



Feature Guide

Change Audit

Publication Date March 25, 2024

© Copyright Netsurion. All Rights Reserved.



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	Ove	rview6
	1.1	Capabilities of Netsurion Open XDR – Change Audit
	1.2	Change Audit Architecture
	1.3	Ports Used by Change Audit
	1.4	Change Audit Events
	1.5	Starting Change Browser
	1.6	Starting Results Summary Console
	1.7	Change Browser User Interface
	1.8	Netsurion Open XDR- Change Audit Icons13
	1.9 1.9.1	Change Audit Components
	1.9.2	Configuration Policy Editor
2	Resu	Ilts Summary Console16
	2.1	Setting Dashboard Preferences
	2.2	Export Change Data
	2.3	Viewing the Summary of Change Details
	2.4	Viewing the Change Details Console
	2.5	Authorizing Unauthorized Changes
	2.6	Viewing the Change Details in the Change Browser27
	2.7	Viewing Change Report
	2.8	Configuration Policy Dashboard
	2.9	Analyzing the Policy Comparison Results
	2.10	Compare Policies
	2.11	Scheduling the Policy Comparison
	2.12	Accessing the Result Analysis Console
3	Chai	nge Browser
	3.1	View Groups option
	3.2	Viewing System Details
	3.3	Viewing the File System Changes
	3.4	Viewing the Registry Changes
	3.5	Full View Option
	3.6	Viewing the Comparison Details



	3.7	Comparing the Details of the Registry Items	44
	3.8	Change View	44
	3.9	Find Changes Option	44
	3.10	Search Strings	46
	3.11	Searching the Strings in the Registry	47
	3.12	Generating the Change Report	48
	3.13 3.13.2	Track File Checksum Feature 1 Enabling File Checksum Tracking	
	3.13.2	2 Enabling the O/S Audit on Files and Folders	51
	3.13.3	3 Enabling the O/S Audit on the Registry Keys	54
	3.14	Assign Change Type	55
4	Sna	pshots	57
	4.1	Take Snapshots on Demand	57
	4.2	Edit Snapshots	59
	4.3	Reinitialize Snapshots	60
	4.4	Back up the Snapshots	61
	4.5	Recover Snapshots	63
		•	
5	Con	figuration	65
5	Con 5.1 5.1.1	figuration Global Configuration Adding/Editing File Change Type	65
5	5.1	Global Configuration	65 72
5	5.1 5.1.1	Global Configuration Adding/Editing File Change Type Configuring the Change Type	65 72 77
5	5.1 5.1.1 5.1.2	Global Configuration Adding/Editing File Change Type Configuring the Change Type	65 72 77 78
5	5.1 5.1.1 5.1.2 5.1.3	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab	65 72 77 78 79 82
5	5.1 5.1.1 5.1.2 5.1.3 5.2 5.3	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration	65 72 77 78 79 82 84
5	5.1 5.1.1 5.1.2 5.1.3 5.2 5.3 5.3.1	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System	65 72 77 78 79 82 84 84
5	5.1 5.1.2 5.1.3 5.2 5.3 5.3.1 5.3.2	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System Apply System Configuration – Remote Systems	65 72 77 78 79 82 84 84 84 84 86 87
5	5.1 5.1.2 5.1.3 5.2 5.3 5.3.1 5.3.2 5.3.3 5.4	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System Apply System Configuration – Remote Systems Apply System Configuration – All Systems Search the Change Events (Netsurion Open XDR Search Interface)	65 72 77 78 79 82 84 84 84 86 87 87
5	5.1 5.1.2 5.1.3 5.2 5.3 5.3.1 5.3.2 5.3.3 5.4 5.4.1 5.5	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System Apply System Configuration – Remote Systems Apply System Configuration – Remote Systems Apply System Configuration – All Systems Search the Change Events (Netsurion Open XDR Search Interface) Option to Log / Forward Snapshot Results to Netsurion Open XDR	65 72 77 78 79 82 84 84 84 86 87 87 90
	5.1 5.1.2 5.1.3 5.2 5.3 5.3.1 5.3.2 5.3.3 5.4 5.4.1 5.5	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System Apply System Configuration – Remote Systems Apply System Configuration – Remote Systems Search the Change Events (Netsurion Open XDR Search Interface) Option to Log / Forward Snapshot Results to Netsurion Open XDR Generating Reports against Change Audit Category.	65 72 77 78 79 82 84 84 84 86 87 87 90 90
	5.1 5.1.2 5.1.3 5.2 5.3 5.3.1 5.3.2 5.3.3 5.4 5.4 5.4.1 5.5 Filte	Global Configuration Adding/Editing File Change Type Configuring the Change Type Checksum Rules tab Apply Global Configuration System Configuration Apply System Configuration – Local System Apply System Configuration – Remote Systems Apply System Configuration – All Systems Search the Change Events (Netsurion Open XDR Search Interface) Option to Log / Forward Snapshot Results to Netsurion Open XDR Generating Reports against Change Audit Category	65 72 77 78 79 82 84 84 84 86 87 87 90 90 90



	6.3.2	Customize Filters
	6.4	Apply Filters Option – Local System
	6.5	Apply Filters Option – Remote Systems
	6.6	Apply Filters Option – All Systems 101
	6.7	Remove Filters Option – Local System
	6.8	Remove Filters – Remote Systems
	6.9	Remove Filters – All Systems
	6.10	Restore Registry Sub-tree 109
	6.11	Restore Logs 110
	6.12	Undo Restore
	6.13 6.13.1	Support for Monitoring a Specific Folder on the System111LProcess after Applying the Update111
7	Con	figuration Policy Editor113
	7.1 7.1.1	Configuration Policy
	7.1.2	Searching a File 115
	7.1.3	Search Folder Option 117
	7.1.4	Searching a Folder and Sub-folder
	7.1.5	Searching Registry Key in Hive
	7.2	Edit Policy Description
	7.3	Edit File/Registry Key Description
	7.4	Add Policy Items Option
	7.5	Compare Systems Option
	7.6	Schedule Policy Comparison
	7.7	Export Configuration Policies
	7.8	Import Configuration Policies
8	Glos	ssary



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.

EventTr	acker - Change Browser 🛛 🛛 🔀
٩	Automated snapshot is in progress for: WEBDOC1 Please try after sometime.
	()

- 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.**



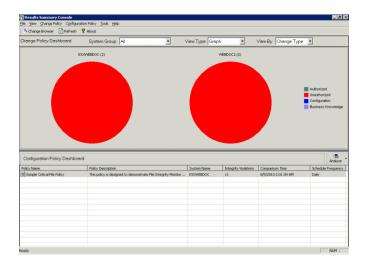
💀 EventTra	cker - Change Bro	wser				
<u>Eile E</u> dit <u>V</u> ie	w Options Reports	Help				
🛃 Groups 🚦	E Change View 👻 🙆	New Snap 🙀 🔶 Show f	Next Change 🗎 🧮 Change F	Report		
UKEBDOC2	,	5/2010 2:02:03 AM		3:53:10 PM 🗨		
	Tracking only selecte	d file types	WEBDOC2	,		
	E-B WEBDOC2		Processor	Page Size	Windows Version	Total Physical Memory
	💾 HKE	Y_LOCAL_MACHINE Y_USERS Y_CURRENT_CONFIG	∰566×1	4036 Bytes	5.1 Service Pack 3	991 MB
System: WEBD	0C2	Type: System Name	Changed :	Added :	Veleted :	

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 d	isplays all the system groups discovered by the Client Manager.
View Type	Select an option to v	iew chart or data on the console.
	Authorized	Detected changes that can be matched to an approved change request.
	Unauthorized	Detected changes that cannot be matched to an approved change request.
Change Type	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.
	Files Added	
	Files Deleted	
	Files Modified	
Object Type	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.



	itle Bar Menu Bar To ser - Change Browser	olbar				_ 8 ×
	v Options Reports Tools Help					
		Next Change 📄 Change	Report			
ESSAVERDOC	Compare AS: 8/5/2010 2:01:42 AM	with AS: 8/4/2010	3.53.27 PM			
	Tracking only selected file types	ESXWEBDOC			1	
	ESXWEBDOC	Processor 8566×1	Page Size 4096 Bytes	5.2 Service Pack 2	Total Physical Memory 1023 MB	
WEBDOC2			4096 Bytes	5.2 Service Pack 2	TU23 MB	
~	Pegiatay Rec_LOCAL_MACHINE KEC_LOSERS HKEY_CURRENT_CONFIG System Bar	w	orkspace			
IP Address: 192.	168.1.24 Type: System Name	Changed :	Added : .			
in Address: 192.	Too. 1.24 Type: System Name	,	, ¥wdded : .			
	`	Status Bar				

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	То
🖫 Groups	Switch to Groups view.
EEE Change View 👻	Toggle between Full View and Change View.
New Snap	Take new Snapshots of the selected system.
<i>#</i> 3	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:

lcon	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.
C ⁴	An item modified in the File System or Registry.
×	An item deleted from the File System or Registry.
B	Unaltered item
8	Folders



	Files
Ň	Registry
	File system folders and Registry keys
2	Computer Groups
	Snapshot in progress
	File changes found.
and the second s	Registry changes found.
F	File and registry changes found.
٠	No changes were found.
?	Fresh item.
~	Items accepted.
١	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.



Policy					
terface allows you to create an can be compared against multij	d manage "configuration control" policy. Each policy contains ent ile systems	ries for files, folders and	registries. This po	licy can be viewed as	a master configural
	File Details				
olicyName	File	Description	Size	Version	Checksum 🔺
ample Critical File Policy	C:\WINDOWS\system32\find.exe	Found integrity	9216	5.1.2600.0	2329F2C682
	C:\WINDOWS\system32\ftp.exe	Found integrity	42496	5.1.2600.5512	4112AA01C1
	C:\WINDOWS\system32\notepad.exe	Found integrity	69120	5.1.2600.5512	7A90F8B051
	C:\WINDOWS\system32\nslookup.exe	Found integrity	76800	5.1.2600.5512	D3E9558130
	C:\WINDOWS\system32\print.exe	Found integrity	9216	5.1.2600.0	2F2AD17264
	C:\WINDOWS\system32\regedt32.exe	Found integrity	3584	5.1.2600.0	DEB00B2DB
	C:\WINDOWS\system32\route.exe	Found integrity	19968	5.1.2600.0	31282AD39F 🚽
				1	
	Registry Details		Description	Data	1
	Registry Details	Value	Description	Data	
		Value	Description	Data	
		Value	Description	Data	
		Value	Description	Data	
	Registry Key	Value Edit Description	Description	Data	

Click	То
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:

Dashboa	rd Preferences 🛛 🗙
	Dashboard Preferences
Results Summary Console	Enable Auto Refresh Auto Refresh Interval (in seconds) 10 Change Summary Dashboard ✓ Make "View by Change Type" as the default option Select the segments to view in graph for View By Change Type ▼ ✓ Authorized ✓ Unauthorized ✓ Configuration System Ø Business Knowledge Make data view as the default view ✓ Show equal sized graphs
2	OK Cancel



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:

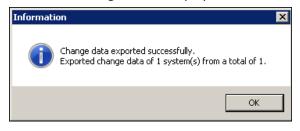
Output Columns		
Select All		
File Name	🔲 File Path	File Attributes
File Size	🔲 File Creation Time	File Last Write Time
🔲 File Last Access Time	File Version	🔲 File Checksum
System(s)		
MCLOON	>> >> <<	
Files Type(s)		
All Files		
, You can enter multiple file Example: exe,dll,sys etc	e extensions separated t	oy a comma(,).
Output Settings		
CSV File Path		
🗖 File Header 🥅 Write		
Create separate file f	or each system	

- 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.



💀 Change Data Export Utility	×
Output Columns I✓ Select All	
File Name File Path File Attributes	
🔽 File Size 🔽 File Creation Time 🔽 File Last Write Tim	e
▼ File Last Access Time ▼ File Version ▼ File Checksum	
System(s)	
MCLOON	
Files Type(s)	
MILLIGS	_
I You can enter multiple file extensions separated by a comma(,). Example: exe,dll,sys etc	
Output Settings	
CSV File Path C:\Users\sunanda\Desktop .	
File Header Write Log File Create separate file for each system	
Export Cancel	

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

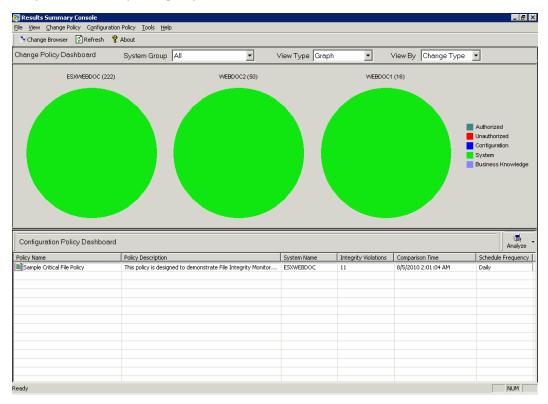


The Data can be viewed regarding the files in the respective CSV file. The list can be imported as discussed in the <u>Active Watch List</u>.



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:

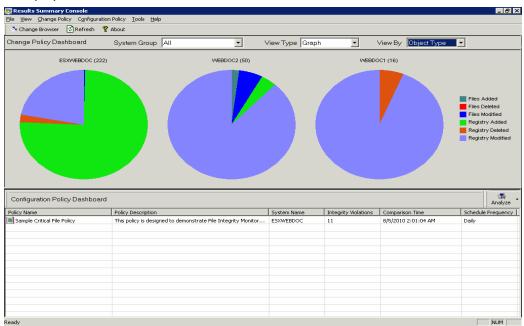
Select the **Data** option from the **View Type** dropdown list.
 (OR) Double-click the pie chart to view the data. The statistical data will be displayed as shown below:



A Change Browse	er 😰 Refresh 💡 A	bout							
Change Policy D	ashboard	System Gro	oup All	• V	/iew Type Data	•	View By	Change Type	•
5ystem Name	Current Snapshot	Time	Previous Snapshot Time	Authorized	Unauthoriz	ed Configur	tion	System	Business Knowledg
ESXWEBDOC	8/5/2010 12:36:09	9 PM	8/5/2010 2:01:42 AM	0	0	0		222	0
WEBDOC2	8/5/2010 12:35:02	2 PM	8/5/2010 2:02:03 AM	0	0	0		50	0
WEBDOC1	8/5/2010 1:10:42	PM	8/5/2010 12:39:54 PM	0	0	0		16	0
Configuration P Policy Name	olicy Dashboard	Policy Descript	tion		System Name	Integrity Violation	; Compar	ison Time	Analyza
-	-		tion designed to demonstrate File In	itegrity Monitor	System Name ESXWEBDOC	Integrity Violation		ison Time 0 2:01:04 AM	Analyz
Policy Name	-			kegrity Monitor					Analyze Schedule Frequen
Policy Name	-			kegrity Monitor					Analyze Schedule Frequen
Policy Name	-			kegrity Monitor					Analyze Schedule Frequen
Policy Name	-			kegrity Monikor					Analyze Schedule Frequen
Policy Name	-			itegrity Monitor					Analyze Schedule Frequen

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.

hboard System Current Snapshot Time 8/5/2010 12:36:09 PM 8/5/2010 12:36:02 PM 8/5/2010 12:36:02 PM 8/5/2010 12:36:02 PM 8/5/2010 12:36:02 PM	Group All Previous Snapshot Time 8/5/2010 2:01:142 AM 6/5/2010 2:02:03 AM 8/5/2010 12:39:54 PM	Authorized 0 0 0	View Type Dete		View By Change Type on System 222 50 16	Business Knowledge 0 0 0 0
8/5/2010 12:36:09 PM 8/5/2010 12:35:02 PM	8/5/2010 2:01:42 AM 8/5/2010 2:02:03 AM	0	0	0	222 50	0
8/5/2010 12:35:02 PM	8/5/2010 2:02:03 AM	0	0	0	50	0
8/5/2010 1:10:42 PM	8/5/2010 12:39:54 PM		0	0		
-	restintion		Sucton Name	Integrity Vielations	Comparison Time	Analyze
		- ha aniha - Maraihan				Daily
		Policy Description	Policy Description	Policy Description System Name	Policy Description System Name Integrity Violations	Policy Description System Name Integrity Violations Comparison Time

3. The Results Summary Console displays the Change Details,

Change I	Details					×
	Change Details					
	System Name:	Object Type:		Object 9	itatus:	Change Type
	WEBDOC1	All	-	All	•	System 💌
	Item Location: HKEY LOCAL MA		General Court	DNU	-	
	Item Name		1	fegistry va Change Ty	lue was Modified. pe: System	
	Seed					
	SSTV ZastTaskRun					
	AppInit_DLLs	Grou	p by Path		Current Snapshot	Previous Snapshot
	SastCheckTime			Data	cf d8 3c 9c 89 5f 59 c8 c8 4	
	LastCheckTime	B	revious	Data Type	REG_BINARY	REG_BINARY
e	LastCheckTime					
20	LastCheckTime		<u>N</u> ext			
ы	LastCheckTime					
^o	LastCheckTime		<u>F</u> ilter			
E .	LastCheckTime					
Ĩ	LastCheckTime	<u>A</u>	uthorize			
Ę	LastCheckTime Count					
S	WextInstance	Acce	ess <u>H</u> istory			
12	Wextinistance					
Results Summary Console	100	<u>M</u>	pre Info			
Re		Char		. 1		
	Select / Unselect All unauthorized	l items	ge Browser	•		
2						OK <u>C</u> lose



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.

