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

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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 Properties 5

Setting NTP Software File Auditor, Windows Edition Database 5

Setting the NTP Software File Auditor, Windows Edition Email 7

Setting the NTP Software File Auditor, Windows Edition Misc Options 8

Setting the NTP Software File Auditor, Windows Edition Security Level 9

Policy Creation 10

NTP Software File Auditor Reports 17

NTP Software Smart Policy Manager™ 30

NTP Software Smart Policy Manager Overview 30

Managing the NTP Software File Auditor Service through a NTP Software File Auditor Admin Client Running on a Different Machine 31

Installing the NTP Software Smart Policy Manager Admin Component 31

Installing the NTP Software File Auditor Admin Component 35

Installing NTP Software File Auditor in Clustered Environments 40

About NTP Software® 43

NTP Software® Professional Services 43

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

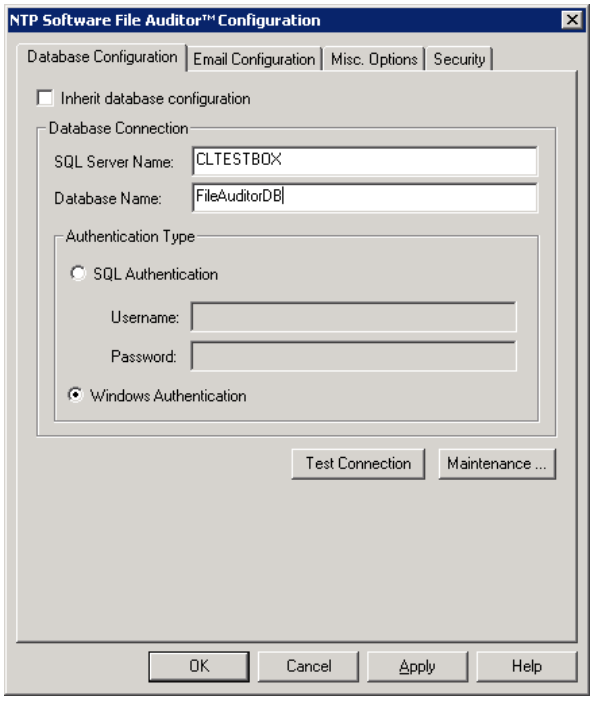
Setting NTP Software File Auditor, Windows Edition Properties

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.

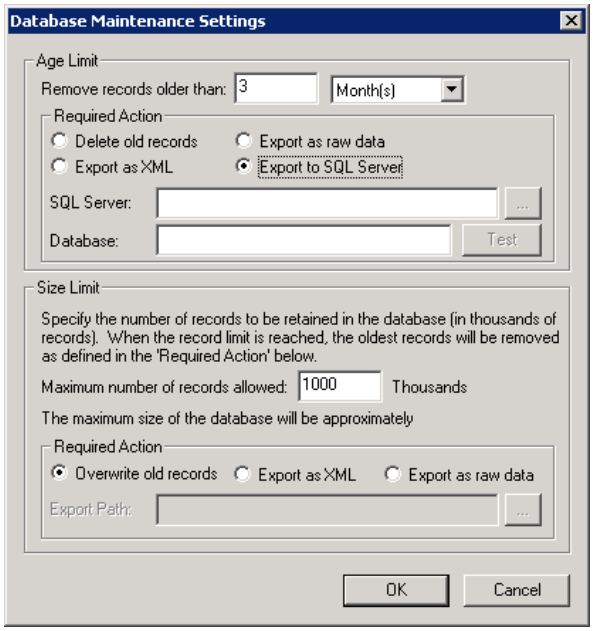


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



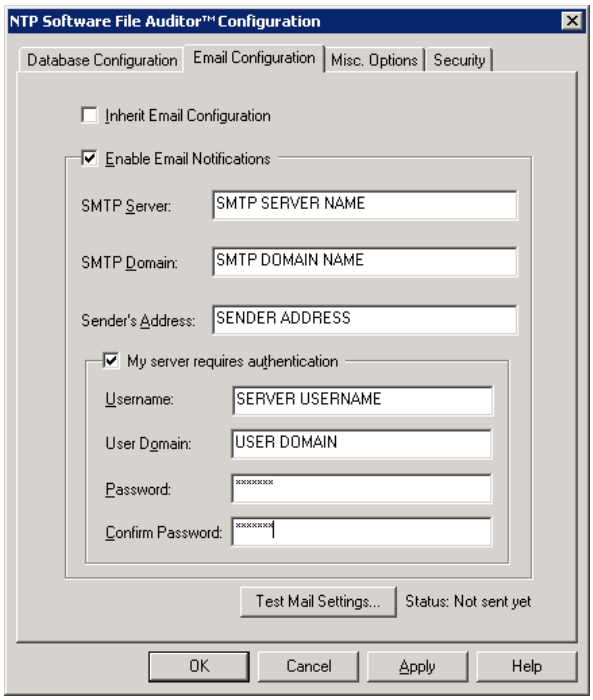
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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** button to test your connection to the specified SMTP Sever.

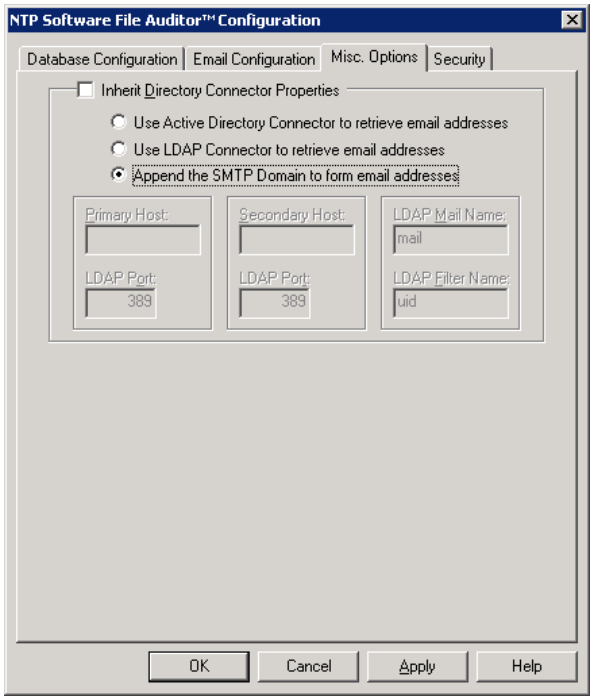


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



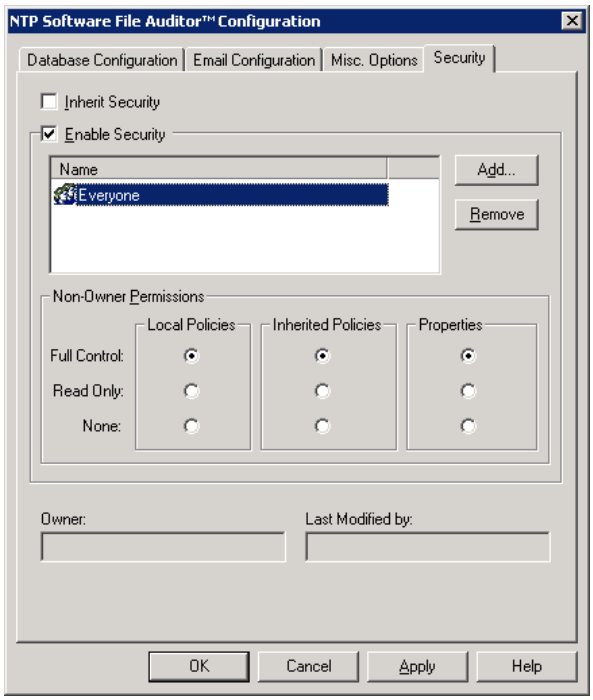
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

Policy Creation

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

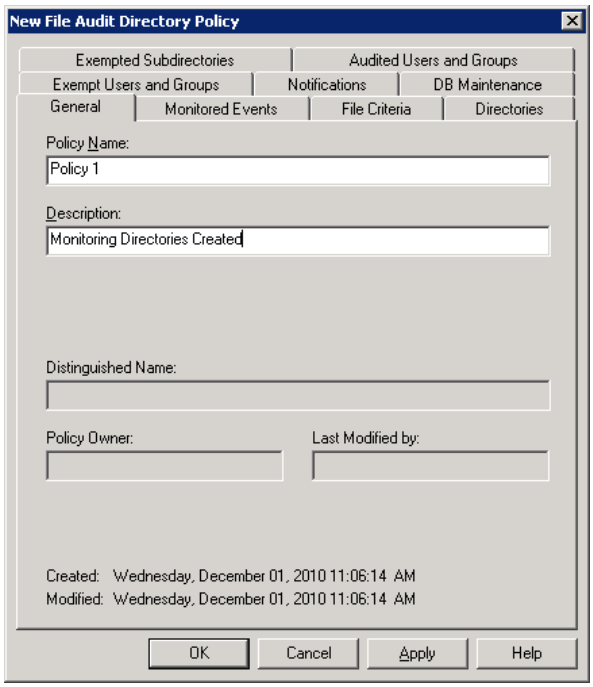
Note:

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

Creating File Audit Policies

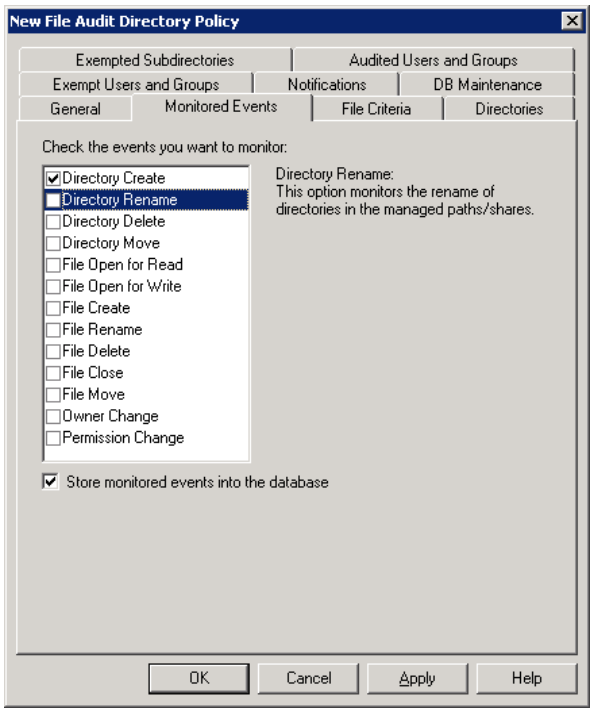
This section walks you through creating a typical file audit policy. We will create a file audit policy for all your user home directories in a typical server configuration. This policy will be applied to all users in your Users directory.

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.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

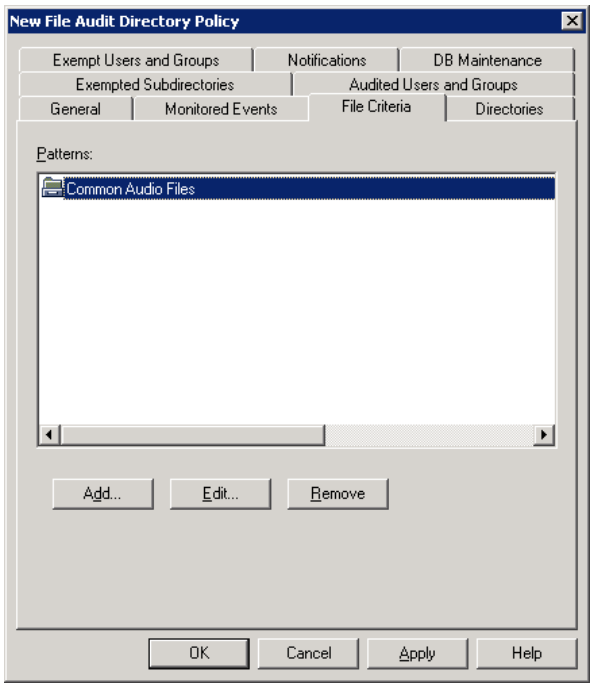
4. Click the **Monitored Events** tab; check the event(s) you want to monitor from the list of events. Check the **Store monitored events into the database** checkbox if you wish to store the monitored events in the File Auditor database. You can clear the "Store monitored events into the database" checkbox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



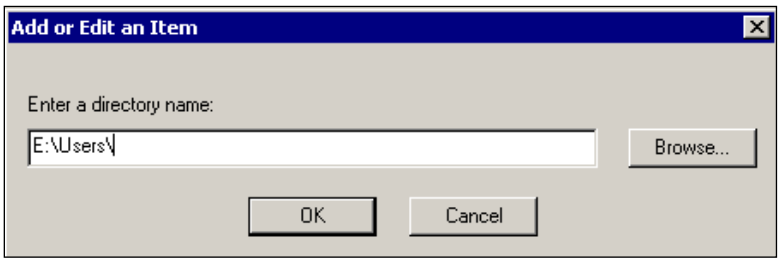
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

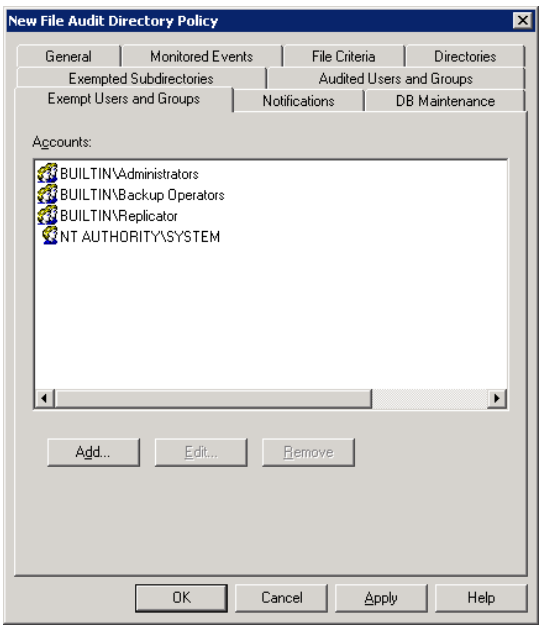


6. Click the **Directories** tab. Click the **Add** button, type the appropriate directory path for your Users directory followed by a backslash.

