

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
C Export as XML (• Export to SUL Server
SQL Server:
Database: Tiest
- Size Limit
specify the number of records to be retained in the database (in thousands or 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 O Export as XML O Export as raw data
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**.

ip: Click the Test Connection button to test your connection to the specified SMTP Sever
NTP Software File Auditor™ Configuration
Database Configuration Email Configuration Misc. Options Security
Inherit Email Configuration
Enable Email Notifications
SMTP SERVER NAME
SMTP Domain: SMTP DOMAIN NAME
Sender's Address: SENDER ADDRESS
My server requires authentication
Username: SERVER USERNAME
User Domain: USER DOMAIN
Password:
Confirm 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.

Inherit Directory Use Active Use LDAF Append th	Connector Properties Directory Connector to ret Connector to retrieve emai e SMTP Domain to form en	rieve email addresses I addresses nail addresses
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
Everyone	9		Bemove
Non-Owner <u>F</u>	Permissions		
	- Local Policies	Inherited Policies	Properties
Full Control:	۲	۲	۲
Read Only:	0	0	0
None:	C	с	0
wner:		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:		
Distinguished t	Name:		
Distinguished I	Name:	Last Modified by:	
Distinguished f	Name:	Last Modified by:	
Distinguished M Policy Owner:	Name:	Last Modified by:	
Distinguished M Policy Owner:	Name:	Last Modified by:	
Distinguished I	Name:	Last Modified by:	
Distinguished I Policy Owner:	Name: dnesday, December 01 thesday, December 01	Last Modified by:	
Distinguished M Policy Owner:	Name: dnesday, December 01 dnesday, December 01	Last Modified by:	

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				×
Exempt Users -	and Groups	Notifications	DB Ma	aintenance	
Exempted 9	Subdirectories	Audited	d Users and (Groups	
General	Monitored Events	File Crite	ria	Directories	Ļ
Patterns:					
Common Aug	lio Files				
		I		!	
	1				
A <u>d</u> d	<u> </u>	<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
Exempted	Subdirectories	Audit	ed Users -	and Groups
Exempt Users	and Groups	Notifications	D	B Maintenance
Accounts:				
	dministrators			
BUILTIN\B	ackup Operators			
BUILTIN\R	eplicator			
SINT AUTHO	RITY\SYSTEM			
•				Þ
•				Þ
Add	Edit	Remove		Þ
∢ A <u>d</u> d	<u><u> </u></u>	<u>R</u> emove]	Þ
∢ Agd	<u>E</u> dit	<u>H</u> emove	1	Þ
Agd	<u>E</u> dit	Eemove		Þ
Add	<u>E</u> dît	<u>R</u> emove		Þ
Add	<u>E</u> dit	<u>H</u> emove		Þ
Agd	<u>E</u> dit	Eemove		×

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

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 audit users through policy %p on servel %s. The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time User Account Deta Size Deta Size Share Name OK Cancel
Email Subject: Notification %n for policy %p Email Body This is a notification email for the specified events generated by audit users through policy %p on servel %s. The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Beceived Time Operation Type Path Bile Size Delta Size Share Name OK Cancel Help
Image: Contract of the specified events generated by audit users through policy %p on served %s. The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time Operation Type Operation Type Path File Size Delta Size Share Name OK Cancel
Email Body This is a notification email for the specified events generated by audit users through policy %p on servet %s. The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time Operation Type Path File Size Delta Size Share Name OK Cancel Help
This is a notification email for the specified events generated by audit users through policy 2p on servel %s. The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time User Account Operation Type Path File Size Delta Size Share Name OK Cancel Help
The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed.
The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Beceived Time User Account Operation Type Path File Size Delta Size Share Name OK Cancel Help
The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time User Account Operation Type Path File Size Delta Size Share Name OK Cancel
The email contains a table of audited users along with events details generated by them. Please choose the the columns to be displayed. Received Time User Account Operation Type Path File Size Delta Size Share Name
Order By Order By Operation Type Path File Size Delta Size Share Name
Utder By User Account Operation Type Path File Size Delta Size Share Name
Operation Type Image: Constraint of the state of the
Path File Size Delta Size Share Name OK Cancel Help
C User
OK Cancel Help
OK Cancel Help
OK Cancel Help
OK Cancer Heip
ail Configurations Properties
General Email Settings Notification Settings Recipients
Notification Frequency
O Notify for every operation
Notify no more than once every 1 Minute(s)
Event types you want to receive:
OK Cancel Help
mail Configurations Properties
General Email Settings Notification Settings Recipients
Notify Triggering User
✓ Notify Owner
Notify Owner Notify Other Recipients
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List:
Notify Owner Notify Other Recipients Other Recipients List: Add Edit

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
		'		i i
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		
	or 1	Canada I		
				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	
1	
Add <u>E</u> dit <u>R</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		×
General Exempt User Exempte	Monitored Events s and Groups d Subdirectories	File Criteria Notifications Audited Us	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	E elit	Remove	
Aga	<u>E</u> dl	Temove	
	OK	Cancel <u>App</u>	bly 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.

