NTP Software QFS® Family of Products User Guide

This User Guide applies to the following editions:

NTP Software QFS for NAS™
Dell™ PowerVault™ Edition, EMC™ NetWin™ Edition,
HP Storage Server Edition, IBM Storage Server Edition

NTP Software QFS for RAID/DAS™
Windows® Host Edition, Windows® Host 64-Bit AMD Edition,
Windows® Host 64-Bit Intel Edition

NTP Software QFS for SAN™
Windows® Host Edition, Windows® Host 64-Bit AMD Edition,
Windows® Host 64-Bit Intel Edition

Abstract

This guide details the method of using NTP Software QFS from an administrator's perspective. Upon completion of the steps within this document, QFS will efficiently manage your enterprise community.

Rev, March 2008

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, what is here 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, QFS, and End User Support Infrastructure (EUSI) 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

TABLE OF CONTENTS

Introduction

NTP Software QFS gives you the ability to manage and control disk space consumption and block or take other action if a user attempts to put unwanted files on your storage resources. You can enforce limits on the users of storage objects or on the objects themselves. It also affords the user the ability to self-manage his or her storage based on the parameters and notifications you configure.

QFS monitors storage use as it occurs and can be configured to do what you need as events unfold. For example, it can do the following:

- Send email and pop-up notification messages.
- Run programs, batch files, and scripts when usage thresholds are reached.
- Any of the above when particular files or file types are created or accessed.

QFS is different from all other quota and file management solutions in several important ways. In particular, it has the lowest post-deployment labor cost, which industry analysts agree represents 75% or more of your total cost of ownership (TCO).

Following are some of the important features that separate NTP Software QFS from other storage management products:

- "Push" installation throughout your enterprise with no server reboot required.
- Configurable policy-based rules management, quickly inherited by all machines in your organization. One policy record, created in an instant, can control hundreds of machines.
- Ability to create disk policies with up to 200 event triggers per policy. This means that there is no practical limit on your ability to manage storage resources automatically as activities occur.
- Flexible file-control policies.
- Ability to set policies for automatic file deletion. (This feature helps you avoid wasting time chasing obsolete and unwanted files.)
- In-depth reporting module and web reporting engine.

Ahead in This Guide

This guide walks you through a typical QFS usage, including the following phases:

- Creating policies — home and shared directory quotas, file screening
- Setting up thresholds for alerts and messages
- Inheritance of policies by other machines
- Pushing QFS to another server on your network
- Generating reports
- Installing the End User Support Infrastructure (EUSI) options
- Utilizing the command-line interface

　　　　Doc #.

Before You Begin

QFS is an excellent product even if you are managing only one machine; however, we recommend that you start with at least two servers. If you want to use email messaging, you need access to an email server.

As you probably already know, the cost-effective way to manage users is by using Windows groups. The examples here use the built-in Windows group Domain Users for much of what we do. In some examples, we use other groups created solely for the purpose of managing users. To complete the examples here, you should be able to create groups, or have available groups that you can use to designate as VIP Users and Large Home Directory Users.

The Role of NTP Software QFS in Storage Resource Management (SRM)

QFS is one part of total storage resource management (SRM) architecture; in and of itself, quota and file control is not a complete SRM solution. However, a good quota and file control solution is crucial to your overall SRM architecture. Taken end-to-end, SRM includes the following features:

- **Provisioning.** Supplying storage resources.
- **Quota and file screening.** Controlling use of the resource.
- **Performance monitoring and management.** Monitoring performance and ensuring the delivery of a predictable level of service.
- **Backup and archiving.** Document maintenance and protection.
- **Reporting and cost allocation.** Analyzing resource consumption and assigning costs where they belong.

In conjunction with other ISVs, NTP Software offers an integrated suite of Smart Policy Manager-enabled products that can be used to create a self-managing end-to-end SRM solution.

Configuring NTP Software QFS

To administer QFS follow the following steps:

1. Log onto the server, using your administrative account.

2. Click the Windows Start button and then choose **Programs** > **NTP Software QFS** > **NTP Software QFS Admin**.

Doc #.
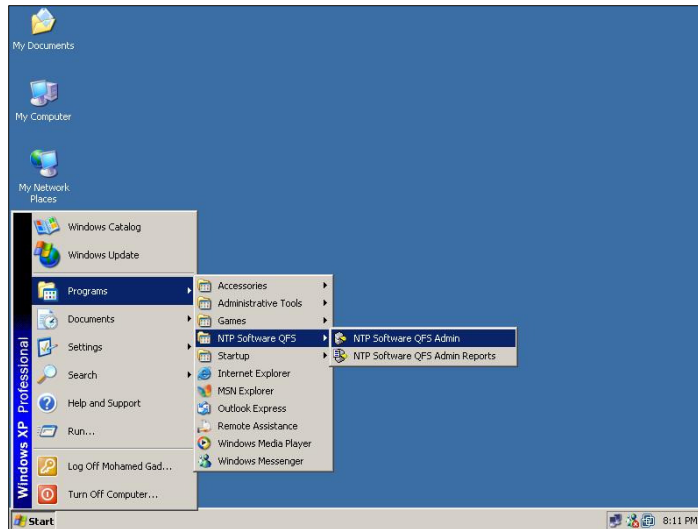
Overview of Smart Policy Manager

The first step in using NTP Software QFS is to lay out your strategy for quota policies and file-control policies. Before doing this, though, let us look at our underlying policy-based rules engine, Smart Policy Manager.
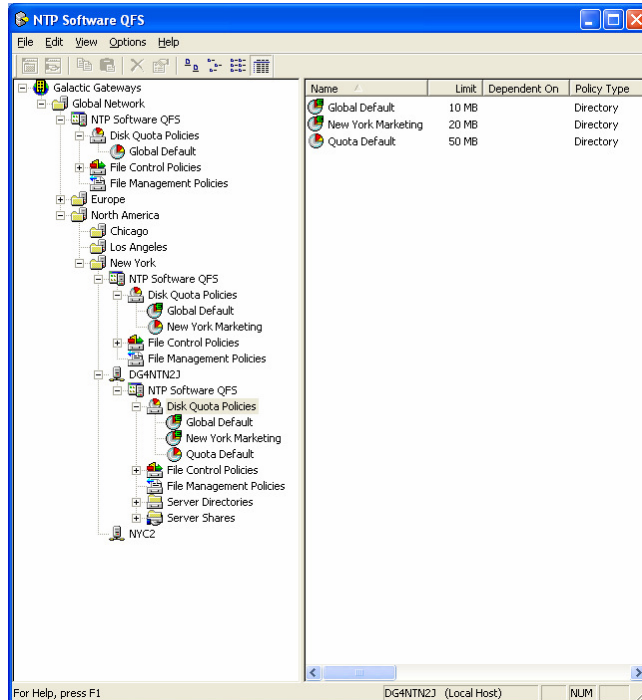

Smart Policy Manager provides the framework in which you specify your SRM policies.

Here we have organized policy settings by geography, a common approach. You may want to use this strategy, or you can choose some other structure that better reflects how you manage your network and its resources.

Smart Policy Manager allows you to organize your SRM policies 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, department, and type of machine. Smart Policy Manager has the flexibility you need to make using NTP Software QFS simple.

Once you have laid out your management structure, 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 our example, Galactic Getaways). This is the Global Network configuration, whose container we created at installation.

Doc #.
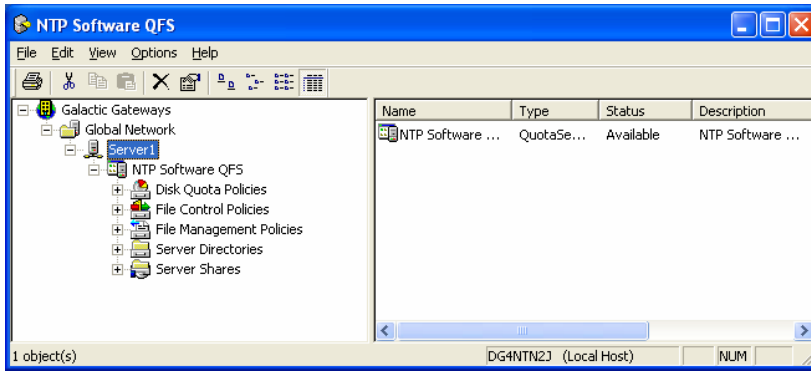
Our installation created the policy hierarchy that you see here. If you have only one server, this is all you need. All the QFS policies can be added under Server1.