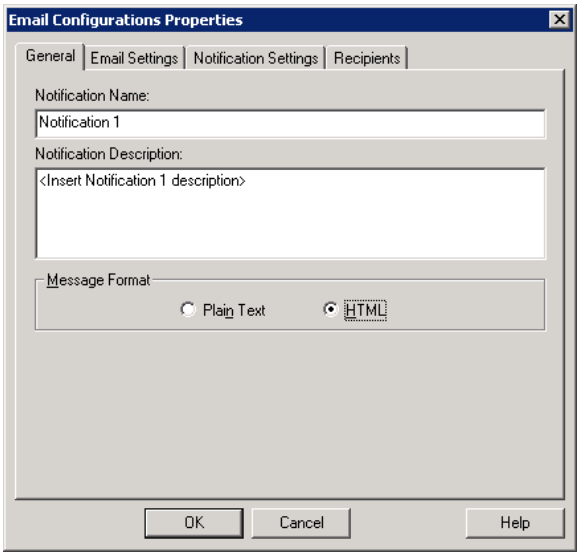


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

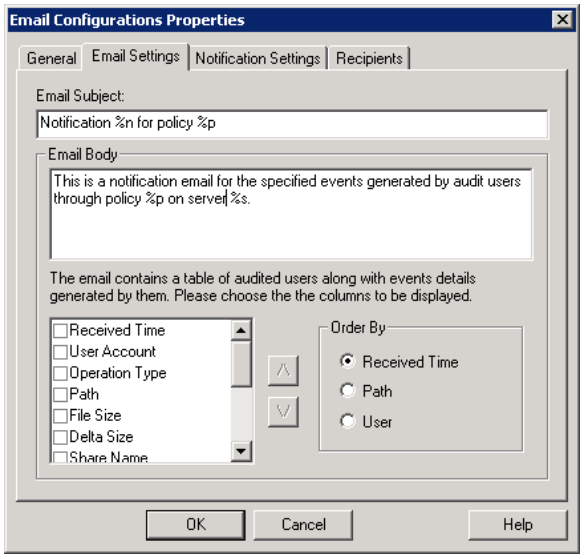
7. Administrators, Backup Operators, Replicators, and the System account are exempt from policies. You can verify this fact by clicking the **Exempt Users and Groups** tab. To change this setting, select the appropriate entry and click **Remove**.

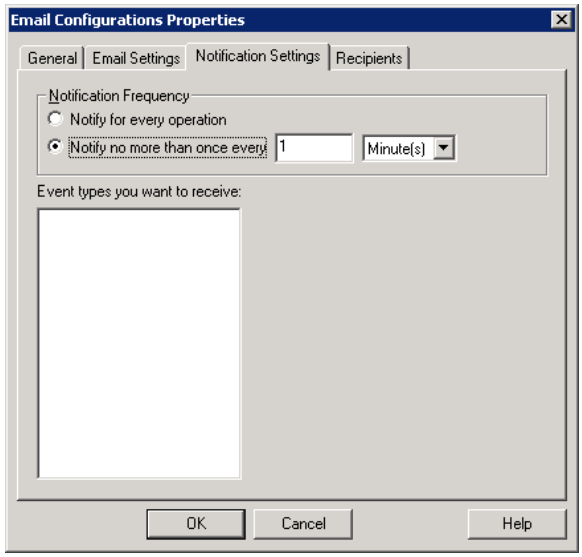


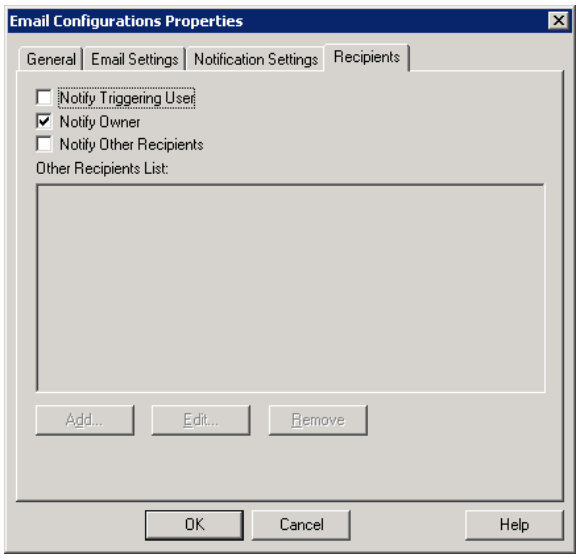
8. Click the **Notifications** tab. Click the **Add** button. On the **Email Configurations Properties dialog General** Tab, specify the notification related details; including the notification name description and message format. On the **Email Settings** Tab, specify the email subject and the email 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.



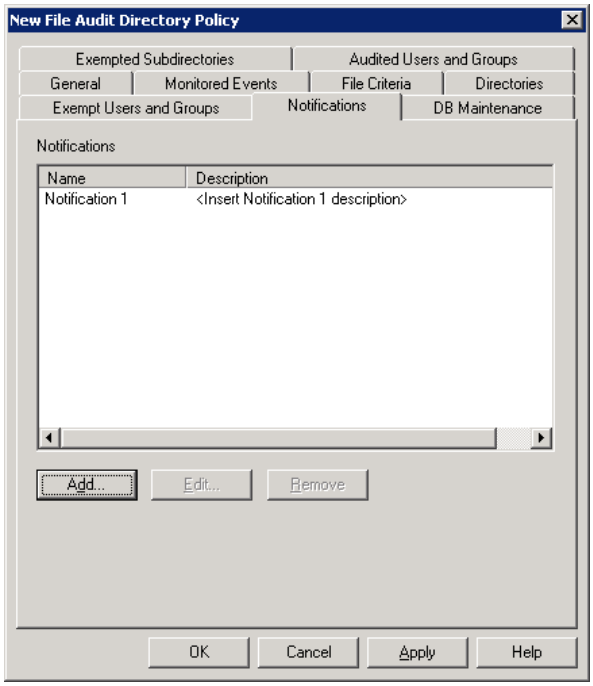
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF



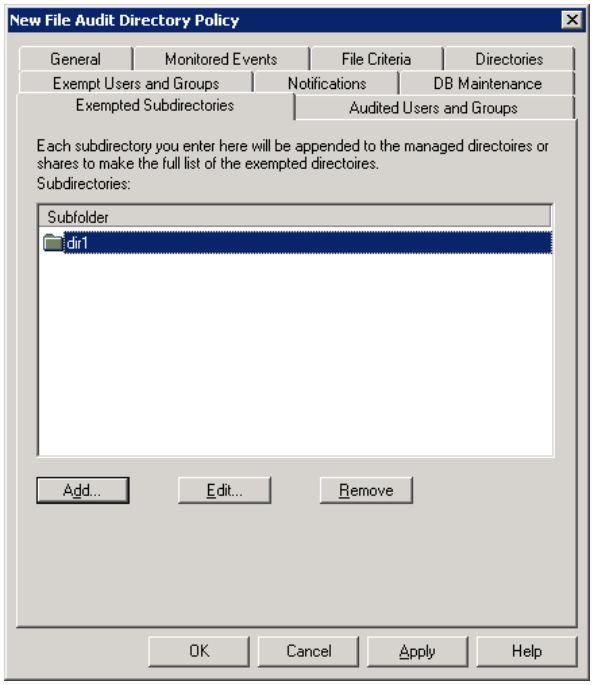




Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

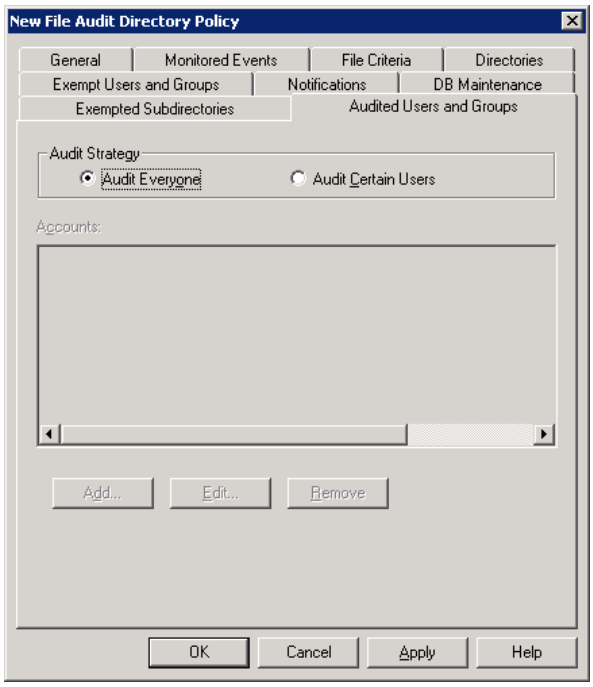


9. Click the **Exempted Subdirectories** tab. Click the **Add** button and type the subdirectory you want to exempt from the monitored directories list.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



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.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

NTP Software File Auditor Reports

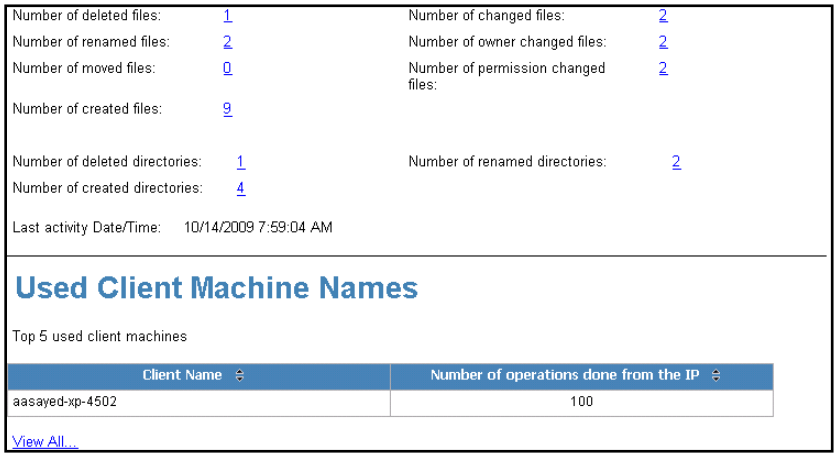
The NTP Software File Auditor, Windows Edition reporting tool allows you to view the file and directory operations that took place at your environment in an easy and efficient display. Reports are categorized by user, file, policy, and folder.

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: 0
Number of permission changed files: 2
Number of created files: 9
Number of deleted directories: 1
Number of renamed directories: 2
Number of created directories: 4
Last activity Date/Time: 10/14/2009 7:59:04 AM

Used Client Machine Names

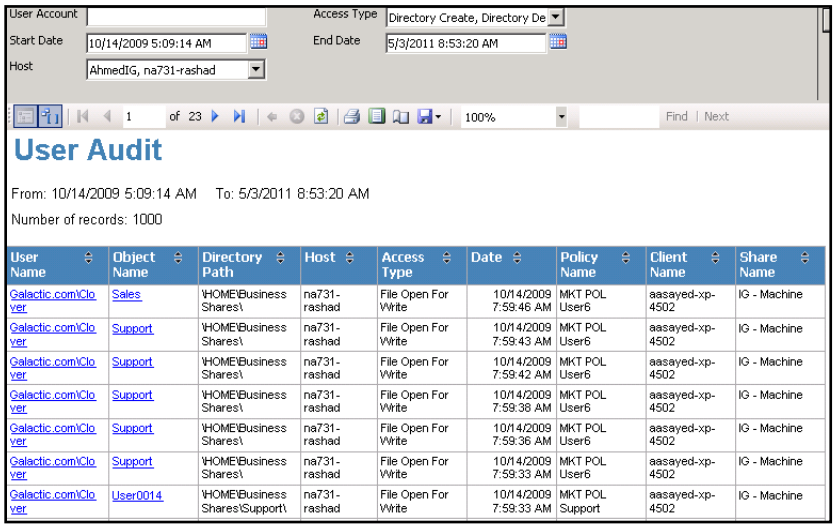
Top 5 used client machines

Client Name	Number of operations done from the IP
aasayed-xp-4502	100

View All...

