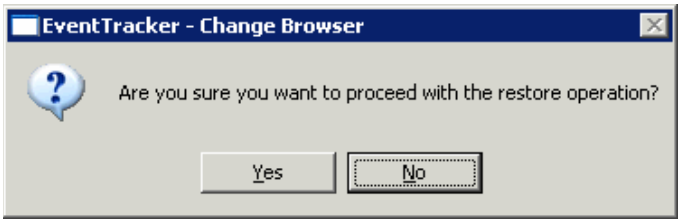
4. Change Audit displays the message as if had you tried to restore the entire registry.



5. Select the appropriate sub-tree from the Registry tree.
6. Click the **Options** menu and select the **Restore Registry sub-tree** option. Change Audit displays the Restore confirmation dialog box.



7. Click **Restore**. Change Audit displays the confirmation dialog box.



8. Click **Yes** to continue. Change Audit displays the Restore status.

6.11 Restore Logs

This option helps you view the restore logs.

To view restore logs, follow the steps below:

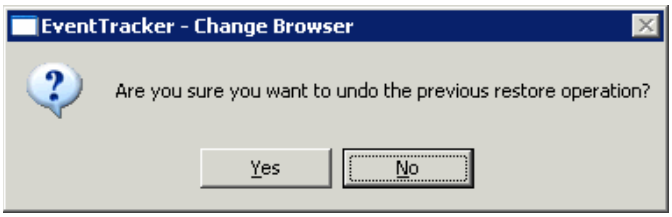
1. Open the Change Browser.
2. Double-click the system on the System Bar.
3. Click the **View** menu and select the **Restore Log** option. Change Audit displays the restore log file in Notepad. It displays an appropriate message if no log exists.

6.12 Undo Restore

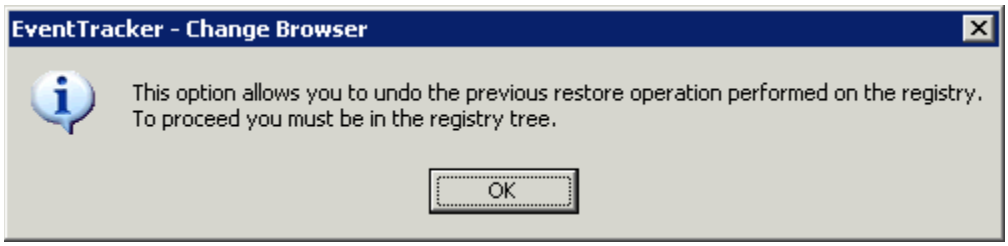
This option helps you undo the registry key restore.

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 dropdown lists.
4. Click the **Options** menu and select the **Undo Restore** option. Change Audit displays the confirmation dialog box.



5. Change Audit displays the information dialog box if you are on the File system tree and trying to undo restore.

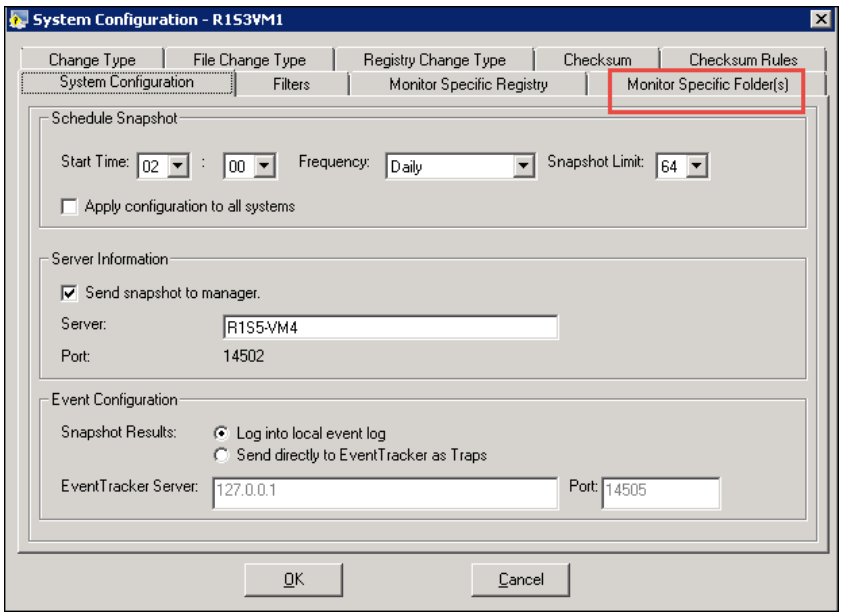


6. Click **Yes** to continue.

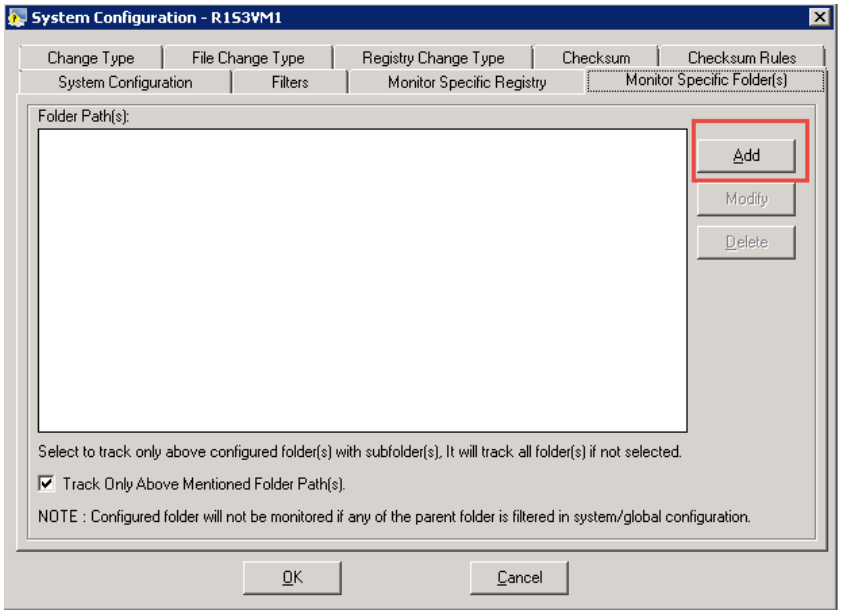
6.13 Support for Monitoring a Specific Folder on the System

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**.

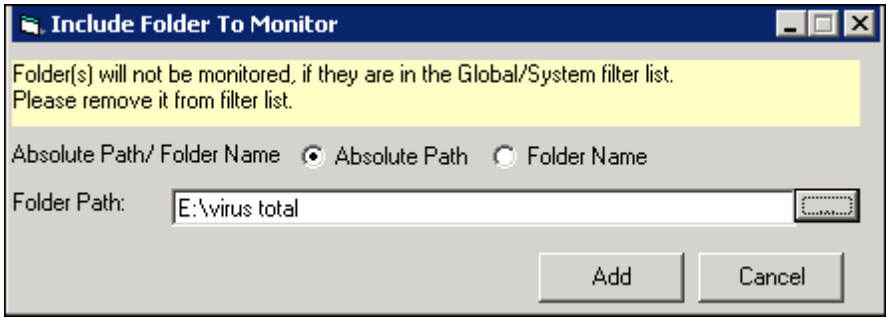


3. The new tab Monitor Specific Folder(s) is added. Using this option, the user can monitor any specific folder(s) from a system.
4. Click the **Monitor Specific Folder(s)** and select the **Add** button to add folders.

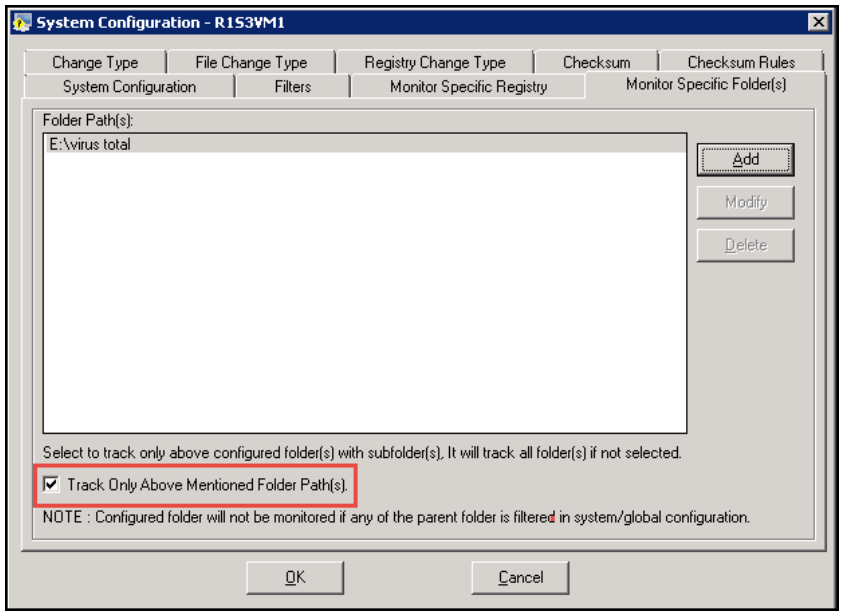


5. Browse the Folder path.

The folders will not be monitored, if Global or System Filter is applied.



6. Click **Add**.



7. Select 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 a new snapshot, the user has to re-initialize the snapshot.