User Account				Access Type	Directory Crea	te, Directory De	-						
Start Date	10/14/2009 5	:09:14	4M 🛄	End Date	5/3/2011 8:53:	20 AM			ľ				
Host	AhmedIG, na	731-ras	had 💌										
E ¶1 K	4 1	of 23	3 🕨 🕅 🔶 🕻) 🛃 🖾 🕻	🛯 🖬 🖬 • 📔	100%	-	Find Next					
User	User Audit												
		-											
From: 10/14.	2009 5:09:1	I4 AM	To: 5/3/2011	8:53:20 AM									
Number of re	ecords: 1000)											
Цери	Object	^	Diverteru A	Linet A	Access .	Data A	Doligu A	Client A	Chave A				
Name	Name	₹	Path	HUSL 👳	Type	Date 🤿	Name 🗸	Name	Name				
Galactic.com\C ver	lo <u>Sales</u>		\HOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:46 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com\C ver	lo <u>Support</u>		\HOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:43 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com\C ver	lo <u>Support</u>		\HOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:42 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com/C	lo <u>Support</u>		\HOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:38 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com/C	lo Support		VHOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:36 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com/C ver	lo Support		VHOME\Business Shares\	na731- rashad	File Open For Write	10/14/2009 7:59:33 AM	MKT POL User6	aasayed-xp- 4502	IG - Machine				
Galactic.com\C ver	lo User0014	L	\HOME\Business Shares\Support\	na731- rashad	File Open For Write	10/14/2009 7:59:33 AM	MKT POL Support	aasayed-xp- 4502	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		Accessed i (Maximum	in the last (days) number: 93852)	78947			
Object Name readm	ne.txt	Access Typ	pe	Director	y Create, Director	y De 💌	
• M M •	1 of 3 🕨	N + 🛛 🖻 🎒	🔲 🛍 🛃 •	100%	•	Find Next	
Access	History						
Number of record	s: 92						
User Name 🖨	Object ‡ Name	Directory Path 💲	Access ≑ Type	Access ≑ Date	Policy 😂 Name	Client 🗘 Name	Share 😂 Name
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Close	10/14/2009 7:56:48 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Open For Write	10/14/2009 7:56:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Close	10/14/2009 7:56:46 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Close	10/14/2009 7:56:46 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/Platt	Readme.txt	VHOMEVBusinessShares\ MarketingVUser0006\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	VHOMEVBusinessShares\ MarketingVUser0006\Old	File Open For Write	10/14/2009 7:56:42 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com/wood	readme.txt	VHOMEVBusinessShares\ Support/User0013\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	of 1 ▷ ▷∥	75%	•		Find Nex	t Select a	ormat	Export	
2 4									
Vlostacti	ve users								
Viost acti umber of records: 6	ve users								
Wost acti lumber of records : { lser :	ve users				Numbe	r of activities 🛊			
Most acti Number of records : 4 Joer : (bgreat.com/Do/a2010	ve users				Numbe	r of activities 🗘	1359		
Most acti Number of records : 4 User : Page at com Vio 1 a 20 10 (bge at com Vio 1 a 20 10	ve users				Numbe	r of activities 💲	1369		
Most acti Aumber of records : 4 (bgreat.com/to/ka2010 (bgreat.com/to/ka2010 (bgreat.com/to)	ve users				Numbe	r of activities 🗄	1359 17 12		
Most acti Aumber of records : (Jeer 2 (depret.com/to/ta21/10 (depret.com/t22101a (depret.com/t00 (depret.com/t00)	ve users				Numbe	r of activities 🔅	1359 17 12 12		

- 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	nedIG, na731-ras	had 💌			[
Start Date	0/14/2009 5:09:14 A	м	End Date 5/3	/2011 8:44:37 AM								
Access Type	File Close, File Create	, File Dele 💌	File Type bmp	o, cpp, doc, h, rtf	, tmp, txt 💌							
E 1 K	4 1 of 2	3 🕨 🎽 🔶 🕻) 🛃 🖾 🛄	💷 🛃 • 10	• •		Find Next					
File Audit												
Erom: 10/14	0000 5:00:17 AM	Te: 5/3/0011	9-44-37 AM									
Number of re	2003 3.03.14 AM	10. 3/3/2011	0.44.37 AN									
Number of re	cords: 1000											
File 🗘	Directory 💲	Host 😂	User 😂	Access 😂	Access 👙	Policy 🗘	Clien 😂	Share 😂				
, tunic			Nume	1700	Dute	- Contraction of the second se	Name					
Readme.txt	VHOME\Business Shares\Marketing	na731-rashad	Galactic.com\P	File Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-	IG - Machine				
	User0006\Old Stuff\		ion.		1.00.04 AM	marketing	1002					
ScreenShoot.b	VHOME\Business	na731-rashad	Galactic.com/P	File Open For Read	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-	IG - Machine				
	VUser0006\Old Stuff\		inter and a second seco	ricuu	1.00.04 AM	marketing	4002					
New Text	HOME\Business	na731-rashad	Galactic.com/P	File Open For	10/14/2009 7:50:00 AM	MKT POL	aasayed-xp-	IG - Machine				
<u>oocumentitxt</u>	User0006\Africa Customers\		ICILL.	V VILC	7.58.00 AM	manicality	4502					
New Text Document.txt	VHOME\Business Shares\Marketing	na731-rashad	Galactic.com\₽ latt	File Rename	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp- 4502	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.