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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 Create, Directory De
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:53:20 AM
Host: AhmedIG, na731-rashad

1 of 23 | 100% | Find | Next

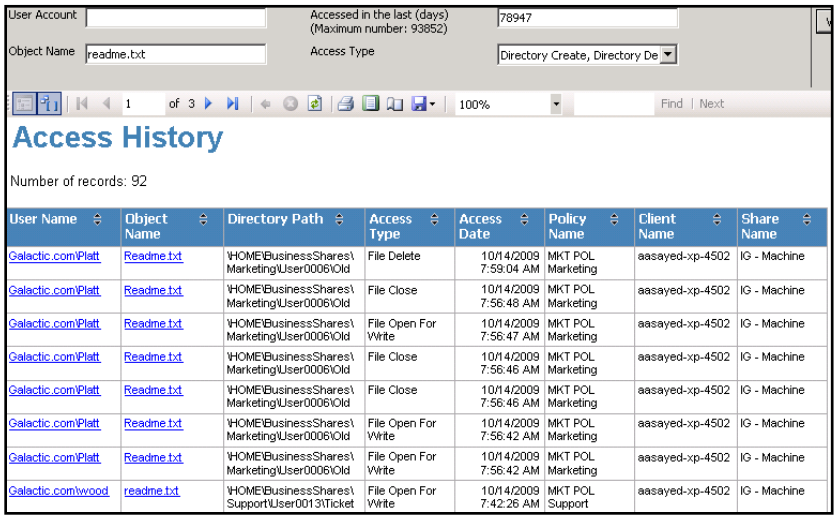
User Audit

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:53:20 AM

Number of records: 1000

User Name	Object Name	Directory Path	Host	Access Type	Date	Policy Name	Client Name	Share Name
Galactic.com\Clover	Sales	\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\Clover	Support	\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\Clover	Support	\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\Clover	Support	\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\Clover	Support	\HOME\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\Clover	Support	\HOME\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\Clover	User0014	\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 in the last (days) (Maximum number: 93852): 78947
Object Name: readme.txt | Access Type: Directory Create, Directory De

1 of 3 | 100% | Find | Next

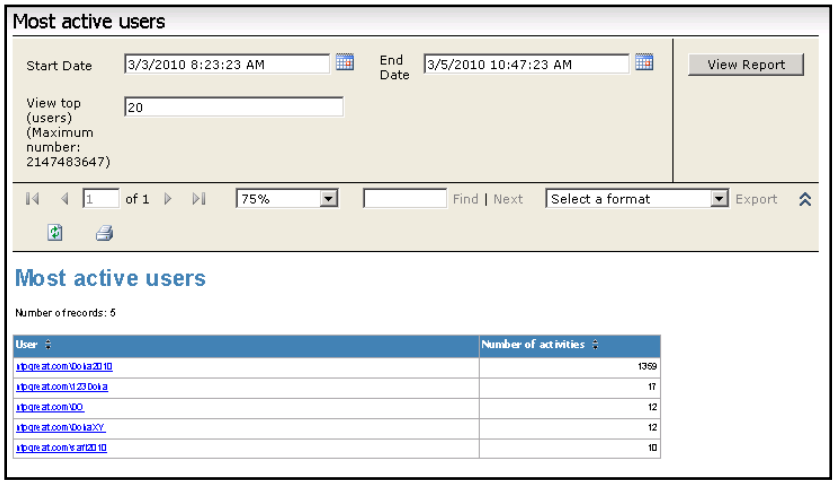
Access History

Number of records: 92

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	10/14/2009 7:56:48 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\Platt	Readme.txt	\HOME\BusinessShares\Marketing\User0006\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	\HOME\BusinessShares\Marketing\User0006\Old	File Close	10/14/2009 7:56:46 AM	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	MKT POL Marketing	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	10/14/2009 7:56:42 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
Galactic.com\wood	readme.txt	\HOME\BusinessShares\Support\User0013\Ticket	File Open For Write	10/14/2009 7:42:26 AM	MKT POL Support	aasayed-xp-4502	IG - Machine

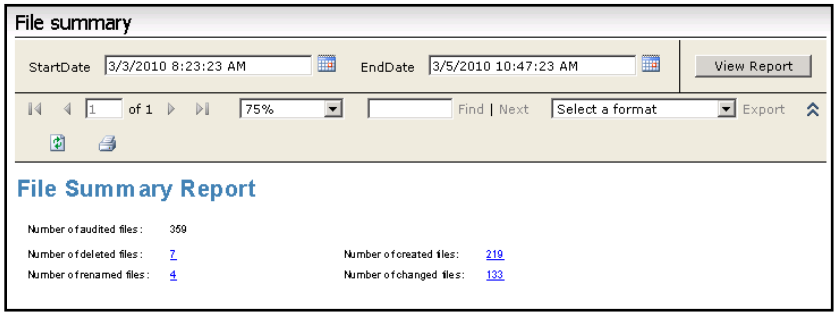
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



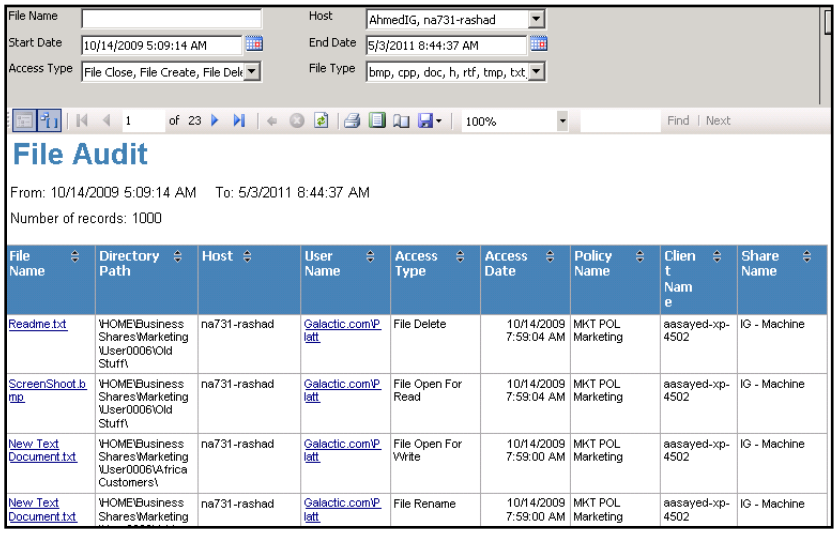
2. The **File Reports** category has nine different views: File Summary, File Audit, Files Changed, Files Deleted, Files Renamed, Files Created, Deletion Compliance, Owner Changed, and Permission Changed.

   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.



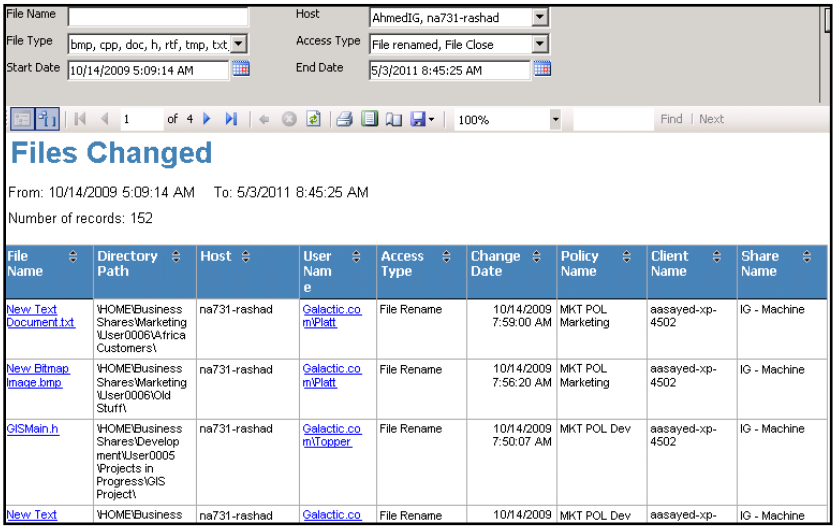
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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	Directory Path	Host	User Name	Access Type	Access Date	Policy Name	Client Name	Share Name
Readme.txt	\HOME\Business Shares\Marketing \User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	File Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
ScreenShoot.bmp	\HOME\Business Shares\Marketing \User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	File Open For Read	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Text Document.txt	\HOME\Business Shares\Marketing \User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	File Open For Write	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Text Document.txt	\HOME\Business Shares\Marketing	na731-rashad	Galactic.com\Platt	File Rename	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine

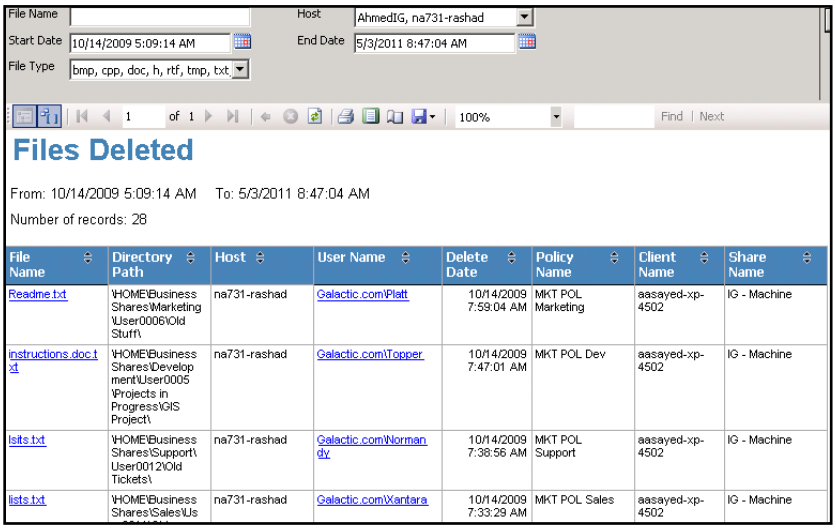
c. **Files Changed:** This report allows you to view all the changed files. The report input is the file name, and/or the host name, and/or the date range, and/or the file type(s). The report displays the file name, the directory path in which the file is located, the user name accessing the file, the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



File Name	Directory Path	Host	User Name	Access Type	Change Date	Policy Name	Client Name	Share Name
New Text Document.txt	\HOME\Business Shares\Marketing \User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	File Rename	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Bitmap Image.bmp	\HOME\Business Shares\Marketing \User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	File Rename	10/14/2009 7:56:20 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
GISMain.h	\HOME\Business Shares\Development\User0005 \Projects in Progress\GIS Project\	na731-rashad	Galactic.com\Topper	File Rename	10/14/2009 7:50:07 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine
New Text	\HOME\Business	na731-rashad	Galactic.co	File Rename	10/14/2009	MKT POL Dev	aasayed-xp-	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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 | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:47:04 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

1 of 1 100% Find | Next

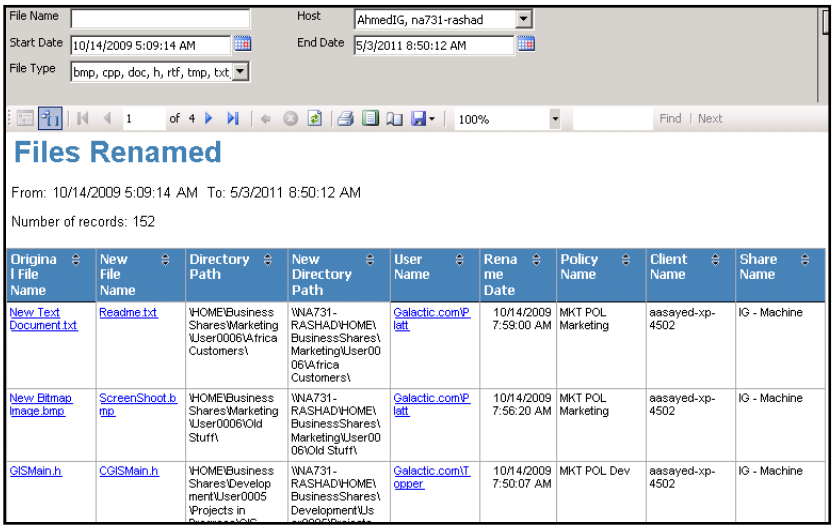
Files Deleted

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:47:04 AM

Number of records: 28

File Name	Directory Path	Host	User Name	Delete Date	Policy Name	Client Name	Share Name
Readme.txt	\HOME\Business Shares\Marketing \User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
instructions.doc.txt	\HOME\Business Shares\Development\User0005 \Projects in Progress\GIS Project\	na731-rashad	Galactic.com\Topper	10/14/2009 7:47:01 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine
lsits.txt	\HOME\Business Shares\Support\ User0012\Old Tickets\	na731-rashad	Galactic.com\Normandy	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: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:50:12 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

1 of 4 100% Find | Next

Files Renamed

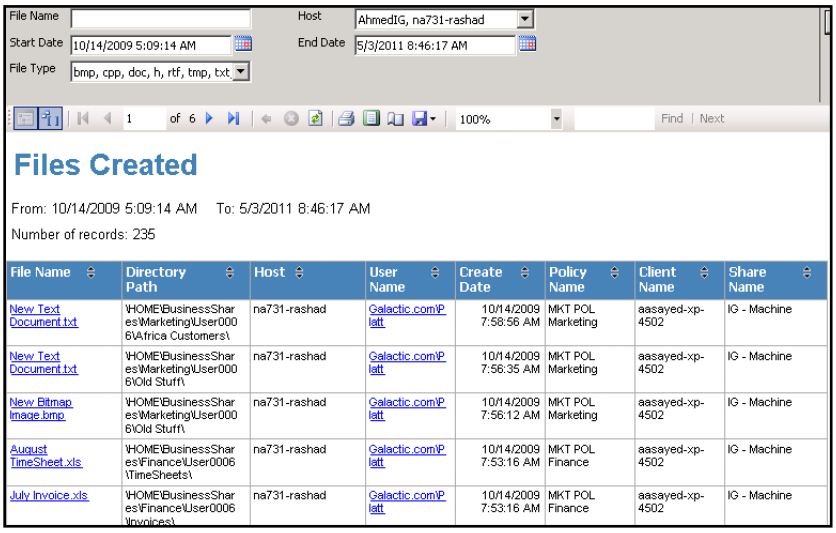
From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:50:12 AM