Add Filte	rs	×
	Add Filters	
	Filter string HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed	
Results Summary Console	Filter the objects by using the filter string to match Exact registry value name and its path Exact registry path (Filter all the children of the path as well) As substring in the registry value or registry path (Applies on all systems) Apply this filter on This system All systems 	
?	OK <u>C</u> lose	

- 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:

Results S	ummary Console 🛛 🕅
?	You have made changes to some configurations that need to be applied on remote systems. Do you want to apply the changes before exiting?
	<u>∑Yes</u> <u>N</u> o

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

Finish

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



11. Click the Filters tab.

Change Type	File Change	Туре	Registry Cha	nge Type	Checks	um C	hecksum Rules
General	File Types	Monit	or Specific Reg	gistry	Monitor Spe	cific Folder	Filters
Name			A	bsolute Path			^
ControlSet002			inty/HKEY_LOCAL				
CurrentControlSet			INVERTING		EMICUNERIC		
Seed		Re	gistry/HKEY_LO	CAL MACHINE	SOFTW/		
							~
[>
neck and click 'R					t the option		
neck and click 'R				ser and selec	t the option.		
heck and click 'R				ser and selec	t the option.	0	1
heck and click 'R				ser and selec	t the option.	Bemove	
heck and click 'R o filter right click o				ser and selec	t the option.	Bemove	
heck and click 'R				ser and selec	t the option.	Bemove	

- 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.

Change Type Fi		isty Change Type	Checksum	Checksum Rul
System Configuration	Filters	Monitor Specific Registry	Mon	tor Specific Folder(s
Name		Absolute Path		
Seed Seed	Registry\HK	EY_LOCAL_MACH	INE\SOFTW	ARE
	"to UnFilter checked nodes.	ge browser and select th	e option.	
	' to UnFilter checked nodes. der or registry key in the chan	ge browser and select the		
		ge browser and select the		emove



2.5 Authorizing Unauthorized Changes

To authorize unauthorized changes, follow the below steps:

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

🏂 Change Browse	er 🔹 Refresh 🤗	About								
Change Policy D	ashboard	System Gr	oup All	- \	/iew Type Data	-	View By	Change Type	•	
System Name	Current Snapsh	ot Time	Previous Snapshot Time	Authorized	Unauthorize	d Configurat	ion	System	Business	Knowledge
ESXWEBDOC	8/5/2010 12:36		8/5/2010 2:01:42 AM	0	0	0		222	0	
WEBDOC1	8/5/2010 2:26:3		8/5/2010 1:10:42 PM	0	0	0		44	0	
WEBDOC2	8/5/2010 2:25:2	8 PM	8/5/2010 2:23:17 PM	0	14	0		17	0	
	Policy Dashboard	[Dolinu Docrai	tion		Suctor Name	Totovitu Vielstiens	(compari	con Timo	Echadula -	. ·
Policy Name	-	Policy Descrip			System Name	Integrity Violations	Compari			Analyze
Configuration P Policy Name Sample Critical Fil	-		ption designed to demonstrate File Ir	ntegrity Monitor	System Name ESXWEBDOC	Integrity Violations		son Time 0 2:01:04 AM	Schedule	Analyze
- Policy Name	-			ntegrity Monitor						Analyze
Policy Name	-			ntegrity Monitor						Analyze
Policy Name	-			ntegrity Monitor						Analyze
Policy Name	-			ntegrity Monitor						Analyze
Policy Name	-			ntegrity Monitor						Analyze
Policy Name	-			ntegrity Monitor						Analyze

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

	System Name:	Object Type:		Object	Status:	Change Type
	WEBDOC2	Al	*	Al	*	Unauthorized
	Item Location: C:\woAiTemp\Ag	and AlTerry Million Pr	deal-linear and			
		en villenp wowro	эксүү көчнөг, көнө	File was D	alated	
	Item Name				pe: Unauthorized	
	WcwPolicyViewex.exe					
	WowService.exe					
	WowWrap.dl		Group by Path		Current Snapshot	Previous Snapshot
	CertLicense dl		2	Size (in b		403328
			Brevious	Version	A	mottracked
	CertLicenseWrap.dl		Discont	Creation	4	8/5/2010 2:22:59 PM
	iniscoss.dl			Last Wit.		8/3/2010 7:14:52 PM
	De InFie.dl		Next	Concernence of the second seco	· ·	8/5/2010 2:23:00 PM
	mic42.dl			Ovecksum		notracked
	SrvShell.exe		Eilter	-		
	WcStvAins.exe					
	WcwAl.exe		Authorize			
	wewer.dl	_				
	Wowlns.dl		Access <u>History</u>			
Ш			More Info			
	Select / Unselect All unauthorize	dillens 0	hange Browser			

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:

Group by	y Path	×
	Group by Path	
	Path	Changes
	C:\wcAiTemp\Agent\	10
	C:\wcAiTemp\Agent\AITemp\	4
Ð		
20		
ü		
~		
Results Summary Console		
듣니		
Su		
<u>ts</u>		
ng l		
R.	Select / Unselect All items	Authorize
?.		<u>C</u> lose

4. Select the items and then click Authorize.

Note

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

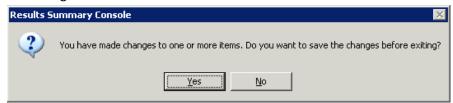
Authoriza	ation Comment	×
	Authorization Comment	
	10 item(s) under the following path:	
Results Summary Console	C:\wcAiTemp\Agent\ Comment	*
ary		
ts Summ		
sault		-
Å	Apply same comment for all items.	
?	ОК	<u>C</u> lose

- 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:

Results S	iummary Console	\times
?	Do you want to Authorize the change item with blank comment?	
	Yes No	



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



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

Change Brows		System Gr		• \	/iew Type Date	<u> </u>	View By Chang	е Туре 🔻	
			• •			_	,		
5ystem Name	Current Snapsh 8/5/2010 12:36		Previous Snapshot Time 8/5/2010 2:01:42 AM	Authorized	Unauthori	ized Configurat	ion System 222	Busine	ss Knowledge
ESXWEBDOC WEBDOC1	8/5/2010 12:36		8/5/2010 1:10:42 PM	0	0	0	44	0	
WEBDOC2	8/5/2010 2:25:		8/5/2010 2:23:17 PM	14	Ő	0	17	0	
									- 11
Configuration F Policy Name	Policy Dashboard	Policy Descrip	ption		System Name	Integrity Violations	Comparison Time	Sched	Analyze
		Policy Descrip	ption designed to demonstrate File Ir	itegrity Monitor	System Name ESXWEBDOC	Integrity Violations	Comparison Time 8/5/2010 2:01:04 /		Analyze

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.



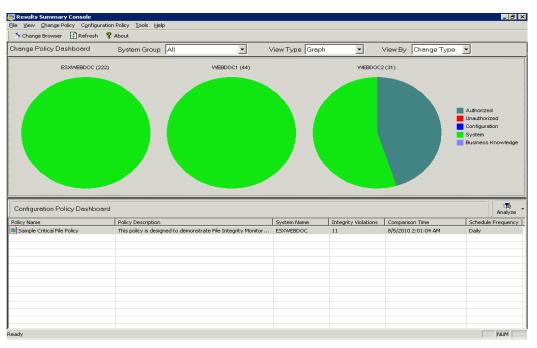
2.7 Viewing Change Report

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.



lcon	Description
	Snapshot in progress.
•	No changes were found.
	File changes found.
1 1 1	Registry changes found.
R	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**.

olicyName	File Details	Description	Size	Version	Checksum 🔺
ample Critical File Policy	C:\WINDOWS\system32\find.exe	Found integrity	9216	5.1.2600.0	2329F2C682
	C:\WINDOWS\system32\ftp.exe	Found integrity	42496	5.1.2600.5512	4112AA01C1
	C:\WINDOWS\system32\notepad.exe	Found integrity	69120	5.1.2600.5512	7A90F8B051
	C:\WINDOWS\system32\notepad.exe	Found integrity	76800	5.1.2600.5512	D3E9558130
	C:\WINDOWS\system32\print.exe	Found integrity	9216	5.1.2600.0	2F2AD17264
	C:\WINDOWS\system32\print.exe	Found integrity	3584	5.1.2600.0	DEB00B2DB
		Found integrity	3384 19968	5.1.2600.0	31282AD 39F -
	C:\WINDOWS\system32\route.exe	Edit Description			
	Select All Remove Add Item		Description	Data	
	Select <u>All</u> <u>Remove</u> <u>Add Item</u>	Edit Description			
	Select <u>All</u> <u>Remove</u> <u>Add Item</u>	Edit Description			
	Select <u>All</u> <u>Remove</u> <u>Add Item</u>	Edit Description			
	Select <u>All</u> <u>Remove</u> <u>Add Item</u>	Edit Description			
	Select <u>All</u> <u>Remove</u> <u>Add Item</u>	Edit Description			

- 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**.



Configuration Policies Systems		
ALL COMPUTERS	ESXWEBDOC Add Add All Bemove Remove All	
Select the systems to be compared.		

- 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**.

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

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.

Change Assessment Results				
System Name: ESXWEBDOC		Policy Name	: Sample Critical File Poli	icy
Total Violations:11		Compared O	n: 8/5/2010 2:01:04 AM	
This policy is designed to demonstrate File Integrity Violations for the included entries to illustrate how F				
This sample policy contains properties of some criti When you run this policy, it will compare properties Item Location: C:\WINDDWS\system32\find.	of the file within t			
Item Name	<u>N</u> ext		Policy Values	Actual Values
? find.exe			9216	10240
? ftp.exe	Previous		5.1.2600.0	5.2.3790.3959
? notepad.exe			8/4/2004 6:30:00 PM 2329F2C682F5C7896980F5	3/25/2003 5:30:00 PM 5 9EDFDE8A522400AA16C14
2 nslookup.exe	Accept	CHECKSUIT	20201 200021 001 0000001 0	320102043224004410014
? print.exe		1		
regedt32.exe	<u>R</u> eject			
? route.exe		1		
? runas.exe	<u>I</u> gnore			
rundli32.exe	Save	Found integrity		
? services.exe	2000	You have four		D
? setup.exe	Save <u>A</u> s	personnel.		on - Please report it to appropriate ns that this violation is not importan
	R <u>u</u> n	to you. Rejecti 3. Accept the	ng it means it is deleted from difference - the master policy	the master policy. v is wrong and you know that you
	Report	properties.	hile on your system. Update iolation for now.	the master policy with the new file
I >	<u>M</u> ore Info			

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 t	o 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.
2	Fresh item.
*	Items accepted.
٢	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.

Policy Name Sample Critical File Policy	1				
1					

- 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.



Policy Co	mparison Results				×			
	Change Assessment Results							
	System Name: WEBDOC2		Policy Nam	e: Sample Critical File Polic	y			
	Total Violations: 10		Compared On: 8/5/2010 4:08:36 PM					
	This policy is designed to demonstrate File Integrity Monitoring using EventTracker Change Management. It has been configured to generate Policy Violations for the included entries to illustrate how Policies can be used to detect changes or problems in both files and registry values.							
	This sample policy contains properties of some critical operating systems files. These files are supplied by Microsoft so they should not be changed. When you run this policy, it will compare properties of the file within the master policy (in this case our demo policy) with the actual properties files							
	Item Name	Next		Policy Values	Actual Values			
e	2 ftp.exe	<u></u>	Size (in b		42496			
je j	7 notepad.exe	Previous	Version	5.1.2600.5512	5.1.2600.5512			
0	7 nslookup.exe		Created At		8/4/2004 5:30:00 PM			
S	7 print.exe	A <u>c</u> cept	Checksum	4112AA01C1484FEF54718A.	4112AA01C1484FEF54718A			
'S	7 regedt32.exe							
a)	? route.exe	<u>R</u> eject						
An	7 runas.exe							
÷ I	7 rundll32.exe	<u>I</u> gnore						
EventTracker - Result Analysis Console	services.exe setup.exe	Save	Found integrity violation.					
er -		Save <u>A</u> s	personnel.		n - Please report it to appropriate s that this violation is not important			
rack		R <u>u</u> n	to you. Reject 3. Accept the	ting it means it is deleted from t difference - the master policy i	he master policy. s wrong and you know that you			
ent]		R <u>e</u> port	properties.	ct file on your system. Update th violation for now.	ne master policy with the new file			
ц,		<u>M</u> ore Info			_			
?					<u>F</u> inish			

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.



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

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.



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

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.



👰 EventTracker - Change Browser				_ 8
Elle Edit View Options Reports Tools Help				
📇 Groups 🔡 Change View 👻 🙆 New Snap 🙀 🔶 Show	Next Change 🗎 🥅 Change	Report		
		· · · · · · · · · · · · · · · · · · ·		
Compare	- with	~		
	Members of group: TOONS	6		
Computers	System	Туре	Description	
	ESXWEBDOC	Windows 2003 - Server	-none-	
	Swebdoc1	Windows XP - Professional	-none-	
	BWEBDOC2	Windows XP - Professional	-none-	
Change Audit managed systems	Change Audit mar	naged systems		
	Changed :	Vadded :	V Deleted -	

- 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.

racke	racker – Change Browser							
View	Options	<u>R</u> eports	I					
✓ Gro	oups	Ctrl+G						
<u>S</u> y:	stems Bar	Ctrl+S						
Eul	View							
⊆h	ange View							
Re	Restore Log							
Rel	fresh	F5						

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

EventTracker - Change Browser 🛛 🗙					
⚠	'Groups' view will close once you load a system.				
	OK				

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.



	ker – Change Browser				
	w Options Reports Tools Help E Change View - 🞯 New Snap 🙌	😔 Show Next Change 🛛 🗮 Ch	ange Report		
ESXWEBDOC	Compare	▼ with	Y		
2011120000	Computer Groups	Members of group: T	DONS		
	+ 🛃 Computers	System	Type	Description	
WEBDOC1		ESXWEBDOC	Windows 2003 - Server	-none-	
WEBDUCI		Sweed of the second sec	Windows XP - Professional	-none-	
		Swebdoc2	Windows XP - Professional	-none-	
WEBD0C2					
		Changed: .		Deleted :	

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.