5tart Date 10,	(14/2009 5:09:14 AM		End Date	5/3/2011 8:45:25	AM			
≣n⊧⊮ Files	Change	▶ н е б d] (1 <mark> -</mark> 1	00%		Find Next	
From: 10/14. Number of re Tile ¢ Name	/2009 5:09:14 AM ecords: 152 Directory ≎ Path	To: 5/3/2011	8:45:25 AM	Access ≑ Type	Change ≑ Date	Policy ≑ Name	Client ≑ Name	Share \$
			е					
lew Text locument.txt	VHOME\Business Shares\Marketing	na731-rashad	Galactic.co mVPlatt	File Rename	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine
	Customers\							
lew Bitmap nage.bmp	User 0000 Anica Customers\ VHOME\Business Shares\Marketing VUser0006\Old Stuff\	na731-rashad	Galactic.co mPlatt	File Rename	10/14/2009 7:56:20 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine
lew Bitmap hage.bmp	User0004/Inda Customers\ HOME/Business Shares/Marketing User0006/Old Stuff\ HOME/Business Shares/Develop ment/User0005 \Projects in Progress(IGS Project)	na731-rashad na731-rashad	Galactic.co mVPlatt Galactic.co m\Topper	File Rename	10/14/2009 7:56:20 AM 10/14/2009 7:50:07 AM	MKT POL Marketing MKT POL Dev	aasayed-xp- 4502 aasayed-xp- 4502	IG - Machine 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	st AhmedIG, na73	1-rashad 📃 💌									
Start Date 10/14/	2009 5:09:14 AM		d Date 5/3/2011 8:47:0	4 AM	3								
File Type bmp, o	app, doc, h, rtf, tmp,	txt 💌											
E 1 K -	🖣 1 of 1 🕽	▶ ← 😣 🛛	2 4 🗉 🖬 🚽	100%	•	Find Next	t						
Files D	Files Deleted												
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	VHOMEVBusiness SharesWarketing VUser0006\Old Stuff\	na731-rashad	Galactic.com/Platt	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine						
i <u>nstructions.doc.t</u> ⊻t	VHOMEVBusiness Shares/Develop ment/User0005 VProjects in Progress/GIS Project\	na731-rashad	Galactic.com\Topper	10/14/2009 7:47:01 AM	MKT POL Dev	aasayed-xp- 4502	IG - Machine						
l <u>sits.txt</u>	VHOME\Business Shares\Support\ User0012\Old Tickets\	na731-rashad	Galactic.comWorman dy	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp- 4502	IG - Machine						
lists.txt	\HOME\Business Shares\Sales\Us	na731-rashad	Galactic.com\Xantara	10/14/2009 7:33:29 AM	MKT POL Sales	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 10/1	4/2009 5:09:14 4	M 🛄	End Date 5/3/20	011 8:50:12 AM				L			
File Type bmp), cpp, doc, h, rtf,	tmp, txt, 💌									
i 📰 📬 M	4 1 of	4 ▶ ▶ (= (3 🛃 🖂 🔲 (100	% .	•	Find Next				
Files	Renam	ed									
From: 10/14/2	2009 5:09:14 A	M To: 5/3/2011	8:50:12 AM								
Number of rec	Number of records: 152										
Origina 💲 I File Name	New \$ File Name	Directory \$ Path	New \$ Directory Path	User \$ Name	Rena ≑ me Date	Policy \$ Name	Client \$ Name	Share ≑ Name			
<u>New Text</u> Document.txt	Readme.txt	\HOME\Business Shares\Warketing \User0006\Africa Customers\	WNA731- RASHAD\HOME\ BusinessShares\ Marketing\User00 06\Africa Customers\	Galactic.com/P latt	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine			
New Bitmap Image.bmp	ScreenShoot.b mp	VHOME\Business Shares\Marketing VUser0006\Old Stuff\	WNA731- RASHAD\HOME\ BusinessShares\ Marketing\User00 06\Old Stuff\	Galactic.com/P latt	10/14/2009 7:56:20 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine			
<u>GISMain.h</u>	<u>CGISMain.h</u>	VHOME\Business Shares\Develop ment\User0005 VProjects in Devenues\OE	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.