Establishing Global Policy Settings

As installed, the only NTP Software QFS policy container is under Server1. This means that the policies we create there would apply only to Server1. This is a fine result for a single-server network, but probably not the best choice for your entire network. What we need to do is create a configuration container for QFS whose scope extends beyond Server1. To do this, we will add the QFS application to the root of our Global Network, as illustrated below.

1. Highlight Global Network.

2. Right-click and select **New** > **NTP Software QFS Application** from the pop-up menu.
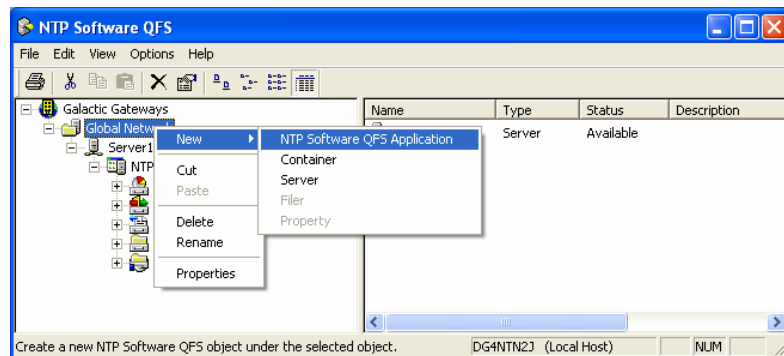
This command creates a configuration container for NTP Software QFS that is global in scope. All containers and servers throughout your enterprise will inherit the settings entered here.
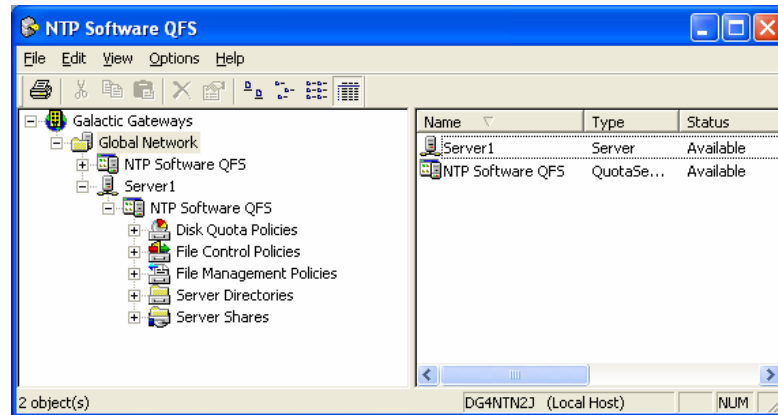
Configuring and Setting QFS Application Properties

1. Right-click **NTP Software QFS** under Global Network in the left pane.
2. Click **Properties** on the pop-up menu.

Doc #.
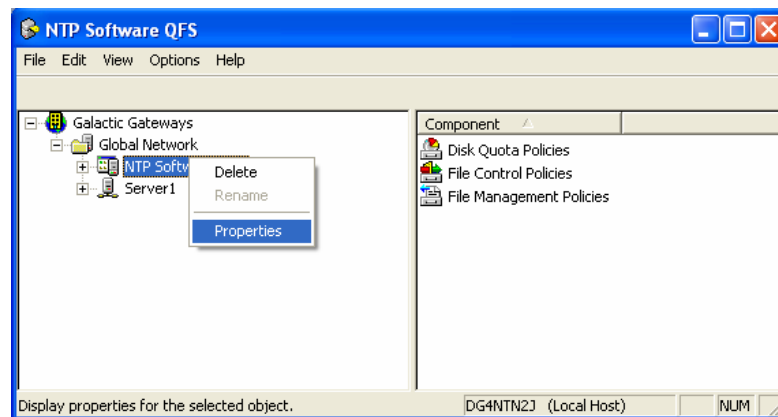
3. On the Email Configuration tab, uncheck the box **Inherit Email Configuration**, check the box **Enable Email Notifications**, enter the correct information in each of the four text boxes as appropriate for your network, and click **OK**.

4. Now let us move on to configuring Simple Network Management Protocol (SNMP), which helps in managing complex networks. Click the **SNMP Configuration** tab. Uncheck the box **Inherit SNMP Configuration**, check the box **Enable SNMP Messages**, enter the SNMP console IP address that will be used to monitor the network, enter the Community Name, and click **OK**.

5. Click the **Event Options** tab and uncheck the box **Inherit Options**.

6. Next, we will configure the desired quota threshold and file management threshold events. Quota thresholds post events when falling below thresholds, when exceeding thresholds, or both. Check the desired settings in the **Quota Threshold Events** section of the dialog box. File management thresholds post events for file management time remaining thresholds, file deletion operations, or both. Check the desired settings in the **File Management Threshold Events** section of the dialog box.

　　　　　　　　Doc #.

NTP Software QFS® Family of Products User Manual
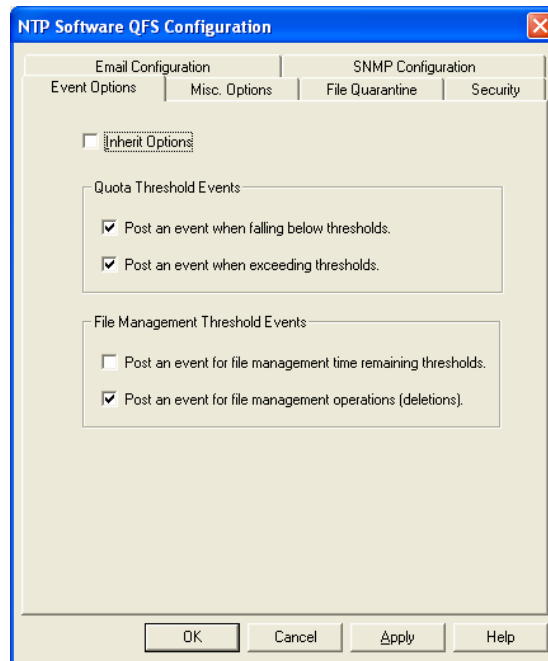
7. Click the **File Quarantine** tab and uncheck the box **Inherit File Quarantine Configuration**.

8. In the **Prohibited File Disposition** choose **Quarantine** to remove the file from its original location and place it in a QFSQuartine directory in case it needs to be replaced or archived.

9. In the **Prohibited File Disposition** choose **Delete** to delete a file permanently.
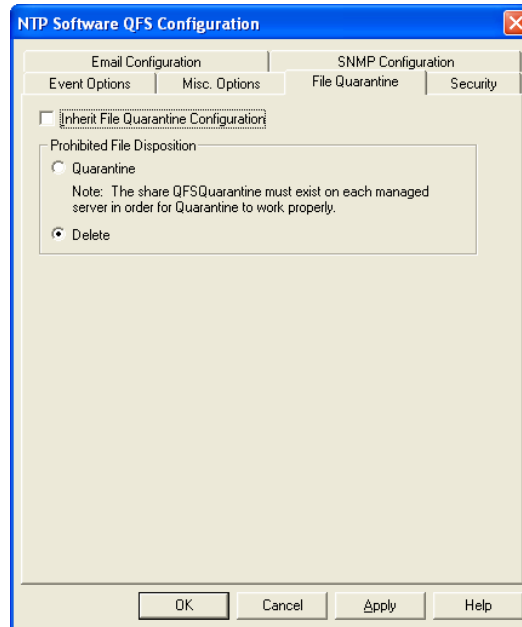
10. Click the **Security** tab. uncheck the box **Inherit Security** and check the box **Enable Security**. Click **Add** to choose the members or groups for which you want to apply security options.

Copyright © 2001–2008 by NTP Software. All rights reserved

13

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

That is all there is to this procedure. Let's move on to creating management policies.
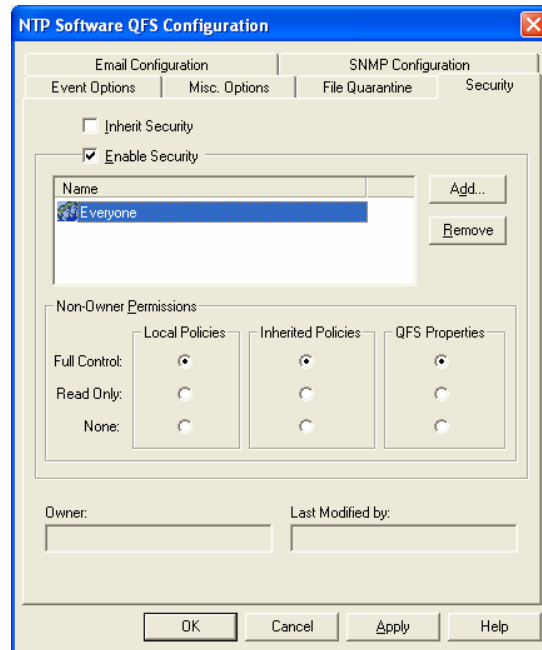
Creating Storage Quota Policies

This section walks you through creating a few typical disk quota policies. We will start with creating a quota policy for all your user home directories in a typical server configuration. Then we will demonstrate how to set up a quota on a shared directory. Finally, we will illustrate the concept of temporary quotas.

