

NTP Software File Auditor™, Windows® Edition



An NTP Software® User Manual

Abstract

This manual details the method for using NTP Software File Auditor[™], Windows[®] Edition, from an administrator's perspective. Upon completion of the steps within this document, NTP Software File Auditor Windows Edition will be used to monitor file and directory operations for users within your enterprise community.

Rev 1.9, July 2015

The information contained in this document is believed to be accurate as of the date of publication. Because NTP Software[®] must constantly respond to changing market conditions, this document should not be interpreted as a commitment on the part of NTP Software[®], and NTP Software[®] cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. NTP SOFTWARE® MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

NTP Software[®], NTP Software File Auditor[™] and NTP Software Smart Policy Manager[™], are either registered trademarks or trademarks of NTP Software[®] in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

NTP Software®, 20A Northwest Blvd. #136, Nashua, NH 03063, USA

Contents

Setting NTP Software File Auditor, Windows Edition Properties5
Setting NTP Software File Auditor, Windows Edition Database5
Setting the NTP Software File Auditor, Windows Edition Email7
Setting the NTP Software File Auditor, Windows Edition Misc Options8
Setting the NTP Software File Auditor, Windows Edition Security Level
Policy Creation10
NTP Software File Auditor Reports17
NTP Software Smart Policy Manager™
NTP Software Smart Policy Manager Overview
Managing the NTP Software File Auditor Service through a NTP Software File Auditor Admin Client Running on a Different Machine
Installing the NTP Software Smart Policy Manager Admin Component
Installing the NTP Software File Auditor Admin Component
Installing NTP Software File Auditor in Clustered Environments40
About NTP Software [®] 43
NTP Software [®] Professional Services43

Introduction

Thank you for your interest in NTP Software File Auditor™, Windows® Edition.

NTP Software File Auditor, Windows Edition lets you monitor your users' file and directory operations. It lets you create and enforce file audit policies that enable you to monitor certain events taking place in your environment. Such events include directories created, renamed, and/or deleted and files opened for read, write, create, rename, delete, close, and move, as well as file permission changes and owner changes in your environment.

NTP Software File Auditor, Windows Edition has two main components:

- 1. NTP Software File Auditor Administrator.
- 2. NTP Software File Auditor Reports.

Each of the above components will be explained in further detail in the next sections.

NTP Software File Auditor, Windows Edition imposes no restrictions on how you monitor your file and directory operations. You can impose policies on individual files, directories, users, and/or groups of users.

To install NTP Software File Auditor, Windows Edition, a login with administrator rights is needed. You will be installing two different services: the NTP Software Smart Policy Manager service and the NTP Software File Auditor service.

Your hardware should be appropriate for the services running on each machine.

Setting NTP Software File Auditor, Windows Edition Properties

Setting NTP Software File Auditor, Windows Edition Database

The NTP Software File Auditor Properties tab enables you to set up several application properties including the application database. Your application database configuration should be adjusted before creating any file audit policies because all the events monitored through the File Auditor policies are saved to your configured database. To configure the database, please follow these steps:

- 1. Right-click **NTP Software File Auditor** under the main application container (**My Organization** in this example).
- 2. Click **Properties** on the pop-up menu.
- 3. On the **Database Configuration** tab, clear the **Inherit Database Configuration** box, enter the correct information in each of the text boxes as appropriate for your database, and click **OK**.

Note: "My Organization" is the main application container, so the database configuration specified here is inherited by any other server created within the tree. This saves the administrators from having to enter the database configuration manually.

TP Software File Audit	or™Configuration
Database Configuration	Email Configuration Misc. Options Security
🔲 Inherit database cor	nfiguration
Database Connection	
SQL Server Name:	CLTESTBOX
Database Name:	FileAuditorDB
- Authentication Typ	e
C SQL Authentic	ation
Username:	
Password:	
Windows Auther	entication
	Test Connection Maintenance
	OK Cancel <u>A</u> pply Help

4. Click the **Maintenance** button if you want to back up/delete old files to maintain the size of your database. This can be adjusted through the **Database Maintenance Settings** dialog box.

Notes:

- 1. The **DB Maintenance** option works on two levels, the server level and the policy level.
- 2. The **Export to SQL Server** option under the Required Action section enables you to specify another database to store the aging data. You can choose to enter server and database names, which could be different from the server and database storing the audited operations. Use the **Test** button to test the connection to the specified database on the specified server.

Database Maintenance Settings
Age Limit
Remove records older than: 3 Month(s)
Required Action
O Delete old records O Export as raw data
Export as XML Export to SQL Server
SQL Server:
Database: Tiest
Specify the number of records to be retained in the database (in thousands of records). When the record limit is reached, the oldest records will be removed as defined in the 'Required Action' below.
Maximum number of records allowed: 1000 Thousands
The maximum size of the database will be approximately
Required Action
Overwrite old records
Export Path:
OK Cancel

Setting the NTP Software File Auditor, Windows Edition Email

The NTP Software File Auditor[™] Properties tab enables you to set up several application properties, including the application emails. To adjust your NTP Software File Auditor[™] application email feature, please follow these steps:

- 1. Right-click NTP Software File Auditor under the main application container.
- 2. Click **Properties** on the pop-up menu.
- 3. Click the **Email Configuration** tab. Clear the **Inherit Email Configuration** box. Check the **Enable Email Notifications** option. Enter the correct information in each of the text boxes as appropriate for your email settings, and click **OK**.

Tip: Click the Test Connection butt	on to test your connection to the specified SMTP Sever.
NTP Software File	e Auditor™Configuration
Database Config	uration Email Configuration Misc. Options Security
🗖 Inher	it Email Configuration
Enat	ele Email Notifications
SMTP <u>S</u>	erver: SMTP SERVER NAME
SMTP <u>D</u>	omain: SMTP DOMAIN NAME
Sender's	Address: SENDER ADDRESS
	ly server requires authentication
<u>U</u> ser	name: SERVER USERNAME
User	Domain: USER DOMAIN
Pass	word:
Conf	irm Password:
	Test Mail Settings Status: Not sent yet
	OK Cancel Apply Help

Setting the NTP Software File Auditor, Windows Edition Misc Options

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application misc options. To adjust your NTP Software File Auditor application misc options, please follow these steps:

- 1. Right-click NTP Software File Auditor under the main application container.
- 2. Click **Properties** on the pop-up menu.
- 3. Click the **Misc Options** tab. Clear the **Inherit Directory Connector Properties** box and select the appropriate directory connector option.

C Use Active C Use LDAF	Connector Properties Directory Connector to ret Connector to retrieve emai e SMTP Domain to form err	laddresses
Primary Host:	Secondary Host:	LDAP <u>M</u> ail Name: mail
LDAP Port: 389	LDAP Port: 389	LDAP <u>Eilter Name</u> : uid

Setting the NTP Software File Auditor, Windows Edition Security Level

The NTP Software File Auditor Properties tab enables you to set up several application properties, including the application security level. To adjust your NTP Software File Auditor, Windows Edition application security level, please follow these steps:

- 1. Right-click NTP Software File Auditor under the main application container.
- 2. Click **Properties** on the pop-up menu.
- 3. Click the **Security** tab. Clear the **Inherit Security** box and check the **Enable Security** box. Click **Add** to choose the members or groups for which you want to apply security options.

Tip: In the **Non-Owner Permissions** section of the dialog box, choose the desired settings for the types of policies and properties.

Name			A <u>d</u> d
E veryone	9		Remove
Non-Owner <u>F</u>	Permissions		
	- Local Policies	Inherited Policies	Properties
Full Control:	۲	۲	۲
Read Only:	0	0	0
None:	0	C	0
lwner:		Last Modified b	iy:

Policy Creation

This section outlines standard NTP Software File Auditor, Windows Edition procedures for creating a file auditor policy.

Note:

• NTP Software File Auditor, Windows Edition monitors two main types of paths: directory paths and share paths.

Creating File Audit Policies

This section walks you through creating a typical file audit policy. We will create a file audit policy for all your user home directories in a typical server configuration. This policy will be applied to all users in your Users directory.

- 1. In the NTP Software Smart Policy Manager[™] hierarchy view, locate the Windows Server. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **File Auditor** to expand the policy types.
- 2. Right-click File Audit Policies and select New > Folder Policy Using Directories.
- 3. In the **New File Audit Directory Policy** dialog box, click the **General** tab. Enter a name and a description for your new policy.

File Audit Dir	ectory Policy		
Exempted	Subdirectories	Audited Use	ers and Groups
Exempt Users	and Groups	Notifications	DB Maintenance
General	Monitored Events	File Criteria	Directories
Policy <u>N</u> ame:			
Policy 1			
, Description:			
Monitoring Dir	ectories Created		
Distantia	lawa		
Distinguished I	Name:		
	Name:		
Distinguished I	Name:	Last Modified by:	
	Name:	Last Modified by:	
	Name:	Last Modified by:	
	Name:	Last Modified by:	
Policy Owner:			
Policy Owner:	dnesday, December 01	, 2010 11:06:14 AM	
Policy Owner:		, 2010 11:06:14 AM	

4. Click the **Monitored Events** tab; check the event(s) you want to monitor from the list of events. Check the **Store monitored events into the database** checkbox if you wish to store the monitored events in the File Auditor database. You can clear the "Store monitored events into the database" checkbox if you wish to use the notifications option without recording the events to the File Auditor database.

5. Click the **File Criteria** tab. Click the **Add** button. Select the files that you wish to monitor and the associated patterns will be displayed automatically, and you can also specify a custom pattern.

Note: If the Patterns list is empty, the policy will audit	all files. To monitor all files, you can also use
the A* pattern.	

New File Audit Dire	ctory Policy				X
Exempt Users -		Notifications	DB Ma	aintenance	
Exempted 9	Subdirectories		d Users and (
General	Monitored Events	File Crite	ria	Directories	Ļ
Patterns:					
E Common Aug	tio Files				
		I		!	
	1 1				
A <u>d</u> d	<u>E</u> dit	<u>R</u> emove			
	ОК	Cancel	Apply	Help	

6. Click the **Directories** tab. Click the **Add** button, type the appropriate directory path for your Users directory followed by a backslash.

Add or Edit an Item		×
Enter a directory name:		
E:\Users\		Browse
	OK Cancel	

7. Administrators, Backup Operators, Replicators, and the System account are exempt from policies. You can verify this fact by clicking the **Exempt Users and Groups** tab. To change this setting, select the appropriate entry and click **Remove**.