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

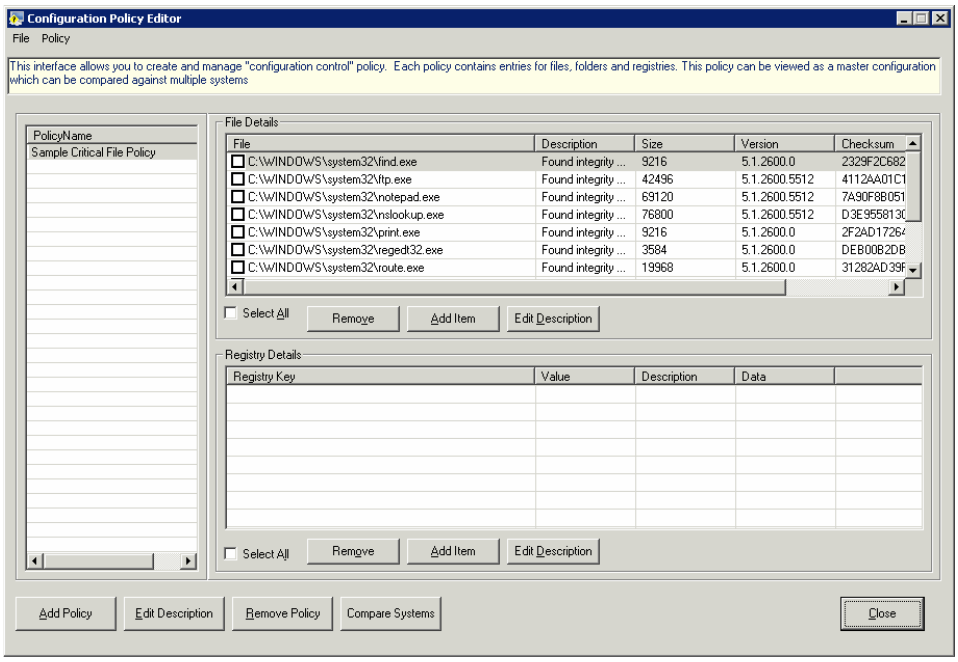
Configuration Policies facilitate the comparison of files, folders, registry items, and registry keys in hives among monitored systems. The advantage of configuring Configuration Policies is that, instantly you will get to know the differences between the comparing and compared systems without initiating 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 resources, cost, and time.

As an administrator of your enterprise network, the responsibility is on you to secure the network from the 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 configure a Configuration Policy and compare the systems. The report generated by Change Audit helps you easily figure out whether it is applied or not to the monitored systems.

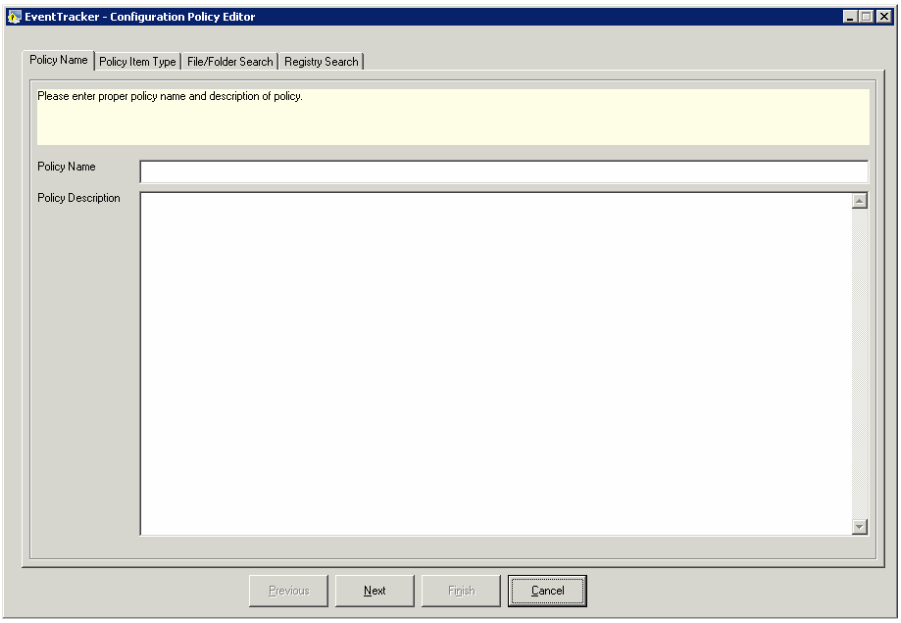
7.1.1 Creating Configuration Policies

To create Configuration Policies, follow the steps below:

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

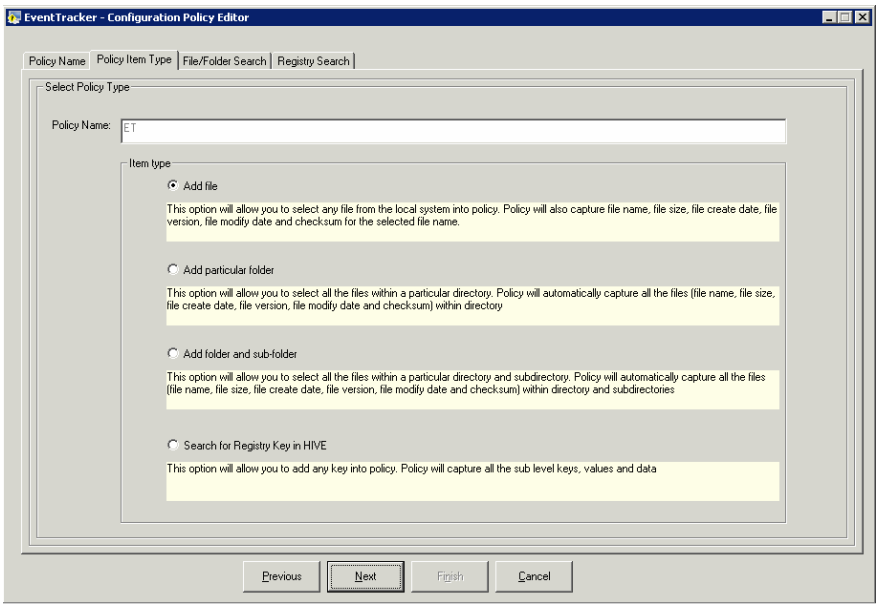


3. Click **Add Policy**. Change Audit displays the Policy Name tab.



4. Type the name and description of the Policy in the **Policy Name** and **Policy Description** fields respectively. Example: ET, EventTracker.

5. Click **Next**. Change Audit displays the Policy Item Type tab.



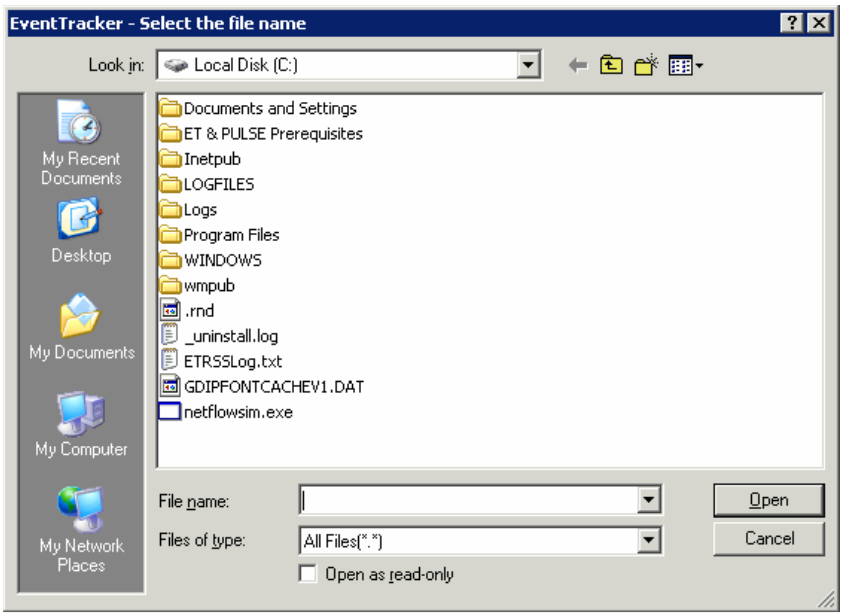
Field	Description
Item Type	
Add file	This option allows you to select any file from the local system into policy. Policy captures the file name, file creation date, file version, file modification, and checksum for the selected file name.
Add particular folder	This option allows you to select all the files within a particular folder. Policy captures details of all the files such as file name, file size, file create date, file version, file modification date, and checksum that reside in that folder.
Select folder and subfolder	This option allows you to select all the files within a particular folder and sub-folder. Policy captures details of all the files such as file name, file size, file create date, file version, file modification date, and checksum that reside in folders and sub-folders.
Search for Registry key in Hive	This option allows you to add any key to the policy. Policy captures all the sub-level keys, values, and data.