Number of records: 152

Original File Name	New File Name	Directory Path	New Directory Path	User Name	Rename Date	Policy Name	Client Name	Share Name
New Text Document.txt	Readme.txt	\HOME\Business Shares\Marketing \User0006\Africa Customers\	\\NA731-RASHAD\HOME\ BusinessShares\ Marketing\User0006\Africa Customers\	Galactic.com\Platt	10/14/2009 7:59:00 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Bitmap Image.bmp	ScreenShoot.bmp	\HOME\Business Shares\Marketing \User0006\Old Stuff\	\\NA731-RASHAD\HOME\ BusinessShares\ Marketing\User0006\Old Stuff\	Galactic.com\Platt	10/14/2009 7:56:20 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
GISMain.h	CGISMain.h	\HOME\Business Shares\Development\User0005 \Projects in	\\NA731-RASHAD\HOME\ BusinessShares\ Development\Us	Galactic.com\Topper	10/14/2009 7:50:07 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:46:17 AM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

1 of 6 | 100% | Find | Next

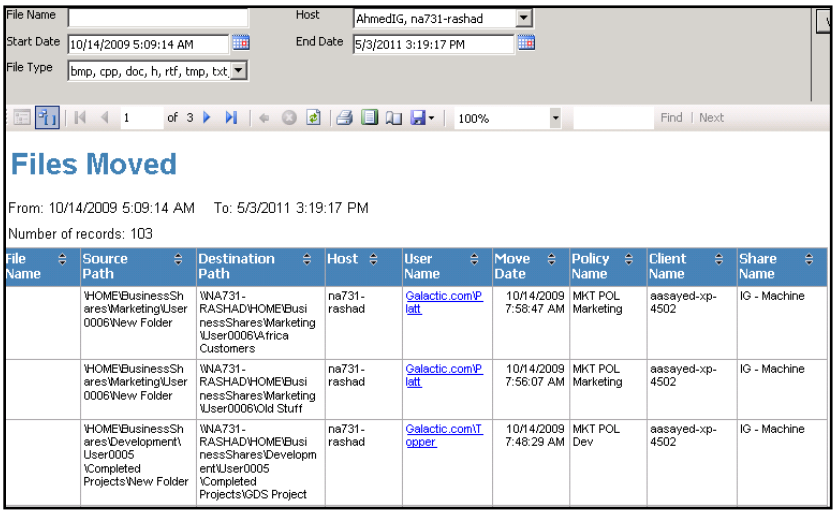
Files Created

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	\HOME\BusinessShares\Marketing\User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:56 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Text Document.txt	\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:35 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
New Bitmap Image.bmp	\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:12 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
August TimeSheet.xls	\HOME\BusinessShares\Finance\User0006\TimeSheets\	na731-rashad	Galactic.com\Platt	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
July Invoice.xls	\HOME\BusinessShares\Finance\User0006\Invoices\	na731-rashad	Galactic.com\Platt	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.



File Name | Host: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 3:19:17 PM
File Type: bmp, cpp, doc, h, rtf, tmp, txt

1 of 3 | 100% | Find | Next

Files Moved

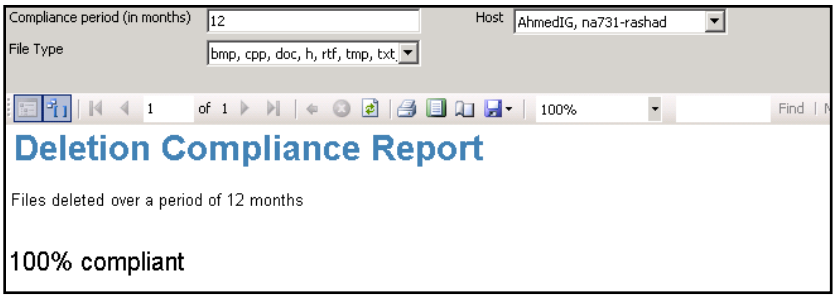
From: 10/14/2009 5:09:14 AM To: 5/3/2011 3:19:17 PM

Number of records: 103

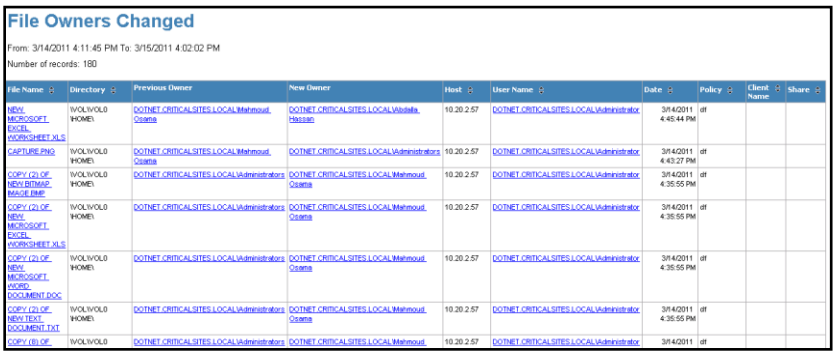
File Name	Source Path	Destination Path	Host	User Name	Move Date	Policy Name	Client Name	Share Name
	\HOME\BusinessShares\Marketing\User0006\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Africa Customers	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
	\HOME\BusinessShares\Marketing\User0006\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Old Stuff	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
	\HOME\BusinessShares\Development\User0005\Completed Projects\New Folder	\\NA731-RASHAD\HOME\BusinessShares\Development\User0005\Completed Projects\GDS Project	na731-rashad	Galactic.com\Topper	10/14/2009 7:48:29 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



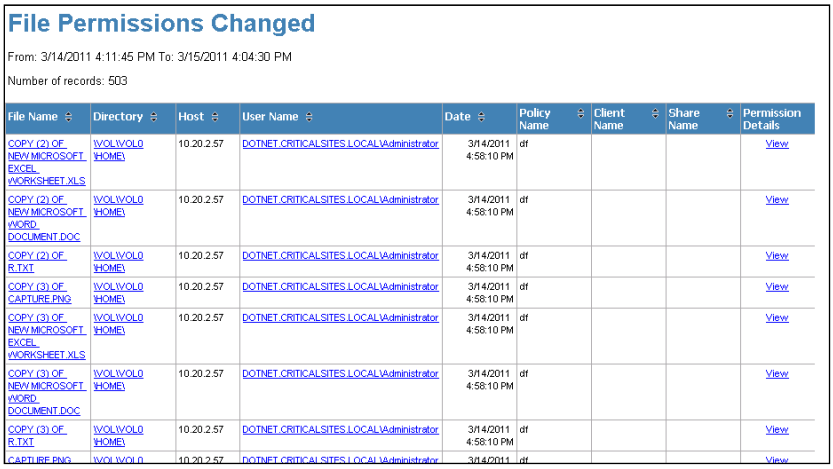
File Owners Changed

From: 3/14/2011 4:11:45 PM To: 3/15/2011 4:02:02 PM

Number of records: 180

File Name	Directory	Previous Owner	New Owner	Host	User Name	Date	Policy	Client Name	Share
NEW MICROSOFT EXCEL WORKSHEET.XLS	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	DOTNET.CRITICALSITES.LOCAL\Abdalla Hassan	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:45:44 PM	df		
CAPTURE.PNG	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	DOTNET.CRITICALSITES.LOCAL\Administrators	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:43:27 PM	df		
COPY (2) OF NEW BITMAP IMAGE.BMP	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (2) OF NEW TEXT DOCUMENT.TXT	\\VOL\VOL0 \HOME\	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud Osama	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:35:55 PM	df		
COPY (8) OF	\\VOL\VOL0	DOTNET.CRITICALSITES.LOCAL\Administrators	DOTNET.CRITICALSITES.LOCAL\Mahmoud	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.



File Permissions Changed

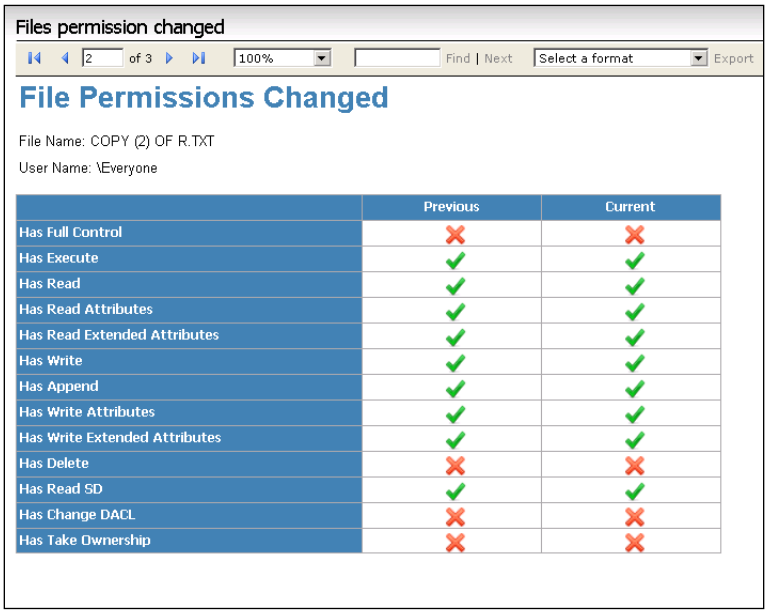
From: 3/14/2011 4:11:45 PM To: 3/15/2011 4:04:30 PM

Number of records: 503

File Name	Directory	Host	User Name	Date	Policy Name	Client Name	Share Name	Permission Details
COPY (2) OF NEW MICROSOFT EXCEL WORKSHEET.XLS	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (2) OF NEW MICROSOFT WORD DOCUMENT.DOC	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (2) OF R.TXT	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF CAPTURE.PNG	\\VOL\VOL0 \HOME\	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	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF NEW MICROSOFT WORD DOCUMENT.DOC	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
COPY (3) OF R.TXT	\\VOL\VOL0 \HOME\	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011 4:58:10 PM	df			View
CAPTURE.PNG	\\VOL\VOL0	10.20.2.57	DOTNET.CRITICALSITES.LOCAL\Administrator	3/14/2011	df			View

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

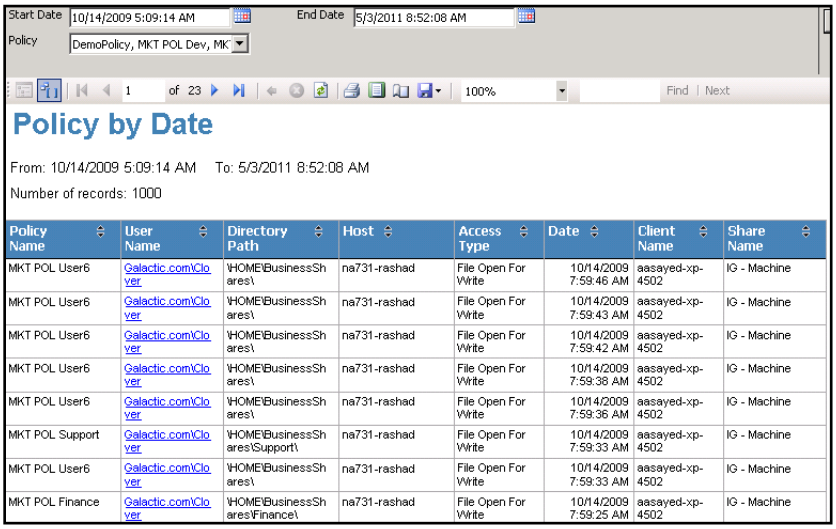
Clicking on the View link of the Permission Details field displays more details as outlined below.



	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	✓	✓
Has Delete	✗	✗
Has Read SD	✓	✓
Has Change DACL	✗	✗
Has Take Ownership	✗	✗

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.