Creating Quota Policies for User Home Directories

This quota policy will be applied to all users in your Users directory. Each user will get a quota limit of 50MB.

1. In the left pane, under **Global Network**, if necessary click the plus sign (+) by **NTP Software QFS** to expand the hierarchy.

2. Right-click **Disk Quota Policies** and select **New** > **Folder Policy Using Directories** from the pop-up menu.
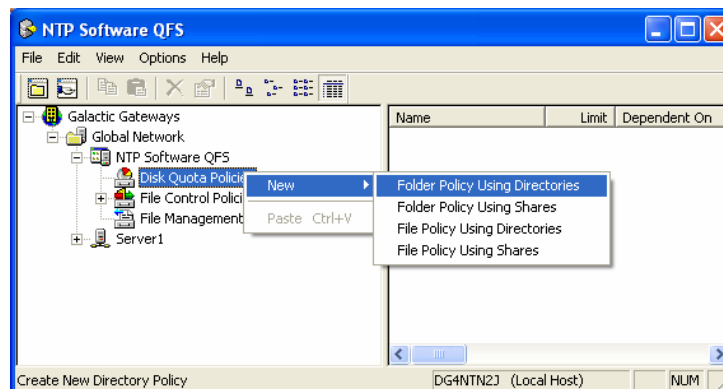
3. In the New Quota Directory Policy dialog box, click the **General** tab. Enter a name and a description for your policy. See the example below.

QFS offers more flexibility and functionality than any other quota and file screening technology.

The "Always enforce this one" feature specifies that a selected management policy is always enforced, regardless of whether multiple policies exist.

Doc #.

4. Click the **Quota** tab. Set a policy quota limit of 50MB, select **Deny Writes at 100% of Quota**, and leave the overdraft option unchecked, as in the following example.

In this example, each user gets a 50MB quota for his or her home directory.

With the "Deny Writes" option selected, the user is prohibited from going above 50MB under any circumstances.

Overdraft privileges (which we won't use in this example) would allow the user to exceed the specified maximum of 50MB for a limited time.
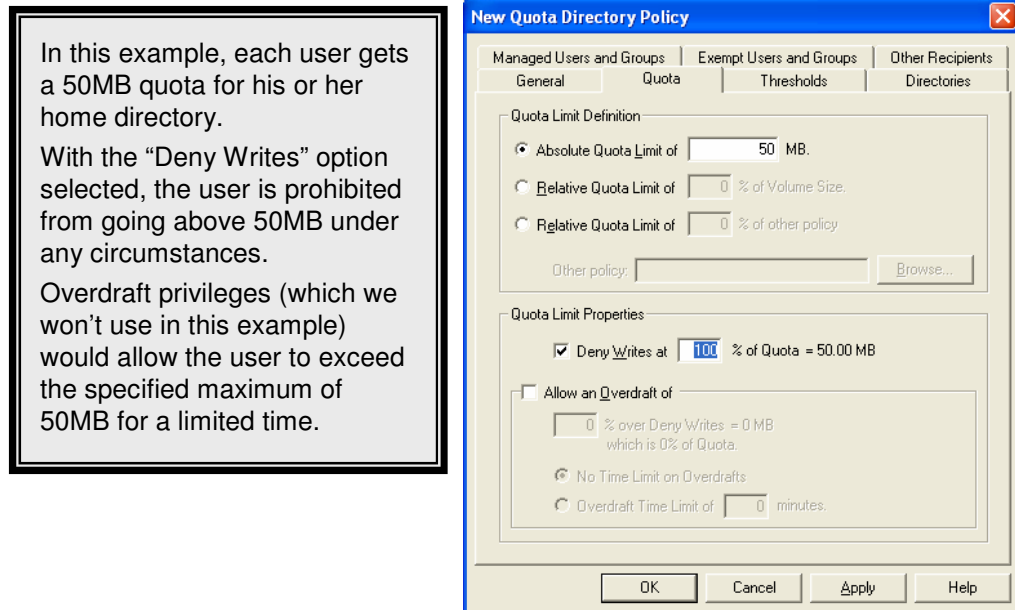
5. Click the **Thresholds** tab to view the thresholds for this quota policy. In the following example, notice that one threshold is already set up: At Quota 100%. Adding more thresholds is as simple as selecting **Add** and filling in the percentage information you want for that threshold. As space is consumed and thresholds are reached, each threshold can send email messages to users, network administrators, the Help Desk, and so on. A threshold trigger can also run a process; for example, deleting .TMP files or starting an archive to tape.

Doc #.

QFS lets you create up to 200 threshold levels for each policy. Common choices for additional levels are 75%, 85%, and 95%. As users reach each of these levels, you can customize your messages to suggest that the user delete some files or contact the Help Desk and request a quota increase before the ability to save new documents runs out.

It is also possible to integrate QFS with your intranet and automate the process to increase storage limits.
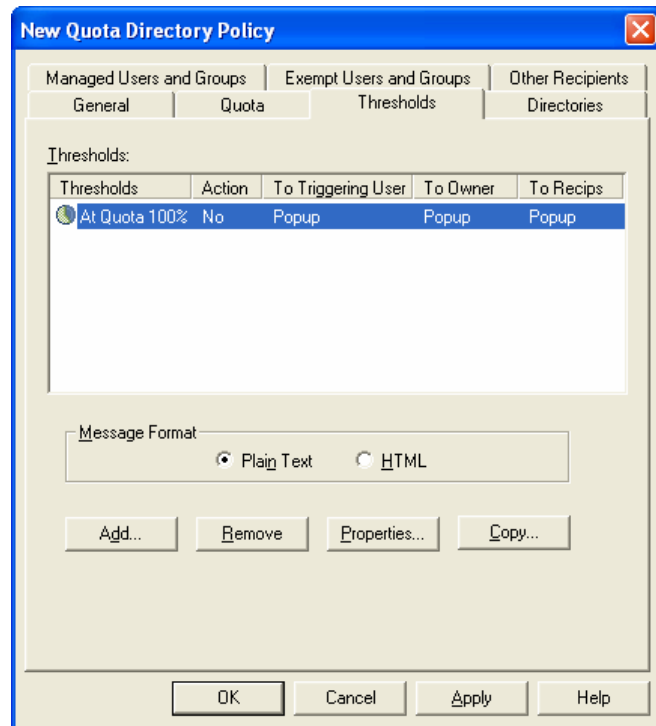
6. Double-click the **At Quota 100%** threshold to display the **Threshold Properties** dialog box for that threshold level (see example, right).

7. The Popup options are already selected. If you configured QFS for email in the earlier steps, select the **Email** checkbox in the **Send to Triggering User** section of the dialog box (see image, right).

    The Messages tabs let you customize the text of the messages that will be sent.

    The Commands tab allows you to specify a program, script, or batch file that will be run when the threshold is reached.

8. After choosing the appropriate settings, click **OK** to return to the New Quota Directory Policy dialog box.
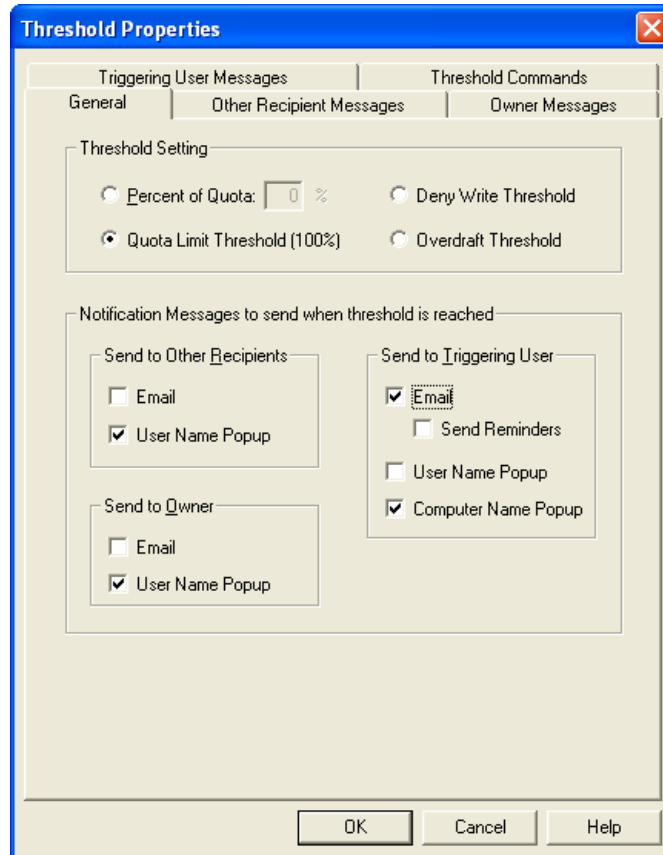
9. Click the **Directories** tab. Click the **Add** button and either type **C:\Users*** or type the appropriate directory name for your system followed by ***** (backslash, asterisk).