7.1.2 Searching a File

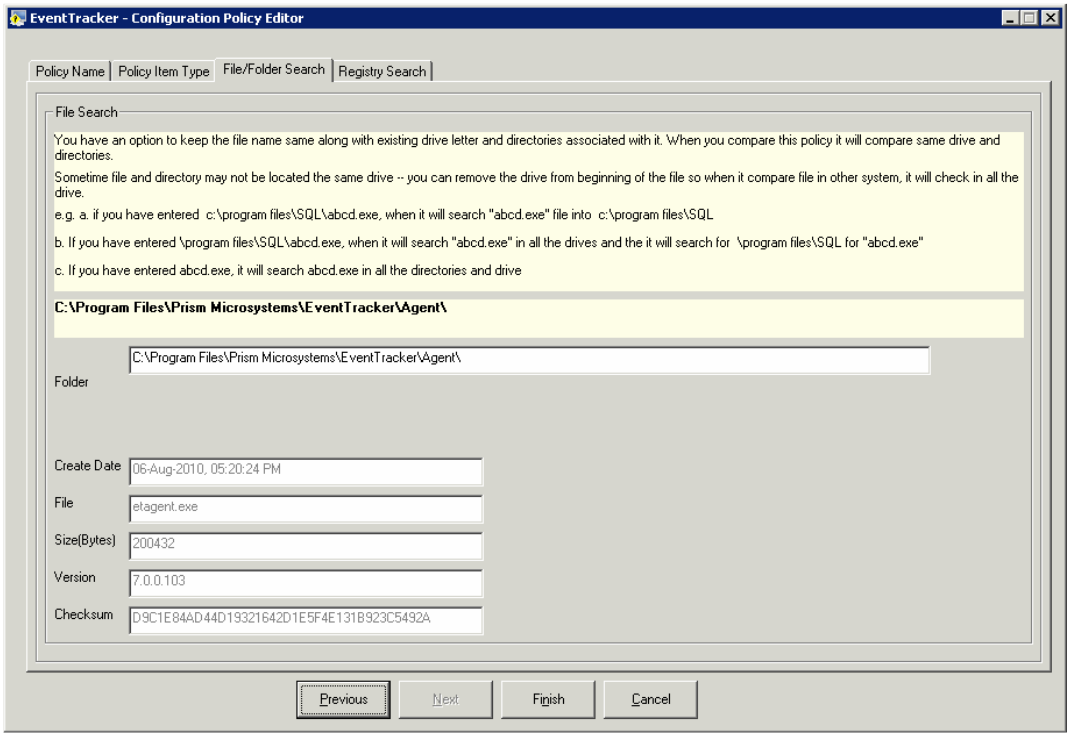
To search a File, follow the steps below:

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

1. Click **Next**. Change Audit displays the Select the file name window.



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**. Change Audit displays the File/Folder Search tab.

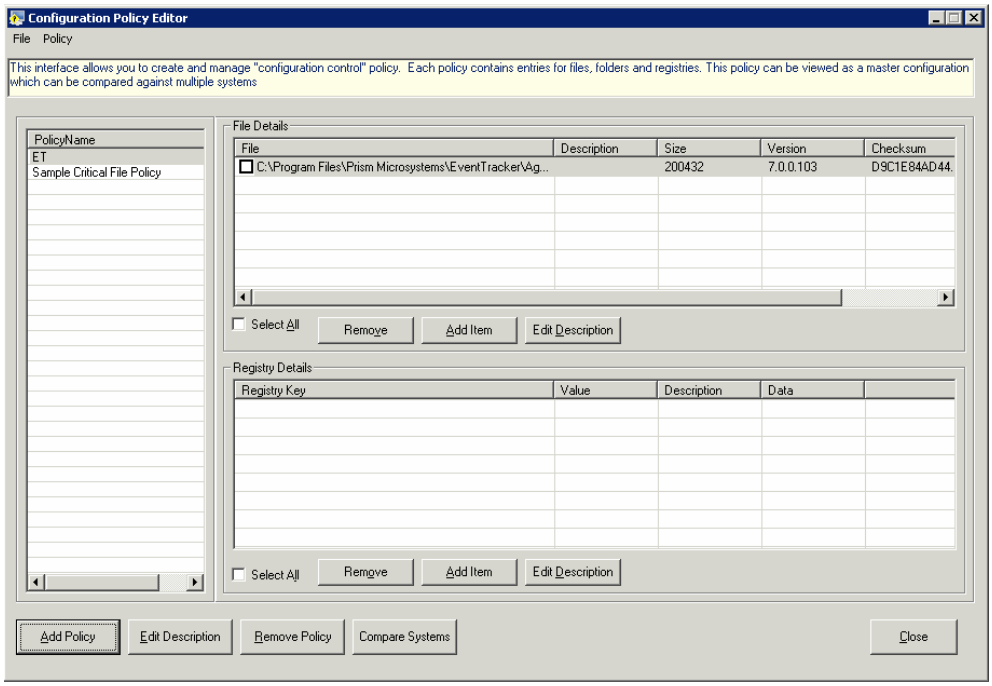


You have the option to keep the file name the same along with the existing drive letter and folders associated with it. When you compare this Policy, Change Audit compares the same drive and folders. Sometimes files and folders may not be located on the same drive. In those circumstances, you can remove the drive letter so that Change Audit searches in all the drives.

Example: If you enter C:\Program Files\SQL\abcd.exe,

Change Audit searches the abcd.exe in C:\Program Files\SQL
If you enter Program Files\SQL\abcd.exe, Change Audit searches the abcd.exe in Program Files\SQL
If you enter abcd.exe, Change Audit searches the abcd.exe in all drives and folders.

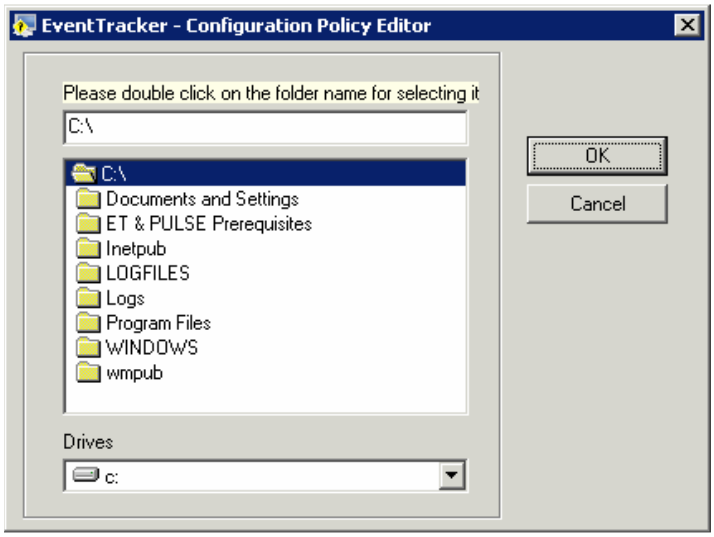
4. Click **Finish**. Change Audit adds the selected file and displays the Configuration Policy Editor.



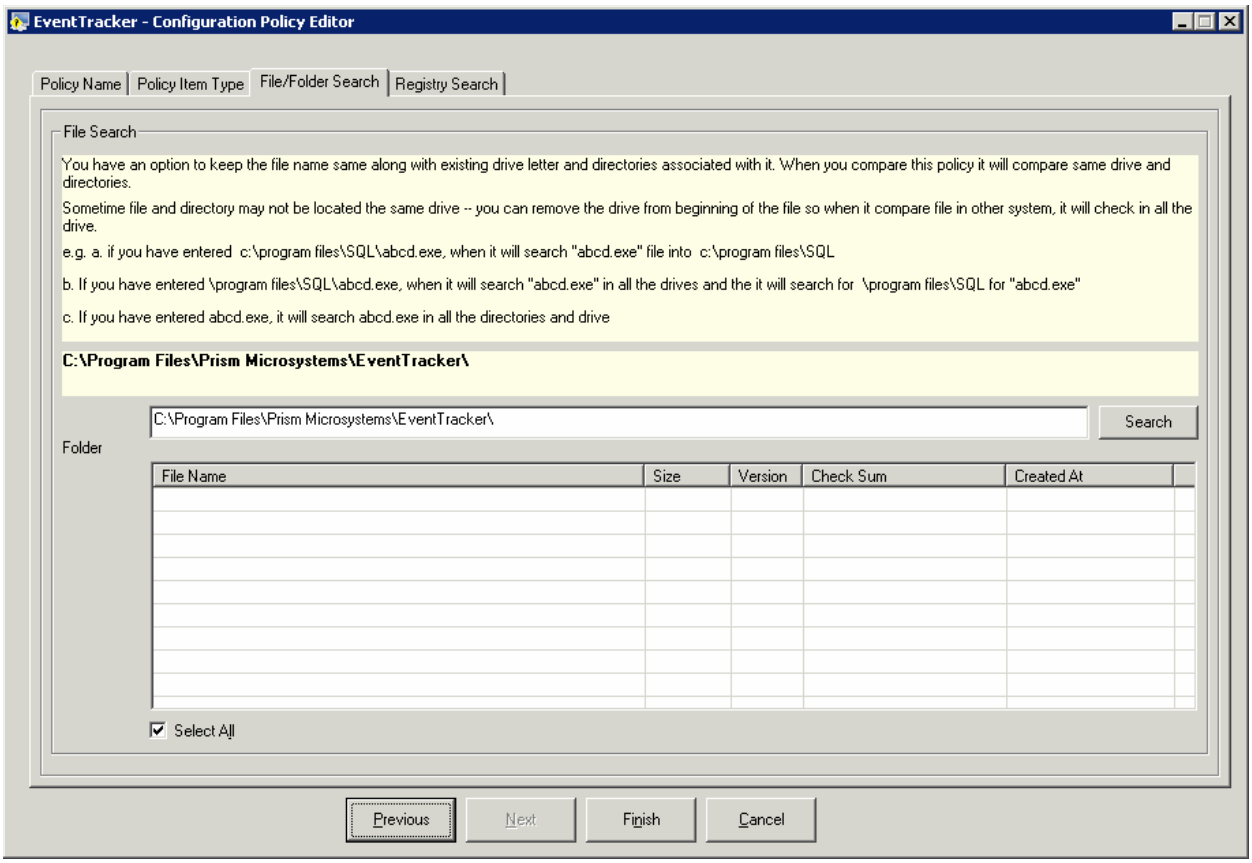
5. Click **Close**.