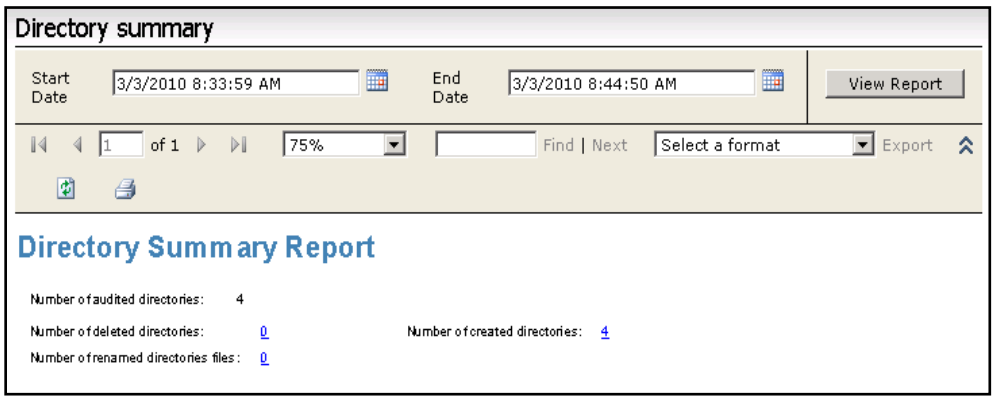


Policy Name	User Name	Directory Path	Host	Access Type	Date	Client Name	Share Name
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:46 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:43 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:42 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:38 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:36 AM	aasayed-xp-4502	IG - Machine
MKT POL Support	Galactic.com\Clover	\HOME\BusinessShares\Support\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp-4502	IG - Machine
MKT POL User6	Galactic.com\Clover	\HOME\BusinessShares\	na731-rashad	File Open For Write	10/14/2009 7:59:33 AM	aasayed-xp-4502	IG - Machine
MKT POL Finance	Galactic.com\Clover	\HOME\BusinessShares\Finance\	na731-rashad	File Open For Write	10/14/2009 7:59:25 AM	aasayed-xp-4502	IG - Machine

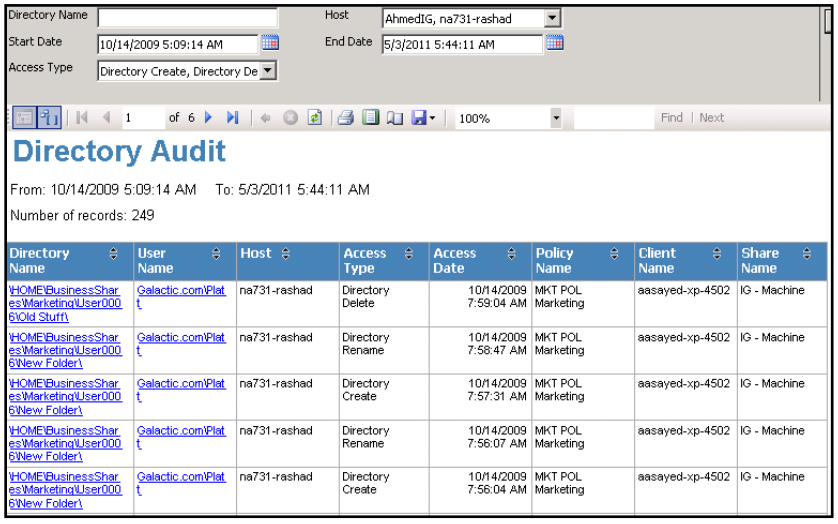
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



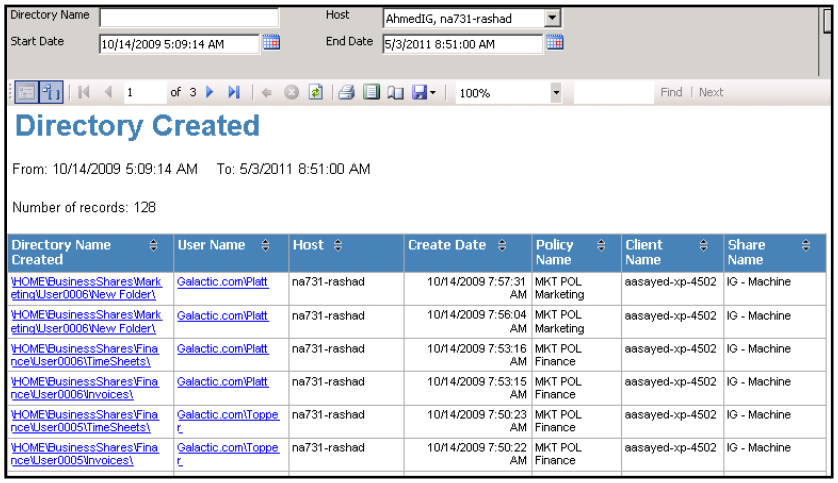
   b. **Directory Audit:** This report allows you to review all the directory operations performed. The report's input is the directory name, and/or the host name, and/or the date range, and/or the access type. The report displays the directory name, the user name accessing the directory, access type, access 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	User Name	Host	Access Type	Access Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\Old Stuff\	Galactic.com\Platt	na731-rashad	Directory Delete	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Rename	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Create	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Rename	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	Directory Create	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 8:51:00 AM

1 of 3 | 100% | Find | Next

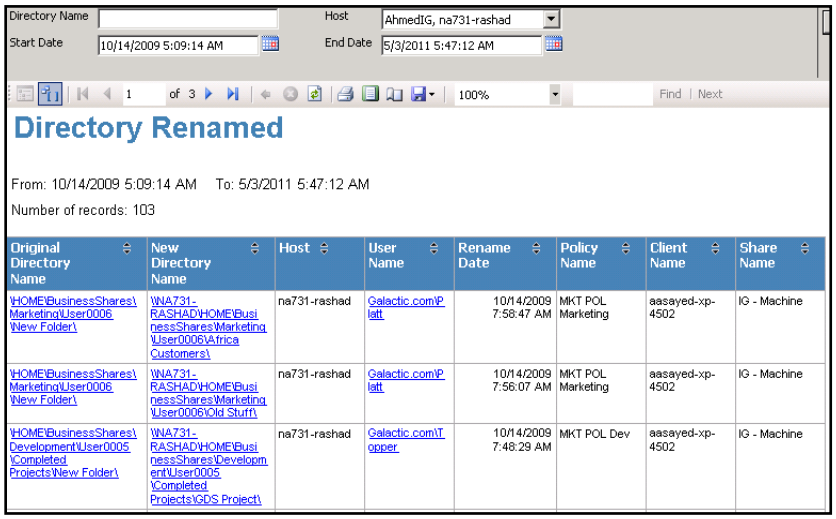
Directory Created

From: 10/14/2009 5:09:14 AM To: 5/3/2011 8:51:00 AM

Number of records: 128

Directory Name Created	User Name	Host	Create Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	10/14/2009 7:57:31 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	Galactic.com\Platt	na731-rashad	10/14/2009 7:56:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0006\TimeSheets\	Galactic.com\Platt	na731-rashad	10/14/2009 7:53:16 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0006\Invoices\	Galactic.com\Platt	na731-rashad	10/14/2009 7:53:15 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0005\TimeSheets\	Galactic.com\Topper	na731-rashad	10/14/2009 7:50:23 AM	MKT POL Finance	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Finance\User0005\Invoices\	Galactic.com\Topper	na731-rashad	10/14/2009 7:50:22 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, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 5:47:12 AM

1 of 3 | 100% | Find | Next

Directory Renamed

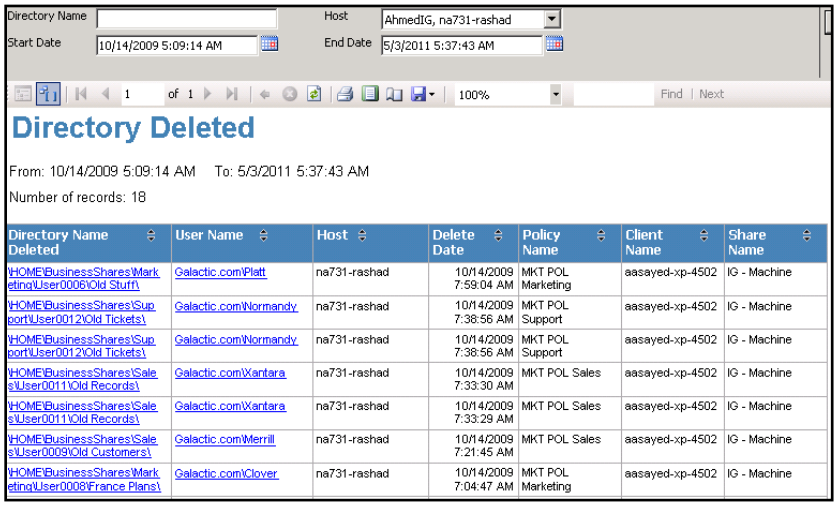
From: 10/14/2009 5:09:14 AM To: 5/3/2011 5:47:12 AM

Number of records: 103

Original Directory Name	New Directory Name	Host	User Name	Rename Date	Policy Name	Client Name	Share Name
\HOME\BusinessShares\Marketing\User0006\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Africa Customers\	na731-rashad	Galactic.com\Platt	10/14/2009 7:58:47 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Marketing\User0006\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Marketing\User0006\Old Stuff\	na731-rashad	Galactic.com\Platt	10/14/2009 7:56:07 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Development\User0005\Completed Projects\New Folder\	\\NA731-RASHAD\HOME\BusinessShares\Development\User0005\Completed Projects\GDS Project\	na731-rashad	Galactic.com\Topper	10/14/2009 7:48:29 AM	MKT POL Dev	aasayed-xp-4502	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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: AhmedIG, na731-rashad
Start Date: 10/14/2009 5:09:14 AM | End Date: 5/3/2011 5:37:43 AM

1 of 1 100% Find | Next

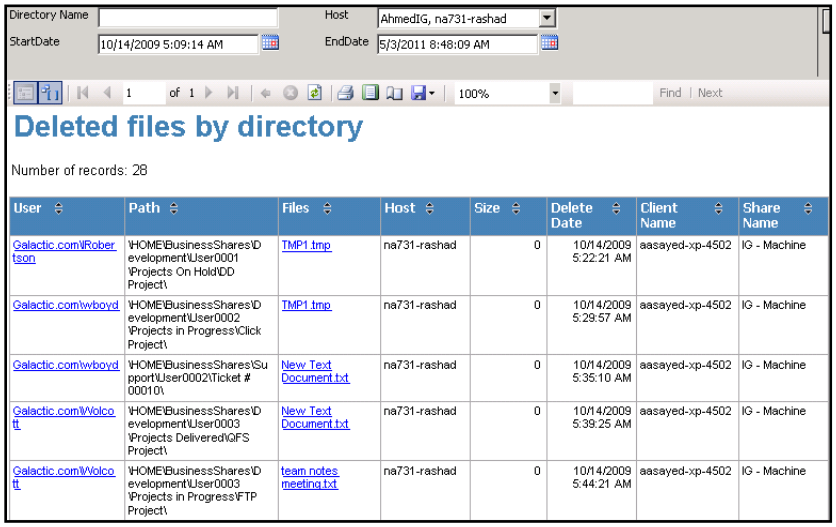
Directory Deleted

From: 10/14/2009 5:09:14 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\Marketing\User0006\Old Stuff\	Galactic.com\Platt	na731-rashad	10/14/2009 7:59:04 AM	MKT POL Marketing	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Support\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\Support\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\Sales\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:30 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Sales\User0011\Old Records\	Galactic.com\Xantara	na731-rashad	10/14/2009 7:33:29 AM	MKT POL Sales	aasayed-xp-4502	IG - Machine
\HOME\BusinessShares\Sales\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\Marketing\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

1 of 1 100% Find | Next

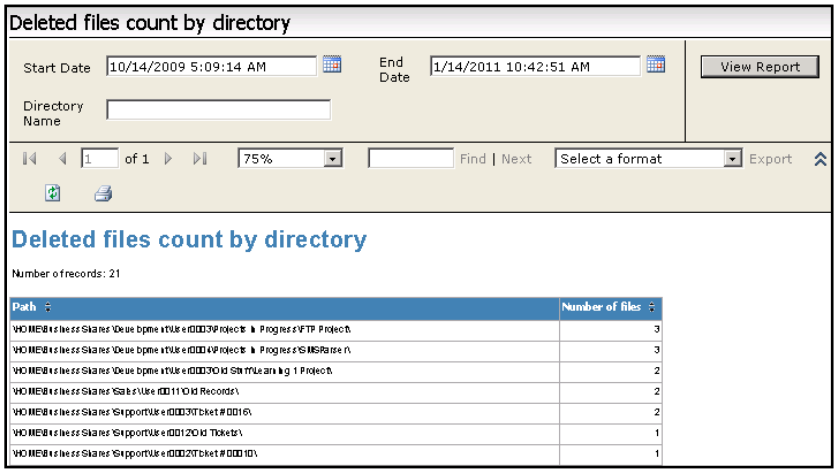
Deleted files by directory

Number of records: 28

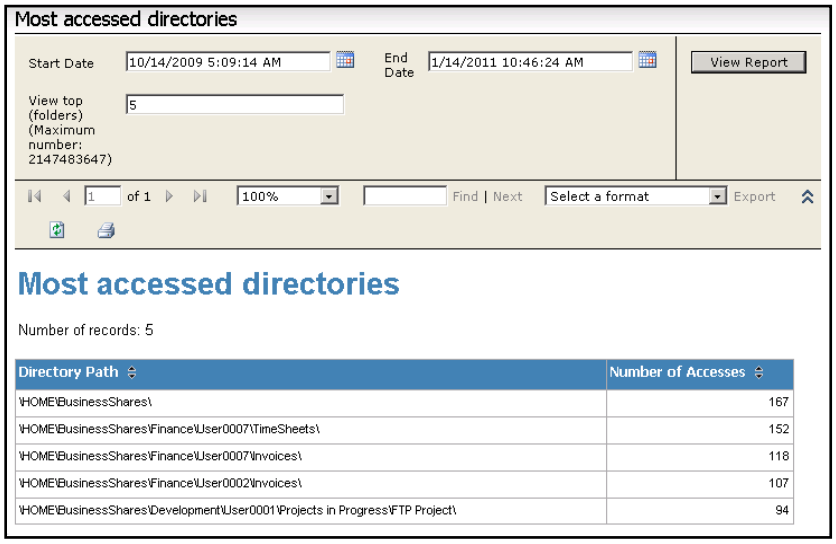
User	Path	Files	Host	Size	Delete Date	Client Name	Share Name
Galactic.com\Robertson	\HOME\BusinessShares\Development\User0001\Projects On Hold\DD Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:22:21 AM	aasayed-xp-4502	IG - Machine
Galactic.com\wboyd	\HOME\BusinessShares\Development\User0002\Projects in Progress\Click Project\	TMP1.tmp	na731-rashad	0	10/14/2009 5:29:57 AM	aasayed-xp-4502	IG - Machine
Galactic.com\wboyd	\HOME\BusinessShares\Support\User0002\Ticket # 00010\	New Text Document.txt	na731-rashad	0	10/14/2009 5:35:10 AM	aasayed-xp-4502	IG - Machine
Galactic.com\Volcott	\HOME\BusinessShares\Development\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\Volcott	\HOME\BusinessShares\Development\User0003\Projects in Progress\FTP Project\	team notes meeting.txt	na731-rashad	0	10/14/2009 5:44:21 AM	aasayed-xp-4502	IG - Machine

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

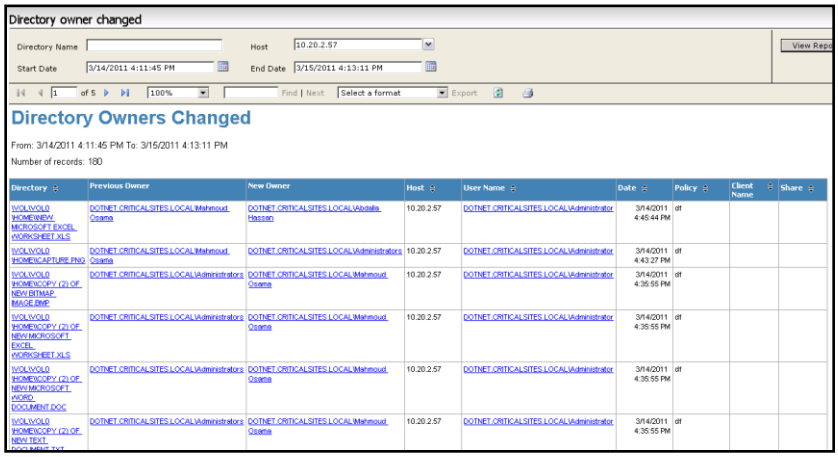


h. **Most Accessed Directories:** This report allows you to review the most-accessed directories. The report's input is the date range, and/or number of most-accessed directories to display. The report displays the directory path and the number of times each directory was accessed.