General	Monitored Events	File Cri	teria	Directories
	Subdirectories	Audit	ed Users -	and Groups
Exempt Users	and Groups	Notifications	D	B Maintenance
Accounts:				
	ackup Operators			
BUILTIN\R				
SINT AUTHO	RITY\SYSTEM			
•				Þ
•				Þ
Add	Edit	Remove		Þ
	<u><u> </u></u>	<u>R</u> emove]	Þ
	<u>E</u> dit	<u>H</u> emove	1	Þ
	<u>E</u> dit	Eemove		Þ
	<u>E</u> dît	<u>R</u> emove		Þ
	<u>E</u> dit	<u>H</u> emove		Þ
	<u>E</u> dit	<u>R</u> emove) Help

8. Click the Notifications tab. Click the Add button. On the Email Configurations Properties dialog General Tab, specify the notification related details; including the notification name description and message format. On the Email Settings Tab, specify the email subject and the email body, customize the displayed information about the authorized users and the associating events, and choose the detail level. On the Notification Settings Tab, specify the notification frequency, along with the types of events you wish to receive. On the Recipients Tab, specify the user(s) who should receive the email.

Email Configurations Properties	x
General Email Settings Notification Settings Recipients	
Notification Name:	
Notification 1	
Notification Description:	
<insert 1="" description="" notification=""></insert>	
Message Format	
OK Cancel Help	

NTP Software File Auditor™, Windows[®] Edition – An NTP Software User Manual

mail Configurations Properties	Z
General Email Settings Notification Settings Recipients	
Email Subject:	
Notification %n for policy %p	
Email Body This is a notification email for the specified events generated by auc	lit uppro
through policy %p on server %s.	nt users
The email contains a table of audited users along with events details	:
generated by them. Please choose the the columns to be displayed.	
Operation Type A Beceived Time	
Path C Path	
□ File Size O User	
Share Name	
OK Cancel	Help
	Пар
nail Configurations Properties	
· · · · · · · · · · · · · · · · · · ·	
General Email Settings Notification Settings Recipients	
_ Notification Frequency	
O Notify for every operation	
Notify no more than once every	
Event types you want to receive:	
OK Cancel	Help
nail Configurations Properties	
General Email Settings Notification Settings Recipients	
Notify Triggering User	
Notify Owner	
Notify Other Recipients	
Other Recipients List:	
A <u>d</u> d <u>E</u> dit <u>B</u> emove	
OK Cancel	Help

NTP Software File Auditor™, Windows[®] Edition – An NTP Software User Manual

New File Audit Dire	ctory Policy			×
Exempted 9	Subdirectories	Audited	Users and Groups	
General	Monitored Events	File Criteri	a Directorie	es
Exempt Users -	and Groups	Notifications	DB Maintenand	e j
		'		1
Notifications				
Name	Description			-
Notification 1	<insert notifi<="" td=""><td>cation 1 description:</td><td>></td><td></td></insert>	cation 1 description:	>	
•				<u> </u>
A <u>d</u> d	<u>E</u> dit	<u>B</u> emove		
	ок	Cancel /	Apply He	
			Apply He	Ψ

9. Click the **Exempted Subdirectories** tab. Click the **Add** button and type the subdirectory you want to exempt from the monitored directories list.

New File Audit Directory Policy
General Monitored Events File Criteria Directories Exempt Users and Groups Notifications DB Maintenance Exempted Subdirectories Audited Users and Groups
Each subdirectory you enter here will be appended to the managed directoires or shares to make the full list of the exempted directoires. Subdirectories:
Subfolder
I
Add <u>E</u> dit <u>B</u> emove
OK Cancel Apply Help

10. Click the **Audited User and Groups** tab. Choose whether you want to audit all users within your environment or specify certain user(s) to audit.

New File Audit Di	rectory Policy			×
· · · · · · · · · · · · · · · · · · ·	Monitored Events s and Groups d Subdirectories	Notifications	Directories DB Maintenance ers and Groups	
Audit Strateg	y t Everyone	C Audit <u>C</u> ertain Use	ers	
A <u>c</u> counts:				
Add	Edit	Remove	<u>▶</u>	
			1	
	OK	Cancel <u>Ap</u>	oly Help	

11. Click **OK** to close the **New File Audit Directory Policy** dialog box. NTP Software File Auditor, Windows Edition will create the new directory policy, which will be inherited by all systems from this point down in your hierarchy.

Viewing Directories

NTP Software File Auditor, Windows Edition enables you to view all the directories that are located on your Windows Server.

In the NTP Software Smart Policy Manager hierarchy view, locate your Windows Server containing the directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.

Viewing Shares

NTP Software File Auditor, Windows Edition enables you to view all the shared directories located your Windows Server.

In the NTP Software Smart Policy Manager hierarchy view, locate your Windows Server with the shared directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.

NTP Software File Auditor Reports

The NTP Software File Auditor, Windows Edition reporting tool allows you to view the file and directory operations that took place at your environment in an easy and efficient display. Reports are categorized by user, file, policy, and folder.

To view NTP Software File Auditor Reports, please follow the following steps:

- 1. Run NTP Software File Auditor Administrator by clicking Start > All Programs > NTP Software File Auditor > NTP Software File Auditor Reports.
- 2. On the left pane, click the report type you want to display.
- 3. On the upper pane, specify the search criteria and click View Report.
- 4. On the lower pane, check the report output.
- 5. NTP Software File Auditor, Windows Edition also allows you to export the report to different formats. Those include XML, CSV, TIFF, PDF, Web Archive, or Excel.

Listed below are the different types of reports provided by NTP Software File Auditor:

- 1. The **User Reports** category has four different views: the User Summary, the User Audit, the Access History, and the Most Active Users.
 - a. User Summary: This report allows you to search by user name. Clicking on a specific user name you can review the count of each operation performed, including the count of the deleted/renamed/moved files, the count of the created/changed/owner changed/permission changed files, the count of the created/deleted directories, and the count of the renamed directories files. In addition, it displays a list of the most-used client names along with the count of operation(s) performed using the specified IP address.

Number of deleted files:	1	Number of changed files:	2
Number of renamed files:	2	Number of owner changed files:	2
Number of moved files:	<u>0</u>	Number of permission changed files:	2
Number of created files:	<u>9</u>		
Number of deleted directories:	<u>1</u>	Number of renamed directories:	2
Number of created directories:	<u>4</u>		
Last activity Date/Time: 10/1	4/2009 7:59:04 AM		
Used Client M	lachine Name	es	
Top 5 used client machines			
Client Nar	ne ≑	Number of operations done f	rom the IP 💠
aasayed-xp-4502		100	
View All			

b. User Audit: This report allows you to review all the file and directory operations performed by user(s). The report input is the user account, and/or the access type, and/or the date range, and/or the host name. The report displays the user's name, the object name, the directory path, the host name, the operation performed, the date the operation was performed, the policy name, the client name, and the share name within the specified criteria.

Jser Account			Access Typ	e Directory Crea	te, Directory De 🛓	<u>-</u>		
Start Date 10,	/14/2009 5:09:14	AM 🛄	End Date	5/3/2011 8:53:	:20 AM	•		
Host Ah	medIG, na731-ra:	shad 🔻						
,		_						
m 11 🛛	🖣 1 of 2	3 🕨 🕅 🔶 🌔	3 🛃 🖂 🕻	🕘 🛍 🛃 • 📔	100%	•	Find Next	
User A	udit							
USEL A	uun							
- From: 10/14/20	09 5:09:14 AN	1 To: 5/3/2011	8:53:20 AM					
		1 10. 5/5/2011	0.00.20 AM					
Number of reco	rds: 1000							
	Object A	Diversion			D-t- A	D-line A	Olivert A	Ob
User 🗘 Name	Object 💲 Name	Directory 💲 Path	Host \$	Access 😂 Type	Date 💲	Policy 🗘 Name	Client \$ Name	Share : Name
Galactic.com\Clo	Sales	(HOME)Business Shares)	na731- rashad	File Open For Write	10/14/2009 7:59:46 AM		aasayed-xp-	IG - Machine
						Liser6	4502	io - maonino
salactic.com/Ulo	Support	VHOME\Business	na731-	File Open For	10/14/2009		4502 aasayed-xp-	IG - Machine
<u>Galactic.com\Clo</u> <u>/er</u>	Support	VHOME\Business Shares\	na731- rashad			MKT POL		
	Support Support			File Open For	10/14/2009	MKT POL User6 MKT POL	aasayed-xp-	
<u>ver</u> Galactic.com\Clo ver Galactic.com\Clo		Shares\ \HOME\Business Shares\ \HOME\Business	rashad na731- rashad na731-	File Open For Write File Open For Write File Open For	10/14/2009 7:59:43 AM 10/14/2009 7:59:42 AM 10/14/2009	MKT POL User6 MKT POL User6 MKT POL	aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	IG - Machine
<u>ver</u> Salactic.com\Clo ver Salactic.com\Clo ver	Support	Shares\ \HOME\Business Shares\	rashad na731- rashad	File Open For Write File Open For Write File Open For Write	10/14/2009 7:59:43 AM 10/14/2009 7:59:42 AM	MKT POL User6 MKT POL User6 MKT POL User6	aasayed-xp- 4502 aasayed-xp- 4502	IG - Machine IG - Machine IG - Machine
<u>ver</u> Salactic.com\Clo ver Salactic.com\Clo ver Salactic.com\Clo	Support	Shares\ VHOME\Business Shares\ VHOME\Business Shares\	rashad na731- rashad na731- rashad	File Open For Write File Open For Write File Open For	10/14/2009 7:59:43 AM 10/14/2009 7:59:42 AM 10/14/2009 7:59:38 AM	MKT POL User6 MKT POL User6 MKT POL User6 MKT POL	aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp- 4502	IG - Machine IG - Machine IG - Machine
rer Balactic.com/Clo rer Balactic.com/Clo rer Balactic.com/Clo rer Balactic.com/Clo	Support	Shares\ VHOME\Business Shares\ VHOME\Business Shares\ VHOME\Business	rashad na731- rashad na731- rashad na731-	File Open For Write File Open For Write File Open For Write File Open For	10/14/2009 7:59:43 AM 10/14/2009 7:59:42 AM 10/14/2009 7:59:38 AM 10/14/2009	MKT POL User6 MKT POL User6 MKT POL User6 MKT POL User6 MKT POL	aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	IG - Machine IG - Machine IG - Machine IG - Machine
<u>/er</u> Galactic.com\Clo	Support Support Support	Shares\ 'HOME\Business Shares\ 'HOME\Business Shares\ 'HOME\Business Shares\ 'HOME\Business	rashad na731- rashad na731- rashad na731- rashad na731-	File Open For Write File Open For Write File Open For Write File Open For Write File Open For	10/14/2009 7:59:43 AM 10/14/2009 7:59:42 AM 10/14/2009 7:59:36 AM 10/14/2009 7:59:36 AM	MKT POL User6 MKT POL User6 MKT POL User6 MKT POL User6 MKT POL MKT POL	aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	IG - Machine

c. Access History: This report allows you to review all the file and directory operations performed within a specified number of days. The report input is the user account, and/or the number of day(s) in which the file/directory was accessed, and/or the file name, and/or the access type performed on the file/directory. The report displays the user's name, the object name, the directory path, the operation performed, the date the operation was performed, the policy name, the client name, and the share name within the specified criteria.