7.1.3 Search Folder Option

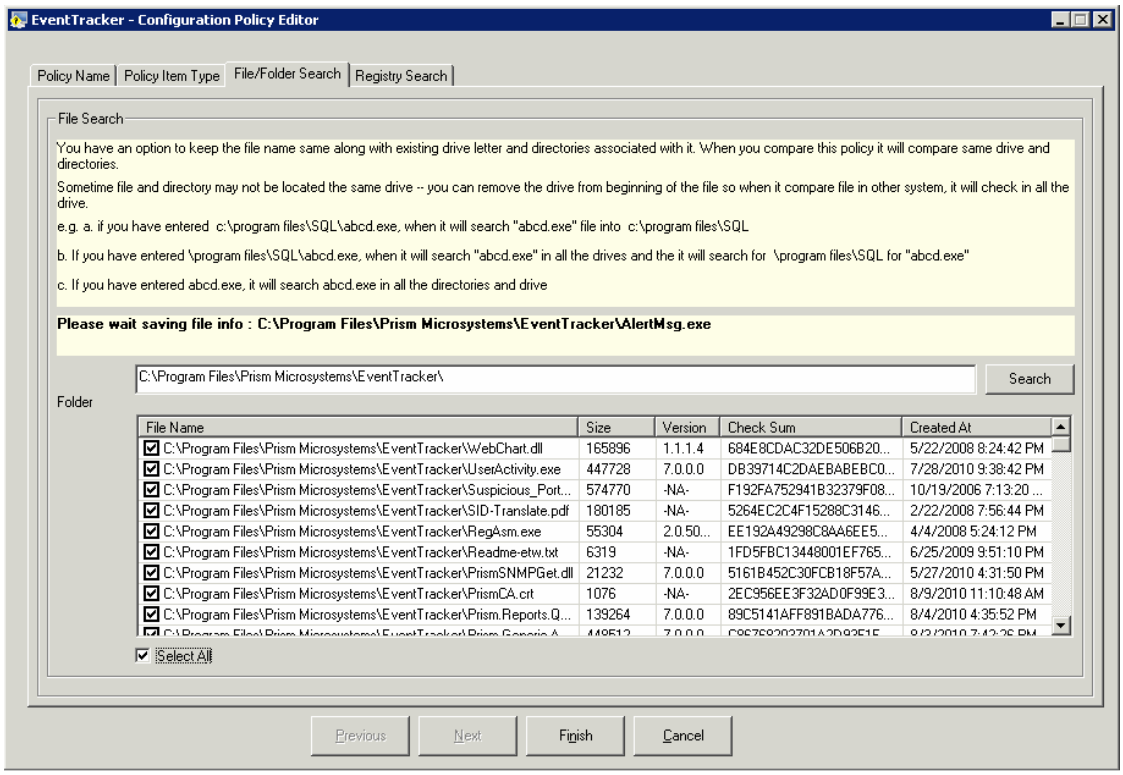
1. Select the **Add folder** option as the item type.
2. Click **Next**. Change Audit displays the Configuration Policy Editor window.



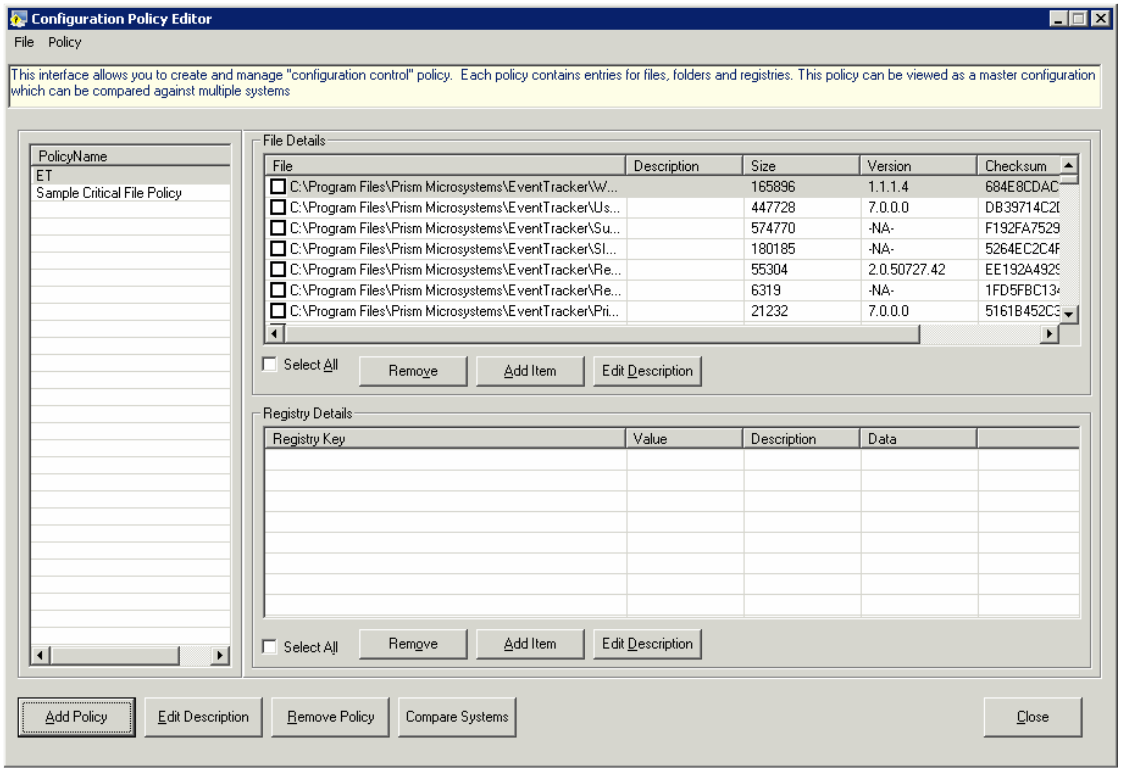
3. Select the drive, select the folder, and then click **OK**.
4. Change Audit displays the File/Folder Search tab.



5. Click **Search**. Change Audit saves the file information and displays the progress.
6. **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.



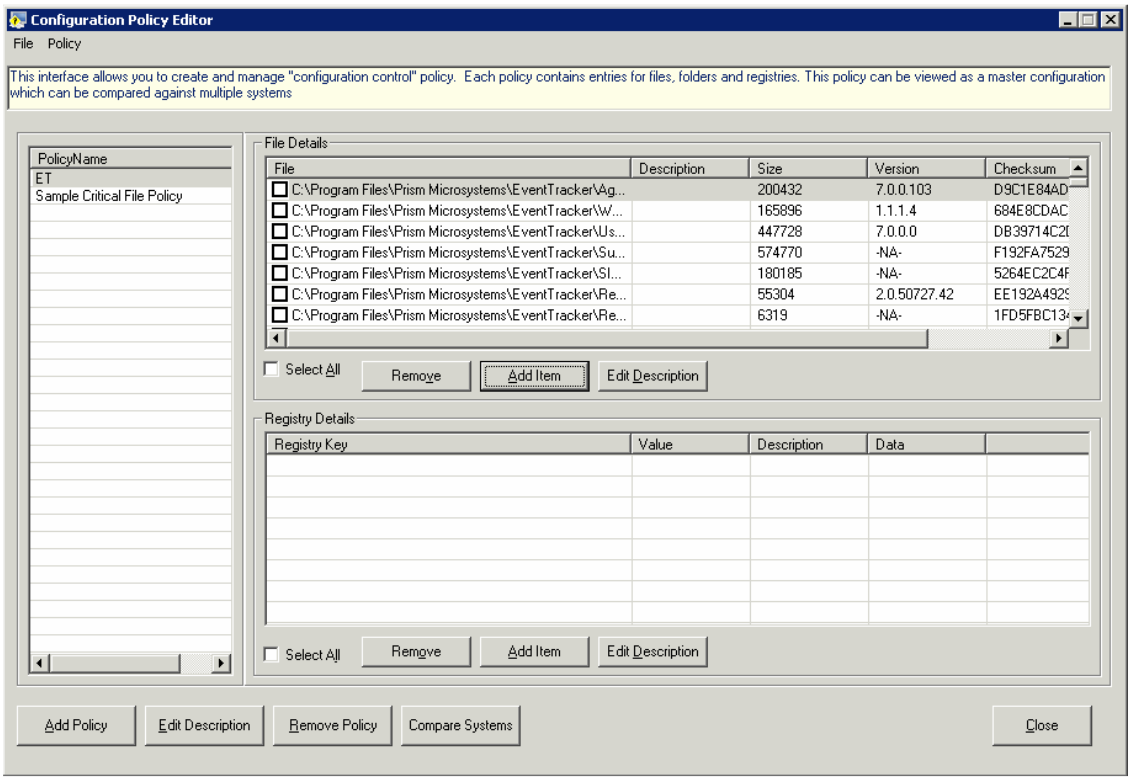
7. Click **Finish**. Change Audit displays the Configuration Policy Editor with the File Details.