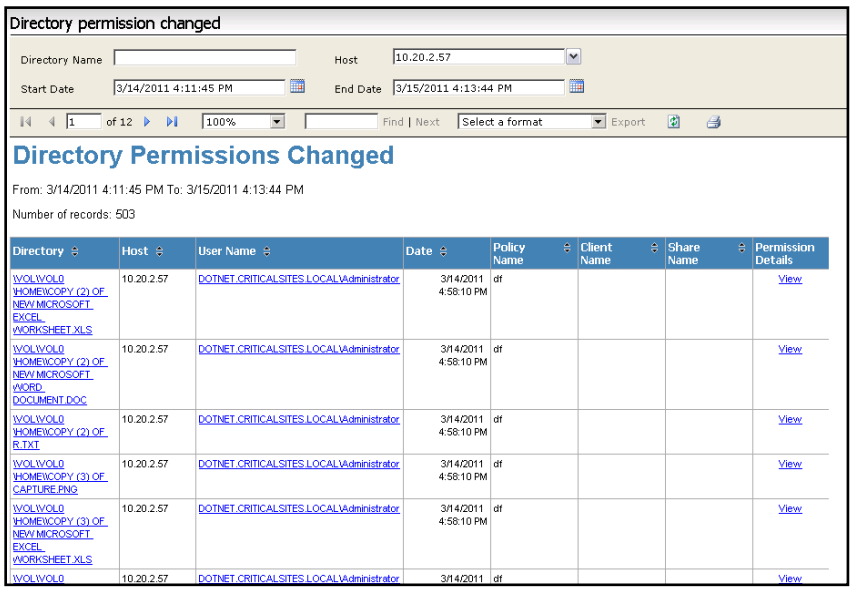


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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



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.



NTP Software Smart Policy Manager™

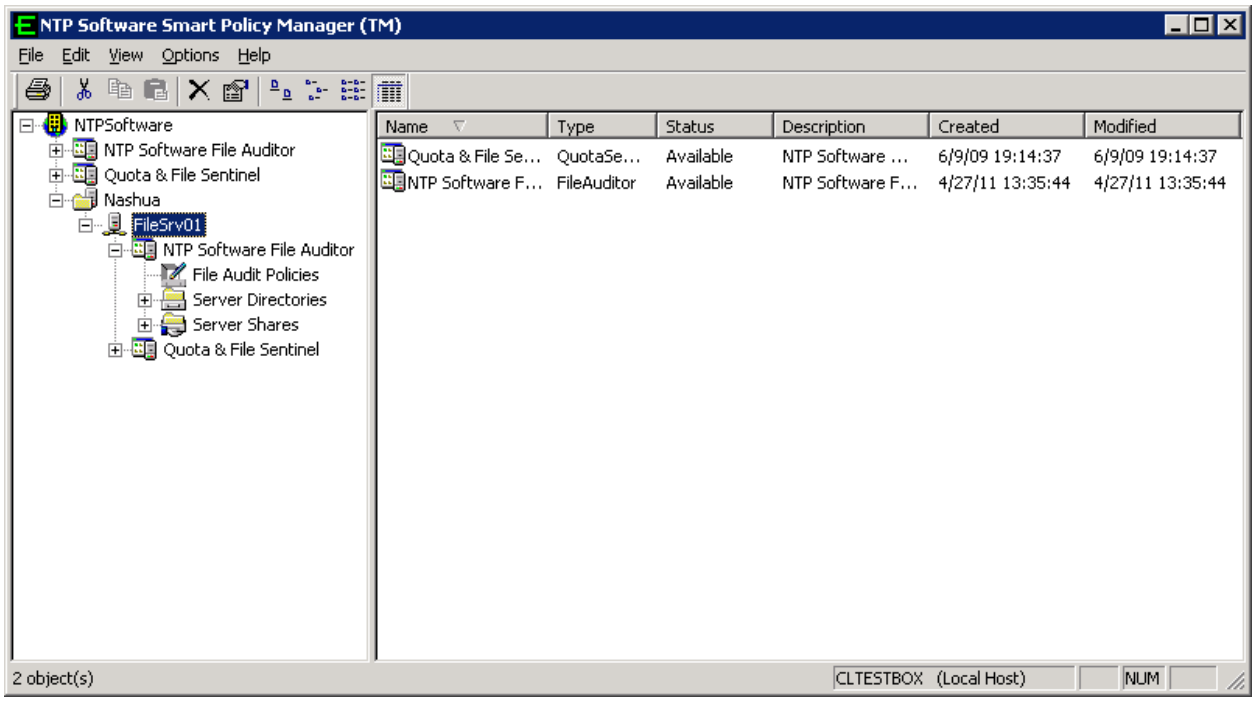
NTP Software Smart Policy Manager Overview

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.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

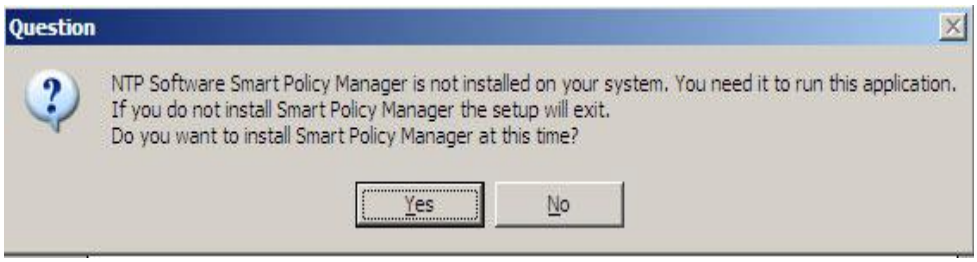
NTP Software File Auditor Admin Client User Interface is using Remote RPC to communicate to the NTP Software Smart Policy Manager service. Therefore, NTP Software File Auditor Administrator needs to have permissions to run and execute Remote RPC on the managed machine. A standard user does not have RPC 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.

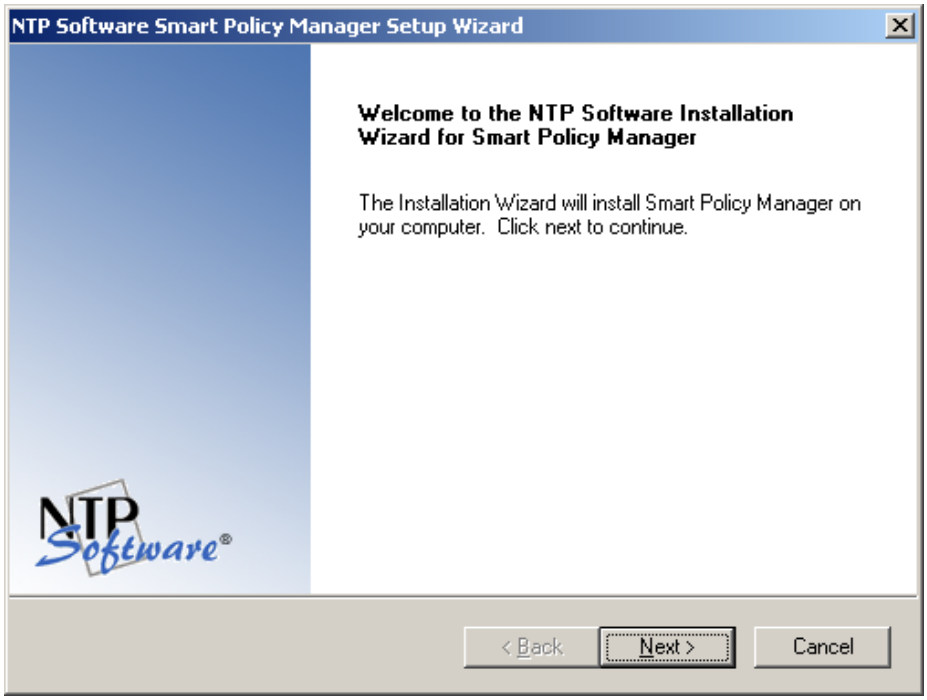
2. On the NTP Software Product Installation page, click your product installation link under the **Product Components** section.

3. When prompted to install NTP Software Smart Policy Manager, click **Yes** to launch the Installation Wizard.

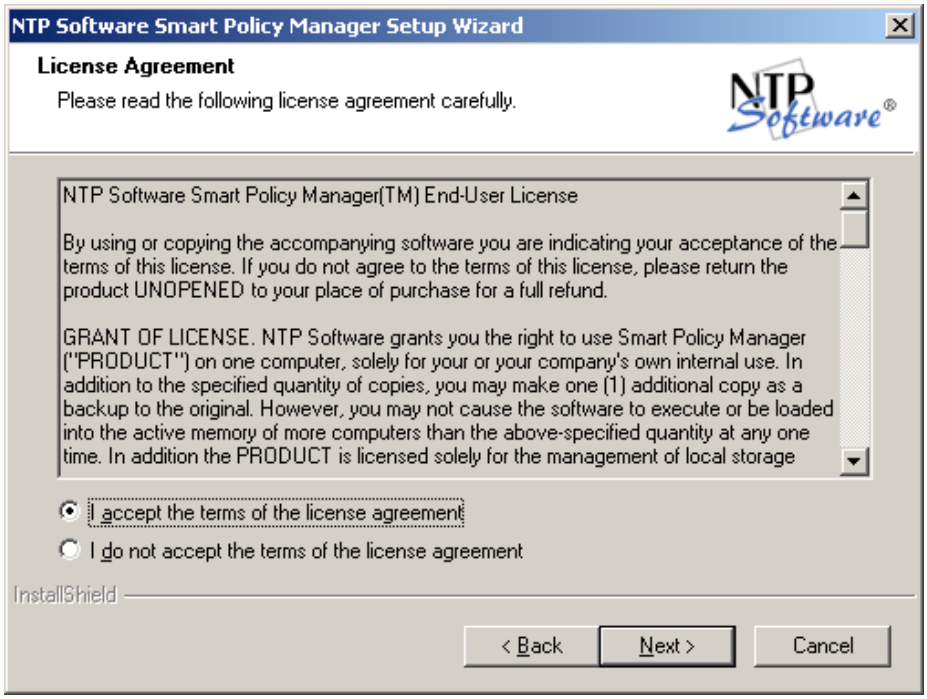


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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

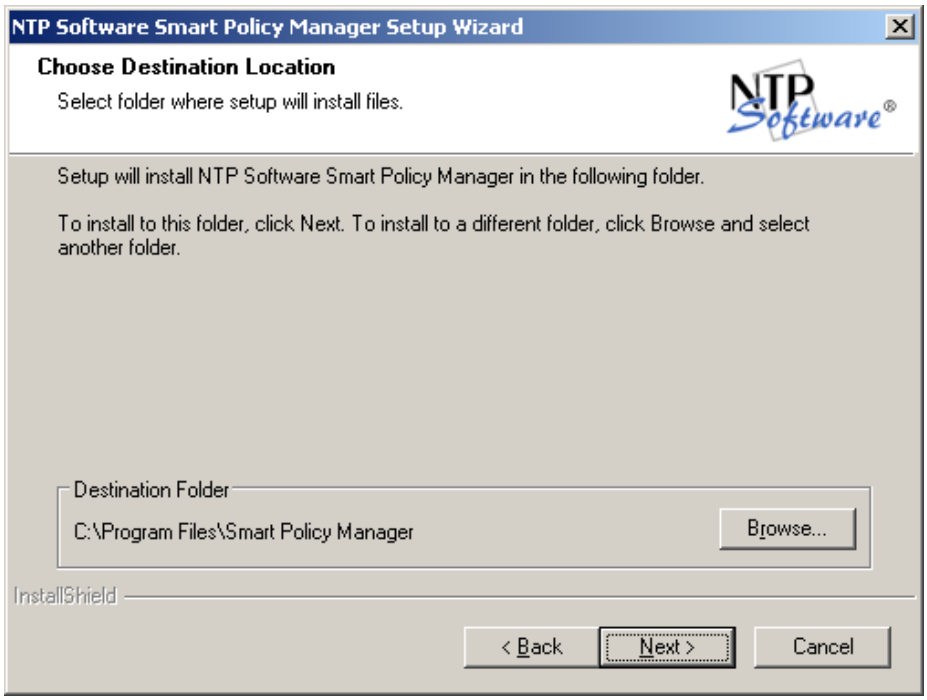


5. Select **I accept the terms of the license agreement** in the **License Agreement** dialog box and then click **Next**.