User Account	ne, bxt		in the last (days) number: 93852) pe	78947 Director	/ Create, Director	ry De ▼	
Access			I û . •	100%	•	Find Next	
User Name	Object ‡ Name	Directory Path 💲	Access 🗘 Type	Access ≑ Date	Policy \$ Name	Client ≑ Name	Share ≎ Name
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Close		MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Open For Write		MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Close	10/14/2009 7:56:46 AM		aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Close	10/14/2009 7:56:46 AM		aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Open For Write	10/14/2009 7:56:42 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	\HOME\BusinessShares\ Marketing\User0006\Old	File Open For Write		MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\wood	readme.txt	HOMEVBusinessShares\ SupportVJser0013\Ticket	File Open For Write	10/14/2009 7:42:26 AM	MKT POL Support	aasayed-xp-4502	IG - Machine

d. **Most Active Users:** This report allows you to review the most active users, with the users' activities sorted in a descending or ascending order. The report input is the date range and/or the number of most active users to view. The report displays the user name and the number of activities performed by this user within the specified criteria.

									-
Start Date	3/3/2010 8:23	1:23 AM		End Date	3/5/2010 10:4	7:23 AM		View Report	
View top (users) (Maximum number: 2147483647)	20								
14 4 1	of1 ▷ ▷∥	75%	•		Find Nex	t Select a	ormat	Export	
0									
Vlostacti	ve users								
kumber of records: (Numbe	r of activities 🛊			
Number of records: 6 User 😩	5				Numbe	r of activities 🗘	1359		
Most acti Number of records : 4 User : upgreat.com/001a2010 upgreat.com/123004a	5				Numbe	r of activities 💲	1369		
Number of records : 4 User 😩 Nogre at.com/100 ka20 10 Nogre at.com/123 Doka Nogre at.com/100	5				Numbe	r of activities 🗄	17 12		
Number of records : 4 User 😩 upgreat.com/Do (a 2010 upgreat.com/123 Doka	5				Numbe	r of activities 🔅	17		

- 2. The **File Reports** category has nine different views: File Summary, File Audit, Files Changed, Files Deleted, Files Renamed, Files Created, Deletion Compliance, Owner Changed, and Permission Changed.
 - a. **File Summary:** This report allows you to review the count of all the audited files. It also displays a breakdown for the count of deleted, renamed, created, or changed files. You can click the count next to any file operation to display a detailed list of the specified file operation.



b. File Audit: This report allows you to review all the file operations performed. The report input is the file name, and/or the host name, and/or the file operation performed, and/or the file type, and/or the date range. The report displays the file name, the directory name where the specified file is located, the user name accessing the file, access type, access date, the name of the policy applied on the directory, the client name, and the share name within the specified criteria.

File Name			Host Ahr	medIG, na731-ras	had 💌			
Start Date 1	0/14/2009 5:09:14 4	M 🛄	End Date 5/3	/2011 8:44:37 AM				
Access Type	file Close, File Create	, File Dele 💌	File Type bm	p, cpp, doc, h, rtf	, tmp, txt 💌			
E 1 M	◀ 1 of 2	3 🕨 🎽 👳	0 1 🖂 🔲	💭 🛃 • 10	0% •		Find Next	
File A	udit							
From: 10/14/	2009 5:09:14 AM	To: 5/3/2011	8:44:37 AM					
Number of re	cords: 1000							
File 🗘 Name	Directory 🖨 Path	Host \$	User ‡ Name	Access 🗘 Type	Access ≎ Date	Policy 🗘 Name	Clien ≑ t Nam e	Share ≎ Name
Readme.txt	VHOMEVBusiness SharesWarketing VUser0006Vold StuffV	na731-rashad	Galactic.com/P latt	File Delete	10/14/2009 7:59:04 AM		aasayed-xp- 4502	IG - Machine
	VHOME\Business Shares\Marketing VUser0006\Old Stuff\	na731-rashad	Galactic.com/P latt	File Open For Read	10/14/2009 7:59:04 AM		aasayed-xp- 4502	IG - Machine
ScreenShoot.b mp New Text Document.txt	Shares/Marketing /User0006/Old	na731-rashad na731-rashad				Marketing MKT POL		IG - Machine IG - Machine

c. **Files Changed:** This report allows you to view all the changed files. The report input is the file name, and/or the host name, and/or the date range, and/or the file type(s). The report displays the file name, the directory path in which the file is located, the user name accessing the file, the access type, the access date, the name of the policy applied, the client name, and the share name within the specified criteria.

			Host	AhmedIG, na731	rashad 🗾			
File Type bmp	p, cpp, doc, h, rtf, tr	np, txt 💌	Access Type	File renamed, File	Close 💌			
Start Date 10/	14/2009 5:09:14 AM		End Date	5/3/2011 8:45:25	AM 🛄			
🖻 🚹 🛛 🕅		▶ N ← €) 🛃 🖾 🕻	I 💷 🛃 - 🗄	.00%	-	Find Next	
Files	Change	d						
i nes	onunge	G						
From: 10/14/	2009 5:09:14 AM	To: 5/3/2011	8:45:25 AM					
Number of re	cords: 152							
Number of re	C0103. 132							
File 😂	Directory 😂	Host 😂	User 😂	Access 😂	Change 😂	Policy 😂	Client 😂	Share 😂
Name	Path		Nam	Туре	Date	Name	Name	Name
lew Text	Path VHOME\Business Shares\Warketing User0006\Africa Customers\	na731-rashad				Name MKT POL		
Name New Text Document.txt New Bitmap mage.bmp	VHOMEVBusiness SharesWarketing VUser0006VAfrica	na731-rashad na731-rashad	e Galactic.co	Туре	Date 10/14/2009 7:59:00 AM	Name MKT POL Marketing MKT POL	Name aasayed-xp-	Name
Vew Text Document.txt Vew Bitmap	HOMEVBusiness Shares/Marketing User0006VAfrica Customers\ HOMEVBusiness Shares/Marketing User0006V0Id		e Galactic.co mPlatt Galactic.co	Type File Rename	Date 10/14/2009 7:59:00 AM 10/14/2009 7:56:20 AM	Name MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp-	Name IG - Machine

d. **Files Deleted:** This report allows you to review all the files that have been deleted. The report's input is the file name, and/or the host name, and/or the date range, and/or the file type. The report displays the file name, the directory path in which the file was located, the user name, the date the file was last accessed, the policy name, the client name, and the share name within the specified criteria.

File Name		Ho	AhmedIG, na73	1-rashad 💌			
Start Date 10/14	/2009 5:09:14 AM	Er	d Date 5/3/2011 8:47:0	14 AM 🛄	1		
File Type bmp,	cpp, doc, h, rtf, tmp	txt. 💌					
🖅 🕅 🛛 🕅	4 1 of 1	▶ ← 😡	2 4 🖬 🖬 🖬 🚽	100%	•	Find Nex	t
Files D)eleted						
From: 10/14/20	09 5:09:14 AM	To: 5/3/2011 8:	47:04 AM				
Number of reco	rds: 28						
File ‡ Name	Directory 🗘 Path	Host 😄	User Name 💲	Delete ≑ Date	Policy ≑ Name	Client ≑ Name	Share Name
Readme.txt	VHOME\Business Shares\Marketing VUser0006\Old Stuff\	na731-rashad	Galactic.com/Platt	10/14/2009 7:59:04 AM		aasayed-xp- 4502	IG - Machine
nstructions.doc.t t	VHOME\Business Shares\Develop ment\User0005 \Projects in	na731-rashad	Galactic.com\Topper	10/14/2009 7:47:01 AM	MKT POL Dev	aasayed-xp- 4502	IG - Machine
	Progress\GIS Project\						
sits.txt		na731-rashad	Galactic.com/Norman dy	10/14/2009 7:38:56 AM		aasayed-xp- 4502	IG - Machine

e. **Files Renamed:** This type of report allows you to review all the files that have been renamed. The report's input is the file name and/or, the host machine name, and/or the date range, and/or the file type. The report displays the original file name before the change, the new file name after the rename, the directory path in which the file is located, the user name, the date the file was accessed, the policy name, the client name, and the share name within the specified criteria.

File Name			Host Ahme	dIG, na731-rasha	d 💌			
Start Date 10	14/2009 5:09:14 /	AM 🛄	End Date 5/3/20	011 8:50:12 AM				
File Type bm	p, cpp, doc, h, rtf;	tmp, txt 💌						
i 🖬 🎦 K	4 1 of	4 🕨 🎽 👄	0 📝 🖂 🔲	🔎 🛃 • 🕴 100	1%	•	Find Next	
Files	Renam	ied						
From: 10/14.	/2009 5:09:14 A	M To: 5/3/2011	8:50:12 AM					
Number of re	cords: 152							
Origina 💲 I File	New 🗘 File	Directory 💲 Path	New Directory	User 🗘 Name	Rena 💲 me	Policy 🗘 Name	Client \$	Share ≑ Name
Name	Name	Paul	Path	Name	Date	Name	Name	Name
<u>New Text</u> Document.txt	Readme txt	VHOMEVBusiness SharesWarketing VUser0006VAfrica Customers\	WNA731- RASHAD/HOME\ BusinessShares\ Marketing/User00 06\Africa Customers\	Galactic.com\P latt	10/14/2009 7:59:00 AM		aasayed-xp- 4502	IG - Machine
New Bitmap Image.bmp	ScreenShoot.b mp	VHOMEVBusiness SharesWarketing VUser0006\Old Stuff\	WNA731- RASHAD/HOME\ BusinessShares\ Marketing/User00 06\Old Stuff\	Galactic.com\P latt	10/14/2009 7:56:20 AM		aasayed-xp- 4502	IG - Machine
<u>GISMain.h</u>	CGISMain.h	VHOMEVBusiness SharesVDevelop mentVJser0005 VProjects in	WNA731- RASHAD/HOME\ BusinessShares\ Development/Us	Galactic.com\T opper	10/14/2009 7:50:07 AM	MKT POL Dev	aasayed-xp- 4502	IG - Machine

f. **Files Created:** This type of report allows you to review all the files that have been created. The report's input is the date range, and/or the file name, and/or the file type, and/or the user account. The report displays the file name, the directory path in which the file exists, the user name, the access type (which is "file create"), the access date, the policy name, the client name, and the share name within the specified criteria.