File Name		Host	AhmedIG, na731-r	ashad 💌							
Start Date 10/14/20	009 5:09:14 AM	End Date	5/3/2011 8:46:17	AM 🛄							
File Type bmp, cp	p, doc, h, rtf, tmp, txt 💌	1									
E 1 K 4	1 of 6 🕨 🎽	4 🔕 🛃 🎒	🔲 ûn 🛃 -	100%	•	Find Nex	t				
Files CI From: 10/14/2009 Number of record	Files Created From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:46:17 AM Number of records: 235										
File Name 🖨	Directory 🗘 Path	Host 😂	User 🗘 Name	Create 💲 Date	Policy 🗘 Name	Client 🗘 Name	Share ≎ Name				
New Text Document.txt	VHOMEVBusinessShar esVMarketingVUser000 6VAfrica CustomersV	na731-rashad	Galactic.com\P latt	10/14/2009 7:58:56 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine				
New Text Document.txt	VHOMEVBusinessShar esWarketingVUser000 6\Old Stuff\	na731-rashad	Galactic.com\P latt	10/14/2009 7:56:35 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine				
New Bitmap Image.bmp	HOME/BusinessShar es/Marketing/User000 6/Old Stuff\	na731-rashad	Galactic.com\P latt	10/14/2009 7:56:12 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine				
August TimeSheet.xls	HOME/BusinessShar es/Finance/User0006 \TimeSheets\	na731-rashad	Galactic.com\P latt	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp- 4502	IG - Machine				
July Invoice.xls	HOME/BusinessShar es/Finance/User0006 Vovoices)	na731-rashad	Galactic.com\P latt	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp- 4502	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.

		Host	AhmedIG	5, na731-rashad	•			
Start Date 1	0/14/2009 5:09:14 AM	End C) Date 5/3/2011	1 3:19:17 PM				L
File Type b	mp, cpp, doc, h, rtf, tr	np, txt. 💌						
E 🚹 🗆	🖣 🖣 1 of 3	H + 3 2		🛃 🗸 100%	-		Find Next	
Files	4/2009 5:09:14 AM	To: 5/3/2011 3:19	:17 PM					
Number of	records: 103							
File 😂 Name I	Source 🗢	Destination 🗘	Host 😂 🚽	User 😂	Move 🚖	Policy 🚖	Client 🚖	Share 🔺
	Patri	Path		Name	Date	Name	Name	Name
	HOME\BusinessSh ares\Marketing\User 0006\New Folder	Path WNA731- RASHAD\HOME\Busi nessShares\Marketing Ulser0006\Africa Customers	na731- rashad	Name Galactic.com/P latt	Date 10/14/2009 7:58:47 AM	Name MKT POL Marketing	Name aasayed-xp- 4502	Name IG - Machine
	HOMEVBusinessSh aresWarketingUJser 0006Wew Folder HOMEVBusinessSh aresWarketingUJser 0006Wew Folder	Path WNA731- RASHADWOMEVBusi nessSharesWarketing User0006VAfrica Customers WNA731- RASHADWHOMEVBusi nessSharesWarketing User0006Vold 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	Name aasayed-xp- 4502 aasayed-xp- 4502	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.

E :1. O:		New word							
File O	whers C	Inanged							
From: 3/14/201	11 4:11:45 PM T	o: 3/15/2011 4:02:02 PM							
Number of reci	ords: 180								
File Name 👙	Directory 😫	Previous Owner	New Owner	Host 🛊	User Name 👙	Date 😫	Policy 😂	Client \$ Name	Share 💲
NEW, MICROSOFT EXCEL, WORKSHEET, XLS	WOLIVOL0 HOME:	DOTNET CRITICAL SITES LOCAL Mehmoud. Oserne	DOTNET CRITICAL SITES LOCAL VANSHIN, Hissein	10.20.2.57	DOTNET. ORTICAL SITES LOCAL Viden instrutor	3/14/2011 4:45:44 PM	df		
CAPTURE PNG	WOLWOLD HOME	DOTNET.CRITICALSITES LOCAL Mahmoud, Osama	DOTNET.CRITICALSITES.LOCALVAdministrators	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:43:27 PM	df		
COPY (2) OF NEW BITMAP MAGE EMP	WOLWOLD (HOME)	DOTNET.CRITICALSITES LOCAL/Administrators	DOTNET_CRITICALSITES_LOCALWebmoud Osema	10.20.2.57	DOTNET_CRITICALSITES LOCAL Vadministrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MCROSOFT EXCEL WORKSHEET XLS	IVOLIVOL0 HOMEL	DOTNET CRITICAL SITES LOCAL VAdministrators	DOTNET_CRITICALSITES_LOCAL/Mehmoud_ Opening	10.20.2.57	DOTNET.CRITICALSITES.LOCALVadministrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MICROSOFT WORD DOCUMENT DOC	WOLIVOLD HOMEL	DOTNET CRITICAL SITES LOCAL Vadministrators	DOTNET CRITICAL SITES LOCAL Mehmoud Oseme	10.20.2.57	DOTNET.ORITICALSITES LOCAL Vidministrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW TEXT DOCUMENT TXT	WOLWOLD HOME!	DOTNET CRITICALSITES LOCAL/Administrators	DOTNET.CRITICALSITES LOCAL Webmoud	10.20.2.57	DOTNET.ORITICALSITES LOCAL Vadministrator	3/14/2011 4:35:55 PM	df		
COPY (8) OF	WOLWOLD	DOTNET CRITICAL SITES LOCAL VAdministrators	DOTNET.CRITICALSITES.LOCAL/Mahmoud	10.20.2.57	DOTNET CRITICAL SITES LOCAL Videninistrator	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.