Because this quota specifically applies to C:\Users*, the asterisk (*) automatically applies the quota to each subdirectory under C:\Users individually, and not to the directory C:\Users itself.

In this example, this specification means that each user's home directory under C:\Users will get this 50MB quota policy and its configuration settings. This quota policy will apply to all current and future subdirectories under C:\Users (both new and old users).

By default, this quota applies to all users. You can verify this fact by clicking the **Managed Users and Groups** and the **Exempt Users and Groups** tabs. We recommend sticking with this configuration. But be careful to remember later on that administrators are exempt from quota enforcement. Alternatively, you can apply the quota to C:\Users (without the *), applying that quota policy to all of C:\Users.

10. Click **OK** to create the new quota directory policy, which will be inherited by all systems from this point down in your Smart Policy Manager hierarchy.
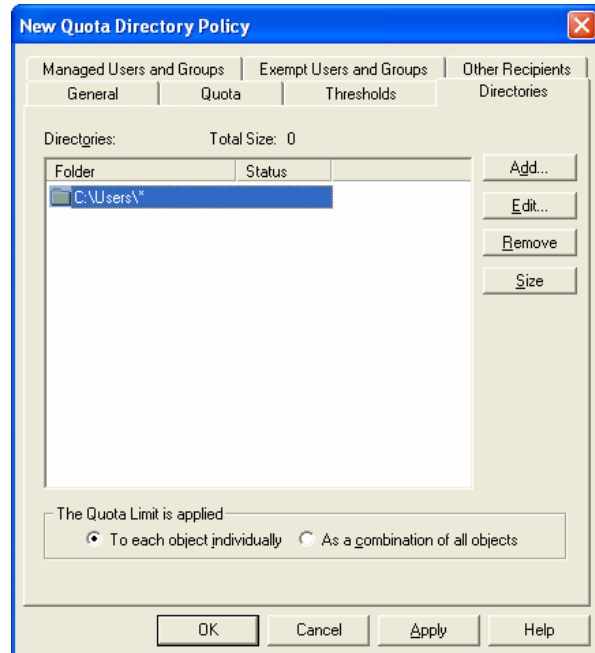
Congratulations! You have just created your first disk quota policy!

Smart Policy Manager now replicates the new policy to all servers below this point in your Smart Policy Manager tree. Go to the server(s) in your Smart Policy Manager tree where QFS is installed. Click **Disk Quota Policies** and then press the F5 key (or choose **View > Refresh**) to refresh the screen. The new policy appears underneath this server. (It may take several minutes for replication to complete, potentially longer over a WAN.)

The fact that a disk quota policy is inherited from above and not created locally is designated by the small green *E* in the upper-right corner of the disk quota policy icon.

Whether you have 100 or 1,000 (or more) servers in your network, Smart Policy Manager will automatically replicate this disk quota policy — in fact, all of your Smart Policy Manager policies — to each of those servers. Smart Policy Manager reduces your post-installation cost and effort to the minimum possible. You can manage 1,000 machines with no more effort than you would use for one.

Next, let's look at the size of the user directories in this inherited policy.

Doc #.

11. Select your server in the tree view. Expand its configuration, if necessary, and then expand its Quota Policies container. Click the inherited policy you just created in the preceding steps. The details of this policy should appear in the right pane (see the background image below).

12. In the right pane click on the + next to C:\Users to expand the directory and see a listing of the user directories (subdirectories of C:\Users) on this server and the status of each of their quotas.
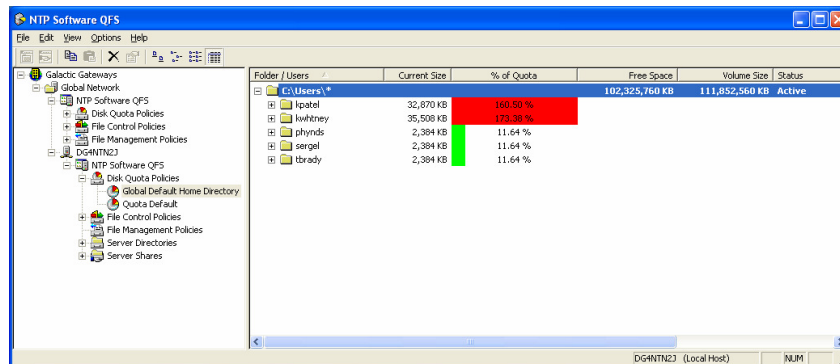
Before moving on, we might want to make a few adjustments in our storage quota policy. The following sections discuss some options.

Adding Exemptions

In many organizations there are people who, by virtue of their roles in the institution, need to be exempt from policies such as disk quotas. Your CEO and vice presidents, for example, may not appreciate having limits on the size of their home directories. Let's make those people exempt.

We have a Windows group, VIP Users that includes those users on our network who get special treatment and are exempt from limits such as home directory quotas. Your network may have a similar group, or you may want to create one.

1. Go back to the QFS application under Global Network, and select the **Global Default Home Directories** in the tree view in the left pane. (Expand the tree view as necessary.)

2. Right-click the entry and select **Properties** from the pop-up menu.

Doc #.
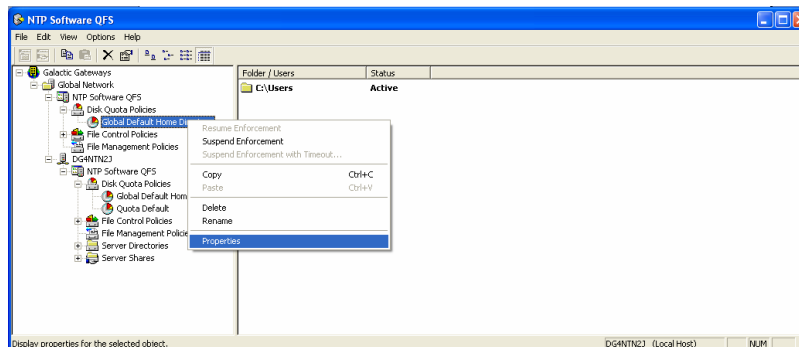
3.   Click the **Exempt Users and Groups** tab.

4.   Click the **Add** button.

5.   Click the **Browse** button and select the Windows group that designates your VIP user community.
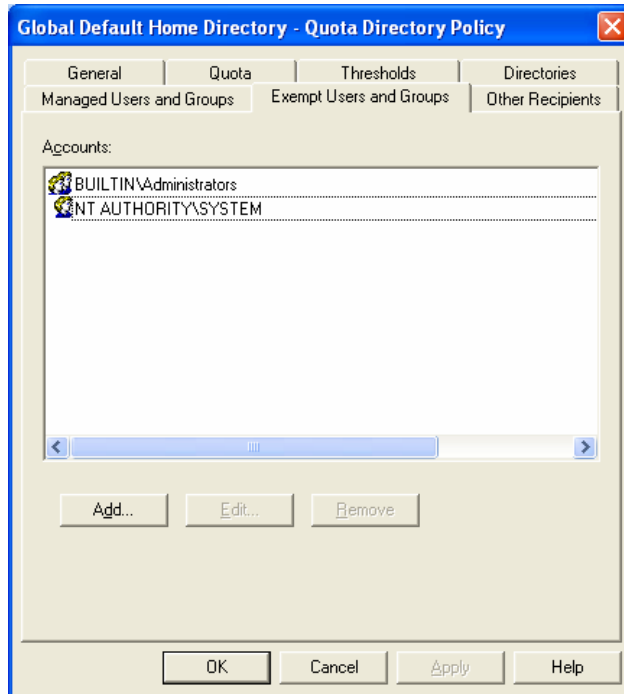
By default, NTP Software QFS excludes administrators, backup operators, file replication, and the system itself from quota enforcement. This arrangement generally lets most system maintenance activities proceed without interference.

You may want to consider whether other groups of users or system accounts should be excluded on your network.

Exempting VIP users from system limits is often a good career move.