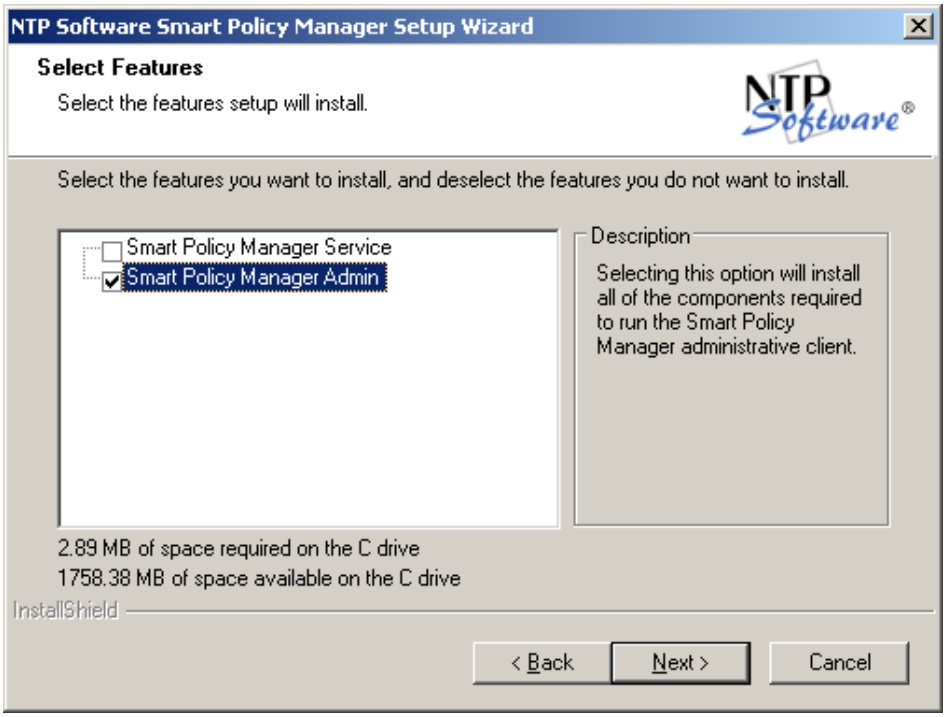


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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

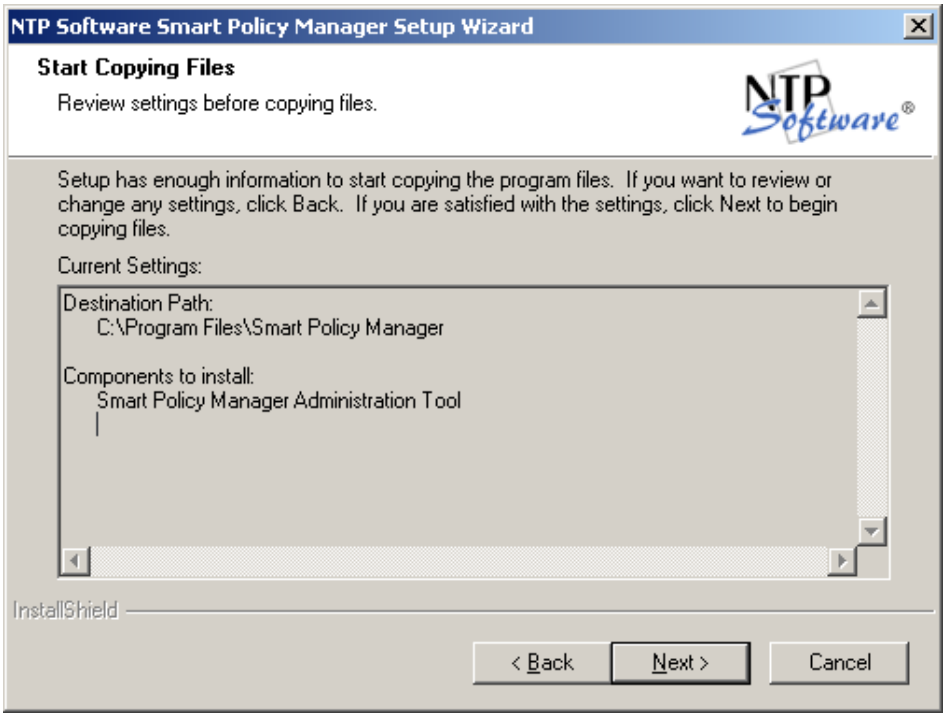


7. Select only the **Smart Policy Manager Admin** component in the **Select Features** dialog box. Click **Next**.

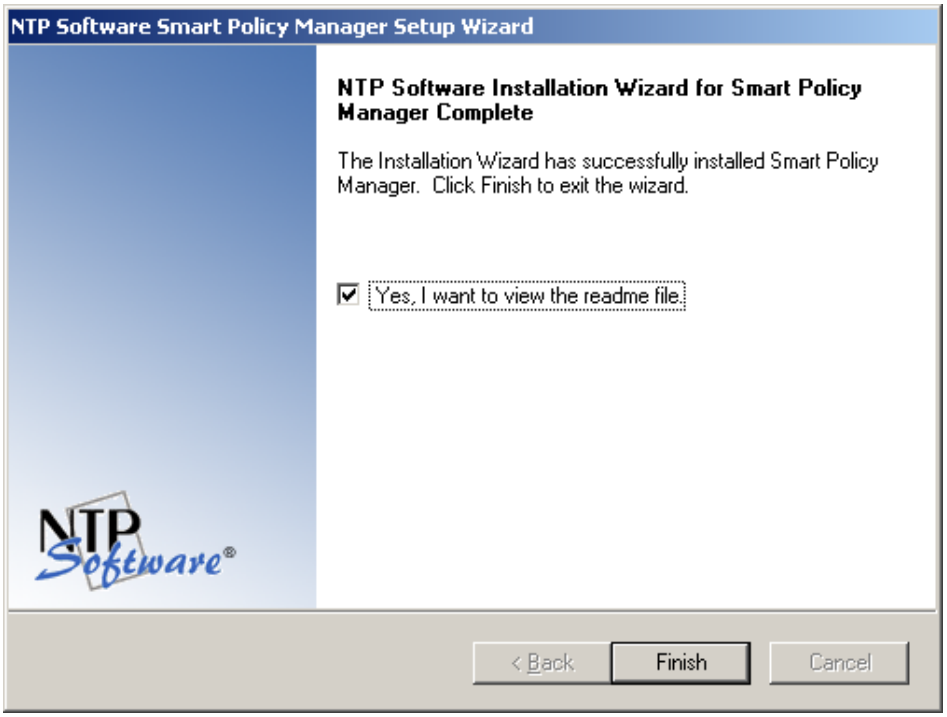


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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



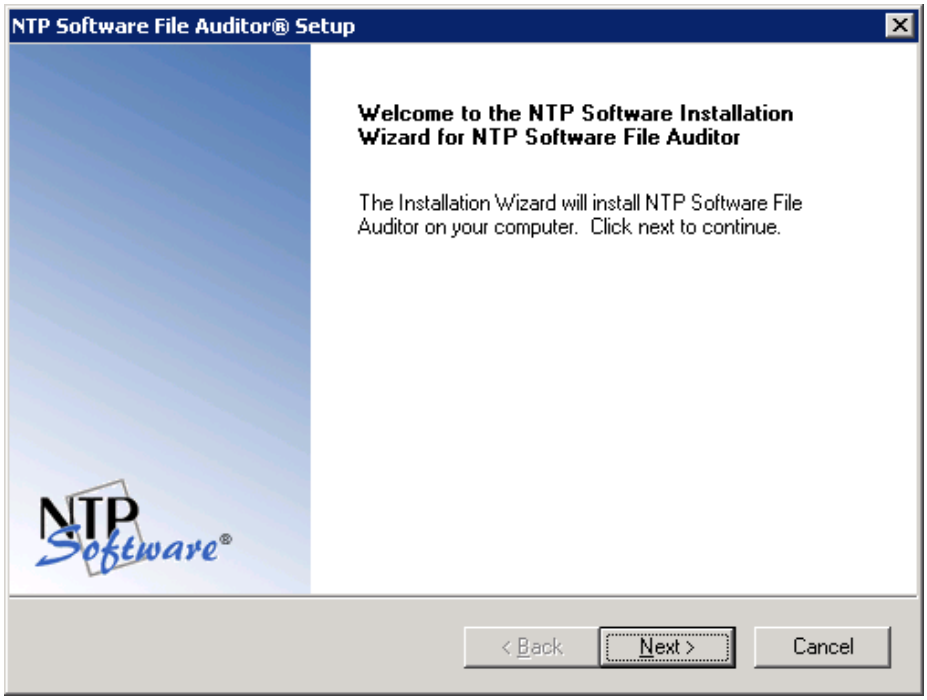
9. When the file installation is complete, a dialog box offers you the opportunity to view the readme file, which may contain documentation updates and other items. If you *do not* want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**.



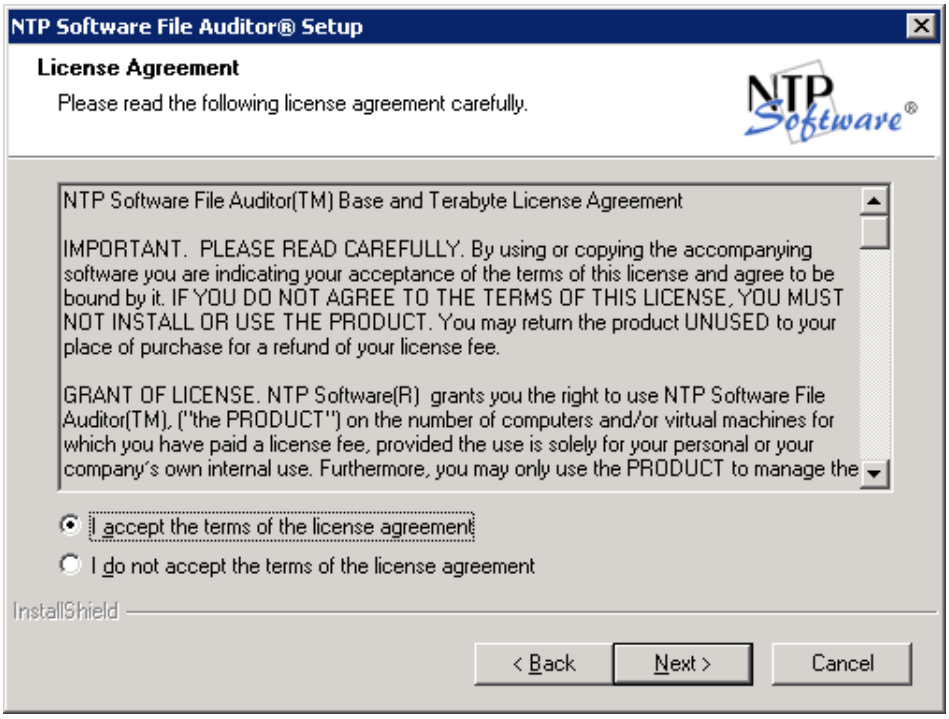
Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