File Pe	rmissio	ons C	hanged						
From: 3/14/201	1 4:11:45 PM T	o: 3/15/2011	4:04:30 PM						
Number of recor	rds: 503								
File Name 💲	Directory 😂	Host 😂	User Name 👙	Date 😂	Policy \$ Name	Client Name	\$ Share Name	¢	Permission Details
COPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	WOLWOLD WHOME	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df				<u>View</u>
COPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	WOLWOLD WOME	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df				View
COPY (2) OF R.TXT		10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df				View
COPY (3) OF CAPTURE.PNG		10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df				View
COPY (3) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	<u>IVOLIVOLO</u> VHOMEL	10.20.2.57	DOTNET.CRITICALSITES LOCALVAdministrator	3/14/2011 4:58:10 PM	df				<u>View</u>
COPY (3) OF NEW MICROSOFT WORD DOCUMENT.DOC	<u>IVOLIVOLO</u> VHOMEL	10.20.2.57	DOTNET.CRITICALSITES.LOCALVAdministrator	3/14/2011 4:58:10 PM	df				<u>View</u>
COPY (3) OF R.TXT	VOLVOLD	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df				View
CAPTURE PMG	WOLWOLD	10 20 2 57	DOTNET CRITICAL SITES LOCAL ladministrator	3/14/2011	dt				View

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	Select a format 💌 Exp
File Permissions Changed	I	
File Name: COPY (2) OF R.TXT		
User Name: \Everyone		
	Previous	Current
Has Full Control	×	×
Has Execute	×	✓
Has Read	✓	✓
Has Read Attributes	✓	✓
Has Read Extended Attributes	✓	✓
Has Write	✓	✓
Has Append	✓	✓
Has Write Attributes	×	✓
Has Write Extended Attributes	 Image: A set of the set of the	✓
Has Delete	×	×
Has Read SD	 Image: A second s	✓
Has Change DACL	×	×
Hao Tako Ownorshin	¥	¥

- 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.

Start Date 10/14/20	109 5:09:14 AM	🛄 End Dat	e 5/3/2011 8:52:08	AM 🛄			
Policy DemoPoli	icy, MKT POL Dev, M	K 💌					
E 🚹 🛛 🖉	1 of 23 🕨	▶ ← 🛛 🛃	a 🛛 🖬 🔒	100%	•	Find Ne:	xt
Policy b	by Date						
From: 10/14/2009	5:09:14 AM T	io: 5/3/2011 8:52:0	8 AM				
Number of record	s: 1000						
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 ver	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 8:33:59 AM III	End Date	3/3/2010 8:44:5	0 AM	View Report	
I4 4 1 of 1 ▷ ▷I 75%		Find Next	Select a format	Export	\$
¢ _					
Directory Summary Report					
Number of audited directories: 4					
Number of deleted directories: 0	Numberofon	eated directories: 4			
Number of renamed directories files : 0_					

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.

Directory Name			Host	AhmedIG, n	a731-rashad	•		[
Start Date 1	0/14/2009 5:09:1	4 AM	End Date	5/3/2011 5:	14:11 AM			ľ
Access Type	irectory Create, I	Directory De 💌						
🖻 🚹 M 🖂	1 of 6	▶ ¥ ← ©) 🛃 📑 🔲	A 🖬 🖬 🖬	100%	•	Find Next	
Directo	ory Au	dit						
From: 10/14/200	9 5:09:14 AM	To: 5/3/2011	5:44:11 AM					
Number of recor	ds: 249							
							1	
Directory Name	♦ User Name	≎ Host ≎	Access Type	≑ Ai Da	icess 🗢 ite	Policy Name	Client \$	Share 😂 Name
VHOME\BusinessSh es\Marketing\User0 6\Old Stuff\	ar <u>Galactic.co</u> 00 t	<u>m)Plat</u> na731-ras	had Directory Delete	/	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOME\BusinessSh es\Marketing\User0 6\New Folder\	ar <u>Galactic.co</u> 00 t	<u>m'Plat</u> na731-ras	had Directory Rename	/	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOME\BusinessSh es\Marketing\User0 6\New Folder\	ar <u>Galactic.co</u> 00 t	<u>m'Plat</u> na731-ras	had Directory Create	/	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOME\BusinessSh es\Marketing\User0 6\New Folder\	ar <u>Galactic.co</u> 00 t	<u>m'Plat</u> na731-ras	had Directory Rename	/	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOMEVBusinessSh esVMarketing/User0 6VNew Folder\	ar <u>Galactic.co</u> 00 t	<u>m'Plat</u> na731-ras	had Directory Create	/	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	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.