		Host	AhmedIG, na731-r	ashad 🗾			
Start Date 10/14/2	2009 5:09:14 AM	End Date	5/3/2011 8:46:17	AM 🛄			
File Type bmp, q	pp, doc, h, rtf, tmp, txt.]					
🗄 🚹 K 🛛	1 of 6 🕨 🎽	🔹 🔕 🏚 🎒	🛛 🕰 🚽	100%	•	Find Ne>	<t< td=""></t<>
Files C	reated						
riles C	reated						
From: 10/14/200	19.5:09:14 AM To: 5	/3/2011 8:46:17 A	M				
Number of recor		0.40.17					
Number of recor	'ds: 235						
File Name 😂	Directory 🗘	Host 🗘	User 😂	Create 😂	Policy 🗘	Client 🗘	Share :
			Name	Date	Name	Name	Name
	VHOMEVBusinessShar esWarketingVUser000 6VAfrica Customers\	na731-rashad	Galactic.com/P	Date 10/14/2009 7:58:56 AM	MKT POL	Name aasayed-xp- 4502	Name IG - Machine
New Text Document.txt New Text Document.txt	VHOMEVBusinessShar esWarketingVUser000	na731-rashad na731-rashad	Galactic.com/P	10/14/2009	MKT POL Marketing MKT POL	aasayed-xp-	
Document.txt	HOME/BusinessShar es/Marketing/User000 6\Africa Customers\ HOME/BusinessShar es/Marketing/User000		Galactic.com/P	10/14/2009 7:58:56 AM 10/14/2009	MKT POL Marketing MKT POL Marketing MKT POL	aasayed-xp- 4502 aasayed-xp-	IG - Machine
New Text Document.txt	HOME/BusinessShar es/Marketing/User000 6V4rtica Customers\ HOME/BusinessShar es/Marketing/User000 6V0Id Sturft\ HOME/BusinessShar es/Marketing/User000	na731-rashad	Galactic.com/P latt Galactic.com/P latt Galactic.com/P	10/14/2009 7:58:56 AM 10/14/2009 7:56:35 AM 10/14/2009	MKT POL Marketing MKT POL Marketing MKT POL MKT POL	aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	IG - Machine IG - Machine

g. **Files Moved:** This type of report allows you to review all the files that have been moved. The report's input is the date range, and/or the file name, and/or the file type, and/or the host name. The report displays the file name, the source path and the destination path of the moved file, the host name, the date on which the file was moved, the policy name, the machine IP address, and the share name within the specified criteria.

File Name	e		Host	AhmedI	G, na731-rashad	-			
5tart Dat	te 1	0/14/2009 5:09:14 AM	End (Date 5/3/201	1 3:19:17 PM				
File Type	• [omp, cpp, doc, h, rtf, tr	np, txt 💌						
1	1	📢 🖣 1 of 3	🕨 🕨 🛭 🙆	🖨 🔲 û	100%	•		Find Next	
File	es	Moved							
From: 1	10/1	4/2009 5:09:14 AM	To: 5/3/2011 3:19	:17 PM					
Numbo	vr of	records: 103							
NULLIDE	01.01	records, roo							
File	n or چ	Source 😂		Host \$	User 🗘	Move \$	Policy 😂	Client 🗘	Share 🗧
			Destination ≑ Path	Host \$	User ≑ Name	Move ≑ Date	Policy ≑ Name	Client ≑ Name	Share : Name
ile		Source ≑ Path ₩OME\BusinessSh	Path WNA731-	na731-	Name Galactic.com/P	Date 10/14/2009	Name MKT POL	Name aasayed-xp-	
ile		Source ≑ Path	Path WNA731- RASHAD\HOME\Busi nessShares\Marketing		Name	Date	Name MKT POL	Name	Name
ile		Source Path WOMEVBusinessSh aresWarketing/User	Path WNA731- RASHAD/HOME/Busi	na731-	Name Galactic.com/P	Date 10/14/2009	Name MKT POL	Name aasayed-xp-	Name
ile		Source Path HOME\BusinessSh aresWarketing\User 0006\New Folder HOME\BusinessSh	Path WNA731- RASHADVHOMEVBusi nessShares/Marketing User0006VAfrica Customers WNA731-	na731- rashad na731-	Name Galactic.com/P latt Galactic.com/P	Date 10/14/2009 7:58:47 AM 10/14/2009	Name MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp-	Name
ile		Source Path HOME/BusinessSh ares/Marketing/User 0006/Wew Folder HOME/BusinessSh ares/Marketing/User	Path WNA731- RASHADHOME'Busi nessShares'Marketing User0006'Africa Customers WNA731- RASHAD'HOME'Busi	na731- rashad	Name Galactic.com/P latt	Date 10/14/2009 7:58:47 AM	Name MKT POL Marketing MKT POL	Name aasayed-xp- 4502	Name IG - Machine
ile		Source Path HOME\BusinessSh aresWarketing\User 0006\New Folder HOME\BusinessSh	Path WNA731- RASHADVHOMEVBusi nessShares/Marketing User0006VAfrica Customers WNA731-	na731- rashad na731-	Name Galactic.com/P latt Galactic.com/P	Date 10/14/2009 7:58:47 AM 10/14/2009	Name MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp-	Name IG - Machine
ile		Source Path HOMEBusinessSh aresWarketingUser 0006Wew Folder HOMEBusinessSh aresWarketingUser 0006Wew Folder HOMEBusinessSh	Path WWA731- RASHADHOMEWBusi nessSharesWarketing User0006VAfrica Customers WWA731- RASHADHOMEWBusi nessSharesWarketing User0006Vold Suff WWA731-	na731- rashad na731- rashad na731-	Name Galactic.com/P latt Galactic.com/P latt Galactic.com/V	Date 10/14/2009 7:58:47 AM 10/14/2009 7:56:07 AM 10/14/2009	Name MKT POL Marketing MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	Name IG - Machine
ile		Source Path Path VHOME'BusinessSh ares Marketing User 0006'Wew Folder VHOME'BusinessSh ares Marketing User 0006'Wew Folder	Path WA31- RASHAD'HOME'Busi nessShares'Warketing User0006VAfrica Customers WA731- RASHAD'HOME'Busi nessShares'Warketing User0006VOId Stuff	na731- rashad na731- rashad	Name Galactic.com/P latt Galactic.com/P latt	Date 10/14/2009 7:58:47 AM 10/14/2009 7:56:07 AM	Name MKT POL Marketing MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp- 4502	Name IG - Machine IG - Machine
File		Source Path HOME/BusinessSh aresWarketing/User 0006/Wew Folder HOME/BusinessSh aresWarketing/User 0006/Wew Folder HOME/BusinessSh aresDevelopment/	Path WA731- RASHAD'HOME'Busi nessShares'Warketing User0006VArtica Customers WNA731- RASHAD'HOME'Busi nessShares'Warketing User0006Vold Stuff WNA731- RASHAD'HOME'Busi RASHAD'HOME'Busi	na731- rashad na731- rashad na731-	Name Galactic.com/P latt Galactic.com/P latt Galactic.com/V	Date 10/14/2009 7:58:47 AM 10/14/2009 7:56:07 AM 10/14/2009	Name MKT POL Marketing MKT POL Marketing MKT POL	Name aasayed-xp- 4502 aasayed-xp- 4502 aasayed-xp-	Name IG - Machine IG - Machine

h. **Deletion Compliance:** This type of report allows you to review the files deleted over the specified compliance period. The report's input is the compliance period in months, the host name and the file type. The report displays the files deleted over the specified period.



i. **Owner Changed:** This type of report allows you to review the file(s) whose owner(s) has changed. The report displays the name of the file whose owner has changed, the previous owner, the new owner, the host IP address, the user name, the policy name, the client name, and the share name within the specified criteria.

From: 3/14/2011 Number of recor		o: 3/15/2011 4:02:02 PM							
File Name 💲	Directory 🛊	Previous Owner	New Owner	Host 💲	User Name 🕴	Date 😫	Policy 💲	Client 9 Name	Share \$
	WOLIVOLD HOMEL	COTNET_CRITICAL SITES LOCAL Mahmoud, Coarne	COTNET.CRITICALSITES.LOCALVANISM. Hissian	10.20.2.57	DOTNET.ORTICALSITES LOCAL/Administrator	3/14/2011 4:45:44 PM	df		
	WOLIVOLD HOME!	DOTNET.CRITICAL SITES LOCAL Mahmoud, Osama	DOTNET.CRITICALSITES.LOCAL\Administrators	10.20.2.57	DOTNET.ORTICALSITES LOCAL Vadministrator	3/14/2011 4:43:27 PM			
	VOLIVOLD HOME\	DOTNET.CRITICALSITES LOCAL/Administrators	DOTNET.CRITICALSITES.LOCALWahmoud Osema	10.20.2.57	DOTNET.ORITICALSITES LOCAL Vadministrator	3/14/2011 4:35:55 PM			
	WOLIVOLD HOME!	DOTNET CRITICAL SITES LOCAL VAdministrators	DOTNET.CR/TICALS/TES.LOCAL/Mshmoud Osoma	10.20.2.57	DOTNET.CRITICALSITES.LOCAL/Administrator	3/14/2011 4:35:55 PM			
	WOLIVOLD HOME!	DOTNET CRITICAL SITES LOCAL VAdministrators	DOTNET CRITICAL SITES LOCAL Webmoud Osome	10.20.2.57	DOTNET. CRITICAL SITES LOCAL Viden instrator	3/14/2011 4:35:55 PM			
	WOLWOLD HOMEL	DOTNET CRITICAL SITES LOCAL VAdministrators	DOTNET.CRITICALSITES.LOCALWahmoud. Osama	10.20.2.57	DOTNET CRITICAL SITES LOCAL Videnivistrator	3/14/2011 4:35:55 PM			
	WOLWOLD	DOTNET.CRITICALSITES LOCAL/Administrators	DOTNET.CRITICALSITES.LOCAL.Wahmoud	10.20.2.57	DOTNET.CRITICALSITES.LOCAL/Administrator	3/14/2011	df		

j. Permission Changed: This type of report allows you to review the file(s) whose permission(s) has changed among user. The report displays the name of the file whose permission has changed, the directory where the file exists, the host IP address, the user name, the policy name, the client name, and the share name, as well as the permission details within the specified criteria.