💀 Event Track	cer – Change	Browse	er											 ð ×
Eile Edit View	# Options	<u>R</u> eports	<u>T</u> ools <u>H</u> elp											
🚰 Groups 🔡	Change Viev	v - 🧿	New Snap	🙌 🥎 Sho	w Next	Ihange 🧮	Change R	eport						
3	Compare	Laurusa			_	with AS: 8								
ESXWEBDOC		,	110 12:36:09 F	-M	_	1	/5/2010 2	:01:42 AM	•					
	Tracking only					WEBDOC				,				
	⊡ ∄ ESX	WEBDOO	D			cessor		Page Size		Windows Ver			Physical Memory	
WEBDOC1		C:				586×1		4096 Bytes		5.2 Service F	ack 2	1023	MB	
	- 😽 I	Registry												
	<u> </u>	🗸 HKEY	LOCAL_MA	CHINE										
WEBDOC2		🎒 HKEY	USERS											
WE00002	-4	🖺 HKEY	CURRENT_	_CONFIG										
IP Address: 192	1691.24		Type: Syster	m Mama		Changed			Added :		Deleted			 _
IF Address: 132.	.100.1.24		Type: Syster	in Name					Magga :		▼ Deleted		···	



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.
- 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.

iystem Details	
Hardware Information	
Computer Name:	ESXWEBDOC
Processor Type:	586
Number of Processors:	1
Page Size:	4096 Bytes
Operating System Informa	ation
Windows Major Version:	5
Windows Minor Version:	2
Latest Service Pack:	Service Pack 2
Root Drive:	C:
Windows Path:	C:\WINDOWS
System Path:	C:\WINDOWS\system32
Memory Status	
Total Physical Memory:	1023 MB
Total Virtual Memory:	2047 MB
Paging File Size:	2469 MB

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.



	cer - Change Brows						
	Elle Edit View Options Reports Tools Help						
	Change View 👻 🄇	🕽 New Snap 🛛 👫 😽 Show Ne	xt Change 📃 Change R	eport			
B ESXWEBDOC		2010 12:36:09 PM	with AS: 8/5/2010 2	:01:42 AM 💌			
	Tracking only select		SXWEBDOC		1	[
	ESXWEBD		Processor 586×1	Page Size 4096 Bytes	Windows Versio 5.2 Service Pag		ysical Memory
WEBDOC1		<u>d</u>	<u>≓</u>) 366 ∧ I	4096 Bytes	5.2 Service Pac	CK Z 1023 MB	5
WEBDOC2							
IP Address: 192.	168.1.24	Type: System Name	Changed :	Added :		VDeleted :	

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.



	ker – Change Brow						_ 8 ×
	w <u>O</u> ptions <u>R</u> eport						
🚦 Groups 🔡	E Change View 👻 🌘	🧿 New Snap 🛛 🙀 🛛 🔶 Shov	w Next Change 🛛 🧮 Chan	ge Report			
	Compare 8/5/	2010 12:36:09 PM	with AS: 8/5/20	10 2:01:42 AM 💌]		
ESXWEBDOC	Tracking only select	ted file types	ESXWEBDOC				
	ESXWEBD	00	Processor	Page Size	Windows Version	Total Physical Memory	
WEBDOC1	En - Anger Begistry En - ▼ HK	Y EY_LOCAL_MACHINE	<u>₽</u> 586×1	4096 Bytes	5.2 Service Pack 2	1023 MB	
	— 🐴 НК	EY_USERS					
	нк 💾 нк	EY_CURRENT_CONFIG					
WEBDOC2							
		T O i N					
IP Address: 192.	.168.1.24	Type: System Name	Changed :	VAdded	: Veleted :		

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.

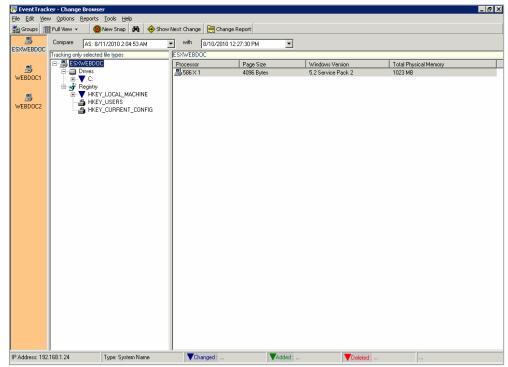




2. Click the **View** menu and select the **Full View** option. Or, Click the toggle button on the toolbar. The Change Audit displays the shortcut menu.



- 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.
- 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**.



SEOLALOCAEDDODLOC 🔽

C: Verogram Files Microso	oft SQL Server\MSSQL.1\MSSQL\LOG\ERRORLOG		-
Snapshot Label:	AS: 8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM	
Snapshot Time:	8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM	
Size:	10 KB (9038 Bytes)	15 KB (14762 Bytes)	
Creation Time:	7/22/2010 1:38:56 PM	7/22/2010 1:38:56 PM	
Access Time:	8/10/2010 11:46:25 PM	8/10/2010 12:27:04 PM	
Last Write Time:	8/10/2010 11:46:25 PM	8/10/2010 12:27:04 PM	
Version:	-none-	-none-	
Checksum:	-not tracked-	-not tracked-	
Attributes:			
Archive:			
Compressed:	Γ		
Directory:	Γ		
Encrypted:			
Hidden:			
Offline:			
Read Only:			
System:			
Temporary:	Γ		

C:\WcWindows.exe	3	*
Snapshot Label:	12/5/2016 2:39:08 PM	12/5/2016 2:38:22 PM
Snapshot Time:	12/5/2016 2:39:08 PM	12/5/2016 2:38:22 PM
Size:	2930 KB (2999088 Bytes)	2969 KB (3039096 Bytes)
Creation Time:	12/5/2016 2:35:56 PM	12/5/2016 2:35:56 PM
Access Time:	12/5/2016 2:35:56 PM	12/5/2016 2:35:56 PM
Last Write Time:	8/2/2016 7:49:48 AM	11/29/2016 9:46:30 PM
File Version:	8.2.0.5	8.2.0.5
Checksum (SHA1):	38C97D172957ABADE7CA411CAF0E102A8B76B766	912313EB6738CABC1562DAD5AC3E9E84CAFA68D1
Checksum (MD5):	48E0EB726495D9CC44F996228A747D96	806637BF46292EC439A49C103E7B9194
Description:	EventTracker - Change Browser	EventTracker - Change Browser
Product Name:	EventTracker	EventTracker
Product Version:	8.2.0.5	8.2.0.5
Signer:	Prism Microsystems, Inc.	Prism Microsystems, Inc.
Counter Signer:	Symantec Time Stamping Services Signer - G4	COMODO SHA-1 Time Stamping Signer
Signer On:	8/2/2016 5:21:01 PM	11/29/2016 9:22:15 PM
Attributes:		
Archive:		v
Compressed:		Ē
Directory:	Γ	Γ
Encrypted:	Π	Ē
Hidden:		
Offline:		Г
Read Only:		Γ
System:	Γ	
Temporary:		

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**.

KEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000003EB\F	
odified Time Of Parent Key: 8/10/2010 7:41:43 PM	
AS: 8/11/2010 2:04:53 AM	
Snapshot time: 8/11/2010 2:04:53 AM	
Type: REG_BINARY (Free form binary)	
Data: 02 00 01 00 00 00 00 00 58 34 80 f5 95 38 cb 01 00 00 00 00 00 00 00 00 0c 17 41 71 24 b9 ca 01 00 00 00 00 00 00 00 00 00 00 00 00	
14 02 00 00 00 00 00 00 00 00 94 01 00 00 00 00 00 00 00 00 00 00 00 00	
Data Size: 80 Bytes	
8/10/2010 12:27:30 PM	
Snapshot time: 8/10/2010 12:27:30 PM	
Type: REG_BINARY (Free form binary)	
Data: 02 00 01 00 00 00 00 00 4d e0 f0 80 b9 37 cb 01 00 00 00 00 00 00 00 00 cc 17 41 71 24 b9 ca 01 00 00 00 00 00 00 00 00 00 00 00 00	
14 02 00 00 00 00 00 00 00 00 00 00 00 00	
Data Size: 80 Bytes	

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.

 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.



💀 Next (From Selected Node) 🔀					
Find: – Look at –––––					
Next Changed					
✓ Next <u>A</u> dded ✓ Next <u>D</u> eleted					
<u>F</u> ind	<u>C</u> ancel				

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.

	ker - Change Browser				_ 8
	w Options Reports Tools Help				
	Change View 👻 🛞 New Snap 🙌 🔶 Show	w Next Change 📙 Change Rep	ort		
BSXWEBDOC	Compare AS: 8/11/2010 2:04:53 AM	with 8/10/2010 12:27:	30 PM		
ESAWEBDUC	Tracking only selected file types	ESXWEBDOC\Drives\C:\Prog	am Files\Microsoft SQL Server\MSS	QL.1\MSSQL\LOG	
	E-B ESXWEBDOC	File Name		8/10/2010 12:27:30 PM	Last Modified Time
WEBDOC1	E B Drives	C ERRORLOG	10 KB (9038 Bytes) 1	15 KB (14762 Bytes)	8/10/2010 11:46:25 PM
	Program Files				
	Microsoft SQL Server				
WEBDOC2	iant MSSQL.1 iant MSSQL				
	E 😽 Registry				
	HKEY_LOCAL_MACHINE				
	HKEY_USERS				
	1				
IP Address: 192	168.1.24 Type: Folder (4)	Changed: 1	Added: 0	Veleted : 0	Total Unauthorized: 0
	· · · · · · · · · · · · · · · · · · ·	,	,		· · · · · · · · · · · · · · · · · · ·

(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.

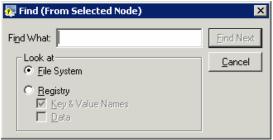


3.10 Search Strings

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.



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



	ker - Change Browser				_ [7] ×
	w <u>O</u> ptions <u>R</u> eports <u>T</u> ools <u>H</u> elp				
遺 Groups 📋	🏽 Full View 👻 🙆 New Snap 🙌 🔶 Show	Next Change 🗎 Change Report			
	Compare AS: 9/11/2010 2:04:52 AM	with 8/10/2010 12:27:30 P			
ESXWEBDOC	. A3. 0/11/2010 2.04.33 AM				
	Tracking only selected file types	ESXWEBDOC\Drives\C:\Program F	Files/Microsoft SQL Server/90	D\Tools\Binn\VSShell\Comm	on7\IDE\1033
	ESXWEBDOC	File Name	AS: 8/11/2010 2:04:53	8/10/2010 12:27:30 PM	Last Modified Time
WEBDOC1	Drives	🗈 cmddefui.dll	461 KB (471552 Bytes)	461 KB (471552 Bytes)	4/21/2008 7:56:20 PM
WEBDUCI		🖹 Microsoft.VisualStudio.Design		3 KB (3072 Bytes)	4/21/2008 5:32:06 PM
	Documents and Settings ET & PULSE Prerequisites	Microsoft.VisualStudio.Export		5 KB (3584 Bytes)	4/21/2008 6:48:10 PM
		Microsoft.VisualStudio.Windo		5 KB (5120 Bytes)	4/21/2008 5:32:12 PM
WEBDOC2		Microsoft.VisualStudioUI.dll	3 KB (3072 Bytes)	3 KB (3072 Bytes)	4/21/2008 5:32:00 PM
	Logs	🗈 msenvui.dll	1127 KB (1152512 Bytes)	1127 KB (1152512 Bytes)	4/21/2008 6:46:42 PM
	Program Files	🗈 vsmsoui.dll	1373 KB (1405952 Bytes)	1373 KB (1405952 Bytes)	4/21/2008 7:59:56 PM
	🕀 🦳 Add Remove Pro	🗈 vssinui.dli	9 KB (9216 Bytes)	9 KB (9216 Bytes)	4/21/2008 6:47:04 PM
	😟 🦲 Business Objects	1			
	🕀 🦲 cmak	1			
	😥 🧰 Common Files	1			
	ComPlus Applications				
	Internet Explorer				
	Microsoft SQL Server	1			
	⊡- <u>©</u> 90 ⊡- <u>©</u> COM	1			
		1			
	I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	1			
	E-C Setup Bootstrap	1			
	E Shared	1			
		1			
	E- Binn	1			
	E Besource	1			
	🗄 🦳 schema	1			
	- Setup				
	🖻 🛄 VSShell	1			
	📄 💼 Con	1			
		1			
		1			
	■				
IP Address: 192	.168.1.24 Type: Folder (4)	Changed : 0	Added : 0	VDeleted : 0	Total Unauthorized: 8
	J				J

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.

👰 Find (From Selected Node)	×
Find What:	<u>Find</u> Next
Look at C Eile System	<u>C</u> ancel
 	



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

EventTrack		Browser Reports Tools Help				
	Full View +		Next Change 🗮 Change Re	port		
B ESXWEBDOC	Compare	, ,	with 8/10/2010 12:27			
	Tracking onl	y selected file types	ESXWEBDOC\Registry\HKE\	LOCAL_MACHINE\SOFTW	ARE\Classes\Prism.Common.CodeCompil	erLibrary.CodeCompiler
3		PNGFilter.CoPNGFil PolyHub.90.Alternat	Value Name	Type REG SZ	AS: 8/11/2010 2:04:53 AM	8/10/2010 12:27:30 PM
WEBDOC1		Bit PolyHuk Skamad Bit PolyHuk Skamads; Bit PolyHuk Akamads; Bit polSkap polSkap				
	1	poSVee ppSVec poSvec poSvec pose pos	Count 2			Table Band C
Address: 192.1	68.1.24	Type: Registry Key (3)	Changed : 0	Added : 0	VDeleted : 0	Total Unauthorized: 0

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.
- Click the **Reports** menu and select the **View Reports** option or click on the toolbar. The Change Audit displays the Select Format window.

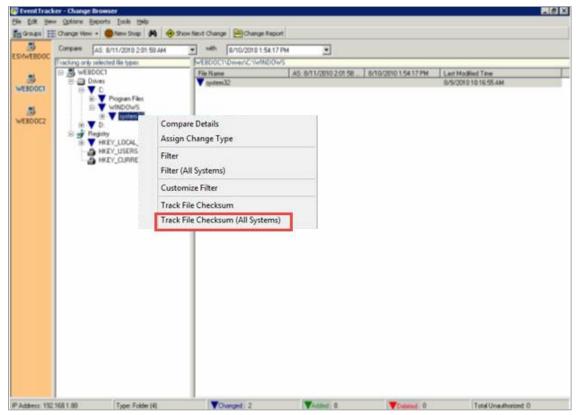
🐺 Select Format	×
View Change Report In:	
 Notepad (Text) 	
C Excel (Tab delir	mited)
<u> </u>	Cancel

- 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.