Adding Global Quotas for Storage Power Users

The global default home directory quota (50MB) we set previously should be adequate for most users, without being wasteful. However, some users probably need more storage space. For example, marketing staff often need larger home directories to accommodate the bitmaps and image files they use. Let's create a default quota for these "power users."

1. Select **Disk Quota Policies** under **NTP Software QFS** in your Global Network container.

2. Right-click the policy record in the right pane and select **Copy** from the pop-up menu.

3. Press Ctrl+V to paste a copy of this policy in your Disk Quota Policies folder.
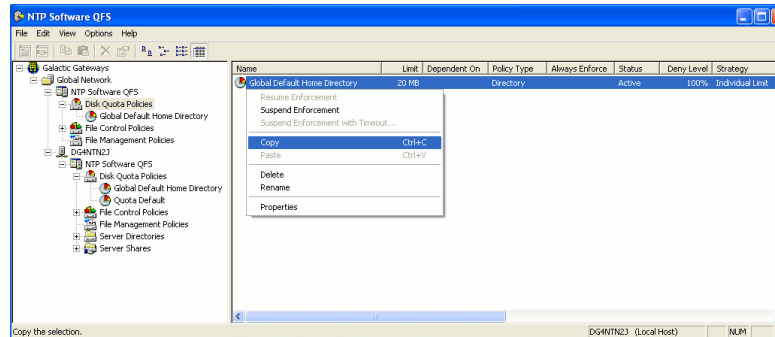
4. Fill in a new name for this policy. (Policy names in each folder have to be unique.) Change the policy's description as appropriate.

5. Click the **Managed Users and Groups** tab and select the **Certain Users** radio button.

6. Click the **Add** button. Select the Windows group for which you want to provide the increased limit. (On our network, we have the "Big Users" group.)

    Because we created this policy by copying the modified global default quota policy, VIP users will be exempted from this limit as well. You can check the **Exempt Users and Groups** tab to verify this setup.

7. Click **OK** to save this policy.

Doc #.
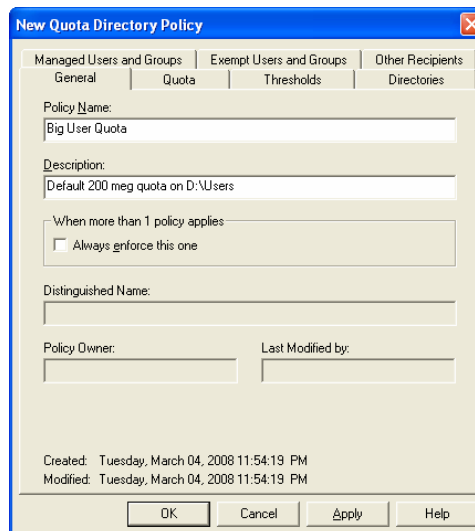
NTP Software QFS includes the ability to deal intelligently with overlaps in scope. In this particular case, it's clear that we want the Big User quota to override the global default quota. Our storage power users in the default quota group should get the Big User quota of 200MB and the global default should be ignored. This is exactly what happens. The logic in QFS ensures that you get what you intend, without having to do complex analysis or calculations.

Creating Shared Directory Quotas

Now that you've learned how to control users' home directories, we'll show you how easy it is to deal with shared folders.

On most networks, users are offered one or more shared spaces in addition to their home directories, where they can work together and exchange documents. For these shared areas, we want to create a different kind of quota. We want to cap the size of this shared space overall, but we don't care about objects within it.

1. Right-click **Disk Quota Policies** under your server's name in the tree in the left pane. Then select **New** > **Folder Policy Using Shares** as shown in the image.
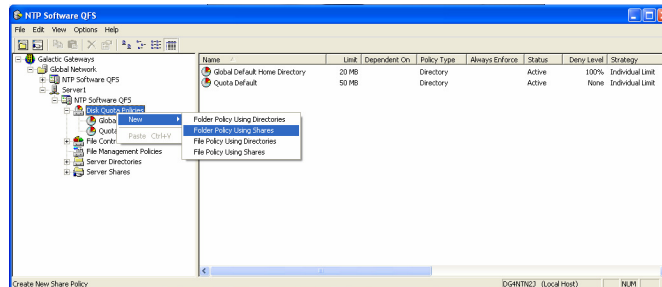
2. Fill in the information on the **General** tab. Call the share policy **Sales Files Share Policy 100MB**, as we'll be putting a 100MB share quota in the Sales Share folder.

3. Click the **Quota** tab and fill in the pertinent quota information. We'll make this a "hard quota": Select the **Deny Writes** option and specify a 10% overdraft for a 60-minute time period (see image). If this share goes past 100MB, the user has an hour before his or her activity is blocked, but at no time can the size exceed 110MB (110% of 100MB).

    QFS not only allows an overdraft — it gives it a time limit, which means that you have the ability to be more flexible in implementing quotas. By granting users some flexibility on quotas, you accomplish several things:

    - Gentler, more user-friendly quota policies.
    - More productivity — users can get important work done (and saved) and then delete unwanted files to return below quota.
    - Without a time limit, an overdraft is just extra space added to each user's quota, which accomplishes nothing.

Doc #.
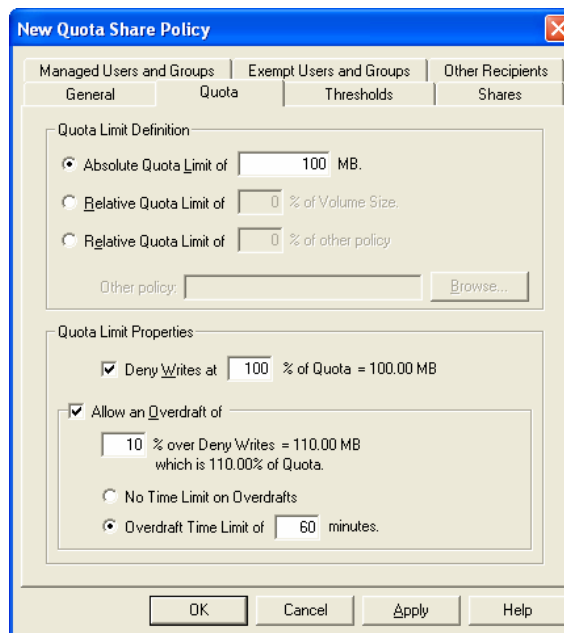
4. Now we need to tell QFS which shared directory to manage. Click the **Shares** tab.

5. Click the **Add** button and then click the **Browse** button. If the Browse button is not active on your system, it means that you're adding a quota at the container level (for example, Global Network), rather than for a particular server.

6. From the shares on your server, select the share you want to manage; then click **OK**.
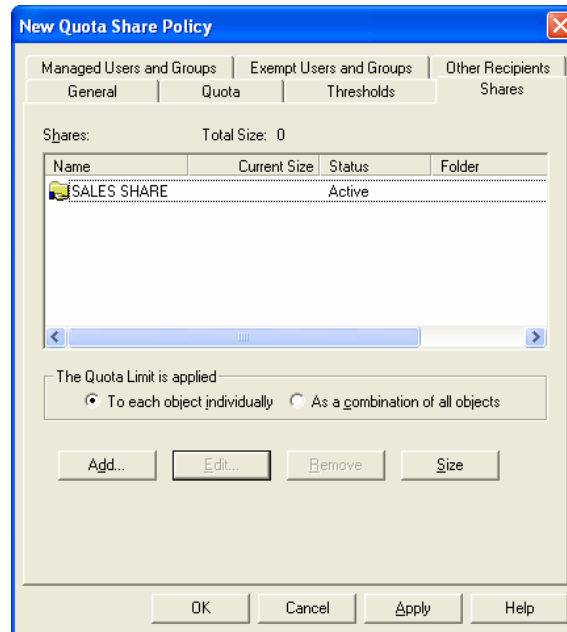
Managing shared space is more complicated than controlling home directories. Often, the person responsible for the space — a department manager, for example — isn't even a user of the space. Therefore, we'll configure quota messages for three recipients:

- Triggering user (the person whose activity fired the quota trigger)
- Owner (usually the network administrator)
- Other recipient (in this case, the sales manager)

7. Click the **Thresholds** tab and add the types of messaging (email and/or pop-up) that you want for your share policy. For this example, we will use the 100% threshold, and notify the triggering user, owner, and sales manager (as "other recipients"), as shown in the image below. Click **OK** when you are done.