7.1.4 Searching a Folder and Sub-folder

To Search a Folder and Sub-folder

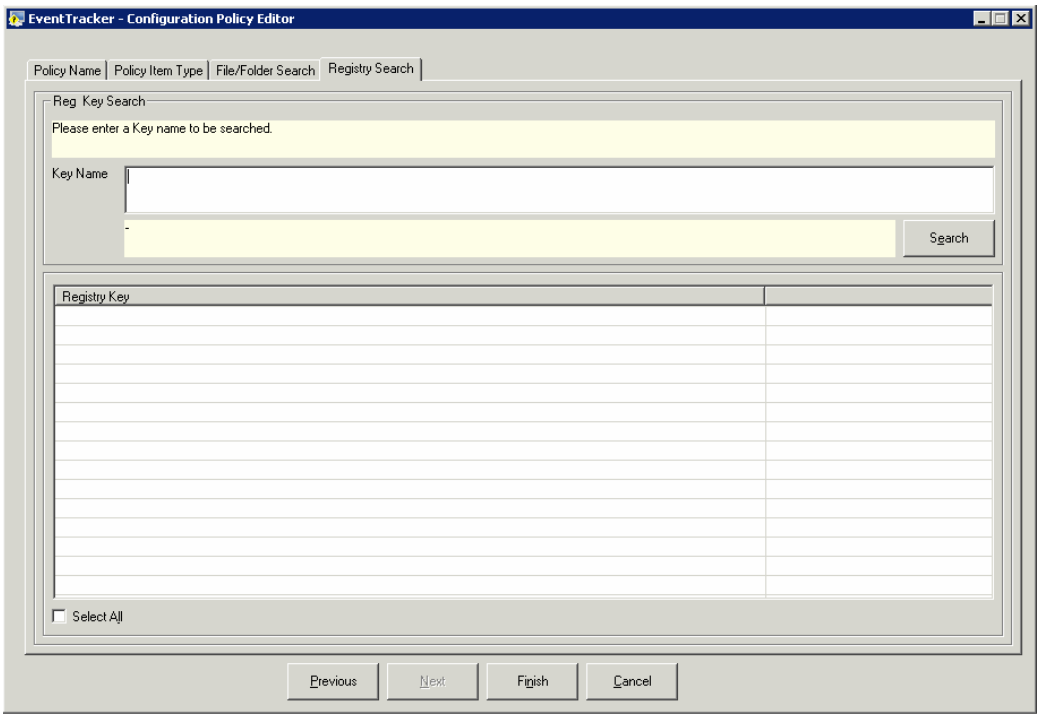
1. Select the **Add folder and sub-folder** option as the item type.
2. Click **Next**. Change Audit displays the Configuration Policy Editor.
3. Select the drive, select the folder, and then click **OK**. Change Audit displays the File/Folder Search tab.
4. Click **Search**. Change Audit saves the file 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**. Change Audit displays the Configuration Policy Editor with the File Details.



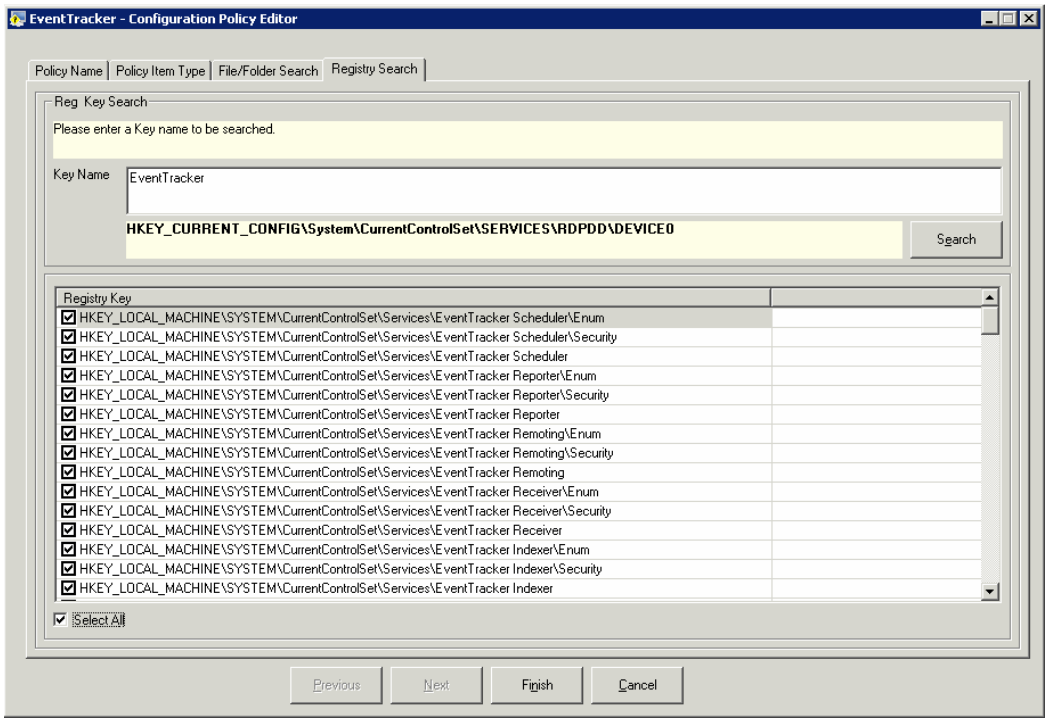
7.1.5 Searching Registry Key in Hive

To Search Registry Key in Hive

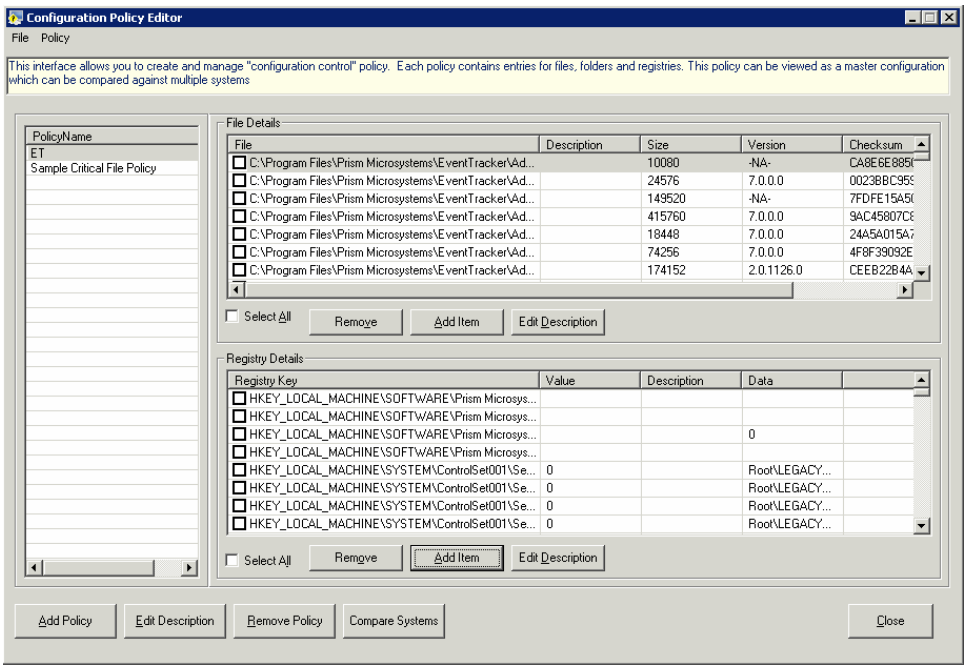
1. Select the Search for Registry Key in the Hive as the item type.
2. Click Next. Change Audit displays the Registry Search tab.



3. Type the name of the key in the Key Name field as shown in the following figure.
4. Click Search. Change Audit searches for the Key name and displays the progress of the search.
5. It displays the Registry Search tab with the list of hives.



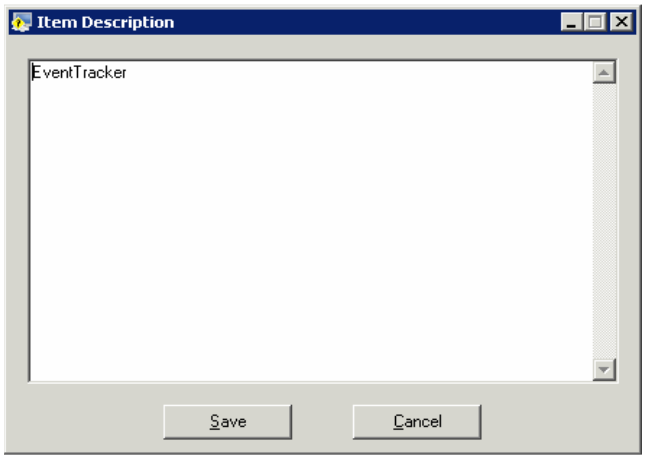
6. Select the keys and then Finish. Change Audit displays the Configuration Policy Editor with the Registry Details.



7.2 Edit Policy Description

To Edit the Policy Description, follow the steps below:

1. Open the **Configuration Policy Editor**.
2. Select a Policy.
3. Click **Edit Description**. Change Audit displays Item Description window.