ds: 503							
Directory 💲	Host 😄	User Name 😄	Date 💲	Policy \$ Name	Client ‡ Name	Share ‡ Name	Permission Details
	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	dif			<u>View</u>
	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df			<u>View</u>
VOLIVOLO VHOMEV	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	dif			View
VOLIVOLO VHOMEV	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df			View
	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			<u>View</u>
	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			<u>View</u>
	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df			View
	VYOLIVOLO HOMES VYOLIVOLO HOMES VYOLIVOLO VYOLIVOLO HOMES VYOLIVOLO HOMES VYOLIVOLO	WOLWOLD 10.20.2.57 HOME 10.20.2.57 WOLWOLD 10.20.2.57	VOLVVOL0 10.20.2.57 DOTNET CRITICAL SITES LOCAL Administrator HOME3 VOLVVOL0 10.20.2.57 DOTNET CRITICAL SITES LOCAL Administrator HOME3	VOLVOL0 10 20 2.57 DOTNET_CRTICALSITES_LOCAL_VAdministrator 314/2011 YOLVOL0 10 20 2.57 DOTNET_CRTICALSITES_LOCAL_VAdministrator 314/2011	Direct Op Prost Te Oster Value Te Date Te Name VOLVOL0 10.20.2.57 DOTNET CRTICALSTES LOCAL/Administrator 3.914/2011 df VOLVOL0 10.20.2.57 DOTNET CRTICALSTES LOCAL/Administrator 3.9	Directory Prost Dist of the control Directory Name Name	Directory Prost Dote Name Name Name VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df 4.55.10 PM VOLVOL0 10.20.257 DOTNET CRTICALSTES LOCAL/Administrator 37.4/2011 df VOLVOL0

Clicking on the View link of the Permission Details field displays more details as outlined below.

i4 4 2 of 3 ▶ ▶i 100% ▼	Find Next S	elect a format	Export
File Permissions Changed			
File Name: COPY (2) OF R.TXT			
User Name: \Everyone			
-	Previous	Current	
Has Full Control	X	×	
Has Execute	×	×	
Has Read	 Image: A second s	 ✓ 	
Has Read Attributes	✓	×	
Has Read Extended Attributes	✓	×	
Has Write	✓	✓	
Has Append	✓	✓	
Has Write Attributes	✓	✓	
Has Write Extended Attributes	✓	✓	
Has Delete	×	×	
Has Read SD	 Image: A set of the set of the	✓	
Has Change DACL	×	×	
Has Take Ownership	×	×	1

- 3. Policy Reports category has one view: the Policy by Date report.
 - a. **Policy by Date:** This report allows you to review all the policy details within a certain date range. The report's input is the date range and/or the policy name. The report displays the policy name, the user name, the directory path on which the policy applies, the access type, the access date, the machine IP address, and the share name within the specified criteria.

	009 5:09:14 AM licy, MKT POL Dev, M	End Dat	e 5/3/2011 8:52:08	AM 🛄			
i 🖻 🚹 M 🖪	1 of 23 🕨	N 🗢 🛛 🛃	/# 🔲 🛍 📕 •	100%	•	Find Ne	xt
Policy	9 5:09:14 AM 1	ō: 5/3/2011 8:52:0	8 AM				
Number of record							
Policy 🗘 Name	User ≑ Name	Directory 🗘 Path	Host 💲	Access 😂 Type	Date 💲	Client ‡ Name	Share ≑ Name
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:46 AM	aasayed-xp- 4502	IG - Machine
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:43 AM	aasayed-xp- 4502	IG - Machine
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:42 AM	aasayed-xp- 4502	IG - Machine
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:38 AM	aasayed-xp- 4502	IG - Machine
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:36 AM	aasayed-xp- 4502	IG - Machine
MKT POL Support	Galactic.com\Clo ver	HOME\BusinessSh ares\Support\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp- 4502	IG - Machine
MKT POL User6	Galactic.com\Clo ver	\HOME\BusinessSh ares\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp- 4502	IG - Machine
MKT POL Finance	Galactic.com\Clo	HOME\BusinessSh ares\Finance\	na731-rashad	File Open For Write	10/14/2009 7:59:25 AM	aasayed-xp- 4502	IG - Machine

- 4. The **Directory Reports** category has eight views: Directory Summary, Directory Audit, Directory Created, Directory Renamed, Directory Deleted, Deleted Files by Folder, Deleted Files Count by Folder, and Most Accessed Folders.
 - a. **Directory Summary:** This report allows you to review the count of all the audited directories. It also displays a breakdown for the count of deleted, renamed, or created directories. You can click the count next to any directory operation to display a detailed list of the specified directory operation.

Directory summary						
Start 3/3/2010 8:33 Date	3:59 AM	End Date	3/3/2010 8:44:5	0 AM	View Report	
]4 4 1 of 1 ▷	▶ 75%	•	Find Next	Select a format	Export	\$
2 🎒						
Directory Summ	n ary Report					
Number of audited directories:	4					
Number of deleted directories:	<u>0</u>	Number of cre	ated directories: 4			
Number of renamed directories fil	es: <u>D</u>					

b. Directory Audit: This report allows you to review all the directory operations performed. The report's input is the directory name, and/or the host name, and/or the date range, and/or the access type. The report displays the directory name, the user name accessing the directory, access type, access date, the name of the policy applied on the directory, the client name, and the share name. You can choose to display the previous information within a certain date range and/or for a certain access type(s) and/or for a certain directory name.

				Host Ahme	edIG, na731-rashad	-		
Start Date	10/14/2009 5	:09:14 AM		End Date 5/3/2	011 5:44:11 AM			
Access Type	Directory Cre	ate, Director	y De 💌					
1 1	∢ 1	of 6 🕨 🌶	+ 🛛 🛃	13 🖬 🖬 🕯	, 100%	•	Find Next	
Direct	orv A	udit						
From: 10/14/20	009 5:09:14	AM To:	5/3/2011 5:44	:11 AM				
Number of reco	ords: 249							
Directory Name	User Name		Host 😂	Access 😂	Access 🗘	Policy Name	♦ Client ♦ Name	Share 😫
				17pc	Date	Ivanie	Ivanie	Name
es/Marketing/User		tic.com/Plat	na731-rashad	Directory Delete	10/14/2009 7:59:04 AM	MKT POL	aasayed-xp-4502	
es/Marketing/User 5\Old Stuff\ HOME\BusinessS es/Marketing/User	1000 t	tic.com/Plat	na731-rashad na731-rashad	Directory	10/14/2009	MKT POL Marketing MKT POL		IG - Machine
HOME/BusinessS es/Marketing/User 6/OId Stuff/ HOME/BusinessS es/Marketing/User 6/New Folder/ HOME/BusinessS es/Marketing/User 6/New Folder/	1000 t Calact 1000 t Calact Calact			Directory Delete Directory	10/14/2009 7:59:04 AM 10/14/2009	MKT POL Marketing MKT POL Marketing MKT POL	aasayed-xp-4502	IG - Machine IG - Machine
es/Marketing/User 6/Old Stuff/ HOME/BusinessS es/Marketing/User 6/New Folder/ HOME/BusinessS es/Marketing/User	0000 t Shar Galact 0000 t Shar Galact 0000 t Shar Galact Shar Galact Shar Galact Galact Galact	tic.com/Plat	na731-rashad	Directory Delete Directory Rename Directory	10/14/2009 7:59:04 AM 10/14/2009 7:58:47 AM 10/14/2009	MKT POL Marketing MKT POL Marketing MKT POL MARKETING	aasayed-xp-4502 aasayed-xp-4502	IG - Machine IG - Machine IG - Machine

c. **Directory Created:** This report allows you to review all the directories created. The report's input is the date range, and/or the directory name, and/or the host name. The report displays the name of the created directory, the user's name performing the directory create operation, the date in which the directory was created, the name of the policy governing this directory creation operation, the IP address of the machine used to perform the directory create operation and the share name based on the specified criteria.