👰 EventTrac	ker - Change B	Browser					
		eports <u>T</u> ools <u>H</u> elp					
🚰 Groups 🚦	Change View	🔹 🔞 New Snap 🛛 🖗	🚯 😔 Show Next	t Change 🗎 Change Report			
SXWEBDOC	Compare	8/11/2010 12:51:09 P	M	with 8/10/2010 1:54:17 PM	•		
LUXWEDDOC		elected file types	[₩E	EBD0C1\Drives\C:\WIND0WS\s	ystem32\CatRoot2\{F750E	6C3-38EE-11D1-85E5-00C04	FC295EE}
	E-B WEBD	001		ile Name	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM	Last Modified Time
WEBDOC1		ives C	0	catdb	7176 KB (7348224 Bytes)	7176 KB (7348224 Bytes)	8/11/2010 12:04:26 PM
WEBDOC2		ien ▼ system32 ien ▼ CatRoot2					
			D0A1D-4EF2- DE6C3-38EE-1				
	•		Þ				
IP Address: 192	.168.1.88	Type: Folder (4	4)	Changed: 1	Added : 0	Veleted : 0	Total Unauthorized: 0

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

C:\WINDOWS\system32 ^v	.CatRoot2\{F750E6C3-38EE-11D1-85E5-00C0	4FC295EE}\catdb
Snapshot Label:	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM
Snapshot Time:	8/11/2010 12:51:09 PM	8/10/2010 1:54:17 PM
Size:	7176 KB (7348224 Bytes)	7176 KB (7348224 Bytes)
Creation Time:	11/15/2008 5:50:46 PM	11/15/2008 5:50:46 PM
Access Time:	8/11/2010 12:04:26 PM	8/10/2010 1:04:37 PM
ast Write Time:	8/11/2010 12:04:26 PM	8/10/2010 1:04:37 PM
/ersion:	-none-	-none-
Checksum: 61B	B84438E3F8D5FF51FE292F00B587DF92956	E4 D944F0FA3AB5E076F543ABBB8B0A165D66D58917
Attributes: Archive: Dompressed: Directory: Encrypted: Hidden: Diffline: Read Only: System: Emporary:		

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.



- 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

- 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.

ache Properties		? >
General Sharing Security Web	Sharing Custor	mize
Group or user names:		
Administrators (ESXWEBDO)	CVAdministrators)	
CREATOR OWNER		
🕵 NETWORK SERVICE		
💈 🕵 Nirmal (nirmal@Toons.local)		
🖉 Power Users (ESXWEBDOC	\Power Users)	_
•		
	A <u>d</u> d	<u>R</u> emove
Permissions for Administrators	Allow	Deny
Full Control	>	
Modify	\checkmark	
Read & Execute	4	
List Folder Contents	1	
Read	\checkmark	
Write	\checkmark	
Coordel Permissions		
 For special permissions or for adva click Advanced. 	nced settings,	Ad <u>v</u> anced
	_	
OK	Cancel	Apply

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



٨dv	anced Secu	irity Settings for Cach	e			? ×
P	ermissions ⁴	Auditing Owner Effectiv	ve Permissions			
	To view more Auditing entrie	information about special	auditing entries, selec	t an auditing entry,	and then click E	dit.
	Auditing engite Type	es. Name	Access	Inherited From	Apply To	—
	Туре	Name	ACCESS	minericed FIOIII	T Abbill 10	
	Add	E dit	Remove	1		
				1	1.0.191.12	
	Allow inhe these with	eritable auditing entries fror n entries explicitly defined h	n the parent to propag here.	jate to this object a	nd all child objec	ts. Include
	Beplace a	auditing entries on all child	objects with entries s	hown here that ann	lu to child object	,
	Theplace a	additing entries on all child	objects with childs a	iowi neie triat app	ly to child object.	°
	Learn more al	bout auditing.				
			Γ	ОК	Cancel	Apply

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

elect User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
Erom this location:	
Toons.local	Locations
Enter the object name to select (<u>examples</u>):	
	Check Names
Advanced	OK Cancel

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

Select the location you want to search. Location: ESXWEBDOC Entire Directory Constlocat POPLTEST POPLITEST POPLVista.test
ESXWEBDOC Finite Directory Fig0 celebrate test Fig0 celebrate test Fig0 PNPL.TEST
Entire Directory Toons.local Celebrate.test POP PNPL.TEST
Toonslocal Celebrate.test Popl_TEST
e 🞲 celebrate.test e 🞲 PNPL.TEST
E S popluista test
E. Ab hubblerest
J
DK Cancel

- 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.



Select User, Computer, or Group	? ×
Select this object type:	
User, Group, or Built-in security principal	Object Types
Erom this location:	
Toons.local	Locations
Enter the object name to select (<u>examples</u>):	
ETAdmin (etadmin@Toons.local)	<u>C</u> heck Names
OKOK	Cancel
Select User, Computer, or Group	×
An object (User, Group, or Built-in security principal) with the f	ollowing name
cannot be found: "etadmins". Check the selected object type accuracy and ensure that you have typed the object name of	es and locations for
this object from the selection.	Shecky, or remove

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

Auditing Entry for Cache			? ×
Object			
Name: ETAdmin (etadmin@Toons Apply onto: This folder, subfolders		<u>C</u> hange	- -
Acce <u>s</u> s:	Successful	Failed	
Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Files / Write Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions			- -
Apply these auditing entries to ob and/or containers within this con		C <u>l</u> ear All	
	OK	Can	cel

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



Auditing Entry for Cache		?	×
Object			
Name: ETAdmin (etadmin@Toons		Change	
Access:	Successful	Failed	
Full Control Traverse Folder / Execute File List Folder / Read Data Read Attributes Read Extended Attributes Create Folders / Append Data Create Folders / Append Data Write Attributes Write Extended Attributes Delete Subfolders and Files Delete Read Permissions Character Permissions			
	ОК	Cancel	1

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.

dvanced Se	curity Settings for Cach	e		? ×
Permissions	Auditing Owner Effectiv	ve Permissions		
To view mo	re information about special	auditing entries, sel	ect an auditing entry,	and then click Edit.
A				
Auditing en	(nes:			
Type	Name	Access	Inherited From	Apply To
All	ETAdmin (etadmin@	Full Control	<not inherited=""></not>	This folder, subfold
these w	Edit heritable auditing entries fron ith entries explicitly defined I e auditing entries on all child	nere.		
Learn more	about <u>auditing</u> .			
			ок	Cancel <u>A</u> pply

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

Note

Similarly, enable auditing for file or registry keys.

3.13.3 Enabling the O/S Audit on the Registry Keys

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

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



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

Permissions for Prism Microsyste	ems	? ×
Security		
Group or user names:		
Administrators (ESXWEBDO)	NAdministrators)	
CREATOR OWNER		
Power Users (ESXWEBDOC	Power Users)	
SYSTEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for Administrators	Allow	Deny
Permissions for Administrators Full Control	Allow	Deny
Full Control		
Full Control Read		

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

Advanced Se	curity Setti	ings for Pris	m Microsystems	;			? ×
Permissions	Auditing (0wner Effect	ive Permissions				
To view mo	ore information	n about specia	I auditing entries, s	elect an audit	ing entry, a	nd then clic	k Edit.
Auditing en	tries:						
Туре	Name		Access	Inherited	d From	Apply To	
A <u>d</u> d.		<u>E</u> dit	<u>R</u> emove				
	heritable aud	liting entries fro	om the parent to pro	pagate to thi:	s object and	d all child ob	ojects. Include
💌 These w	vith entries ex	plicitly defined	here.				
🔲 Re <u>p</u> lac	e auditing en	tries on all chil	d objects with entri	es shown here	e that apply	to child obj	ects
	about <u>auditir</u>						
Lean more	about <u>auditir</u>	<u>ny</u> .					
				ОК		Cancel	Apply

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.

Assign Change 1	уре			
Node Name: ESXW	/EBDOC\Drives\C:\P	rogram File	s\Microsoft SC	QL Server\MSSQ
Absolute Path: Driv	es\C:\Program Files\M	dicrosoft S	QL Server\MS	SQL.1\MSSQL\L
System				•
🗖 Replace change	e type on all child obje	cts		
Apply on all syst				
	Assign	ſ	ancel	

- 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.

🗛 Assign Change Type	×
Node Name: ESXWEBDOC\Drives\C:\Program Files\Microsoft SQL Server\MSSI	Q
Absolute Path: Drives\C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL'	
Configuration	
Replace change type on all child objects	
Apply on all systems	
<u>A</u> ssign <u>C</u> ancel	

- 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.

EventTra	cker - Change Browser 🛛 🔀
2	This configuration change will be saved locally. To propagate it to the remote system please select [Options Apply Configuration]. Do you want to apply locally?
	Yes No



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.



👧 Snapsho	t Details	×
9	Snapshot taken successfully.	
Time of snap:	8/10/2010 10:27:18 AM	_
Snap label:	8/10/2010 10:27:18 AM	
	🔲 Keep Snap Forever	
	Start <u>C</u> ompare	

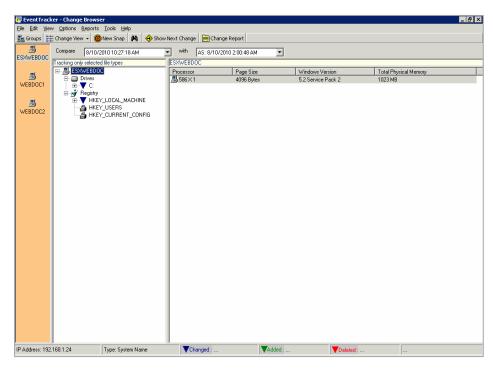
Field	Description
Time of snap	Displays the date and time when the Snapshot was taken.
Snap label	Displays the name of the Snapshot. You can edit and rename the Snapshot.
Keep Snap Forever	Select this check box if you want to preserve the Snapshot forever.
Start to Compare	Click this button for the Change 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:

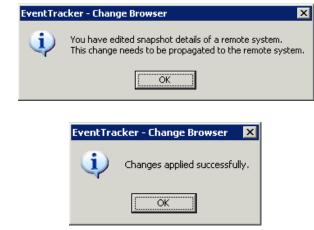
- 1. Open the Change Browser.
- 2. Double-click the computer on the System Bar.
- 3. Click the **Options** menu and select the **Edit Snapshots** option. Change Audit displays the Snap Editor.

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:

EventTrac	cker - Change Browser 🛛 🔀
?	This will delete all previous snaps for this system and initialize it with a new baseline snap. Do you want to proceed?
	<u>Y</u> es <u>N</u> o

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.



	cer - Change Brow						
	v Options <u>R</u> eports						
😼 Groups 🏢	Full View 👻 🧕	New Snap 🙌 🔶 Show I	Next Change 🧮 Change	Report			
SXWEBDOC			with Baseline Sna	p 💌			
	Tracking only select		WEBDOC2	Dana Cira	Arte dama Marian	Total Physical Memory	
	E-B Drives		Processor	Page Size 4096 Bytes	Windows Version 5.1 Service Pack 3	991 MB	
WEBDOC1	🗼 🕀 🛄 C:						
e i	<u>(</u> D: 						
WEBDOC2	- 🔁 F:						
	G: ⊡∰r Registry	1					
	📔 🕀 📋 HKE	EY_LOCAL_MACHINE					
	HKE	EY_USERS EY_CURRENT_CONFIG					
IP Address: 192.	J .168.1.74	Type: System Name	Changed :	Added :	VDeleted :		
		J. J. P. C. Strend Hound	y changou .	• • • • • • • • • • • • • • • • • • • •		··· J···	

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.



👰 Backup / R	ecovery Tool Fo	or Snapshot Files		×
Label	Date & Time	Path		
<u>B</u> ackup	F	ecover	Remove	Exit
	1	Tecover	TIETTOAC.	<u></u>

Button	Description
Backup	Back up the Snapshots of the current system.
<u>R</u> ecover	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:



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

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:

Success	×
i	Snap files backed up successfully.
	(OK

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

👰 Backup / R	ecovery Tool F	or Snapshot Files 🛛 🗙
Label	Date & Time	Path
WEBDOC1 S	8/10/2010 1	\\Webdoc1\shared\WEBDOC1 SNAPS
<u>B</u> ackup	F	Remove Exit

9. Click Exit.

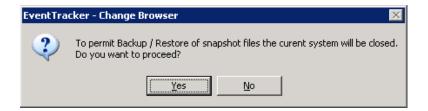
4.5 Recover Snapshots

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.

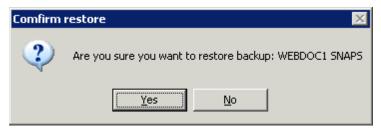




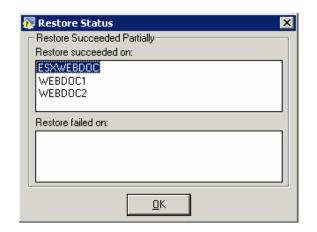
3. Click Yes to proceed. Change Audit displays the Backup / Recovery Tool.

👰 Backup / Re	ecovery Tool Fo	or Snapshot Files		×
Label	Date & Time	Path		
WEBDOC1 S	8/10/2010 1	\\Webdoc1\shared\V	/EBDOC1 SNAPS	
		. 1	- 1	1
<u>B</u> ackup	E	lecover	Remove	E <u>x</u> it

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.

🐺 Restore Status 🛛 🗙
Restore Succeeded Partially
Restore succeeded on:
ESXWEBDOC
Restore failed on:
WEBDOC1 WEBDOC2
<u><u> </u></u>

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:



Global Configurati	on	5		
Change Type	File Change Type	Registry Change Type	Checksum	Checksum Rules
General	File Types	Monitor Specific Registry	Monitor Specific Fo	lder Filters
Working Directory:	C:\Program Files (>	:86)\Prism Microsystems\WCWin	idows	_
Data Storage Directory:	C:\Program Files (>	86)\Prism Microsystems\WCWin	dows\SnapShots	
License Server:	VMESX3-VM1			
License Server Port:	14503			
Server Name, Port N	are moved to 'System (umber SventTracker Server P	-		

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.

Change Type General	File Change T	ype Regi MonitorSper	stry Change Type cific Registry	Checksum Monitor Specific	Folder Filters
ile types:					· · ·
pl	OCX				
	sys				Add
drv	vxd				
exe					
nsc					<u>D</u> elete
		e e la estica e suill tre el			
elect to track	only these file types, un	selecting will trac	k all files.		
Track Only	Files Of The Above Ty	bes			
7 D. NOT					
Do NOT co	nsider a file changed if	only file attributes	are changed		
For files with not change	n checksum tracking er d.	nabled, Do NOT o	consider a file char	nged if its checksum h	las



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.

<u>0</u> K	
<u>C</u> ancel	
	<u>O</u> K <u>C</u> ancel

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



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



Change Type	File Change Type	Registry Change Type	Checksum	Checksum Rules
General	File Types	Monitor Specific Registry	Monitor Specific Fold	er Filters
File types:				
cpl	OCX]
dll drv	sys txt			Add
exe	vxd			
msc				<u>D</u> elete
Select to track o	nly these file types, unseld	ecting will track all files		
		ootang maraon da moo.		
💌 Track Unly F	iles Of The Above Types			
	sider a file changed if only	/ file attributes are changed		
🔽 Do NOT cor	iolaor a nio oriangoa ir oriņ			
	checksum tracking enabl	ed, Do NOT consider a file chang	ed if its checksum has	
For files with	checksum tracking enabl	ed, Do NOT consider a file chang	ed if its checksum has	

- 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.