Directory Name		Host Al	nmedIG, na731-rashad	•		
Start Date 10/14/2009 5	:09:14 AM 🛄	End Date 5/	3/2011 8:51:00 AM			
i <mark>≣ 1</mark> 4 4 1	of 3 🕨 🎽 🐗	3 🖻 🎒 🗐 A] 	•	Find Next	
Directory C	reated					
From: 10/14/2009 5:09:14	AM To: 5/3/201	1 8:51:00 AM				
Number of records, 100						
Number of records: 128						
Directory Name 🛛 🗘 Created	User Name	Host 💲	Create Date 💲	Policy 🗘 Name	Client ≑ Name	Share ≑ Name
VHOMEVBusinessSharesVMark etingVUser0006VNew Folder\	Galactic.com/Platt	na731-rashad	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOMEVBusinessSharesVMark etingVUser0006VNew/Folder\	Galactic.com/Platt	na731-rashad	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
VHOMEVBusinessSharesVFina nceVUser0006\TimeSheets\	Galactic.com/Platt	na731-rashad	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
VHOME\BusinessShares\Fina	Galactic.com/Platt	na731-rashad	10/14/2009 7:53:15 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
nce\User0006\Invoices\						
nce/User0006/Invoices/ HOME/BusinessShares/Fina nce/User0005/TimeSheets/	Galactic.com\Toppe	na731-rashad	10/14/2009 7:50:23 AM	MKT POL Finance	aasayed-xp-4502	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 🛛 💌]		[
Start Date 10/14/20	009 5:09:14 AM	End Da	:e 5/3/2011 5:4	7:12 AM	1		
1 🖬 🛐 🛛 🖓 🔹	of 3 🕨 🎽 🗇	3 🛃 🎒	🛛 🕼 🖉 -	100%		Find Next	
Directory	Renamed	ł					
From: 10/14/2009 5:0	9:14 AM To: 5/3/20	011 5:47:12 AM	Л				
Number of records: 10	13						
Original ≑ Directory Name	New ≑ Directory Name	Host \$	User ≎ Name	Rename ≑ Date	Policy 🗘 Name	Client ≑ Name	Share ≑ Name
VHOMEVBusinessShares\ MarketingVUser0006 VNew Folder\	WNA731- RASHAD/HOME/Busi nessShares/Marketing User0006/Africa Customers/	na731-rashad	Galactic.com\P latt	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine
VHOMEVBusinessShares\ MarketingVJser0006 VNew Folder\	WNA731- RASHADVHOMEVBusi nessShares/Marketing VUser0006/Old Stuff/	na731-rashad	Galactic.com/P latt	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp- 4502	IG - Machine
HOMEYBusinessShares\ Development/User0005 \Completed Projects\New Folder\	WNA731_ RASHAD\HOME\Busi nessShares\Developm ent\User0005 \Completed Projects\GDS Project\	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 Obroedi	5 pa731-rachad	-		
Start Date 10/14/2009 5	5:09:14 AM	End Date 5/3/201	1 5:37:43 AM			
1011 (2003 0		10/0/201	1 3137713 HIT			
📰 🎦 14 🖪 1	of 1 🕨 🕅 👄 🔘	2 4 🛛 🖬 🚽	• 100%	•	Find Next	
Directory D	eleted					
5 40/4 4/2020 5-00-4	ANA T- 500044 5	27.42.414				
From: 10/14/2009 5:09:14	4 AM To: 5/3/2011 5:	37:43 AM				
Number of records: 18						
Directory Name 🛛 😂 Deleted	User Name 👙	Host 💲	Delete ≑ Date	Policy 🗘 Name	Client ≎ Name	Share ≎ Name
HOME/BusinessShares/Mark eting/User0006/Old Stuff/	Galactic.com/Platt	na731-rashad	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
<u>HOME\BusinessShares\Sup</u> port\User0012\Old Tickets\	Galactic.com/Normandy	na731-rashad	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp-4502	IG - Machine
HOME\BusinessShares\Sup port\User0012\Old Tickets\	Galactic.com/Normandy	na731-rashad	10/14/2009 7:38:56 AM	MKT POL Support	aasayed-xp-4502	IG - Machine
VHOMEVBusinessShares\Sale s\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:30 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
VHOME\BusinessShares\Sale s\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:29 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
VHOME/BusinessShares/Sale s/User0009/Old Customers/	Galactic.com/Merrill	na731-rashad	10/14/2009 7:21:45 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
HOME\BusinessShares\Mark eting\User0008\France Plans\	Galactic.com\Clover	na731-rashad	10/14/2009 7:04:47 AM	MKT POL Marketing	aasayed-xp-4502	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	10/14/2009 5:09:14 AM	EndDate	5/3/2011 8:48:09	AM			ľ
E 1 K	4 1 of 1 ▶ ▶ ↓	3 👌 🖾 🗖	🗋 💭 🖌 🕴 10	00%	•	Find Next	
Delete	Deleted files by directory						
User 😂	Path ≑	Files 🗘	Host \$	Size 💲	Delete ≑ Date	Client ≑ Name	Share ≑ Name
Galactic.com\Ro tson	ber VHOMEVBusinessSharesVD evelopmentVUser0001 VProjects On HoldVDD Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:22:21 AM	aasayed-xp-4502	IG - Machine
Galactic.com/w/k	oyd VHOMEVBusinessSharesVD evelopment/User0002 VProjects in ProgressVClick Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:29:57 AM	aasayed-xp-4502	IG - Machine
Galactic.com/w/k	WOME\BusinessShares\Su pport\User0002\Ticket # 00010\	New Text Document.txt	na731-rashad	0	10/14/2009 5:35:10 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Wo tt	ICO HOME\BusinessShares\D evelopment\User0003 \Projects Delivered\QFS Project\	New Text Document.txt	na731-rashad	0	10/14/2009 5:39:25 AM	aasayed-xp-4502	IG - Machine
Galactic.com\W/c tt	ICO VHOMEVBusinessSharesVD evelopment/User0003 VProjects in ProgressVFTP 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	L 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 MEVBILIS helds Shares Value oppment Vulse (CICID 3/Projects In Progress VFTP Project).	з	
VIO MEBBis she sa Sika res "Deue opment"Us en DED 4/P rojects in Progress s'S MSParse n	з	
VIO MERII siness Shares Veue boment Vise d'0030 id Striff Learning 1 Projects	2	
WOILEVELS hess States Sales Use not 11 Old Records \	2	
WO MEM is like so Skares 'Skipport Word DD 3/T bleet # 0016\	2	
WO MEM (shess Shares 'Support Wile (IDD12O k) Trakets')	1	
VHO MENE is the sis Shares 'Support'Use in DED 20Th ket # DED 10 \	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 directorie	es								
Start Date View top (folders) (Maximum number: 2147483647)	10/14/2009 5: 5	09:14 AM		End Date	1/14/2011 10:	16:24 AI	м 🗰		View Rep	ort
14 4 1	of 1 🕨 🕅	100%	•		Find Next	Sele	ct a format	t -	▼ Expor	t
2 🛃										
Most a	CCESSE(ords: 5	d direc	tori	es						
Most a Number of reco Directory Patl	CCESSE(ords: 5	d direc	tori	es			Numb	per of	Accesses ¢	
Most a Number of reco Directory Patl WOMEVBusinesss	CCESSE(ords: 5 1 ÷	d direc	tori	es			Numb	per of	Accesses 🔤	167
Most a Number of reco Directory Path HOME'Businesss HOME'Businesss	CCESSE(ords: 5 1 0 Shares\ Shares\Shares\User	d direc	stori	es			Numb	per of	Accesses ≑	167
Most a Number of reco Directory Path HOME/Business HOME/Business	CCESSE(ords: 5 h = shares\ shares\FinanceUser shares\FinanceUser	d direc	: tori	es			Numb	per of	Accesses 🗧	167 152 118
Most a Number of reco Directory Path HOMEYBUSINESS HOMEYBUSINESS HOMEYBUSINESS	CCESSE(ords: 5 h e shares\ shares\FinanceUser shares\FinanceUser shares\FinanceUser	d direc	st	es			Numb	oer of	Accesses 🕀	167 152 118