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:

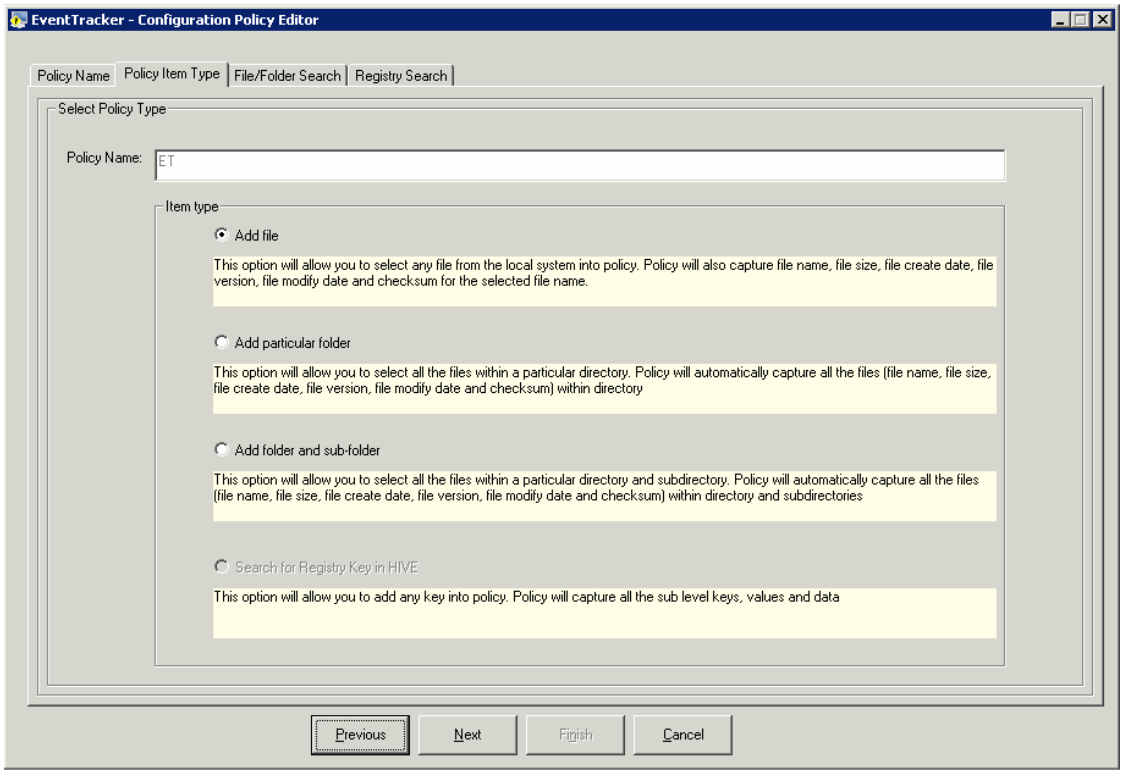
1. Open the Configuration Policy Editor.
2. Select an item on the File Details or Registry Details pane.
3. Click **Edit Description**. Change Audit displays Item Description window.
4. Edit the description and then click **Save**.
5. Click **Close**.

7.4 Add Policy Items Option

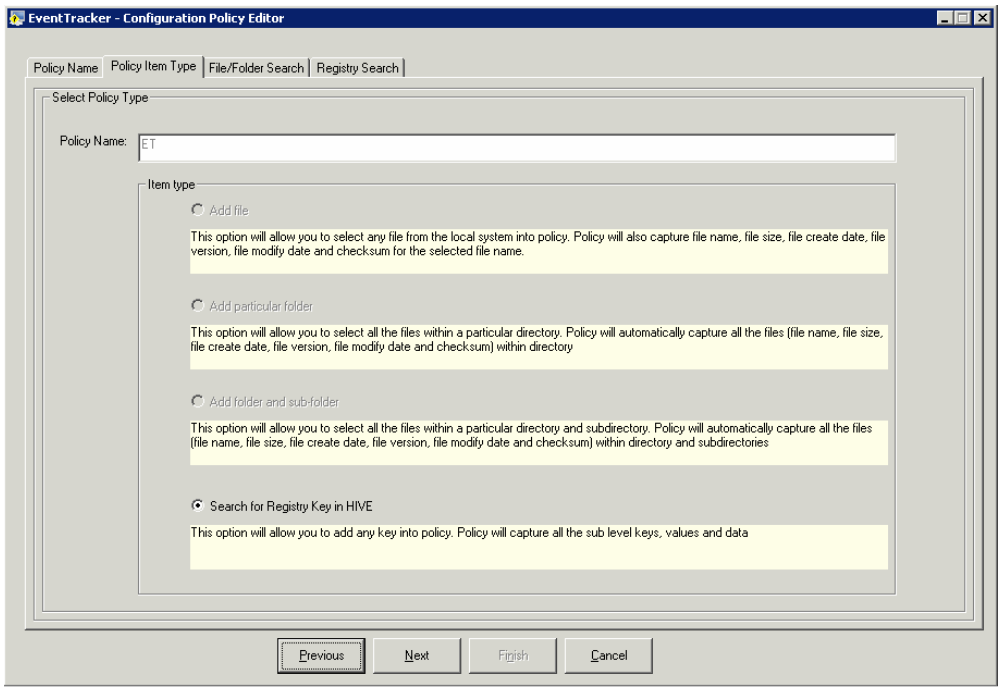
This option helps you add file/folder and registry key details to a Policy.

To add policy items, follow the steps below:

1. To add file items, click **Add Item** on the **File Details** pane. Change Audit displays the Configuration Policy Editor window.



2. Select an appropriate option and then add file items.
3. To add file items, click **Add Item** on the **Registry Details** pane. Change Audit splays the Configuration Policy Editor window.



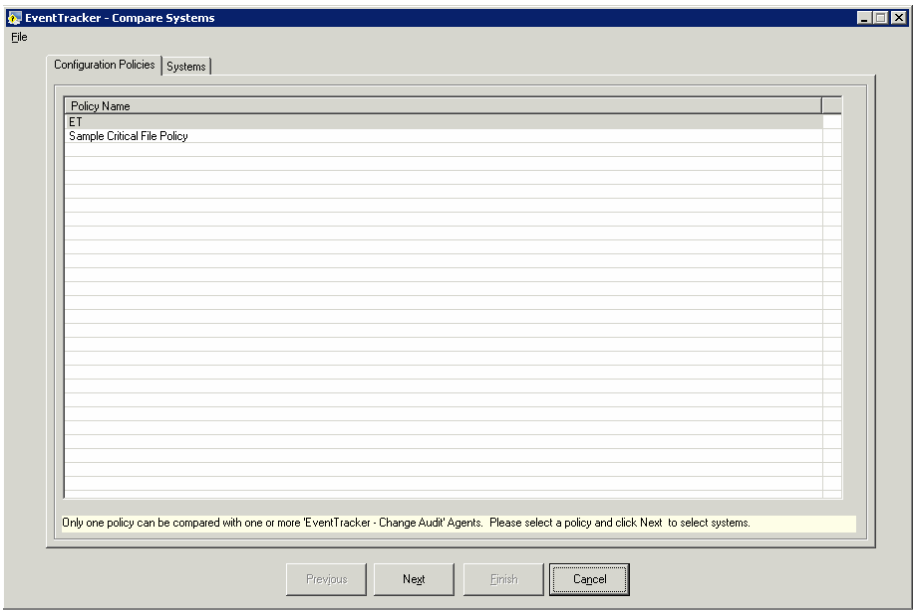
7.5 Compare Systems Option

This option helps you compare Policies between monitored computers.

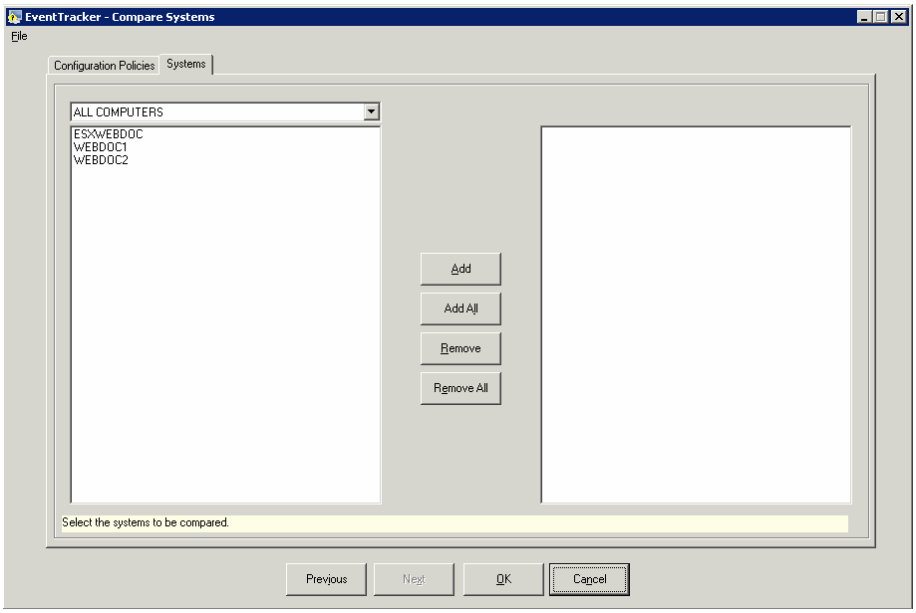
To compare systems, follow the steps below:

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. Change Audit displays the Compare Systems window.



3. Select a Policy and then click Next. You can select only one Policy for comparison.
4. Change Audit displays the Systems tab.