Change Type File Change Ty	pe Registry Change Type	Checksum	Checksum Rule
General File Types	Monitor Specific Registry	Monitor Specific Fold	der Filters
Name	Absolute Path		
My Documents		_DRIVE)\My Docume	ents
Wy Download Files		 	
My Installations	Drives\\$(ROOT		ons
My Music	Drives\\$(ROOT	_DRIVE)\My Music	
- profile	Drives\#(POOT	DDN/ENerofile	
`			
Check and click 'Remove' to UnFilter cl o filter right click on a folder or registry		the option.	
		-	iove

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.

Global Configura General	File Types 🔰 🕅	onitor Specific Registry	Monitor Specific Fo	older Eil	lters
Change Type	File Change Type	Registry Change Type	Checksum	Checksum R	
change rype	I nie change i ype	negistiy change rype	Checksum	Checksum h	luies
Name	Absolute Path	Change Type		Recursive	
Nume	Absolute Fatt			riccuisive	
Currently no subtre	es are assigned global ch	inge type.			
	es are assigned global ch jht click on a folder in the	inge type. change browser and select the o	ption.		
			ption.		
				1	
				emove	
				emove	
				emove	
		change browser and select the o	<u><u> </u></u>	emove	

Field	Description
	Authorized: Detected changes that can be matched with an approved change request.
Change Type	Unauthorized : Detected changes that cannot be matched to an approved change request.
Change Type	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.



Company	8/18/2010 10:27:18 AM	with AS: 8/10/2010	2 00.48 AM		
	only selected file types	ESXWEBOOC/Registy/H93			
EB00C1	SXWEBDOC Drives II-V C: Registry	Value Name	Type	8/10/2010 10:27:18 AM	AS: 8/10/2010 2:00:48 AM
EBDOC2	HKEY LOCAL MACHINE	Compare Details			
CBUULE	HKEY_CURRENT_CO	Assign Change Type			
		Filter Filter (All Systems)			
		Customize Filter			

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

🗛 Assign Change Type	×
Node Name: MCLOON\Registry\HKEY_LOCAL_MACHINE	
Absolute Path: Registry\HKEY_LOCAL_MACHINE	
System 💌	
Replace change type on all child objects	
Apply on all systems	
<u>A</u> ssign <u>C</u> ancel	

Field	Description
	For the following classification of Change Type, Change Audit considers all as the System Change Type.
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.

EventTra	cker - Change Browser 🛛 🔀
•	You need to propagate this change to all managed (EventTracker - Change Audit) systems. You can do this from [Options Apply Configuration Apply global configuration to all systems].
	OK]

- 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.

2	Global Configuration	n						\times
	General	File Types	Monitor Specific	Registry	Monitor Specific F	Folder	Filters	
Ĺ	Change Type	File Change Type	e Registry	Change Type	Checksum	Chec	sksum Rules	
	Name	Absolute Path		Change Type		Recursiv	e	
	MCLOON\Regist		MACH Unauthoriz		Yes		•	111
	Currently no subtrees	are assigned global	change tune					11
	To start tracking right			er and select the	option.			
					E	emove		
-			,					
			<u>0</u> K	<u>_</u>	ancel			

- 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.



Global Configu	uration					×
General	File Types	Monitor Specific Registry		Monitor Specific Fo	older Filters	
Change Type	File Change 1	ype Registry (Change Type	Checksum	Checksum Rules	
Path String	Path Operation	FileName String	FileName C)per Change Type		
		*.exe *.ocx *				
		*.ini *.cfg *.inf		-		
		*.xls *.doc *.xl	Case Inser	isitiv Business Know	vl	
Check and click	. 'Remove' to delete th		Add	<u>E</u> dit <u>R</u> e	move	
		<u>о</u> к		<u>C</u> ancel		

Field	Description				
	For the following classification of Change Type, Change Audit considers all as System Change Type.				
File 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.



💀 File Change Type 🛛 🗙
Search for matching file path
File Path String
File Path Operator
Equal
Search for matching file name
File Name String
File Name Operator
Equal
Change Type
System 💌
<u>Save</u>

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.

EventTra	cker - Change Browser 🛛 🔀
i	You need to propagate this rule to all managed (EventTracker - Change Audit) systems. You can do this from [Options Apply Configuration Apply global configuration to all systems].
	(OK

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



General Change Type	File Types File Change Ty	Monitor Specific pe Registry	c Registry 📔 🕅 Change Type 📔	fonitor Specific Fold Checksum	der Filte Checksum Rul
Key String	Key Operation	Value String	Value Operation	Data String	Data Operatio
<					
	rules for extended ct	hange type assignm	ent for registry objects	<u>.</u>	
	rules for extended cf	hange type assignm			nove
	rules for extended cł	hange type assignm	1		nove

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

Field	Description
	But for the following classification of Change Type, Change Audit considers all as System Change Type.
Registry 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.



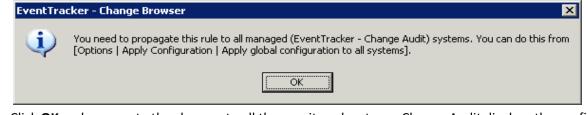
🗛 Registry Change Type 🛛 🗙
Search for matching registry key path
Registry Key Path String
Registry Key Path Operator
Equal
Search for matching registry value name
Value Name String
Value Name Operator
Equal
Search for matching registry data
Data String
Data Operator
Equal
Change Type
System
<u>Save</u>

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.
Search for matching registry data Data String Data Operator	Select this check box. Change Audit enables Data String an Data Operator fields. Type the data string. Select an operator 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.

EventTra	cker - Change Browser 🛛 🔀
2	You have changed the enterprise wide configuration. Do you want to save and apply to all systems?
	Yes No

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

General	File Types	Moni	itor Specific Registry	Monitor Sp	ecific Folde	er	Filters
Change Type	File Change T	ype	Registry Change Type	Checks		Checksun	n Rules
Name	Absolute Path						
🔲 system32	Drives\\$(SYST	•					
Check and click 'R	emove' to delete th	e rule.					
			ange browser and select I	he option.			
			ange browser and select t	he option.	Remo	ive	
			ange browser and select I	he option.	<u>R</u> emo	ve	
			ange browser and select I	he option.	<u>R</u> emo	ive	

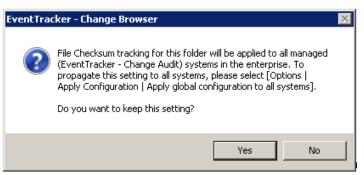


5.1.2 Configuring the Change Type

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

Pluchag ork antered He type: Pluchag ork antered He type: Plucha		4/30/2015/5/2418 PM 1/27/2015/5/14:40 PM 3/15/2014:4:06:14 PM	AG 5/27/2015 2 36 59 AM	AS: 5/27/2015 2 48:25 AM				Company A5 5/27/2015 2 48 2	
Image: Compare Details 40000552418/PM Image: Compare Details 1/27/27511440/PM Image: Compare Details 500005124186/PM Image: Compare Details 500005124186/PM Image: Compare Details 500005124186/PM Image: Compare Details 50000512186/PM Image: Compare Details 50000512187/PM Image: Compare Details 50000512187/PM Image: Compare Details 5000071112172 Image: Compare Details 5000071112172 Image: Compare Det		4/30/2015/5/2418 PM 1/27/2015/5/14:40 PM 3/15/2014:4:06:14 PM	AG: 5/27/2015 2 36 59 AM	AS: 5/27/2015 2:48:26 AM		and the second se	Ne typer		
107/2025 11 40 PM 107/2025 11 40 PM 107/2025 11 40 PM 9/10/2014 40 14PM 107/2025 12 40 PM 9/10/2014 128 PM 107/2025 12 40 PM 10/10/2014 189 PM 10/10/2014 189 PM 10/10/2014 189 PM 10/2020 11 15 14 AM 10/2020 11 15 14 AM 10/2020 11 15 14 AM 10/2020 11 15 14 AM 10/2020 11 15 14 AM 10/2020 11 28 PM 10/2020 12 12 15 PM 10/2020 11 28 PM 10/2020 12 12 15 PM 10/2020 11 28 PM 10/2020 11 28 PM 10/2020 11 28 PM 10/2020 11 28 PM 10/2020 12 13 PM 10/2020 12 13 PM 10/2020 12 13 PM 10/2020 12 13 PM 10/2020 13 PM 10/2020 18 PM 10/2020 18 PM <t< th=""><th></th><th>1/27/2015 5 14 40 PM 3/15/2014 4 06 14 PM</th><th></th><th></th><th></th><th></th><th></th><th></th></t<>		1/27/2015 5 14 40 PM 3/15/2014 4 06 14 PM							
Compare Details \$100,000,112,84,8194 Assign Change Type \$107,000,413,8494 Filter \$107,000,413,8594 Filter \$107,000,413,856,944 Filter \$107,000,413,956,944 Customize Filter \$107,000,413,950,944 Track File Checksum \$107,000,413,950,294,944 Track File Checksum \$100,000,113,944,944 100,000,113,944,944,944 \$100,000,113,944,944 100,000,113,944,944,944 \$100,000,113,944,944 Track File Checksum \$100,000,113,944,944 100,000,113,944,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944 100,000,113,944,944 \$100,000,113,944,944						56 mc backup		*▼c *0 *2 *2 *3	
Filter 12/20/2013/21/96/PM Filter 21/30/2013/21/96/PM Filter (All Systems) 21/30/2013/21/96/PM Customize Filter 12/00/2013/21/96/PM Track File Checksum 12/00/2013/21/96/PM Track File Checksum (All Systems) 12/2009/2013/25/96/PM 12/00/2013/21/96/PM 12/2009/2013/25/96/PM 12/00/2013/21/96/PM 12/2009/2013/25/96/PM 12/00/2013/25/96/PM 12/2009/2013/25/96/PM 12/00/2013/25/96/PM 12/2009/2013/25/96/PM	e	9/30/2014 12:46:48 PM 10/1/2014 4 19:49 PM							
Filter (All Systems) 0/15/03/51/20/59/14 Customize Filter 1/16/03/23/21/20/51/24 Track File Checksum 1/20/20/51/21/26/64 Track File Checksum (All Systems) 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64 1/20/20/51/21/56/64		11/5/2014 2 23:36 PM				ge Type		3	
Customize Filter 11/20/2014/39/12/94 Track File Checksum 51/2012/21/85/PM Track File Checksum (All Systems) 12/2020/22/12/55/PM 12/2020/22/22/55/PM 12/2020/22/22/55/PM 12/2020/22/22/55/PM 12/2020/22/22/55/PM 12/2020/22/22/25/FM 12/2020/22/22/55/PM	4	4/15/2015 2:53:41 PM 11/18/2014 5:06:02 PM				tems)	and the second		
Track File Checksum Track File Checksum (All Systems) Track File Checksum (All Systems) 1/2/00/54/54/54/54 1/2/00/54/54/54/54 1/2/00/54/54/54/54 1/2/00/54/54/54/54 1/2/00/54/54 1/2/00/54 1/2/00/54	11/20/2014 3:58:12 PM				lter	Customize Fil			
Track File Checksum (All Systems) 12/00/2010 21956 PM 8/13/00/4 3/98 49 PM		9/3/2014 10:47:10 AM				ecksum	Track File Che		
		12/30/2013 2:19:56 PM			tems)	ecksum (All Syst	Track File Che	121	
			246686 KB (252605800 Bytes)	246686 KB (252605800 Bytes)		2 cantasia.eve			

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.



💀 Global Configu	ration							Х
General	File Types	Monit	or Specific Registry	/	Monitor Specific Fo	older	Filters	
Change Type	File Change T	vpe	Registry Change	Туре	Checksum	Che	ecksum Rules	
Name	Absolute Path							
system32	Drives\\$(SYST							
G:	Drives\G:							
	'Remove' to delete th							
To start tracking	right click on a folder	n the chai	nge browser and se	elect the	option.			
					Re	move	1	
		OK	1	C-	ancel			
		<u>0</u> K		<u>L</u> a				

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.).

Global Configurat	ion			×					
General	File Types 👘 🕺 🕺	Ionitor Specific Registry	Monitor Specific Fol	der Filters					
Change Type	File Change Type	Registry Change Type	Checksum	Checksum Rules					
Path String									
Check and click 'Re	Check and click 'Remove' to delete the rule.								
	4 <u>0</u>	(<u>C</u> ancel						

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



🔁 Checksum Configuration 🛛 🗙
Search for matching file path
File Path String
File Path Operator
Equal
Search for matching file name
File Name String
File Name Operator
Equal
Save Cancel

- 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.

🐺 Checksum Configuration	×
Search for matching file path	
File Path String	
File Path Operator	
Equal	-
 Search for matching file name File Name String 	
*.exe *.ocx *.dll *.sys *.drv *.msc *.cpl *.vxd	
File Name Operator	
Case Insensitive Wildcard	•
<u>Save</u> <u>Cancel</u>	

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.

Select Configurat	lion
	uration to all systems
	guration to current system guration to selective systems
Here a second connig	guiden to colocitro systems
-Merge Configuration	n Options
💿 Overwrite	
	ve the selected configuration section(s) completely uration section(s) from the loaded configuration.
	and on section (s) from the loaded conligeration.
C Merge	
	nove the selected configuration section(s) I the configuration section(s) from the loaded
configuration.	
-Configuration Selec	tion
Filters	🥅 File Change Type
🔲 Change Type	Registry ChangeType
🔲 Checksum	🔲 Checksum Rules
🗖 Server	Event Configuration
Custon Colostian	
-System Selection—	
	Y
	>>> [
	<<
	>
1	
)K Cancel

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



📧 Select Configuratio	in	X	
	ration to all systems uration to current system uration to selective systems		
Merge Configuration	Options		
© Overwrite			
	e the selected configuration section(s) completely ation section(s) from the loaded configuration.		
C Merge			
	we the selected configuration section(s) he configuration section(s) from the loaded		
Configuration Selection	on		
Filters	🔲 File Change Type		
🗖 Change Type	Registry ChangeType		
Checksum	🔲 Checksum Rules		
E Server	Event Configuration		
System Selection	⊂ System Selection		
	v		
	>>		
	>		
	<		
<u> </u>	<u>C</u> ancel		

- 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.

💀 System Configuration -	NTPLDTBLR163	\times
Change Type Fil System Configuration	e Change Type Registry Change Type Checksum Checksum Rules Filters Monitor Specific Registry Monitor Specific Folder(s)	
Schedule Snapshot Start Time: 02 - : Apply configuration	00 Frequency: Daily Snapshot Limit: 64	
Server Information		
Port:	14502	
Event Configuration		
Snapshot Results:	 Log into local event log Send directly to EventTracker as Traps 	
EventTracker Server:	127.0.0.1 Port 14505	
	<u>Q</u> K <u>C</u> ancel	



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'.	
	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.	
Log into the local event log	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.	



		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.
	Send directly to Netsurion Open XDR as Traps	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.