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 owner changed								
Directory Name Host 10.20.2.57 Image: Control of Control o							View Rep	
14 4 1 0	f5 🕨 🔰 🚺 100% 💌	Find Next Select a format	💌 E)	oport 🔮 🍠				
Directory Owners Changed From: 3/4/2011 4:11:45 PM To: 3/16/2011 4:13:11 PM Number of records: 180								
Directory 🛊	Previous Owner	New Owner	Host ‡	User Name 👙	Date 🛊	Policy 🛊	Client ‡ Name	Share 😫
WOLWOLD HOMEWEW MCROSOFT EXCEL WORKSHEET XLS	DOTNET CRITICAL SITES LOCAL Molynoud. Qoama	DOTNET. CRITICAL SITES LOCAL VAluation. Hassan	10.20.2.57	DOTNET ORTICALSITES LOCAL/Administrator	3/14/2011 4:45:44 PM	df		
WOLWOLD HOMEWCAPTURE PNG	DOTNET.CRITICALSITES.LOCALIMatimoud. Osama	DOTNET.ORITICAL SITES LOCAL Vidministrators	10.20.2.57	DOTNET.CRITICALSITES LOCAL Widministrator	3/14/2011 4:43:27 PM	df		
WOLWOLD WOMENCOPY (2) OF NEW BITMAP MAGE.BMP	DOTNET_CRITICALSITES LOCAL/Administrators	DOTNET_ORITICAL SITES LOCAL Mahmoud Osama	10.20.2.57	DOTNET.ORITICALSITES LOCAL/Administrator	3/14/2011 4:35:55 PM	df		
WOLIVOLO HOMEWCOPY (2) OF NEW MICROSOFT EXCEL WORKSHEET XLS	DOTNET CRITICAL SITES LOCAL Vadministrators	DOTNET. CRITICAL SITES LOCAL Wahmoud Opening	10.20.2.57	DOTNET.ORITICALSITES LOCAL Valministrator	3/14/2011 4:35:55 PM	df		
WOLWOLD HOMEWCOPY (2) OF, NEW MICROSOFT, WORD DOCLMENT DOC	DOTNET_CRITICAL SITES LOCAL Vadministrators	DOTNET_CRITICAL SITES LOCAL Mehmoud Osenne	10.20.2.57	DOTNET_ORITICALSITES_LOCAL/Administrator	3/14/2011 4:35:55 PM	df		
WOLWOLD HOMEWCOPY (2) OF. NEW TEXT	DOTNET.CRITICAL SITES LOCAL VAdministrators	DOTNET.CRITICAL SITES LOCAL Mehmoud. Oseme	10.20.2.57	DOTNET.ORITICALSITES LOCALVadministrator	3/14/2011 4:35:55 PM	df		