With this configuration, when the 100% threshold is reached, the triggering user (the user who caused the threshold to be reached), the owner of the managed area, and the other recipients (the sales manager, in this case) will all receive notification that this threshold has been reached
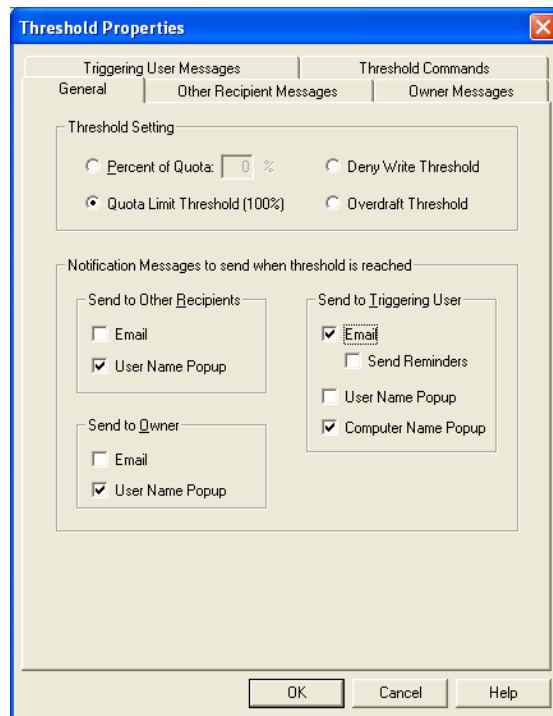
Pop-up messages use the Windows messenger service. This is automatically available for Windows NT, 2000, and XP computers. For Windows 98 or Windows 95 machines to receive popup messages, the optional Win popup service must be started.

For Terminal Server users, set the Triggering User pop-up to User Name, since all Terminal Server users are on the same computer.

Email messages necessitate the configuration of QFS for email, as shown earlier in this guide.

8. (Optional) If we are going to send messages to "other recipients," we have to tell QFS who those recipients are. Click the **Other Recipients** tab. enter the ID of the recipient (the sales manager, in this example) or browse the list of users and select the ID. Then click **OK**.
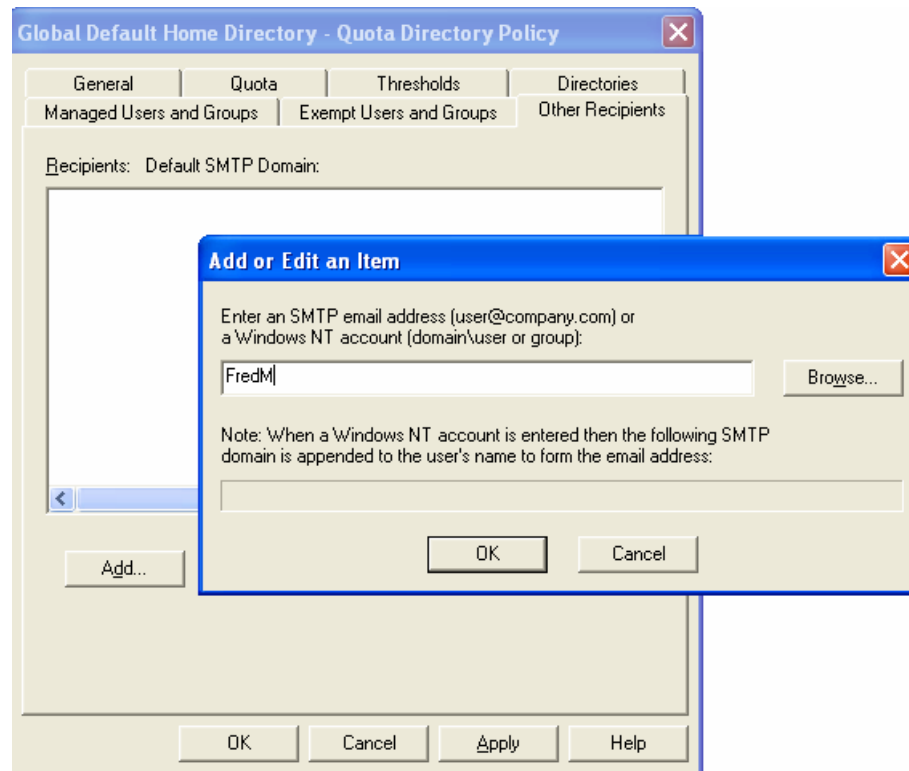
9. Click **OK** to finish setting the quota. You should see something like the following image. Notice that our new quota is active. The size of the share and percentage of quota are displayed.

28
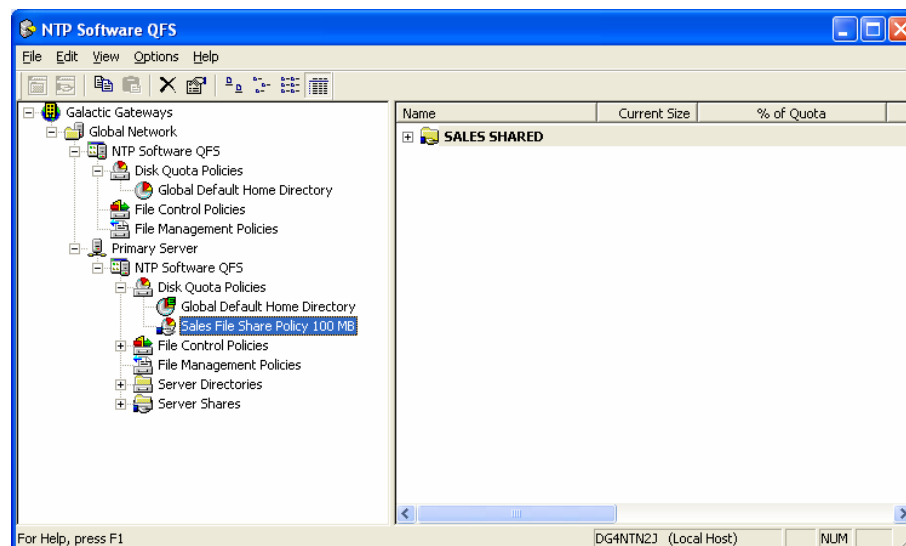
The previous examples created disk quota policies for directories and shares. What about using the same methodology for files?

Creating File Policies Using Directories

1. In the left pane, under Server1, if necessary click the plus sign (+) by **NTP Software QFS** to expand the hierarchy.

2. Right-click **Disk Quota Policies** and select **New** > **File Policy Using Directories** from the pop-up menu.
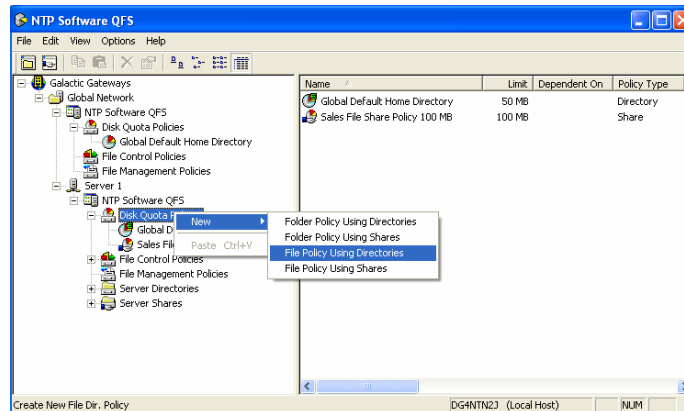
3. In the New Quota File Policy dialog box, click the **General** tab. Enter a name and a description for your policy.