System Configuration - NTPLDTBLR163 ×				
Change Type Fi	le Change Type Registry Change Type Checksum Checksum Rules			
System Configuration	Filters Monitor Specific Registry Monitor Specific Folder(s)			
Schedule Snapshot Start Time: 02 🖵 :	00 • Frequency: Daily • Snapshot Limit: 64 •			
Server Information	nanager.			
Server:	NTPLDTBLR163			
Port:	14502			
Event Configuration				
Snapshot Results:	 Log into local event log Send directly to EventTracker as Traps 			
EventTracker Server:	127.0.0.1 Port 14505			
	<u>D</u> K <u>C</u> ancel			

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

👼 System Configuration -	NTPLDTBLR163			×
Change Type Fi System Configuration	e Change Type Filters	Registry Change Type Monitor Specific Reg	Checksum gistry Mo	Checksum Rules
Schedule Snapshot Start Time: 02 - :	00 V Frequency	^{y:} Daily	Snapshot Limit:	64 💌
Server Information				
Port:	14502			
- Event Configuration				
Snapshot Results:	 Log into local event Send directly to Event 	-		
EventTracker Server:	127.0.0.1		Port: 14505	
	<u>0</u> K	<u>C</u> ar	ncel	

Change Audit displays the dialog box as shown below:



EventTracker - Change Browser 🛛 🔀				
You have changed the configuration of a remote syst Do you want to apply the changes?				
	<u>Yes</u> <u>N</u> o			

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.

🐺 Configuration Status	×
Apply Configuration Succeeded	7
Configuration changes were successfully applied to:	
ESXWEBDOC	
WEBDOC1	
WEBDOC2	
Configuration changes could not be applied to:	
<u>0</u> K	

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.

2	System Configuration -	NTPLDTBLR163	×	
	Change Type Fi System Configuration	le Change Type Registry Change Type Checksum Checksum Rule Filters Monitor Specific Registry Monitor Specific Folder(s)		
	Schedule Snapshot	00 V Frequency: Daily V Snapshot Limit: 64 V		
	Apply configuration			
	Server Information			
	🔽 Send snapshot to	nanager.		
	Server:	NTPLDTBLR163		
	Port:	14502		
	Event Configuration			
	Snapshot Results:			
	EventTracker Server:	127.0.0.1 Port 14505		
L				
		<u>D</u> K <u>C</u> ancel		

🐺 System Configuration ·	MCLOON
System Configuration Filter	s Change Type File Change Type Registry Change Type Checksum Checksum Rules
Automation	
Start Time: 02 💌 :	00 V Frequency: Daily V Snapshot Limit: 64 V
Apply configuration	
1 Apply conliguration	to an systems
Server Information	
Send snapshot to r	nanager.
Server:	ESXWEBDOC
Port:	14502
Event Configuration	
Snapshot Results:	C Log into local event log
	C Send directly to EventTracker as Traps
EventTracker Server:	127.0.0.1 Port 14505
	QK Cancel



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'.

	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.
Log into the local event log	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.



→ 🖻 📧 😭 🔂	Application 2	2.402 augst/s)				-	_		_
Application		/ beat				1.2	1		
Security System	Туре	Date	Time	Source	Category	Event	User	Computer	
System	Information	8/10/2010	2:06:54 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
Internet Explorer	Information	8/10/2010	2:06:51 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
	Information	8/10/2010	2:06:48 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
		8/10/2010	2:06:46 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
	Information	8/10/2010	2:06:44 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
	Information	8/10/2010	2:06:41 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
	Information	8/10/2010	2:06:39 PM	EventTracker	Disk	3279	nirmal	WEBDOC1	
	Information	8/10/2010	2:04:51 PM	EventTracker	None	3413	SYSTEM	WEBDOC1	
	Information	8/10/2010	2:04:03 PM	EventTracker	None	3412	SYSTEM	WEBDOC1	
		8/10/2010	2:04:00 PM	EventTracker	None	3407	SYSTEM	WEBDOC1	
	🔥 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	🚺 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3404	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	2.02 2.02	2:04:00 PM	EventTracker		3405	SYSTEM	WEBDOC1	
	Warning Warning	8/10/2010			None				
		8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	🔔 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	🔔 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	🔔 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	🚺 🙆 Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	
	Warning	8/10/2010	2:04:00 PM	EventTracker	None	3405	SYSTEM	WEBDOC1	

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

vent Pro	perties			?
Event				
D <u>a</u> te:		222	EventTracker	+
Ti <u>m</u> e:	2:04:00 PM	- 영양 같은 사람과 주변이		-
Concernence of the second	Information	그 맛있는 아니는 것은 구매했어.		
	NT AUTHO	RITY\SYST	EM	E
C <u>o</u> mpute	r: WEBDOC1			
Descripti	op:			
Keys Ac Keys Ma Keys Da Authoriz Unautho Configu System:	odified: 49 eleted: 0 ed: 0 prized: 0 ration: 0			
Data: (● <u>B</u> ytes ○ <u>W</u> e	ords		
				~ ~
		()K Cancel	Apply

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

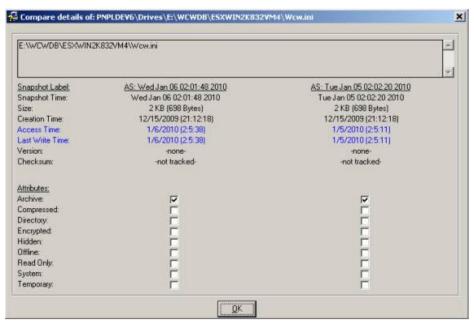
"E:\WCWDB\ESXWIN2k832VM4\wcw.ini' before adding the filters.

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

Previous Snapshot: 2010-01-05T02:02:20



E:\WDWDB\PNPLDEV	6\Wow.ini		
Snapshot Labet	AS: Wed Jan 06 02:01:48 2010	AS: Tue Jan 05 02:02:20 2010	
Snapshot Time:	Wed Jan 06 02:01:48 2010	Tue Jan 05 02:02:20 2010	
Size:	2 KB (1195 Bytes)	2 KB (1195 Bytes)	
Creation Time:	12/15/2009 (21:7:41)	12/15/2009 (21:7:41)	
Access Time:	1/6/2010 (2:1:27)	1/5/2010 (2:1:30)	
Last Write Time:	1/6/2010 (2:1:27)	1/5/2010 (2:1:30)	
Version:	-none-	none-	
Checksum:	-not tracked-	-not tracked-	
Attributes:			
Archive:	v	v	
Compressed:	Г	_	
Directory:			
Encrypted:	Г		
Hidden:	E .	_	
Offine:	Г	—	
Read Only:	Г	F	
System:	Г	Г	
Temporary:	Г	Г	



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



E:\WCWDB\PNPLDEV	6\Wcw.ini	
Snapshot Labet	AS: Wed Jan 06 02:01:48 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 02:01:48 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (1195 Bytes)	2 KB (1195 Bytes)
Creation Time:	12/15/2009 (21:7:41)	12/15/2009 (21:7:41)
Access Time:	1/6/2010 (2:1:27)	12/24/2009 (2:4:12)
Last Write Time:	1/6/2010 (2:1:27)	12/24/2009 (2:4:12)
Version	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	v	
Compressed:	_	
Directory:		
Encrypted:	_	E I
Hidden:		
Offline:		
Read Only:		Г
System:	Г	
Temporary:	F	Г

E:\WCWDB\ESXWIN2	K832VM4\Wcw.mi	
Snapshot Labet	AS: Wed Jan 06 02:01:48 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 02 01:48 2010	Thu Dec 24 02:04:42 2009
Size: Creation Time:	2 KB (698 Bytes)	2 KB (697 Bytes)
Access Time:	12/15/2009 (21:12:18) 1/6/2010 (2:5:38)	12/15/2009 (21:12:18) 12/24/2009 (2:4:11)
Access Time: Last Write Time:	1/6/2010 (2:5:38)	12/23/2009 (23.4:38)
Version	none-	12/23/2009 (23.4.50) -none-
Checksum	-not tracked-	-not tracked-
Attributes: Archive: Compressed: Directory: Encrypted: Hidden: Offine: Read Only: System:		

3. Add a customized filter to the folder "wcwdb\pnpldev6'.



Filter Name .err .tmp .www.db\pnpidev6 .www.db\pnpidev6 .tmp .two Existing Filters. Check and click 'Remove' to UnFilter checked rules. .memove .tmp .tmp .two .tmp .two	r files	[
err Imp wowdb\pppldev6 wowdb\pppld		
the two devices and click 'Remove' to UnFilter texisting Filters. Check and click 'Remove' to UnFilter texe and then click 'Add' button. If all the 'exe' files has to be filtered out enter texe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter ter the file folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.		ĺ –
		i
Existing Filters. Check and click 'Remove' to UnFilter checked rules. Remove ther the file/folder name to filter it. If all the 'exe' files has to be filtered out enter we' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter imp' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter we' and then click 'Add' button. If directories has to be filtered out then enter lder\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.		
Existing Filters. Check and click 'Remove' to UnFilter Remove Existing Filters. Check and click 'Remove' to UnFilter Remove The term of the file/folder name to filter it. If all the 'exe' files has to be filtered out enter twe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter mp' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter lder\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.		
hter the file/folder name to filter it. If all the 'exe' files has to be filtered out enter xe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter mp' and then click 'Add' button. If directories has to be filtered out then enter Ider\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.		
hter the file/folder name to filter it. If all the 'exe' files has to be filtered out enter xe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter mp' and then click 'Add' button. If directories has to be filtered out then enter Ider\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.	nd click 'Remove' to UnFilter	1
xe' and then click 'Add' button. If all the 'temp' folders has to be filtered out ente mp' and then click 'Add' button. If directories has to be filtered out then enter Ider\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.	Re <u>m</u> ove	
xe' and then click 'Add' button. If all the 'temp' folders has to be filtered out ente mp' and then click 'Add' button. If directories has to be filtered out then enter Ider\sub_folder name e.g. 'temp\installer' will filter out all the files in cwtemp\installer, etwtemp\installer, windowstemp\installer, etc. Add File or Folder to Filter.		
	outton. If all the 'temp' folders has to be filtered out ent	er
	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in	er
	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in p\installer, windowstemp\installer, etc.	er
<u>800</u>	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in p\installer, windowstemp\installer, etc.	er
	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in p\installer, windowstemp\installer, etc. Iter.	
	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in p\installer, windowstemp\installer, etc. Iter.	er
ok	button. If all the 'temp' folders has to be filtered out ent button. If directories has to be filtered out then enter g. 'temp\installer' will filter out all the files in p\installer, windowstemp\installer, etc. Iter.	er

4. Add a normal filter to filter the folder "E:\WCWDB\ESXWIN2k832VM4\'.

💀 System Configuration - NTPI	DTBLR163		×
Change Type File Cha System Configuration	nge Type Registry Ch Filters Monitor	ange Type Checks Specific Registry	um Checksum Rules Monitor Specific Folder(s)
Name		Absolute Path	
ESXWIN2K832VM4	Drives\E:\WCWD	B\ESXWIN2K832VM4	
Check and click 'Remove' to Ur To filter right click on a folder or		vser and select the option	
			Remove
			<u>R</u> emove
	<u>0</u> K	<u>C</u> ancel	

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.



	and Change Browser					1814 A
Autom 1		which there				
	Corpora (and Souther IN 114040 2010		-			
NUMBER OF	Taking mis official file parts	PARTY CONTRACTOR	2			
	A S PHODE	The large	48.3548.0018.18.48.48.2911	45 Yorkin: # 19,0194,221	Loc Hulled Tex.	
1 1 L.	T (3 Iver	por mes		The state is stated as		
MERCIN	# C + C #					
5	11 T E					
INNINAL	a car a caracteristic					
	Cal Directio					
25	il 25ant 10 V Shanful					
arianian .	10 CT					
100	in 🕞 Schlege					
PARTIN	ili 🔮 SilVeistagin ili 🍑 Leterillativa					
and the second	H T WOULD					
PHYLICIA	C310553-015540					
-	ESI-MATANT ESSEMEN					
1111	T meatow					
	2158					
3	E a faces					
Shid Kitte	- W MEY LIKE MIDNE					
	A HIEY OWN					
P-188er: 152		the PSA	8 Table	2 Time		Tabal (Australiand U
	COULT AND	ISTO IN THE REAL	1000			Market all researchers

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



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

E:\WDWDB\ESXWIN2	K832VM4\Wcw.ini	
Snapshot Labet	AS: Wed Jan 06 16:56:12 2010	AS: Wed Jan 06 15:40:48 2010
Snapshot Time:	Wed Jan 06 16:56:12 2010	Wed Jan 06 15:40:48 2010
Size:	2 KB (696 Bytes)	2 KB (698 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (16:44:46)	1/6/2010 (2:5.38)
Last Write Time:	1/6/2010 [13:57:17]	1/6/2010 (2:5:38)
Version:	-none-	none
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	5	2
Compressed:	E C	
Directory:		
Encrypted	Г	_
Hidden:	F	—
Offine:	Г	F
Read Only:	Г	E .
System:	Г	Г
Temporary:	Г	Г

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

E:\WCWDB\PNPLDEV	6/Wow.m	
Snapshot Labet Snapshot Time: Size: Creation Time: Access Time: Last Write Time: Version: Checksum:	<u>AS: Wed Jan 06 16:56:12 2010</u> Wed Jan 06 16:56:12 2010 2 KB (1195 Bytes) 12/15/2009 (21:7.41) 1/6/2010 (16:56.6) 1/6/2010 (16:56.6) none- -not tracked-	AS: Thu Dec 24 02:04:42 2009 Thu Dec 24 02:04:42 2009 - Not Present - - Not Present -
Attributes: Archive: Compressed: Directory: Encrypted Hidden: Offine: Read Only: System: Temporary:	BLLLLLL	

E:\WCWDB\ESXWIN2	K832VM4\Wcw.ini	
Snapshot Labet	AS: Wed Jan 06 16:56:12 2010	AS: Thu Dec 24 02:04:42 2009
Snapshot Time:	Wed Jan 06 16:56:12 2010	Thu Dec 24 02:04:42 2009
Size:	2 KB (696 Bytes)	2 KB (697 Bytes)
Creation Time:	12/15/2009 (21:12:18)	12/15/2009 (21:12:18)
Access Time:	1/6/2010 (16:44:46)	12/24/2009 (2:4:11)
Last Write Time:	1/6/2010 [13:57:17]	12/23/2009 (23:4:38)
Version:	-none-	-none-
Checksum:	-not tracked-	-not tracked-
Attributes:		
Archive:	5	₹
Compressed:	F	Г
Directory:	E	
Encrypted	F	—
Hidden:	F	
Offine:	Г	Г
Read Only:	Г	
System:	פרררר	_
Temporary:	E.	_



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.

💀 Customizing filters for files 🛛 🛛 🗙
]
Filter Name
mcscan32.dl
.tmp
.err
Existing Filters. Check and click 'Remove' to UnFilter Remove
'exe' and then click 'Add' button. If all the 'temp' folders has to be filtered out enter 'temp' and then click 'Add' button. If directories has to be filtered out then enter folder\sub_folder name e.g. 'temp\installer' will filter out all the files in wcwtemp\installer, etwtemp\installer, windowstemp\installer, etc.
Add File or Folder to Filter.
Add
οĸ

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.

Change Type	File Change Type 📔 Reg	istry Change Type	Checksum	Checksum Rule
System Configuratio	n Filters	Monitor Specific Registry	Monito	or Specific Folder(s)
Name		Absolute Path		
D C:	Drives\C:			
Check and click 'Remo	ove' to UnFilter checked nodes.			
	ove' to UnFilter checked nodes. folder or registry key in the chan	ge browser and select the	option.	
		ge browser and select the		nove
		ge browser and select the		nove

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:

EventTra	cker - Change Browser 🛛 🔀
?	This configuration change will be saved locally. To propagate it to the remote system please select [Options Apply Configuration]. Do you want to apply locally?
	<u>Yes</u> <u>N</u> o

- 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.