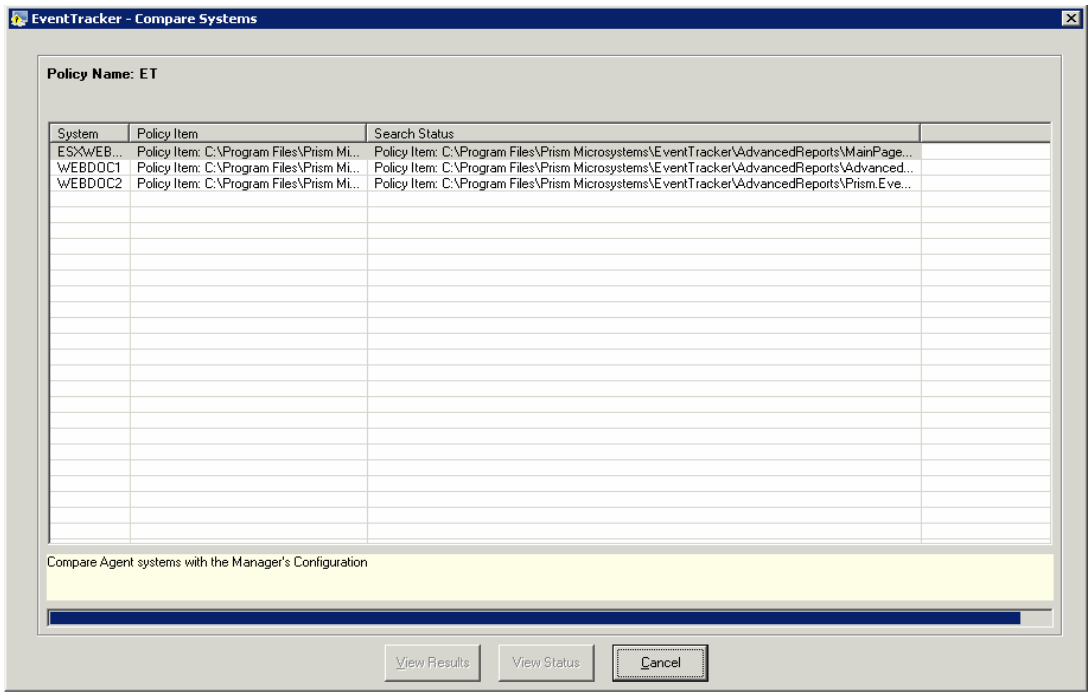


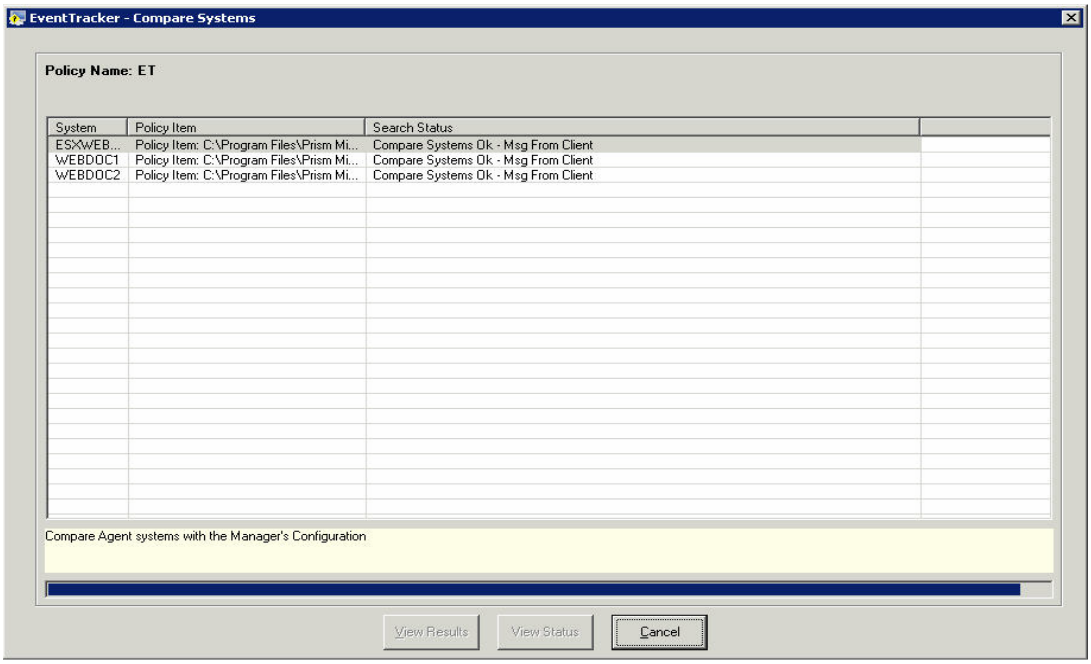
Select the domain from the drop-down list. Change Audit displays all the monitored computer members of that domain. By default, Change Audit displays all the monitored computers irrespective of domains. You can select any number of systems for comparison.

5. Select the computers and then click Add.
   (OR)

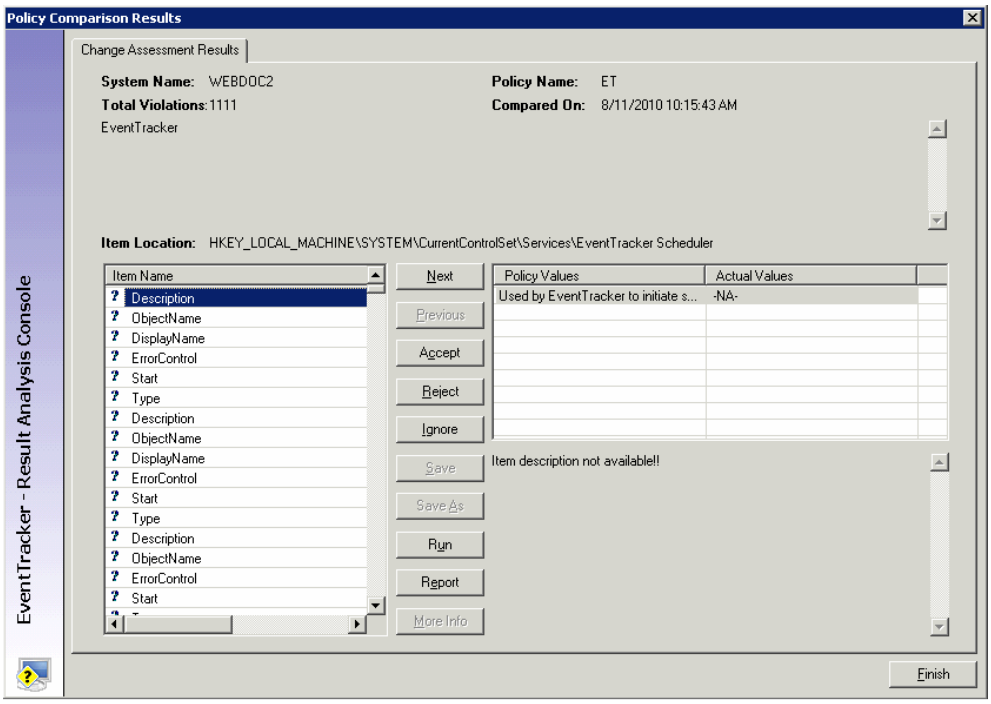
   Click Add All to add all the computers. Change Audit displays the Systems tab with the selected computers.

6. Click OK. Change Audit displays the comparison progress.

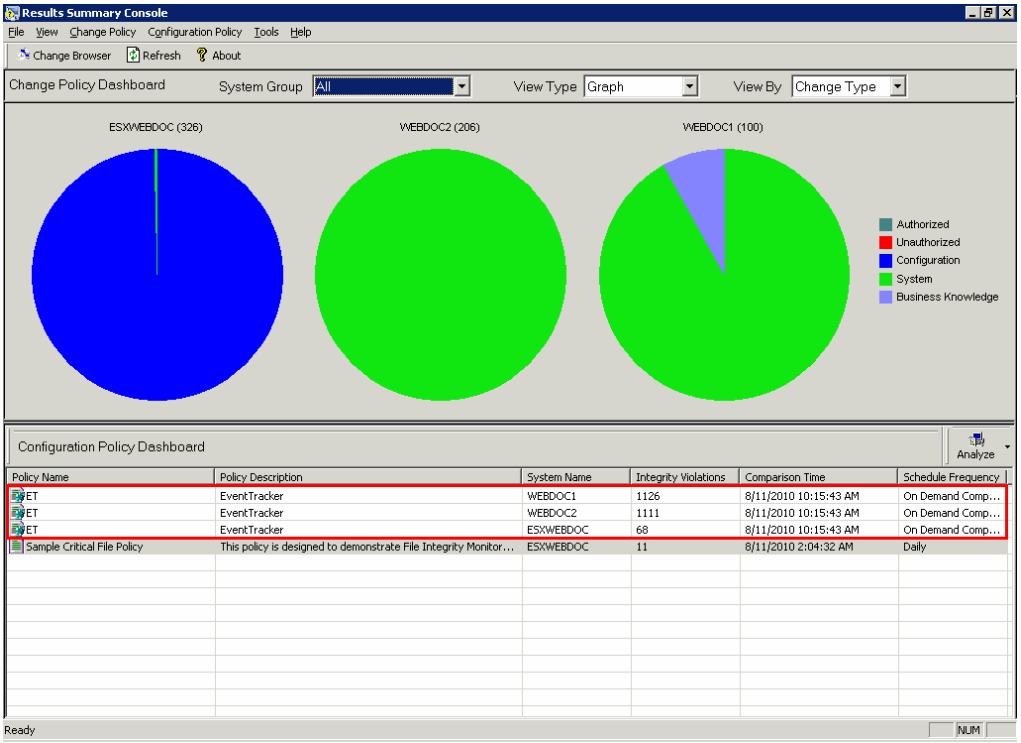




After comparing, Change Audit displays the result in the Policy Comparison Results window.