4. Let's make the policy dependent on a previously created folder policy. Click the **Browse** button.

Doc #.
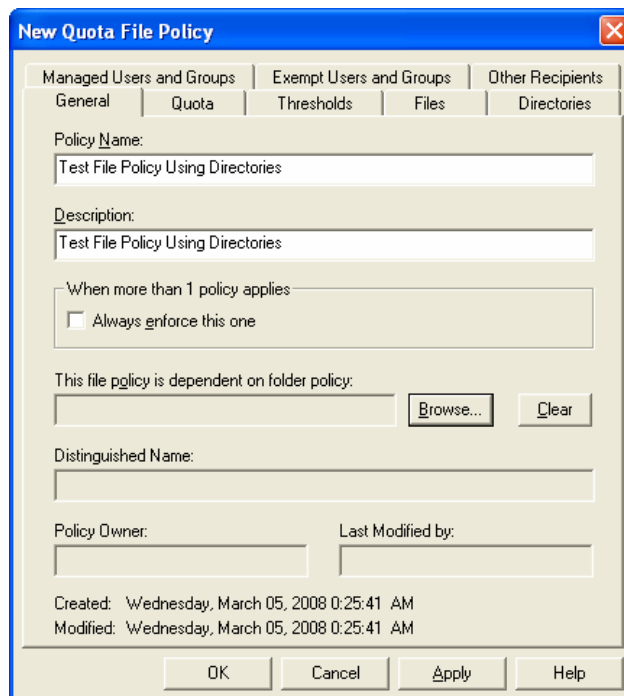
5. In the Choose Policy dialog box, select the dependent policy's name. Click **OK**.
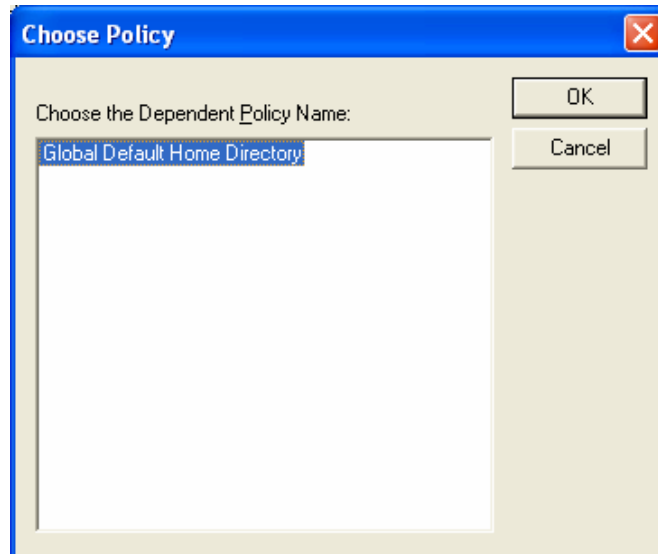
6. Click the **Quota** tab and fill in the pertinent quota information. Set a policy quota limit of 100MB, select the **Deny Writes at 100% of Quota**, check the box **Allow an Overdraft of** and specify a 10% overdraft for a 60-minute time period. If this share goes past 100MB, the user has an hour before his or her activity is blocked, but at no time can the size exceed 110MB (110% of 100MB).
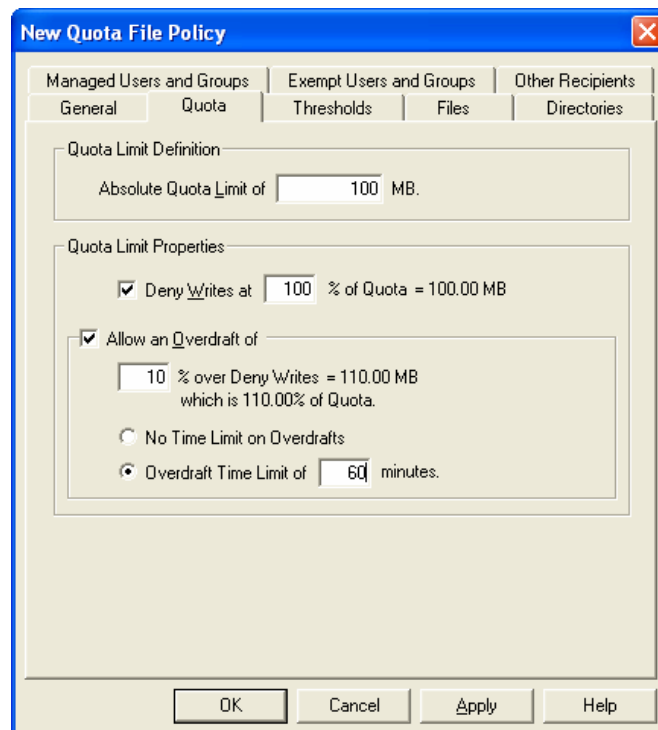
7. Click the **Files** tab. Click **Add** and enter the file patterns you want (for example, *.AVI, *.MP3, *.VBS, and so on). In this example, we've entered ***.MP?** to include *.MP3, *.MP2, *.MPG, etc. — all music files.

    Note: QFS follows the normal Windows rules for specifying files with wildcards. Be sure to include the asterisk and period (*.) before the file type.

Click the **Directories** tab. The directories listed on this tab are similar to the directories found in the dependent policy. Note that no other directories can be added, due to the presence of the dependent policy.
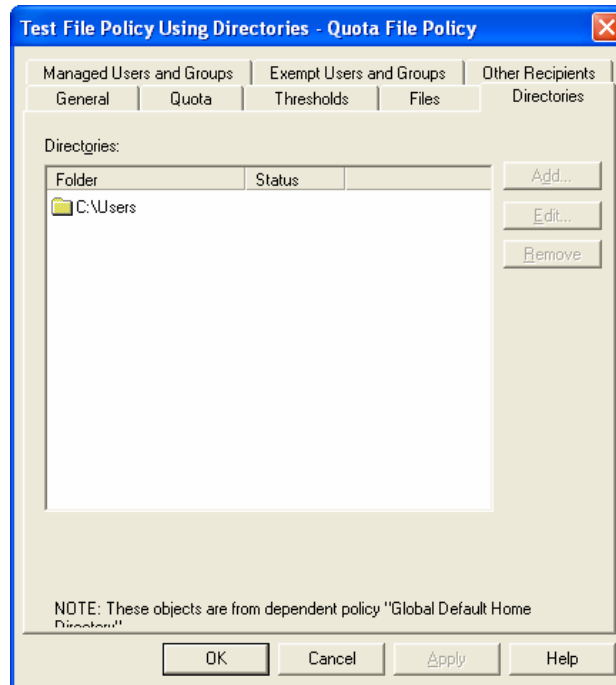
## Creating File Policies Using Shares

1. In the left pane, under Server1, if necessary click the plus sign (+) by **NTP Software QFS** to expand the hierarchy.

2. Right-click **Disk Quota Policies** and select **New** > **File Policy Using Shares** from the pop-up menu.
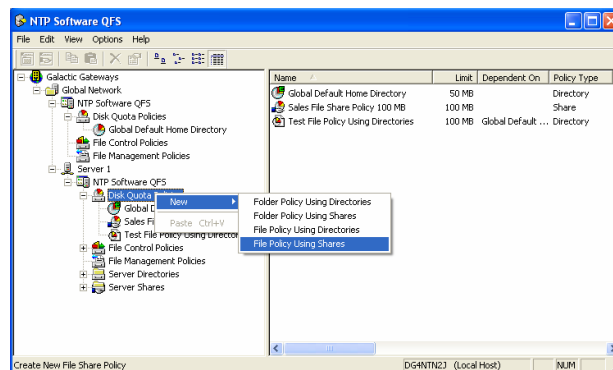
3. In the New Quota File Policy dialog box, click the **General** tab. Enter a name and a description for your policy.

4. We will make the policy dependent on a previously created folder policy. Click the **Browse** button.

5. In the Choose Policy dialog box, select the dependent policy and click **OK**.

6. Click the **Quota** tab. Set a policy quota limit of 100MB, select **Deny Writes at 100% of Quota**, check the overdraft option, and specify a 10% overdraft for a 60-minute time period. If this share goes past 100MB, the user has an hour before his or her activity is blocked, but at no time can the size exceed 110MB (110% of 100MB).

7. Click the **Files** tab. Click **Add** and enter the file patterns you want (for example, *.AVI, *.MP3, *.VBS, and so on). In this example, we've entered ***.MP?** to include *.MP3, *.MP2, *.MPG, etc. — all music files.

   Note: QFS follows the normal Windows rules for specifying files with wildcards. Be sure to include the asterisk and period (*.) before the file type.

8. Click the **Shares** tab. The directories listed on this tab are similar to the directories found in the dependent policy. Note that no other directories can be added, due to the presence of the dependent policy.

Creating Management Policies for Directories

1. In the left pane, under Server1, if necessary click the plus sign (+) by **NTP Software QFS** to expand the hierarchy.

2. Right-click **File Management Policies** and select **New** > **Folder Policy Using Directories** from the pop-up menu.
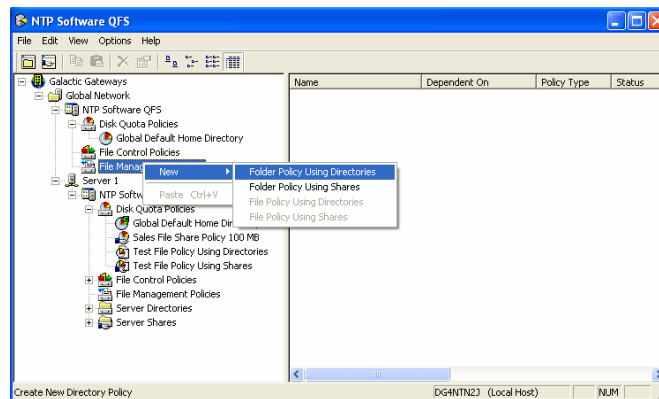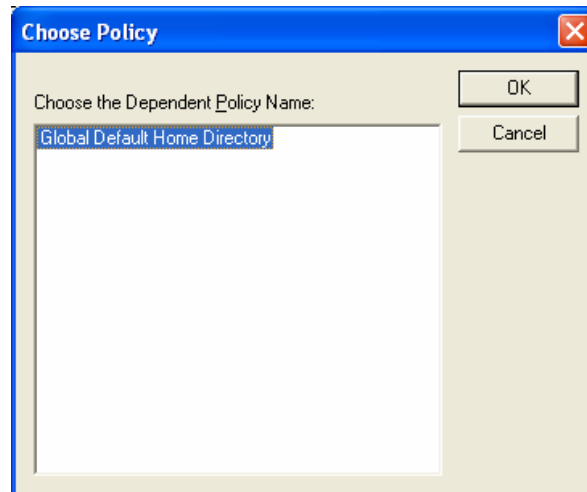
3. In the New File Management Directory Policy dialog box, click the **General** tab. Enter a name and a description for your policy.