		Host A	hmedIG, na731-rashad	-			
Start Date 10/14/2009 5	:09:14 AM	End Date 5	/3/2011 8:51:00 AM				
등 월 년 4 1	of 3 🕨 🔰 🐗	8 2 4 1	100%	-	Find Nex	t	
Directory C	reated						
		4 0 54 00 414					
From: 10/14/2009 5:09:14	AM To: 5/3/201	1 8:51:00 AM					
Number of records: 128							
	the set blocks		Consta Data	D-line A		Ola ava	•
	User Name 💲	Host 💲	Create Date 💲	Policy ‡ Name	Client ‡ Name	Share Name	ŧ
Created HOME/BusinessShares/Mark	User Name 💠	Host 👙 na731-rashad	10/14/2009 7:57:31				ŧ
Created HOME'BusinessShares'Mark eting'User0006'Wew Folder\ HOME'BusinessShares'Mark	· · · · · ·		10/14/2009 7:57:31 AM 10/14/2009 7:56:04	Name MKT POL Marketing	Name	Name	\$
Directory Name Created HOMEBusinessSharesWark elinaUser0008New FolderN YOMEBusinessSharesWird HindUser0006New FolderN YCMEBusinessSharesFina nesuSer00001/misShets	Galactic.com/Platt	na731-rashad	10/14/2009 7:57:31 AM 10/14/2009 7:56:04 AM 10/14/2009 7:53:16	Name MKT POL Marketing MKT POL Marketing	Name aasayed-xp-4502	Name IG - Machine	4
Created HOMEBusinessSharesMark etingUser0006New Folder\ HOMEBusinessSharesMark etingUser0006New Folder\ VHOMEBusinessSharesVina	Galactic.com/Platt	na731-rashad na731-rashad	10/14/2009 7:57:31 10/14/2009 7:57:31 10/14/2009 7:55:04 AM 10/14/2009 7:53:16 AM 10/14/2009 7:53:16	Name MKT POL Marketing MKT POL Marketing MKT POL Finance	Name aasayed-xp-4502 aasayed-xp-4502	Name IG - Machine IG - Machine	•
Created HOME BusinessSharesWark etinaWiser0006Wew Folder\ HOME BusinessSharesWark etinaWiser0006Wew Folder\ HOME BusinessSharesVina nexUser0006WimeSheets\ HOME BusinessSharesVina	Galactic.com/Platt Galactic.com/Platt Galactic.com/Platt	na731-rashad na731-rashad na731-rashad	10/14/2009 7:57:31 10/14/2009 7:57:31 10/14/2009 7:56:04 AM 10/14/2009 7:53:15 AM 10/14/2009 7:53:15 AM	Name MKT POL Marketing MKT POL Marketing MKT POL Finance MKT POL Finance	Name aasayed-xp-4502 aasayed-xp-4502 aasayed-xp-4502	Name IG - Machine IG - Machine IG - Machine	•

d. **Directory Renamed:** This report allows you to review all the renamed directories. The report's inputs are the directory name, and/or the host name, and/or the date range. The report displays the original directory name before the renaming operation, the new directory name after renaming, the user's name performing the directory rename operation, the date in which the directory was renamed, the name of the policy governing this directory rename operation, the IP address of the machine used to perform the directory rename operation, and the share name based on the specified criteria.

Directory Name		Host	AhmedIG, na	731-rashad 🛛]		
5tart Date 10/14/	2009 5:09:14 AM	🔋 End Da	te 5/3/2011 5:4	7:12 AM	0		
🗄 👘 🕅 🔌 1	of 3 🕨 🔰 🗍	3 👌 🎒	🛛 🕰 🖬 •	100%	•	Find Next	
Directory	/ Rename	d					
From: 10/14/2009 5	:09:14 AM To: 5/3/2	011 5:47:12 AM	4				
Number of records:	103						
Original 🗘	New 🚊	Host 🚖	User 😩	Rename 🚖	Policy 😂	Client 🗘	Share 😂
Directory Name	Directory Name	HUSL	Name	Rename ≑ Date	Policy 🗘 Name	Client ≑ Name	Snare ⇒ Name
HOME\BusinessShares Marketing\User0006 New Folder\	<u>\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</u>	na731-rashad	Galactic.com/P	10/14/2009 7:58:47 AM		aasayed-xp- 4502	IG - Machine
VHOMEVBusinessShares MarketingVUser0006 VNew Folder\	<u>WNA731-</u> <u>RASHAD/HOME/Busi</u> nessShares/Marketing <u>User0006/Old Stuff</u>	na731-rashad	Galactic.com\P latt	10/14/2009 7:56:07 AM		aasayed-xp- 4502	IG - Machine
HOME\BusinessShares Development\User0005 ICompleted Projects\New Folder\	<u>WNA731-</u> RASHAD/HOME/Busi nessShares/Developm ent/User0005 VCompleted	na731-rashad	Galactic.com\T opper	10/14/2009 7:48:29 AM	MKT POL Dev	aasayed-xp- 4502	IG - Machine

e. **Directory Deleted:** This report allows you to review all the deleted directories. The report's input is the date range, and/or the directory name, and/or the host name. The report displays the name of the deleted directory, the user's name performing the directory delete operation, the date in which the directory was deleted, the name of the policy governing this directory deletion operation, the client name used to perform the directory delete operation, and the share name based on the specified criteria.

Directory Name		Host AhmedI	G, na731-rashad	•			
5tart Date 10/14/2009 5	5:09:14 AM	End Date 5/3/201	1 5:37:43 AM				
E 🛐 🕅 🖣 1	of 1 🕨 🕅 🗢 🔕	2 3 🗆 🖬 🖵	• 100%	•	Find Nex	t	
Directory D	eleted						
From: 10/14/2009 5:09:14	4 AM To: 5/3/2011 5	37:43 AM					
Number of records: 18	- AM 10. 3/3/2011 3.	or to min					
				D.F.		CI	
Directory Name 🛛 🖨 Deleted	User Name 👙	Host 💲	Delete 🗘 Date	Policy 🗘 Name	Client ‡ Name	Share Name	ŧ
HOME\BusinessShares\Mark eting\User0006\Old Stuff\	Galactic.com\Platt	na731-rashad	10/14/2009	MKT POL	aasayed-xp-4502	IG - Machine	
			7:59:04 AM	Marketing		indicitation in the	
	Galactic.comWormandy	na731-rashad	7:59:04 AM 10/14/2009 7:38:56 AM	MKT POL	aasayed-xp-4502	IG - Machine	
HOME'BusinessShares\Sup bort/User0012\Old Tickets\ HOME'BusinessShares\Sup bort/User0012\Old Tickets\	Galactic.com/Normandy Galactic.com/Normandy	na731-rashad na731-rashad	10/14/2009	MKT POL Support MKT POL			
oort/User0012\Old Tickets\ HOME\BusinessShares\Sup			10/14/2009 7:38:56 AM 10/14/2009 7:38:56 AM	MKT POL Support MKT POL	aasayed-xp-4502	IG - Machine	
oort/User0012/Old Tickets/ HOME/BusinessShares/Sup oort/User0012/Old Tickets/ HOME/BusinessShares/Sale	Galactic.comWormandy	na731-rashad	10/14/2009 7:38:56 AM 10/14/2009 7:38:56 AM 10/14/2009 7:33:30 AM	MKT POL Support MKT POL Support	aasayed-xp-4502 aasayed-xp-4502	IG - Machine IG - Machine	
ort/User0012/0ld Tickets\ HOME/BusinessShares/Sup ort/User0012/0ld Tickets\ HOME/BusinessShares/Sale VUser0011/0ld Records\ HOME/BusinessShares/Sale	Galactic.comWormandy Galactic.comWantara	na731-rashad na731-rashad	10/14/2009 7:38:56 AM 10/14/2009 7:38:56 AM 10/14/2009 7:33:30 AM 10/14/2009 7:33:29 AM	MKT POL Support MKT POL Support MKT POL Sales	aasayed-xp-4502 aasayed-xp-4502 aasayed-xp-4502	IG - Machine IG - Machine IG - Machine	

f. Deleted Files by Directory: This report allows you to review all the deleted files grouped by directory. The report's input is the directory name, and/or the host, and/or the date range. The report displays the user's name who has deleted the file(s), the path from which the file was deleted, the file name, the host name, the file size, the date on which the file was deleted, the client name used to perform the file delete operation, and the share name based on the specified criteria.

Directory Name		Host	AhmedIG, na731	-rashad	•		
StartDate 10/1	4/2009 5:09:14 AM	EndDate	5/3/2011 8:48:09	9 AM			
E 1 1 4	1 of 1 ▶ ▶ ↔	3 2 3	1	00%	•	Find Next	
Deleted	files by dir	ectory					
Number of records	: 28						
User 🗘	Path 😂	Files 😂	Host 🗘	Size 😂	Delete ≎ Date	Client 🗘 Name	Share \$ Name
Galactic.com\Rober tson	\HOME\BusinessShares\D evelopment\User0001 \Projects On Hold\DD Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:22:21 AM	aasayed-xp-4502	IG - Machine
Galactic.com/wboyd	\HOME\BusinessShares\D evelopment\User0002 \Projects in Progress\Click Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:29:57 AM	aasayed-xp-4502	IG - Machine
Galactic.com\wboyd	VHOMEVBusinessShares\Su pport\User0002\Ticket # 00010\	<u>New Text</u> Document.txt	na731-rashad	0	10/14/2009 5:35:10 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Wolco tt	VHOMEVBusinessSharesVD evelopment/User0003 VProjects Delivered/\QFS Project\	New Text Document.txt	na731-rashad	0	10/14/2009 5:39:25 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Wolco tt	\HOME\BusinessShares\D evelopment\User0003 \Projects in Progress\FTP Project\	t <u>eam notes</u> meeting.txt	na731-rashad	0	10/14/2009 5:44:21 AM	aasayed-xp-4502	IG - Machine

g. **Deleted Files Count by Directory:** This report allows you to review the number of deleted files with a directory. The report's input is the date range and/or the directory name. The report displays the folder path and the number of files deleted within the specified directory/directories within the specified date range.

Deleted files count by directory		
Start Date 10/14/2009 5:09:14 AM End Date 1/14/2011 10:42:51	1 AM	View Report
Directory Name		
I4 4 1 of 1 ▷ ▷ 75% ▼ Find Next	Select a format	Export :
ð <i>3</i>		
Deleted files count by directory Number of records: 21		
Path 🛊	Number of files 💲	
VHO MERBIS is as so value oppoint this end cost of Progress VFTP Projects	з	
VIO MEBAIs he so Shares 'Deue opment'Us ended 4P rojects in Progress'S MSParsen's	3	
VIO MERII siness Shares Veue boment Vise d'0030 id Striff Learning 1 Projects		
VHO INERATIVESS Shares 'Sales' Use not 11'Old Records'	2	
VHO MEM is like so Skales 'Skipport Wise in DED 3/T block # 0016/	2	
WO MEM (shess Shares 'Support We ef DE12O ki Tickets')	1	
VHO MEMBAS he as Skares 'SupportVike r0002(Tbket #00010)	1	

h. **Most Accessed Directories:** This report allows you to review the most-accessed directories. The report's input is the date range, and/or number of most-accessed directories to display. The report displays the directory path and the number of times each directory was accessed.