Select Configuration	n	
	ration to all systems uration to current system uration to selective systems	
Merge Configuration Overwrite	Options]
	 the selected configuration section(s) completely ation section(s) from the loaded configuration. 	
completely and add t configuration.	ove the selected configuration section(s) the configuration section(s) from the loaded	
Configuration Selecti		٦
Filters	File Change Type	
🗖 Change Type		
Checksum	Checksum Rules	
E Server	Event Configuration	
System Selection		
<u> </u>		

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.

1	System Config	uration - NTF	PLDTBLR163					×
	Change Type System Config		ange Type Filters	 Change Type tor Specific Rej		necksum Monit	Checksum Rule tor Specific Folder(s)	
	Name		Drives\C:	Absolute Path	h			
	Check and click To filter right clicl			rowser and sele	ect the op	tion.		
						<u>B</u> e	emove	
			<u>0</u> K	<u>C</u> a	ncel			

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)**.



EventTra	cker - Change Browser 🛛 🔀
2	A 'Global Filter' is applied to all managed (EventTracker - Change Audit) systems in the enterprise. To propagate this setting to all systems, please select [Options Apply Configuration Apply global configuration to all systems].
	Do you want to keep this setting?
	<u>Yes</u> <u>N</u> o

- 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.

Global Configura	tion		>
Change Type	File Change Type Registry Change Type C	Checksum Ch	necksum Rules
General	File Types Monitor Specific Registry Mon	nitor Specific Folder	Filters
Name	Absolute Path		~
My Download Files		1	
My Installations	Drives\\$(R00T_DRIVE)\My Installations		
	Drives\\$(ROOT_DRIVE)		
			~
<			>
	emove' to UnFilter checked nodes. on a folder or registry key in the change browser and select the or	ption.	
		ption. <u>R</u> emove	

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.



Select Configurati	ion		
Apply global configu	uration to all sys	stems	
Apply system config			
Apply system config	juration to selec	ctive systems	
Merge Configuration	Options		
Overwrite			
		configuration section(s) com	
and add the configu	ration section(s	s) from the loaded configurati	on.
C Merge			
		ed configuration section(s)	
completely and add configuration.	the configuration	on section(s) from the loaded	
Configuration Select	tion		
Filters	🔲 File Cha	ange Type	
Change Type	🗖 Registr	y ChangeType	
Checksum	Checks	sum Rules	
Server	Event (Configuration	
001701		sonngaradon	
System Selection			
	Y		
, 			_
	<	< _	
		<u>, </u>	
	<		
	K	<u>C</u> ancel	

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



Overwrite Overwrite will remove the selected configuration section(s) complete and add the configuration section(s) from the loaded configuration. C Merge Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration. Configuration Selection Filters Filters File Change Type Checksum Checksum Checksum Server Event Configuration System Selection	-Merge Configuration	n Options
and add the configuration section(s) from the loaded configuration. Merge Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration. Configuration Selection Filters Filte Change Type Change Type Registry Change Type Checksum Checksum Checksum Rules Server Event Configuration System Selection	© Overwrite	
Merge will NOT remove the selected configuration section(s) completely and add the configuration section(s) from the loaded configuration. Configuration Selection Filters File Change Type Change Type Registry Change Type Checksum Checksum Rules Server Event Configuration		
completely and add the configuration section(s) from the loaded configuration. Configuration Selection Filters File Change Type Change Type Registry Change Type Checksum Checksum Rules Server Event Configuration	C Merge	
Filters File Change Type Change Type Registry Change Type Checksum Checksum Rules Server Event Configuration	completely and add	
Change Type Registry Change Type Checksum Checksum Event Configuration System Selection	- Configuration Selec	tion
Checksum Checksum Rules Server Event Configuration System Selection	Filters	🥅 File Change Type
Server Event Configuration System Selection	🔲 Change Type	🔲 Registry ChangeType
System Selection	🗖 Checksum	🔲 Checksum Rules
	🗖 Server	🔲 Event Configuration
<<	System Selection—	
<<		_
		>>
\rightarrow		
		>
2		
		<

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.

🐺 Configuration Status	X
Apply Configuration Succeeded	
Configuration changes were successfully applied to:	
ESXWEBDOC	
WEBDOC1	
WEBDOC2	
Configuration changes could not be applied to:	
<u> </u>	

9. Click **OK**.

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



🐺 Configuration Status 🛛 🛛 🛛
Apply Configuration Succeeded
Configuration changes were successfully applied to:
ESXWEBDOC WEBDOC1
Configuration changes could not be applied to:
WEBDOC2
<u>D</u> K

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.

EventTracker - Change Browser 🛛 🛛 🔀					
?	This configuration change will be saved locally. To propagate it to the remote system please select [Options Apply Configuration]. Do you want to apply locally?				
	<u>Y</u> es <u>N</u> o				

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



Apply system config	uration to selective systems	
Merge Configuration	Options	
© Overwrite		
	e the selected configuration section(s) completel ration section(s) from the loaded configuration.	
C Merge		
completely and add	ove the selected configuration section(s) the configuration section(s) from the loaded	
configuration.		
Configuration Select	tion	
Filters	File Change Type	
🗖 Change Type	Registry ChangeType	
🗖 Checksum	🗖 Checksum Rules	
F Server	Event Configuration	
System Selection —		
System Selection		
	<u> </u>	
	>>	
	<<	
	<u>></u>	
	1	

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

EventTracker - Change Browser 🛛 🗙				
(Configuration changes applied successfully.			
	ОК			

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.



ì.	System Configuration - N	PLDTBLR163				×
	Change Type File (System Configuration		try Change Type Ionitor Specific Regis	Check	 Checksum Rules r Specific Folder(s)	
	Name	Drives\C:	Absolute Path			
	Check and click 'Remove' to UnFilter checked nodes. To filter right click on a folder or registry key in the change browser and select the option.					
		<u>0</u> K	<u>C</u> ano	el		

- 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.

	EventTracker - Change Browser 🛛 🔀
	You have changed the configuration of a remote system. Do you want to apply the changes?
	<u>Y</u> es <u>N</u> o
13. Click Yes.	
	EventTracker - Change Browser
	Configuration settings applied successfully.
	ОК

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.
- 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.

EventTra	cker - Change Browser 🛛 🔀
2	This is a 'Global Filter'. To propagate this setting to all systems, please select [Options Apply Configuration Apply global configuration to all systems].
	Do you want to keep this setting?
	<u>Y</u> es <u>N</u> o

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.

EventTra	cker - Change Browser 🛛 🗙
i	You can restore only a subtree at a time, not the entire registry.
	OK

- 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.



👰 Restore	×
Restore registry subtree of sys WEBDOC1\Registry\HKEY_L	em 'WEBD0C1' starting from key .0CAL_MACHINE' .
and values that were deleted.	particular snap will restore the keys / modified, it will also delete the ie snap was taken. This may cause g.
<u>R</u> estore	<u>C</u> ancel

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

🔲 Event	Tracker - Change Browser 🛛 🛛 🔀
2	Are you sure you want to proceed with the restore operation?
	Yes O

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.

EventTra	cker - Change Browser 🛛 🔀
i	This option allows you to undo the previous restore operation performed on the registry. To proceed you must be in the registry tree.
	OK

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**.

Change Type Fi	ile Change Type 📔 Registry Change Type 📔 Checksum 🗍 Checksum Rule:
System Configuration	Filters Monitor Specific Registry Monitor Specific Folder(s)
Schedule Snapshot	
Start Time: 02 💌 :	: 00 V Frequency: Daily Snapshot Limit: 64 V
Apply configuration	n to all systems
Server Information	
🔽 Send snapshot to i	manager.
Server:	R1S5-VM4
Port:	14502
Event Configuration	
	C Log into local event log
Snapshot Results:	C Send directly to EventTracker as Traps
Snapshot Results: EventTracker Server:	C Send directly to EventTracker as Traps 127.0.0.1 Port

- 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.



Change Type File Cl	nange Type	Registry Change Type	Checksum	Checksum Rule
System Configuration	Filters	Monitor Specific Regis	try Moni	tor Specific Folder(s)
older Path(s):				
				Add
				<u></u> <u>A</u> aa
				Modify
				Distate
				Delete
elect to track only above cor	nfigured folder(s) with	subfolder(s), It will track all	folder(s) if not selec	ted.
Track Only Above Mentior	ned Folder Path(s).			
		ny of the parent folder is filte	red in sustem/aloba	configuration
	iot de mortituleu li ar	iy or the parent tolder is tille	reu in system/gioba	r coninguration.

5. Browse the Folder path.

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

🐂 Include Fo	lder To Monitor		_ 🗆 🗙
Folder(s) will not Please remove it	be monitored, if they are in the Global from filter list.	I/System filter list.	
Absolute Path/ F	older Name 💿 Absolute Path 🔿	Folder Name	
Folder Path:	E:\virus total		
		Add	Cancel

6. Click Add.

🗛 System Configuration - R153¥M1	X
Change Type File Change Type Registry Change Type Checksum Checksum Rules System Configuration Filters Monitor Specific Registry Monitor Specific Folder(s)	
Folder Path(s):	11
E:\virus total	
Select to track only above configured folder(s) with subfolder(s), It will track all folder(s) if not selected. Track Only Above Mentioned Folder Path(s). NDTE : Configured folder will not be monitored if any of the parent folder is filtered in system/global configuration.	
<u>O</u> K <u>Cancel</u>	



- 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.



'olicyName	- File Details	1	1	[1
ample Critical File Policy	File C:\WINDOWS\system32\find.exe	Description Found integrity	Size 9216	Version 5.1.2600.0	Checksum 2329F2C682
	C:\WINDOWS\system32\trail.exe	Found integrity	42496	5.1.2600.5512	4112AA01C1
	C:\WINDOWS\system32\notepad.exe	Found integrity	42436 69120	5.1.2600.5512	7A90F8B051
	C:\WINDOWS\system32\nslookup.exe	Found integrity	76800	5.1.2600.5512	D3E9558130
	C:\WINDOWS\system32\print.exe	Found integrity	9216	5.1.2600.0	2F2AD17264
	C:\WINDOWS\system32\regedt32.exe	Found integrity	3584	5.1.2600.0	DEB00B2DB
	C:\WINDOWS\system32\route.exe	Found integrity	19968	5.1.2600.0	31282AD 39F
		r oand mogility	13300	0.1.2000.0	01202AD 001
	Select All Remove Add Item Registry Details	Edit <u>D</u> escription			
		Edit <u>D</u> escription	Description	Data	
	Registry Details		Description	Data	
	Registry Details		Description	Data	

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

lease enter proper policy n	ame and description of policy.			
olicy Name				
olicy Description				A

- 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.



elect Policy Type	۶ <u>ــــــــــــــــــــــــــــــــــــ</u>
Policy Name:	ET
	Item type
	Add file
	This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.
	C Add particular folder
	This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory.
	C Add folder and sub-folder
	This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories
	C Search for Registry Key in HIVE
	This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

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.



EventTracker - 9	elect the file nan	ne				? ×
Look jn:	🧇 Local Disk (C	:)		•	- 🗈 💣	
My Recent Documents Desktop My Documents My Computer	Documents an ET & PULSE Pri LOGFILES DI LOGFILES Program Files WINDOWS WINDOWS WINDOWS UNINCOWS Commonstall.log ETRSSLog.txt GDIPFONTCAC netflowsim.exc	HEV1.DAT				
My Network Places	File <u>n</u> ame: Files of <u>t</u> ype:	All Files(*.*)	ad-only		•	<u>O</u> pen Cancel

- 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.

ve and :k in all th
k in all th
_

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.

File C:\Program Files\P	rism Microsystems\EventTracker\	Description Ag	Size 200432	Version	Checksum
			200432	7.0.0.103	D9C1E84AD44
(1	Þ
Select All	1				
	amoye Add Item	Edit Description			
ecistru Details					
		Value	Description	Data	
riegisty key		Value	Description		
Select All R	emove Add Item	Edit Description			
		Select <u>A</u> ll <u>Remove</u> <u>A</u> dd Item egistry Details	Select <u>All</u> <u>Remove</u> <u>Add Item</u> Edit <u>Description</u>	Select <u>All</u> Remove <u>Add Item</u> Edit <u>Description</u>	Select <u>All</u> <u>Remove</u> <u>Add Item</u> Edit <u>Description</u>

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.

New Stracker - Configuration Policy Editor	×
Please double click on the folder name for selecting it C:\ Documents and Settings ET & PULSE Prerequisites Inetpub LOGFILES Logs Program Files WINDOWS wmpub	Cancel
Drives	

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



File Search	h						
You have directories.	an option to keep the file name same a s.	along with existing drive lette	r and directories associa	ated with it. W	hen you compare this p	olicy it will compare same	e drive and
Sometime I drive.	file and directory may not be located th	ie same drive you can rem	iove the drive from begin	nning of the file	e so when it compare file	e in other system, it will c	heck in all th
e.g. a. if yo	ou have entered c:\program files\SQL'	\abcd.exe, when it will searc	ch "abod.exe" file into io	::\program file:	s\SQL		
b. If you ha	ave entered \program files\SQL\abcd.	exe, when it will search "abo	d.exe" in all the drives a	and the it will s	earch for \program files	SQL for "abcd.exe"	
c. If you ha	ave entered abcd.exe, it will search ab	cd.exe in all the directories a	and drive				
C:\Progra	ram Files\Prism Microsystems\Ev	entTracker\					
F 11.	C:\Program Files\Prism Microsyster	ns\EventTracker\					Search
Folder		ms\EventTracker\	Circ	Moreion	Chook Sum	Crosted At	Search
Folder	C:\Program Files\Prism Microsyster	ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search
Folder		ms\EventTracker\	Size	Version	Check Sum	Created At	Search

- 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.