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



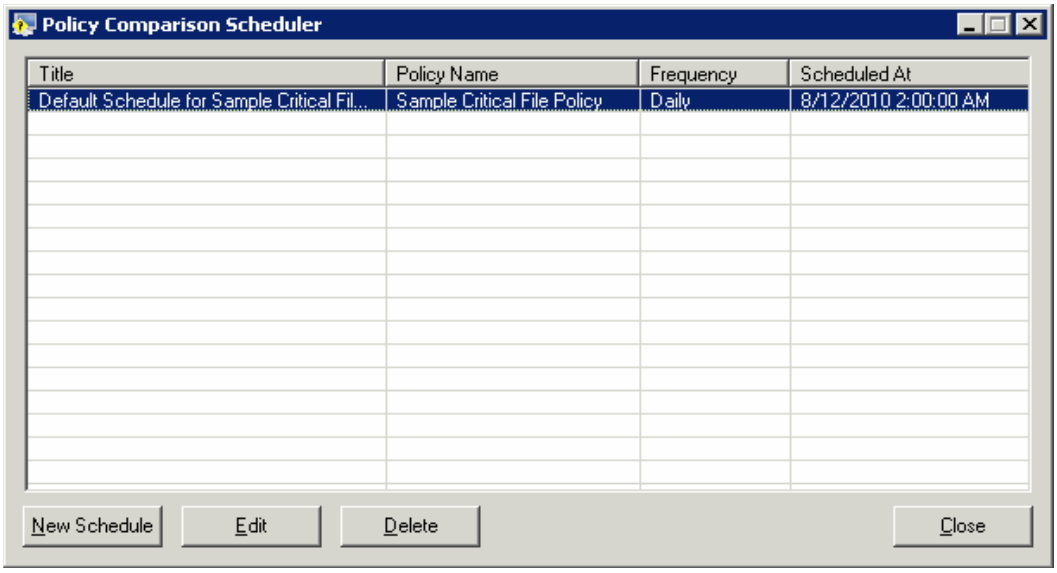
7.6 Schedule Policy Comparison

This option helps you schedule Policy comparison.

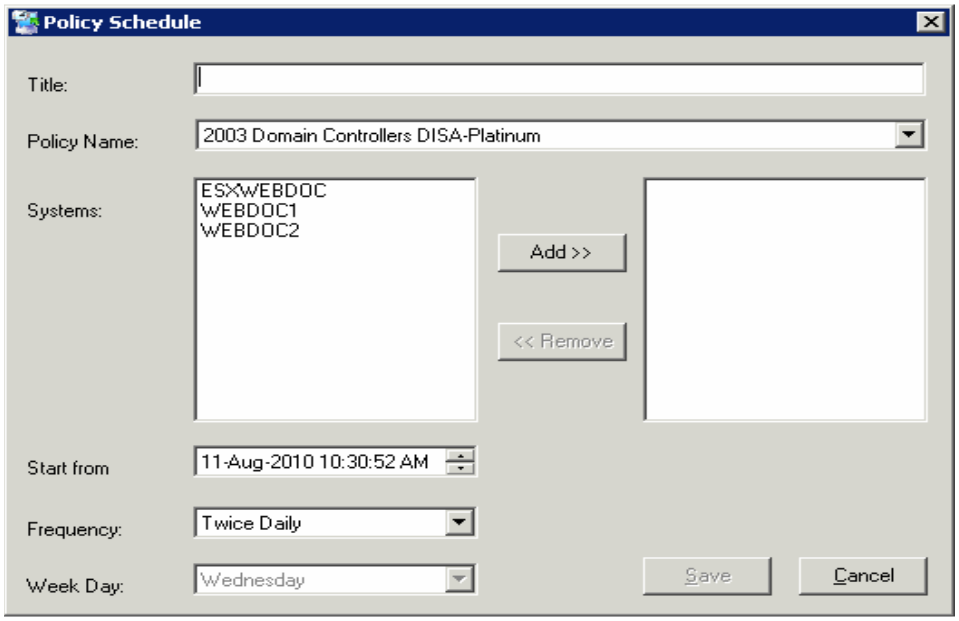
To schedule a Policy comparison, follow the steps below:

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. Change Audit displays the Policy Comparison Scheduler.

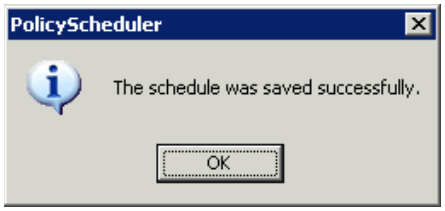


3. Click **New Schedule**. Change Audit displays the Policy Schedule window.

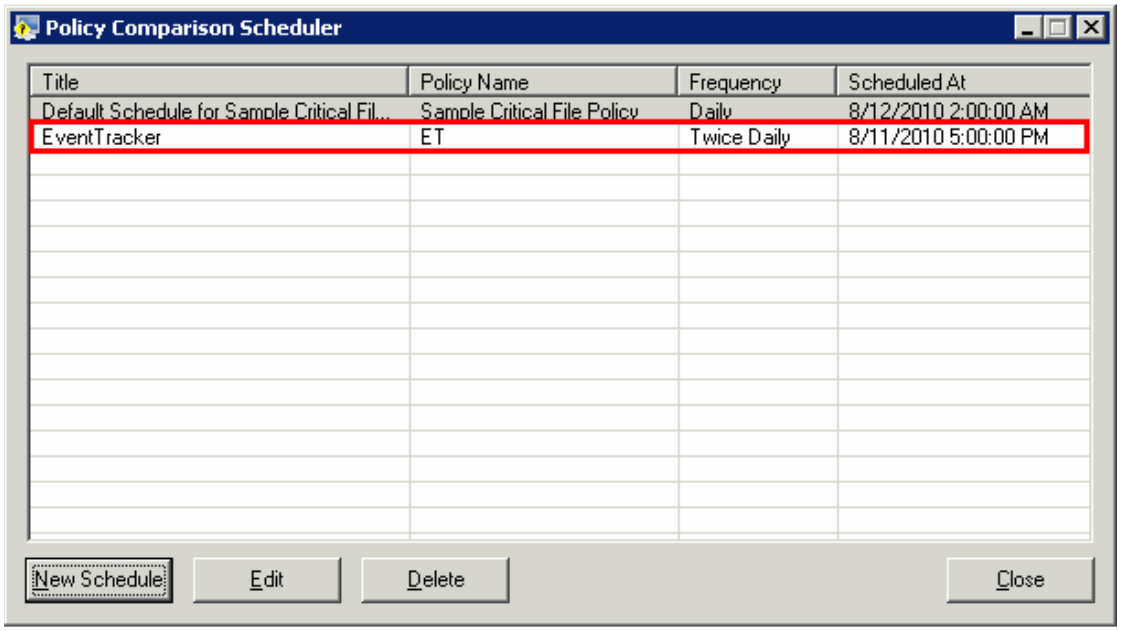


4. Type the name of the schedule in the **Title** field.

5. Select a policy from the **Policy Name** drop-down list, for example, ET.
6. Select **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. Change Audit enables the Weekday drop-down list only when you select Frequency as Weekly.
9. Click **Save**. Change Audit displays the **Policy Scheduler** message box.



10. Click **OK**. Change Audit displays the Policy Comparison Scheduler with the newly configured schedule.



11. Select a schedule and then click **Edit** to change the settings.
12. Select a schedule and then click **Delete** to delete the schedule details.

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. Change Audit displays the Configuration Policy Editor.
3. Click the **Policy** menu and select the **Export** option. Change Audit displays the Export Configuration Policy window.
4. Select a Policy and then click **Export**. Change Audit displays the Select Export File window.

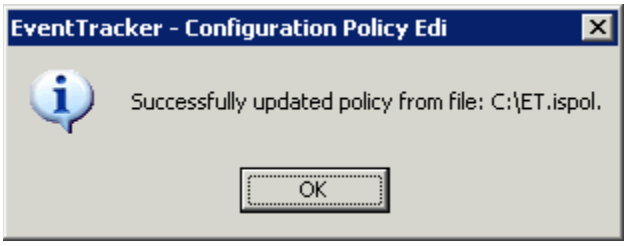
5. Go to the appropriate folder, enter the name in the File name field, and then click **Save**. The valid export file format is .ispol.
   After exporting successfully, Change Audit displays the success message.

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. Change Audit displays the Configuration Policy Editor.
3. Click the **Policy** menu and select the **Import** option. Change Audit displays the Select Import File window.
4. Go to the appropriate folder, select the file, and then click **Open**. After importing successfully, Change Audit displays the success message.



8 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	Change Audit displays the items that are added, modified, and deleted in the File System and Registry.
Client	A tiny footprint is 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.
Filters	Filters are set to exclude folders and files from tracking.
Full View	Change Audit displays the items that are added, modified, and deleted in the File System and Registry. Also, displays the unaltered items in the 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	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.
System Configuration	Configure Snapshot automation, Snapshot limit, and filters to the current system. System Configuration can also be propagated to all other systems in the network.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support