Most acces	sed directori	es								
Start Date View top (folders) (Maximum number: 2147483647)	10/14/2009 5: 5	:09:14 AM		End Date	1/14/2011 10:	46:24 A	M		View Ro	port
14 4 1	of 1 ▷ ▷ ▮	100%	•		Find Next	Sel	ect a forr	nat	▼ Exp	ort
🔹 📑										
	ccesse	d direct	tori	es						
Number of reco	CCESSE	d direc	tori	es			Nu	mber o	f Accesses	;
Most a Number of reco Directory Path HOME/BusinessS	CCESSE(ords: 5	d direc	tori	es			Nu	mber o	f Accesses	167
Number of reco Directory Patl HOME\BusinessS	CCESSE(ords: 5			es			Nu	mber o	f Accesses	·
Number of reco Directory Patl VHOMEVBusinessS VHOMEVBusinessS	CCESSE ards: 5 h e Sharesl	r0007\TimeSheets\		es			Nu	mber o	f Accesses	167
Number of reco Directory Path HOME\BusinessS HOME\BusinessS HOME\BusinessS	CCESSE(ords: 5 h ÷ Shares\ Shares\Vinance\Use	r0007\TimeSheets\ r0007\Invoices\		es			Nu	mber o	f Accesses	167 152

i. **Directory Owner Changed:** This report allows you to review all directories whose owners have changed. The report displays the directory name, the previous and new owners, the host IP address, the user name, the date, the policy name, the client name and the share name based on the specified criteria

Directory owne	r changed							
Directory Name		Host 10.20.2.57	~					View Re
Start Date	3/14/2011 4:11:45 PM	End Date 3/15/2011 4:13:11 PM						
14 4 1 of	5 🕨 🚺 100% 💌	Find Next Select a format	E)	cport 👔 🍠				
Directory	/ Owners Changed	1						
From: 3/14/2011 4:1	1:45 PM To: 3/15/2011 4:13:11 PM							
Number of records:								
Directory 👙	Previous Owner	New Owner	Host 😄	User Name 😄	Date 😂	Policy 😂	Client	\$ Share \$
	DOTNET.CRITICALSITES.LOCALIMohmoud Ocome	DOTIVET. CRITICAL SITES LOCAL VAbdalla. Hassan	10.20.2.57	DOTNET ORTICALSITES LOCAL Vadministrator	3/14/2011 4:45:44 PM	df		
WOLIVOLD WOMEWCAPTURE PNG	DOTNET.CRITICALSITES.LOCALIMatimoud. Osama	DOTNET.ORITICAL SITES LOCAL Vidministrators	10.20.2.57	DOTNET.ORITICALSITES LOCAL Wdministrator	3/14/2011 4:43:27 PM	df		
WOLWOLD WOMEWCOPY (2) OF NEW BITMAP MAGE EMP	DOTNET.CRITICALSITES LOCAL/Administrators	DOTNET.ORITICALSITES.LOCAL.Wahmoud. Osama	10.20.2.57	DOTNET.ORITICALSITES LOCAL/Administrator	3/14/2011 4:35:55 PM			
WOLWOLD HOMEWCOPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	DOTNET.CRITICALSITES LOCAL/Administrators	DOTNET.CRITICALSITES LOCAL/Mahmoud Osama	10.20.2.57	DOTNET.ORITICALSITES.LOCALV4dministrator	3/14/2011 4:35:55 PM			
WOLWOLD HOMEWCOPY (2) OF NEW MICROSOFT WORD DOCUMENT DOC	DOTNET_CRITICALSITES_LOCAL\Administrators	COTNET.CRITICALSITES LOCAL Mehmoud Osene	10.20.2.57	DOTNET.ORITICALSITES LOCAL Vadministrator	3/14/2011 4:35:55 PM			
WOLWOLD HOMEWCOPY (2) OF NEW TEXT	DOTNET_CRITICAL SITES LOCAL/Administrators	DOTNET.CRITICAL SITES LOCAL Mehmoud. Oseme	10.20.2.57	DOTNET.ORITICAL SITES LOCAL Vadministrator	3/14/2011 4:35:55 PM			

j. **Directory Permission Changed:** This report allows you to review all directories whose permissions have changed. The report displays the directory name, the host IP address, the user name, the date, the policy name, the client name, the share name, and the permission details based on the specified criteria.

Directory Name		Host	10.20.2.57	~	•		
Start Date	3/14/2011 4:	11:45 PM 🔲 End Date 🕄	3/15/2011 4:13:4	4 PM			
	f 12 🕨 🕅	100% T	d Next Selec	t a format	Export	¢ _	
Discotor	Dam	inciana Ohenned					
Director	y Perm	nissions Changed					
From: 3/14/2011 4:	11:45 PM To:	3/15/2011 4:13:44 PM					
Number of records:	503						
			A	Policy 🗘	Client 😩	Share 🔒	Permission
Directory 😂	Host 💲	User Name 👙	Date 😂	Name	Name	Name =	Details
WOLWOLD WHOMEWCOPY (2) OF NEW MICROSOFT EXCEL WORKSHEET XLS	10.20.2.57	DOTNET.CRITICALSITES LOCAL Vadministrator	: 3/14/2011 4:58:10 PM	df			View
WOLIVOLD HOMEWCOPY (2) OF NEVV MICROSOFT WORD DOCUMENT.DOC	10.20.2.57	DOTNET.CRITICALSITES LOCAL Vadministrator	: 3/14/2011 4:58:10 PM	df			View
WOLWOLD WOMEWCOPY (2) OF R.TXT	10.20.2.57	DOTNET.CRITICALSITES LOCALVAdministrator	3/14/2011 4:58:10 PM	df			View
WOLWOLD HOMEWCOPY (3) OF CAPTURE.PNG	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df			View
VOLVOLD VHOMEVCOPY (3) OF NEW/MICROSOFT EXCEL WORKSHEET XLS	10.20.2.57	DOTNET.CRITICALSITES LOCAL Vadministrator	3/14/2011 4:58:10 PM	df			View

NTP Software Smart Policy Manager™

NTP Software Smart Policy Manager Overview

The first step in using NTP Software File Auditor, Windows Edition is to lay out your strategy for managing users' file and directory operations. Before doing this, though, let us look at our underlying policy-based rules engine: NTP Software Smart Policy Manager™.

NTP Software Smart Policy Manager allows you to monitor your users' file and directory operations in a way that is a unique fit to your organization. If you manage by geography or administrative unit, you can use that plan. If you manage by class of machine, that approach works just as well. Often, companies use a mixed mode—perhaps geography, a department, and a machine type. NTP Software Smart Policy Manager has the flexibility you need to make using NTP Software File Auditor, Windows Edition simple.

Once you have laid out your management structure, NTP Software Smart Policy Manager provides policy replication throughout your enterprise. It allows machines to access the policies in their containers and inherit policies from all levels above that point in your hierarchy. You no longer need to configure and manage the machines on your network one by one.

As you start to configure the software you have installed, begin with the top-level container under the root organization (in the following example, *My Site*). This is the Global Network configuration, whose container is created during installation.



Managing the NTP Software File Auditor Service through a NTP Software File Auditor Admin Client Running on a Different Machine

This section provides step-by-step instructions on installing the NTP Software File Auditor Admin Client, enabling you to administer the NTP Software File Auditor service running on a different machine. This kind of NTP Software File Auditor Admin Client installation enables NTP Software File Auditor administrators to easily administer NTP Software File Auditor that is installed on all the servers over the entire network. This can be done through a local user interface that is easily installed on the administrator's local machine.

For an NTP Software File Auditor administrator to be able to use the NTP Software File Auditor Admin Client, NTP Software Smart Policy Manager Admin and NTP Software File Auditor Admin components should be installed on the administrator's local machine per the following instructions.

IMPORTANT NOTES

There is a slight difference in the installation of NTP Software Smart Policy Manager and NTP Software File Auditor on an NTP Software File Auditor Server versus the installation on an administrator's local machine.

NTP Software File Auditor Admin Client User Interface is using Remote RPC to communicate to the NTP Software Smart Policy Manager service. Therefore, NTP Software File Auditor Administrator needs to have permissions to run and execute Remote RPC on the managed machine. A standard user does not have RPC Permission by default. So if the user performing the administration is not an administrator in the domain, the user needs to be added to the **Distributed COM Users** group on the machine to be managed.

Installing the NTP Software Smart Policy Manager Admin Component

- 1. Log on to your local computer, using an account with administrator privileges.
- 2. On the NTP Software Product Installation page, click your product installation link under the **Product Components** section.
- 3. When prompted to install NTP Software Smart Policy Manager, click **Yes** to launch the Installation Wizard.



4. In the NTP Software Smart Policy Manager installation welcome dialog box, click Next.



5. Select I accept the terms of the license agreement in the License Agreement dialog box and then click Next.

NTP Software Smart Policy Manager Setup Wizard	×
License Agreement Please read the following license agreement carefully.	Software [®]
NTP Software Smart Policy Manager(TM) End-User License By using or copying the accompanying software you are indicating your accepterms of this license. If you do not agree to the terms of this license, please reliproduct UNOPENED to your place of purchase for a full refund. GRANT OF LICENSE. NTP Software grants you the right to use Smart Policy ("PRODUCT") on one computer, solely for your or your company's own intern addition to the specified quantity of copies, you may make one (1) additional of backup to the original. However, you may not cause the software to execute into the active memory of more computers than the above-specified quantity at time. In addition the PRODUCT is licensed solely for the management of local	turn the Manager al use. In copy as a or be loaded at any one
I go not accept the terms of the license agreement I go not accept the terms of the license agreement InstallShield < <u>Back</u> Next >	Cancel

6. In the **Choose Destination Location** dialog box, browse to the needed location and then click **Next**.

NTP Software Smart Policy Manager Setup Wizard	×
Choose Destination Location Select folder where setup will install files.	NTP Software®
Setup will install NTP Software Smart Policy Manager in the following folder.	
To install to this folder, click Next. To install to a different folder, click Browse a another folder.	and select
Destination Folder C:\Program Files\Smart Policy Manager	Browse
<u> ≺ B</u> ack <u>Next</u> >	Cancel

7. Select only the Smart Policy Manager Admin component in the Select Features dialog box. Click Next.

NTP Software Smart Policy Manager Setup Wizard	×
Select Features Select the features setup will install.	Software
Select the features you want to install, and deselect the Smart Policy Manager Service Smart Policy Manager Admin	e features you do not want to install. Description Selecting this option will install all of the components required to run the Smart Policy Manager administrative client.
2.89 MB of space required on the C drive 1758.38 MB of space available on the C drive InstallShield	ack <u>N</u> ext > Cancel

8. The Start Copying Files dialog box prompts you to begin copying files.

NTP Software Smart Policy Manager Setup Wizard
Start Copying Files Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Destination Path: C:\Program Files\Smart Policy Manager Components to install: Smart Policy Manager Administration Tool
InstallShield <u>American Cancel</u> Cancel

9. When the file installation is complete, a dialog box offers you the opportunity to view the readme file, which may contain documentation updates and other items. If you *do not* want to view the readme file at this time, clear the option **Yes**, **I want to view the readme file**. Click **Finish**.