-File Search	h 					
You have a directories.	an option to keep the file name same along with existing drive letter and directorio	es associate	ed with it. Wi	hen you compare this policy it wi	ill compare same drive an	d
Sometime fi drive.	ile and directory may not be located the same drive you can remove the drive l	from beginni	ing of the file	e so when it compare file in othe	r system, it will check in a	dl tł
e.g. a. if yo	u have entered ic:\program files\SQL\abcd.exe, when it will search "abcd.exe"	file into lc:∖	program files	s\SQL		
b. If you ha	we entered \program files\SQL\abcd.exe, when it will search "abcd.exe" in all th	ne drives an	d the it will s	earch for \program files\SQL fo	or "abcd.exe"	
	we entered abcd.exe. it will search abcd.exe in all the directories and drive					
c. Il you na	ve enteleu abculexe, it will search abculexe in all the ullectories and ullve					
DI	- A service Clarific Collinguation File (Drive Missession) - (Free Ta					
Please W	ait saving file info : C:\Program Files\Prism Microsystems\EventTra	ackervale	rtmsg.exe			
	C:\Program Files\Prism Microsystems\EventTracker\				Searc	:h
Folder	C:\Program Files\Prism Microsystems\EventTracker\				Searc	:h
Folder	C:\Program Files\Prism Microsystems\EventTracker\ File Name	Size	Version	Check Sum	Created At	h
Folder		Size 165896	Version 1.1.1.4	Check Sum 684E8CDAC32DE506820		
Folder	File Name		_		Created At 5/22/2008 8:24:42 PM	-
Folder	File Name ☑ C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll	165896	1.1.1.4	684E8CDAC32DE506B20	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM	1
Folder	File Name ✓ C:\Program Files\Prism Microsystems\E ventTracker\WebChart.dll ✓ C:\Program Files\Prism Microsystems\E ventTracker\UserActivity.exe	165896 447728	1.1.1.4	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM	- 1 -
Folder	File Name C:\Program Files\Prism Microsystems\E ventTracker\WebChart.dll C:\Program Files\Prism Microsystems\E ventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\E ventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\E ventTracker\UserActivity.exe	165896 447728 574770	1.1.1.4 7.0.0.0 -NA-	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM 10/19/2006 7:13:20	1 1 1
Folder	File Name C:\Program Files\Prism Microsystems\E ventTracker\WebChart.dll C:\Program Files\Prism Microsystems\E ventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\E ventTracker\Suspicious_Port C:\Program Files\Prism Microsystems\E ventTracker\Suspicious_Port C:\Program Files\Prism Microsystems\E ventTracker\Suspicious_Port	165896 447728 574770 180185	1.1.1.4 7.0.0.0 -NA- -NA-	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08 5264EC2C4F15288C3146	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM 10/19/2006 7:13:20 2/22/2008 7:56:44 PM	1 1 1
Folder	File Name C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll C:\Program Files\Prism Microsystems\EventTracker\Suspicious_Port	165896 447728 574770 180185 55304 6319	1.1.1.4 7.0.0.0 -NA- -NA- 2.0.50	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08 5264EC2C4F15288C3146 EE192A49298C8AA6EE5	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM 10/19/2006 7:13:20 2/22/2008 7:56:44 PM 4/4/2008 5:24:12 PM	1 1 1
Folder	File Name C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll C:\Program Files\Prism Microsystems\EventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\EventTracker\Supcious_Port C:\Program Files\Prism Microsystems\EventTracker\Slp-Translate.pdf C:\Program Files\Prism Microsystems\EventTracker\Slp-Translate.pdf C:\Program Files\Prism Microsystems\EventTracker\Slp-Translate.pdf C:\Program Files\Prism Microsystems\EventTracker\Negdsmexe C:\Program Files\Prism Microsystems\EventTracker\Negdsmexe	165896 447728 574770 180185 55304 6319	1.1.1.4 7.0.00 -NA- -NA- 2.0.50 -NA-	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08 5264EC2C4F15288C3146 EE192A49298C8AA6EE5 1FD5FBC13448001EF765	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM 10/19/2006 7:13:20 2/22/2008 5:24:12 PM 6/25/2009 9:51:10 PM	- 1 - 1 1 1
Folder	File Name C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll C:\Program Files\Prism Microsystems\EventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\EventTracker\Supcicus_Port C:\Program Files\Prism Microsystems\EventTracker\Supcicus_Port C:\Program Files\Prism Microsystems\EventTracker\Supcicus_Port C:\Program Files\Prism Microsystems\EventTracker\RegAsm.exe	165896 447728 574770 180185 55304 6319 21232	1.1.1.4 7.0.0.0 -NA- 2.0.50 -NA- 7.0.0.0	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08 5264E2C4F15288C3146 EE192A49298C8AA6EE5 1FD5FBC13448001EF765 5161B452C30FCB18F57A	Created At 5/22/2008 8:24:42 PM 7/28/2010 9:38:42 PM 10/19/2006 7:13:20 2/22/2008 7:56:44 PM 4/4/2008 5:24:12 PM 6/25/2009 9:51:10 PM 5/27/2010 4:31:50 PM	- 1 - 1 1 1
Folder	File Name C:\Program Files\Prism Microsystems\EventTracker\WebChart.dll C:\Program Files\Prism Microsystems\EventTracker\UserActivity.exe C:\Program Files\Prism Microsystems\EventTracker\Suspicious_Port C:\Program Files\Prism Microsystems\EventTracker\Suspicious_Port C:\Program Files\Prism Microsystems\EventTracker\Suspicious_Port C:\Program Files\Prism Microsystems\EventTracker\PrismSert C:\Program Files\Prism Microsystems\EventTracker\PrismSert C:\Program Files\Prism Microsystems\EventTracker\PrismSMMPGet.dll C:\Program Files\Prism Microsystems\EventTracker\PrismSMMPGet.dll C:\Program Files\Prism Microsystems\EventTracker\PrismSMMPGet.dll C:\Program Files\Prism Microsystems\EventTracker\PrismSMMPGet.dll	165896 447728 574770 180185 55304 6319 21232 1076	1.1.1.4 7.0.0.0 -NA- 2.0.50 -NA- 7.0.0.0 -NA-	684E8CDAC32DE506B20 DB39714C2DAEBABEBC0 F192FA752941B32379F08 5264E2C24F15288C3146 EE192A49298C8A46EE5 F161FBC13448001EF765 5161B452C30FCB16F76A 2EC956EE3F32AD0F99E3	Created At 5/22/2008 8:24:42 PM 7/28/2010 3:38:42 PM 10/19/2006 7:13:20 2/22/2008 7:56:44 PM 4/4/2008 5:24:12 PM 6/25/2009 3:51:10 PM 5/27/2010 4:31:50 PM 8/9/2010 11:10:48 AM	1 1 1 1 1

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

olicyName	File Details File Description	Size	Version	Checksum 🔺
r ample Critical File Policy	C:\Program Files\Prism Microsystems\EventTracker\W	165896	1.1.1.4	684E8CDAC
ample Unitical File Policy	C:\Program Files\Prism Microsystems\EventTracker\Us	447728	7.0.0.0	DB39714C2I
	C:\Program Files\Prism Microsystems\EventTracker\Su	574770	-NA-	F192FA7529
	C:\Program Files\Prism Microsystems\EventTracker\SI	180185	-NA-	5264EC2C4F
	C:\Program Files\Prism Microsystems\EventTracker\Re	55304	2.0.50727.42	EE192A4925
	C:\Program Files\Prism Microsystems\EventTracker\Re	6319	-NA-	1FD5FBC134
	C:\Program Files\Prism Microsystems\EventTracker\Pri	21232	7.0.0.0	5161B452C3 🗸
				Þ
	Select All Remove Add Item Edit Description Registry Details			
		Description	Data	
	Registry Details	Description	Data	



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.

	File Details				
licyName	File	Description	Size	Version	Checksum 4
mple Critical File Policy	C:\Program Files\Prism Microsystems\EventTracl	ker\Aq	200432	7.0.0.103	D9C1E84AD
Tiple Childar File Folicy	C:\Program Files\Prism Microsystems\EventTracl	ker\W	165896	1.1.1.4	684E8CDAC
	C:\Program Files\Prism Microsystems\EventTracl	ker\Us	447728	7.0.0.0	DB39714C2I
	C:\Program Files\Prism Microsystems\EventTracl	ker\Su	574770	-NA-	F192FA7529
	C:\Program Files\Prism Microsystems\EventTracl		180185	-NA-	5264EC2C4F
	C:\Program Files\Prism Microsystems\EventTracl		55304	2.0.50727.42	EE192A4925
	C:\Program Files\Prism Microsystems\EventTracl		6319	-NA-	1FD5FBC134
	▼ Select <u>A</u> ll Remove <u>A</u> dd Item Registry Details	Edit Description			•
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item	Edit <u>D</u> escription	Description	Data	<u> </u>
	Select <u>All</u> Remo <u>v</u> e		Description	Data	<u> </u>
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	
	☐ Select <u>A</u> ll <u>Remov</u> e <u>A</u> dd Item		Description	Data	

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.



Reg KeySearch				
Please enter a Key name	o be searched.			
Key Name				
-				Search
Registry Key				

- 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.

lease ente	a Key name to be searched.	
ey Name	EventTracker	
	HKEY_CURRENT_CONFIG\System\CurrentControlSet\SERVICES\RDPDD\DEVICE0	Sgarch
Registry K	ey l	A
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler\Enum	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTrackerScheduler\Security	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Scheduler	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter\Enum	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter\Security	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Reporter	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting\Enum	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting\Security	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Remoting	
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Receiver\Enum LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Receiver\Security	
	LOCAL_MACHINE \S151EIM \CurrentControlSet\Services\EventTracker Receiver	
	LOCAL_MACHINE (STSTEM CurrentControlSet\Services\EventTracker Indexer\Enum	
	LOCAL_MACHINE STSTEM Culter ControlSet/Services Levent Tacker Indexer/Security	
		•
	LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Indexer\Security LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventTracker Indexer	

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

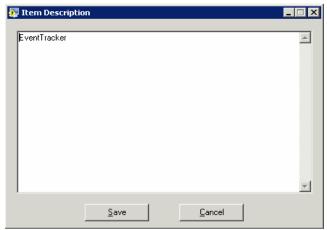


	- File Details				
PolicyName	File	Description	Size	Version	Checksum 🔺
ET	C:\Program Files\Prism Microsystems\EventTracker\A		10080	-NA-	CA8E6E885(
Sample Critical File Policy	C:\Program Files\Prism Microsystems\EventTracker\4		24576	7000	0023BBC955
	C:\Program Files\Prism Microsystems\EventTracker\4		149520	-NA-	7EDEE15A5(
	C:\Program Files\Prism Microsystems\EventTracker\A		415760	7.0.0.0	9AC45807CE
	C:\Program Files\Prism Microsystems\EventTracker\4		18448	7.0.0.0	2445401547
	C:\Program Files\Prism Microsystems\EventTracker\4		74256	7.0.0.0	4F8F39092E
	C:\Program Files\Prism Microsystems\EventTracker\4		174152	2.0.1126.0	CEEB22B4A
		Edit <u>D</u> escription	1		
	Remove Add Item Registry Details	Edit <u>D</u> escription	Description		
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry Key	Edit <u>D</u> escription	Description	Data	
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry Key HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros	Edit <u>D</u> escription	Description	Data	
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry Key HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros	Edit Description	Description		
	Registry Details Registry Details Registry CoCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros	Edit Description	Description	Data 0	
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry Key HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros	Edit Description	Description	0	
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SYSTEM\ControlSei001\S	Edit Description	Description	0 Root\LEGACY	
	Select <u>All</u> Registry Details Registry Details Registry Key HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism HKEY_LOCAL_MACHINE\SOFTWARE\Prism HKEY_LOCAL_MACHINE\SOFTWARE\Prism HKEY	Value 's 's s e 0	Description	0	
	Select <u>All</u> Remove <u>Add Item</u> Registry Details Registry LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SOFTWARE\Prism Micros HKEY_LOCAL_MACHINE\SYSTEM\ControlSei001\S	Edit Description Value %	Description	0 Root\LEGACY Root\LEGACY	

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.

Select Policy Typ	8
Policy Name:	ET
Γ	Item type
	Add file
	This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.
	C Add particular folder
	This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory
	C Add folder and sub-folder
	This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories
	C Search for Registry Key in HIVE
	This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

- 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.



lect Policy Typ	e
olicy Name:	
olicy Hame.	ET
ſ	Item type
	C Add file
	This option will allow you to select any file from the local system into policy. Policy will also capture file name, file size, file create date, file version, file modify date and checksum for the selected file name.
	C Add particular folder
	This option will allow you to select all the files within a particular directory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory
	C Add folder and sub-folder
	This option will allow you to select all the files within a particular directory and subdirectory. Policy will automatically capture all the files (file name, file size, file create date, file version, file modify date and checksum) within directory and subdirectories
	C Search for Registry Key in HIVE
	This option will allow you to add any key into policy. Policy will capture all the sub level keys, values and data

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.
- 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.



Policy Name ET		 		<u> </u>
Sample Critical File Policy				

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

ALL COMPUTERS ESSWEBDOC WEBDOC1 WEBDOC2	▲dd Add All Bemove Rgmove All	
--	--	--

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.



olicy Name	ET		
System	Policy Item	Search Status	
ESXWEB WEBDOC1	Policy Item: C:\Program Files\Prism Mi Policy Item: C:\Program Files\Prism Mi Policy Item: C:\Program Files\Prism Mi	Policy Item: C:\Program Files\Prism Microsystems\E ventTracker\AdvancedReports\MainPage Policy Item: C:\Program Files\Prism Microsystems\E ventTracker\AdvancedReports\Advanced Policy Item: C:\Program Files\Prism Microsystems\E ventTracker\AdvancedReports\Prism.Eve	
ompare Agen	t systems with the Manager's Configuration		

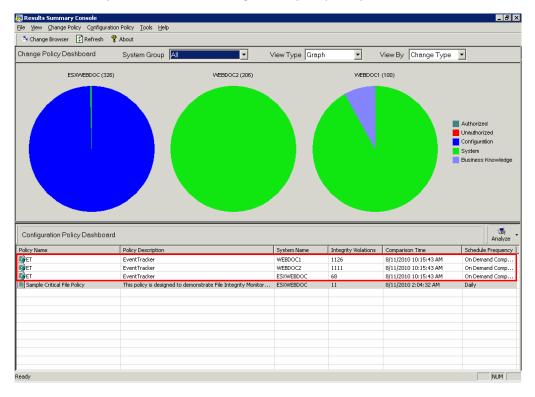
System	Policy Item	Search Status	
ESXWEB	Policy Item: C:\Program Files\Prism Mi	Compare Systems Dk - Msg From Client	
WEBDOC1	Policy Item: C:\Program Files\Prism Mi Policy Item: C:\Program Files\Prism Mi	Compare Systems Ok - Msg From Client Compare Systems Ok - Msg From Client	
WEBDOC2	Policy Item: C:\Program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

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



Change Assessment Results				
System Name: WEBDOC2		Policy Name: ET		
Total Violations: 1111		Compared On: 8/11/2010 10:15:4	43 AM	
EventTracker				
Item Location: HKEY_LOCAL_MACHIN		rolSet\Services\EventTracker Scheduk	er	
				,
Item Name	<u>N</u> ext	Policy Values	Actual Values	
2 Description		Used by EventTracker to initiate s	-NA-	
2 ObjectName	Previous			
2 DisplayName	Accept			
ErrorControl Start				
Start Type	<u>R</u> eject			
Type Description				
ObjectName	<u>I</u> gnore			
2 DisplayName		Item description not available!!		
? ErrorControl	Save	ten acceptor net available.		
2 Start	Save As			
7 Type	Jave As			
P Description	Run			
2 ObjectName				
2 ErrorControl	Report			
7 Start				
- ovar				
	▶ <u>M</u> ore Info			
	More Into			

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.
- 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.

Policy Comparison Scheduler			
Title	Policy Name	Frequency	Scheduled At
Default Schedule for Sample Critical Fil	Sample Critical File Policy	Daily	8/12/2010 2:00:00 AM
New Schedule <u>E</u> dit	<u>D</u> elete		<u>C</u> lose

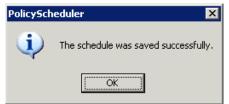
3. Click New Schedule. Change Audit displays the Policy Schedule window.

🖉 Policy Schee	lule	×
Title: Policy Name:	2003 Domain Controllers DISA-Platinum	- न
Systems:	ESXWEBDOC WEBDOC1 WEBDOC2 Add >>	
Start from	11-Aug-2010 10:30:52 AM	
Frequency:	Twice Daily	
Week Day:	Wednesday Save Cancel	

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.

itle	Policy Name	Frequency	Scheduled At
efault Schedule for Sample Critical Fil	Sample Critical File Policy	Daily	8/12/2010 2:00:00 AM
ventTracker	ET	Twice Daily	8/11/2010 5:00:00 PM

- 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 <u>www.netsurion.com</u>.

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