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 perm	ission cha	nged					
Directory Name Start Date	3/14/2011 4:	Host 1	.0.20.2.57 1/15/2011 4:13:4	4 PM			
I4 4 1 0	f12 🕨 🕅	100% 💌 Find	d Next Sele	st a format	Export	2 🔒	
Director	v Perm	issions Changed					
From: 3/14/2011 4: Number of records:	11:45 PM To: 503	3/15/2011 4:13:44 PM					
Directory 🖨	Host \$	User Name 🗧	Date 💠	Policy ‡ Name	Client ≑ Name	Share ‡ Name	Permission Details
VOLVOLO VHOMEWCOPY (2) OF NEW/ MICROSOFT EXCEL WORKSHEET XLS	10.20.2.57	DOTNET.CRITICALSITES LOCAL VAdministrator	3/14/2011 4:58:10 PM	df			<u>View</u>
WOLWOLD HOMEWCOPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	10.20.2.57	DOTNET.CRITICALSITES LOCAL VAdministrator	3/14/2011 4:58:10 PM	df			View
VOLVOLO VHOMEWCOPY (2) OF R.TXT	10.20.2.57	DOTNET.CRITICALSITES LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
VOLVOLO VHOMEWCOPY (3) OF CAPTURE.PNG	10.20.2.57	DOTNET.CRITICALSITES LOCALVAdministrator	3/14/2011 4:58:10 PM	df			View
WOLVOLD HOMEWCOPY (3) OF NEW MICROSOFT EXCEL WORKSHEET XLS	10.20.2.57	DOTNET.CRITICALSITES LOCAL Vadministrator	3/14/2011 4:58:10 PM	df			View
WOLWOLD	10 20 2 57	DOTNET CRITICAL SITES LOCAL Vadministrator	3/14/2011	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.	IP oftware®
NTP Software Smart Policy Manager(TM) End-User License By using or copying the accompanying software you are indicating your acceptan- terms of this license. If you do not agree to the terms of this license, please return to product UNOPENED to your place of purchase for a full refund. GRANT OF LICENSE. NTP Software grants you the right to use Smart Policy Mar ("PRODUCT") on one computer, solely for your or your company's own internal us addition to the specified quantity of copies, you may make one (1) additional copy backup to the original. However, you may not cause the software to execute or be into the active memory of more computers than the above-specified quantity at an time. In addition the PRODUCT is licensed solely for the management of local stor	the the ager e. In as a e loaded y one age ▼
I accept the terms of the license agreement I do not accept the terms of the license agreement InstallShield <u>Rack</u>	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.	Sefeware*
Setup will install NTP Software Smart Policy Manager in the fe	ollowing folder.
To install to this folder, click Next. To install to a different folde another folder.	er, click Browse and select
Destination Folder	
C:\Program Files\Smart Policy Manager	Browse
InstallShield	
< <u>B</u> ack	Next > 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 I	eatures 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 < <u>B</u> a	ck <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 Non- Review settings before copying files. Non-	ware®
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 begit copying files.	n
Current Settings:	
Destination Path: C:\Program Files\Smart Policy Manager Components to install: Smart Policy Manager Administration Tool	<u>م</u> ۲
InstallShield	
< <u>Back</u> <u>Next</u> > Ca	incel

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 LICENSI NOT INSTALL OR USE THE PRODUCT. You may return the product UNI 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 virtual 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 PRODUCT I go not accept the terms of the license agreement InstallShield	ompanying d agree to be 5, YOU MUST JSED to your Software File machines for ynal or your f to manage the v
< <u>B</u> ack <u>N</u> ext >	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	older listed below. You may type a new folder t. Click Next to continue.
<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>] Cance	

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	e				
OK Cancel H	elp				

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)								
<u>File Edit View Options H</u> elp								
🎒 X 🖻 🛍 🗙 😭 🏪 🗄 🖽								
🙂 MyOrganization	Name 🗸	Туре	Status	Description	Created	Modified		
INTP Software File Auditor Quota & File Sentinel MySite FileSrv01 File Audit Policies File Audit Policies Server Directories Server Shares Quota & File Sentinel	UvySite Quota & File NTP Software	QuotaSe FileAuditor	Available Available	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		
					and Hart			
o object(s)				CLIEDIBOX (L	ocarnoscy j			

- 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