Installing the NTP Software File Auditor Admin Component

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

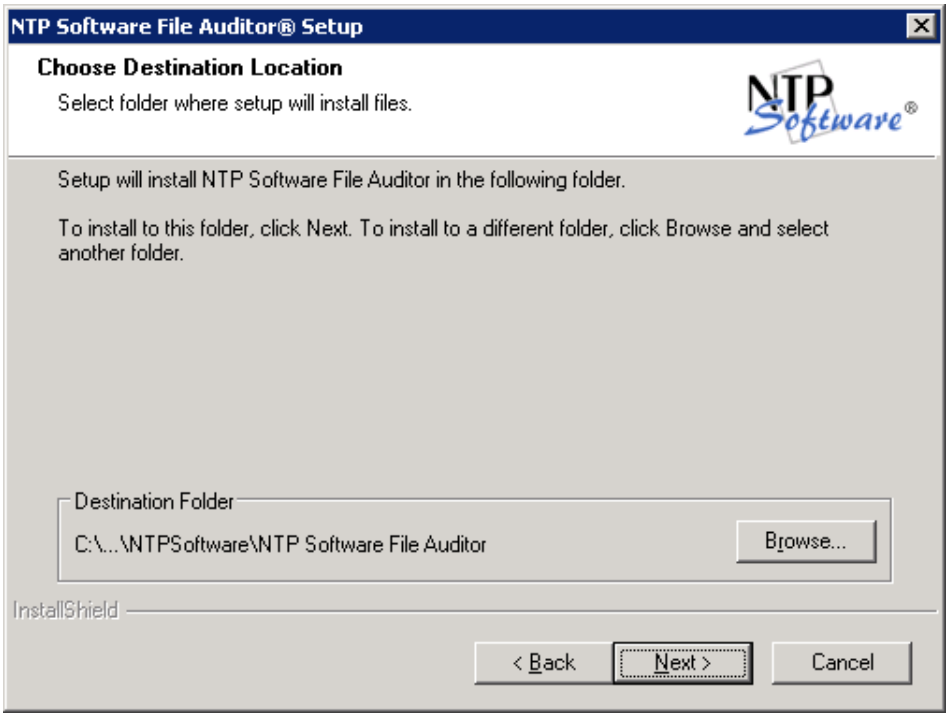


2. In the **License Agreement** dialog box, select **I accept the terms of the license agreement**; then click **Next**.

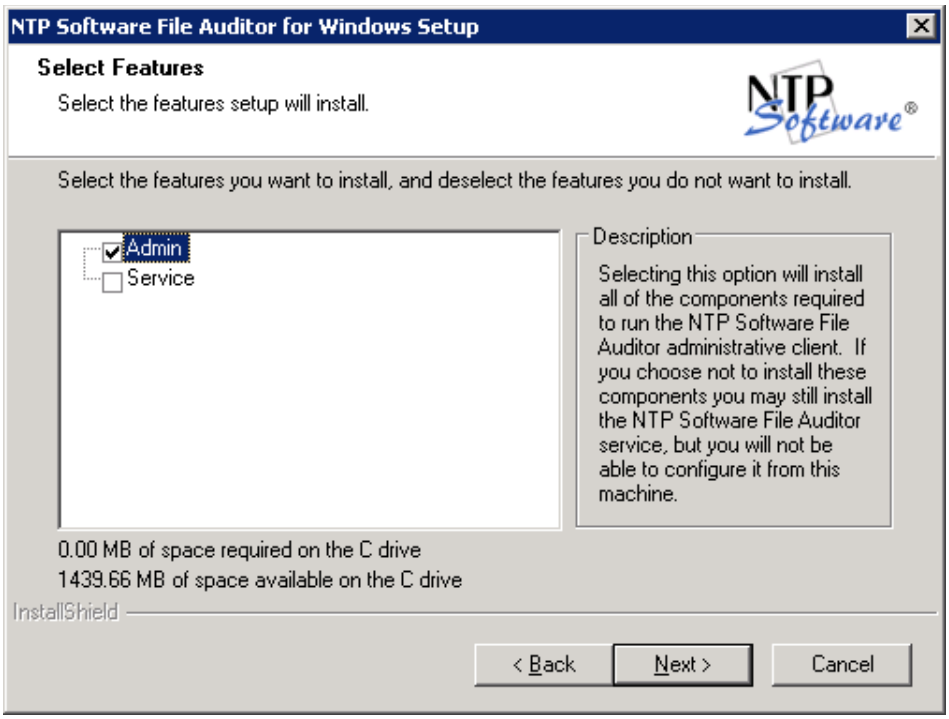


Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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



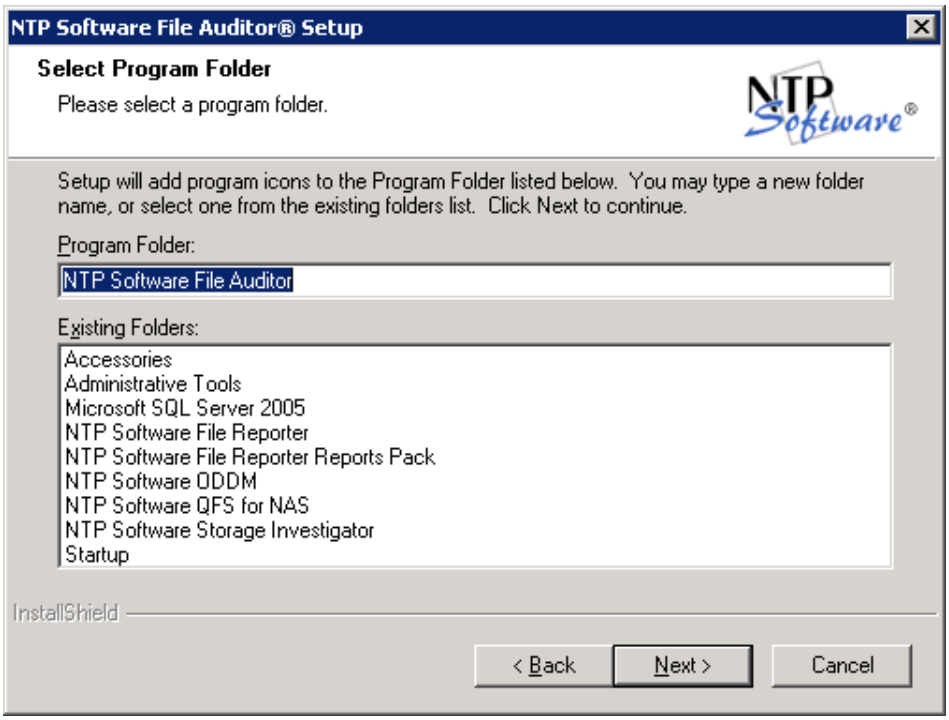
4. In the **Select Features** dialog box, make sure that only the **Admin** component is selected, then click **Next**.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

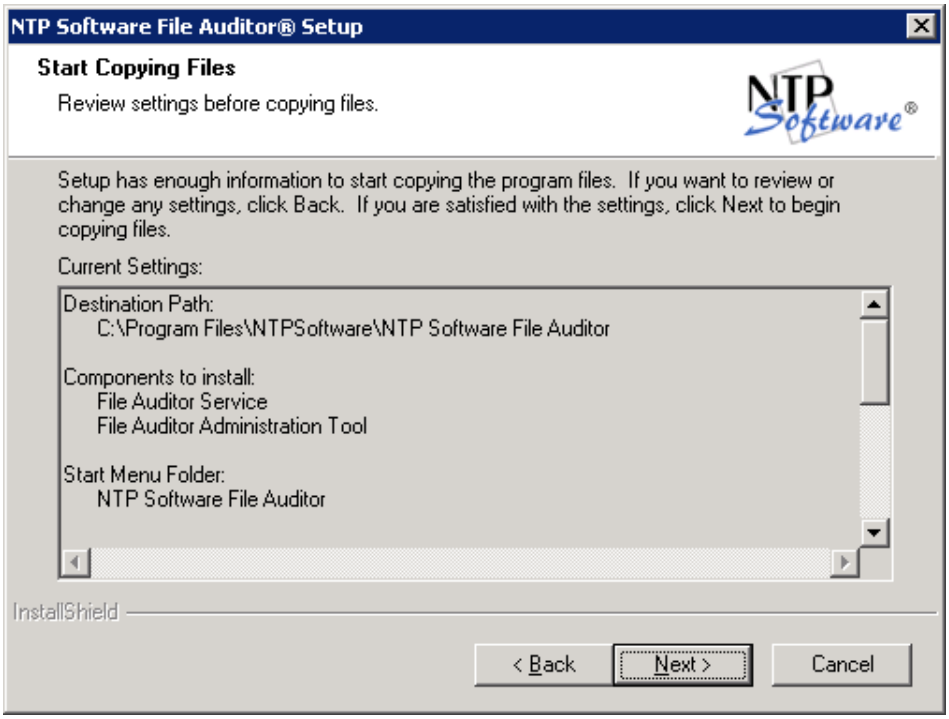
> **IMPORTANT**:
> Because we just need the Admin User Interface to manage and configure the policies, we checked the Admin Client only. We are not seeking a full NTP Software File Auditor, Windows Edition installation.

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.

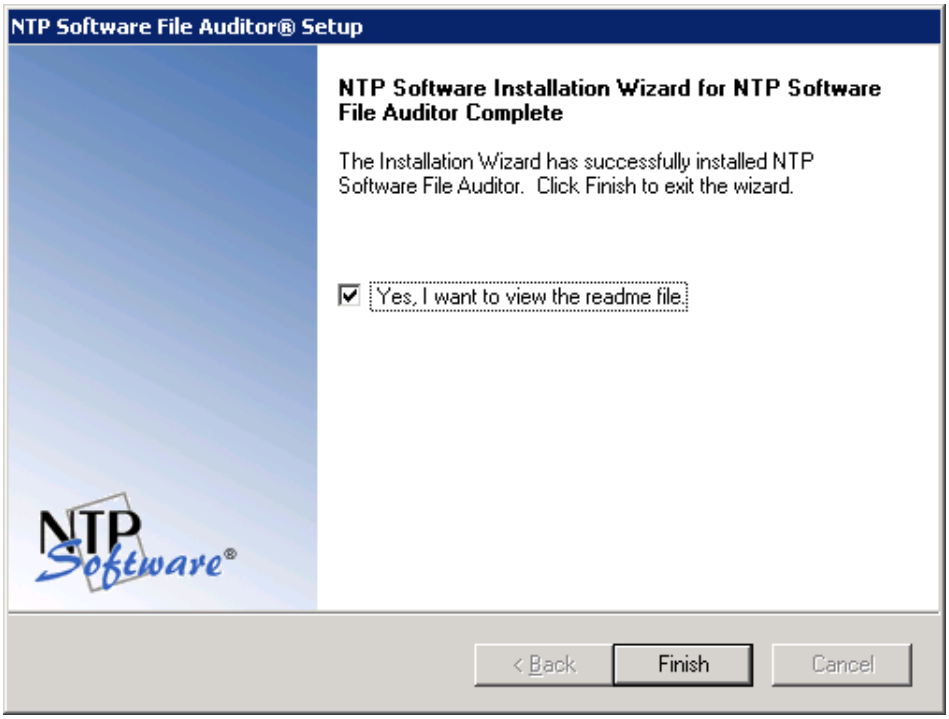


6. Click **Next** when the **Start Copying Files** dialog box appears (assuming that the destination paths are correct). NTP Software File Auditor setup begins transferring files to the specified locations.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF



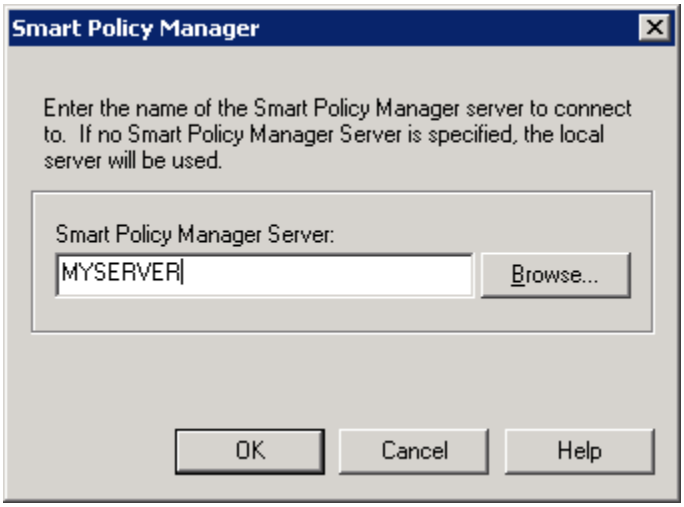
7. When the files' installation is complete, a dialog box offers you the opportunity to view the readme file. If you *do not* want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**. By this step, NTP Software File Auditor installation is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



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.



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.

1. 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.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

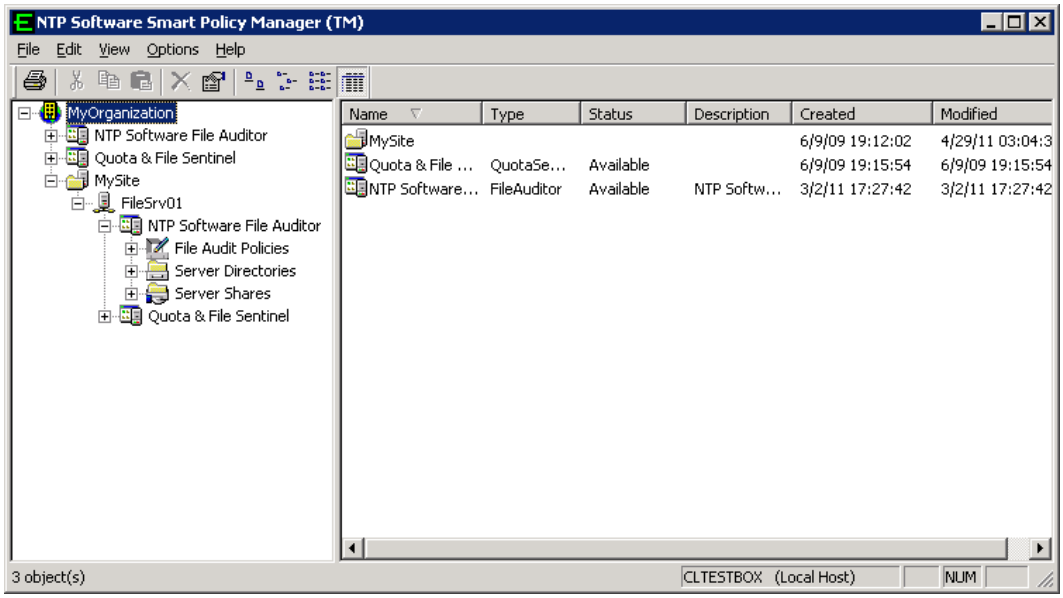
.

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.



Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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.

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF

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: info@ntpsoftware.com
Web Site: http://www.ntpsoftware.com

Copyright © 2015 by NTP Software®. All rights reserved. Doc#4825EF