Installing the NTP Software File Auditor Admin Component

1. The NTP Software File Auditor welcome dialog box pops up automatically. Click **Next** to continue.



2. In the License Agreement dialog box, select I accept the terms of the license agreement; then click Next.

NTP Software File Auditor® Setup	×
License Agreement Please read the following license agreement carefully.	Software®
NTP Software File Auditor(TM) Base and Terabyte License Agreement IMPORTANT. PLEASE READ CAREFULLY. By using or copying the acc software you are indicating your acceptance of the terms of this license an bound by it. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENS NOT INSTALL OR USE THE PRODUCT. You may return the product UN place of purchase for a refund of your license fee. GRANT OF LICENSE. NTP Software(R) grants you the right to use NTP S Auditor(TM), ("the PRODUCT") on the number of computers and/or vitual which you have paid a license fee, provided the use is solely for your perso company's own internal use. Furthermore, you may only use the PRODUC © Laccept the terms of the license agreement InstallShield	d agree to be E, YOU MUST USED to your Software File machines for onal or your T to manage the v
InstallShield <u>American American Ameri American American Ameri American American Ameri Americ</u>	Cancel

3. In the **Choose Destination Location** dialog box, browse to the desired destination or click **Next** if the default destination location is appropriate.

NTP Software File Auditor® Setup	×
Choose Destination Location Select folder where setup will install files.	Software [®]
Setup will install NTP Software File Auditor in the following folder.	
To install to this folder, click Next. To install to a different folder, click Browse another folder.	and select
Destination Folder	- 1
C:\\NTPSoftware\NTP Software File Auditor	Browse
InstallShield	
< <u>B</u> ack <u>Next</u> >	Cancel

4. In the **Select Features** dialog box, make sure that only the **Admin** component is selected, then click **Next**.

NTP Software File Auditor for Windows Setup	×
Select Features Select the features setup will install.	Software [®]
Select the features you want to install, and dese	Description Select the features you do not want to install. Description Selecting this option will install all of the components required to run the NTP Software File Auditor administrative client. If you choose not to install these components you may still install the NTP Software File Auditor service, but you will not be able to configure it from this machine.
0.00 MB of space required on the C drive 1439.66 MB of space available on the C drive InstallShield	< <u>B</u> ack <u>N</u> ext > Cancel

IMPORTANT:

Because we just need the Admin User Interface to manage and configure the policies, we checked the Admin Client only. We are not seeking a full NTP Software File Auditor, Windows Edition installation.

5. Specify the program folder (using the default program folder is recommended) and click **Next**. The setup program adds program icons to the program folder.

NTP Software File Auditor® Setup	×
Select Program Folder Please select a program folder.	Software*
Setup will add program icons to the Program Fo name, or select one from the existing folders list	
<u>P</u> rogram Folder:	
NTP Software File Auditor	
Existing Folders:	
Accessories Administrative Tools Microsoft SQL Server 2005 NTP Software File Reporter NTP Software File Reporter Reports Pack NTP Software 0DDM NTP Software QFS for NAS NTP Software Storage Investigator Startup	
InstallShield	
	< <u>B</u> ack <u>N</u> ext > Cancel

6. Click **Next** when the **Start Copying Files** dialog box appears (assuming that the destination paths are correct). NTP Software File Auditor setup begins transferring files to the specified locations.

NTP Software File Auditor® Setup	×
Start Copying Files Review settings before copying files.	are®
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.	
Current Settings:	
Destination Path: C:\Program Files\NTPSoftware\NTP Software File Auditor Components to install: File Auditor Service File Auditor Administration Tool Start Menu Folder: NTP Software File Auditor	
InstallShield	
< <u>B</u> ack <u>Next</u> > Cano	el

7. When the files' installation is complete, a dialog box offers you the opportunity to view the readme file. If you *do not* want to view the readme file at this time, clear the option **Yes**, **I want to view the readme file**. Click **Finish**. By this step, NTP Software File Auditor installation is completed.

NTP Software File Auditor® Setup					
	NTP Software Installation Wizard for NTP Software File Auditor Complete				
	The Installation Wizard has successfully installed NTP Software File Auditor. Click Finish to exit the wizard.				
	Yes, I want to view the readme file				
Sefeware*					
	< <u>B</u> ack Finish Cancel				

Administering NTP Software File Auditor through an NTP Software File Auditor Admin Client Running on a Different Machine

- 1. Click Start > Programs > NTP Software File Auditor[™] > NTP Software File Auditor[™] Admin.
- 2. In the Smart Policy Manager dialog box, specify the Smart Policy Manager Server that you want to connect to.

Smart Policy Manager	×				
Enter the name of the Smart Policy Manager server to connect to. If no Smart Policy Manager Server is specified, the local server will be used.					
Smart Policy Manager Server: MYSERVER					
OK Cancel Help					

Note: The Smart Policy Manager Admin component is installed on the local machine, so there is no Smart Policy Manager service installed. Thus, NTP Software File Auditor, Windows Edition cannot talk to the local Smart Policy Manager service because it does not exist, so we specify the Smart Policy Manager service that NTP Software File Auditor, Windows Edition should communicate with.

In very large organizations, you may have offices all over the world. Make sure you connect to the server(s) at reasonable distance to maintain good speed.

As shown, the NTP Software File Auditor Admin Client User interface is displayed with **MYSERVER** as a node in the left menu tree and all the NTP Software File Auditor policy details.

 To connect to more than one Smart Policy Manager service at the same time, click File > Active Server, then insert the server name or the server IP address. This allows you to add all the servers on your entire network to administer them as needed.

Installing NTP Software File Auditor in Clustered Environments

Note

• NTP Software File Auditor, Windows Edition requires a manual setup by an administrator for clustered environments.

Installing NTP Software File Auditor, Windows Edition in Clustered Environments

To install NTP Software File Auditor, Windows Edition in a clustered environment, apply the following steps:

- 1. Install NTP Software File Auditor, Windows Edition on a server, as described in NTP Software File Auditor installation guides.
- 2. After NTP Software File Auditor, Windows Edition is installed successfully, open NTP Software File Auditor, Windows Edition to find the global container (**My Organization** in this example) at the top of the hierarchy. Click the plus sign (+) to expand the container.
- 3. Click the plus sign (+) to expand your site container in the second tier of the hierarchy.

Notice the installation server in the third tier of the hierarchy. The NTP Software File Auditor, Windows Edition application is also in the third tier.

TP Software Smart Policy Manager (TM)							
File Edit View Options Help							
🍯 🕺 🖻 🖻 🗡 🖆 🕒 🏥	m						
	Name 🗸	Туре	Status	Description	Created	Modified	
WTP Software File Auditor Quota & File Sentinel WySite WySit	GIMySite ☐ Quota & File ☐ NTP Software			NTP Softw	6/9/09 19:12:02 6/9/09 19:15:54 3/2/11 17:27:42	4/29/11 03:04:3 6/9/09 19:15:54 3/2/11 17:27:42	
	•						
3 object(s)				CLTESTBOX (L	ocal Host)		

- 4. Right-click the site container and then select **New > Container** from the pop-up menu to create your cluster container. Give the new container the name of the cluster. In the example, we have used **Cluster 1** as the name.
- 5. Right-click the cluster container and select **New** > **NTP Software File Auditor Application** from the pop-up menu.

Notes:

To add the rest of the Nodes of the Cluster follow one of these options:

• Push software to node.

To push the software to the new node follow these steps:

- a. Add a server object to the cluster container.
- b. You will be asked to install Smart Policy Manager on the new node.
- c. After the new node is added, add a File Auditor application object to the new server object.
- d. You will be asked if you want to install File Auditor onto the remote machine.
- Use a local install.

To perform a local install of File Auditor onto the other nodes of the cluster follow these steps:

a. Choose the **Join an Existing Hierarchy** option during the installation of Smart Policy Manager.

- b. When that completes, the installation of File Auditor will continue.
- c. When File Auditor has been installed, you will need to move the new node under the 'cluster' container.
- 6. Open the cluster container in the NTP Software Smart Policy Manager hierarchy and use the drag-and-drop method to move the nodes into the cluster container. They will appear at the same level as the container File Auditor[™] application.
- 7. Click the plus sign (+) next to the NTP Software File Auditor, Windows Edition application you have just added to view the global (cluster) policies. Create all policies within this application that will be applied to both nodes. They will be propagated automatically to all nodes within the container.

Installing NTP Software File Auditor onto a Node Server

To install NTP Software File Auditor, Windows Edition onto a node server, apply the following steps:

- 1. NTP Software File Auditor, Windows Edition enables you to push installation to each of the added nodes.
- 2. Right-click the site container and select **New > Container** to create a container for the cluster. Give the new container the cluster name.
- 3. Click the existing server (node) and, while holding down the mouse button, drag and drop the server onto the cluster container to move the server into the cluster hierarchy.
- 4. Right-click the cluster container and select **New > NTP Software File Auditor Application** from the pop-up menu.
- 5. To view the global (cluster) policies, click the plus sign (+) next to the NTP Software File Auditor, Windows Edition application you have just added.

Note:

If you choose to install both nodes locally, then you need to perform a join operation during the smart policy manager install and then move each added cluster node under the appropriate container.

Create all policies within this application that will be applied to both nodes. They will be propagated down automatically to all nodes within the container.

About NTP Software®

NTP Software[®] is the worldwide leader in user-focused, policy-based storage management. We create platform-independent products that enable companies to automatically control the compliance, access, quotas, content, and lifespan of their users' stored files. NTP Software[®] solutions also gather the analysis and planning data necessary for both short- and long-term decision making, providing everything necessary to actively control all aspects of a user's relationship with local and shared storage.

NTP Software® Professional Services

For further assistance with NTP Software File Auditor[™] or in creating a corporate storage management policy, contact your NTP Software[®] representative at 800-226-2755 or 603-622-4400.

NTP Software[®] Professional Services offers training and consulting services in support of the deployment and configuration of your storage resource management software.

NTP Software 20A NW Boulevard #136 Nashua, NH 03063 Toll Free: 800-226-2755 International: 1-603-622-4400 E-mail: <u>info@ntpsoftware.com</u> Web Site: http://www.ntpsoftware.com