4. Click **Browse**.

5. In the Choose Policy dialog box, select the dependent policy and click **OK**.

Doc #.

6. Click the **Criteria** tab. Select the criteria you wish to operate on then select the action whether to Audit, delete or quarantine the files.


7. Click the **Directories** tab. The directories listed on this tab are similar to the directories found in the dependent policy. Note that no other directories can be added, due to the presence of the dependent policy.

Doc #.

Creating Management Policies for Shares

1. In the left pane, under Server1, if necessary click the plus sign (+) by **Quota & File Sentinel** to expand the hierarchy.

2. Right-click **File Removal Policies** and select **New** > **Folder Policy Using Shares** from the pop-up menu.
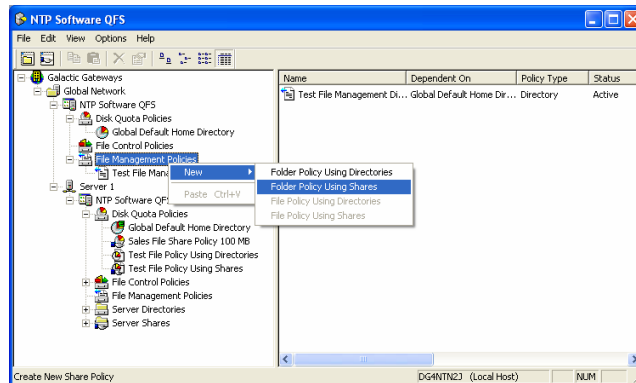
3. In the New File Removal Share Policy dialog box, click the **General** tab. Enter a name and description for your policy.

4. Click **Browse**.

Doc #.

39
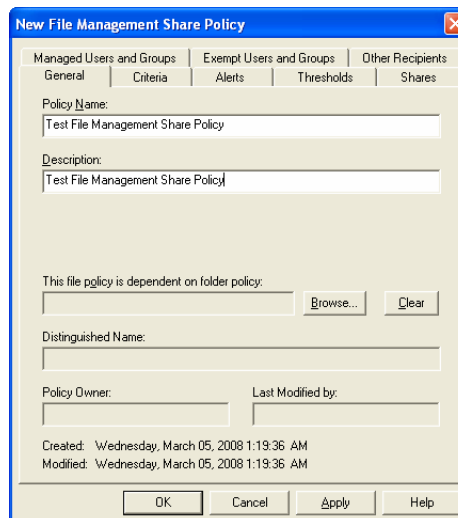
5.   In the Choose Policy dialog box, select the dependent policy and click **OK**.

6.   Click the **Criteria** tab. Select the criteria you wish to operate on then select the action whether to Audit, delete or quarantine the files.

40
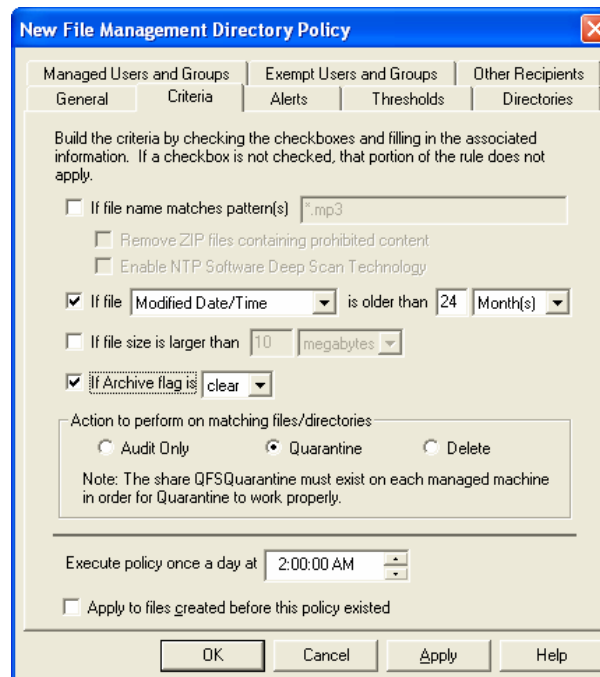
7. Click the **Shares** tab. The directories listed on this tab are similar to the directories found in the dependent policy. Note that no other directories can be added, due to the presence of the dependent policy.
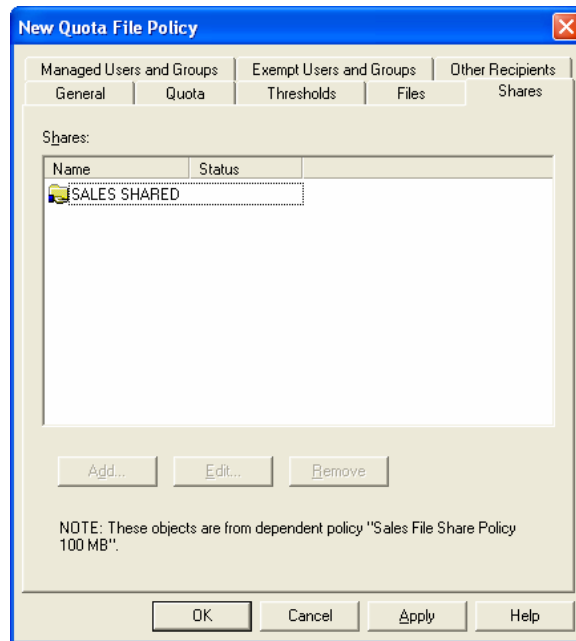
Creating File Control Policies

This section shows you how to create file control policies. Our example company has a corporate policy that forbids downloading music files from the Internet. To help their staff comply with this policy, Galactic Getaways has a file-screening policy that prohibits creating music files on the server. Follow these steps to create this policy:

1. In the tree view (left pane), expand the **Global Network** container and then expand the **NTP Software QFS** application.

2. Right-click **File Control Policies** and select **New** > **Folder Policy Using Directories**.

3. Give your new policy a name and description (see image).

4.   Click the **Criteria** tab. Click **Add** and enter the file patterns you want to block or select a pattern from the predefined collections list.

      Note: QFS follows the normal Windows rules for specifying files with wildcards. Be sure to include the asterisk and period (*.) before the file type.

5.   Click **OK**.
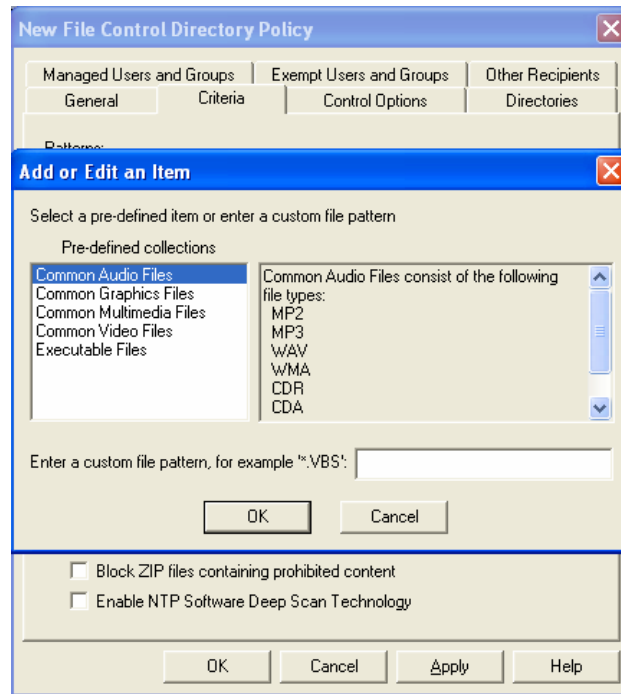
6.   Click the **Control Options** tab. Since our policy is designed to prevent the creation of these files, check **Create New** and make sure that the **Always Deny** radio button is selected.
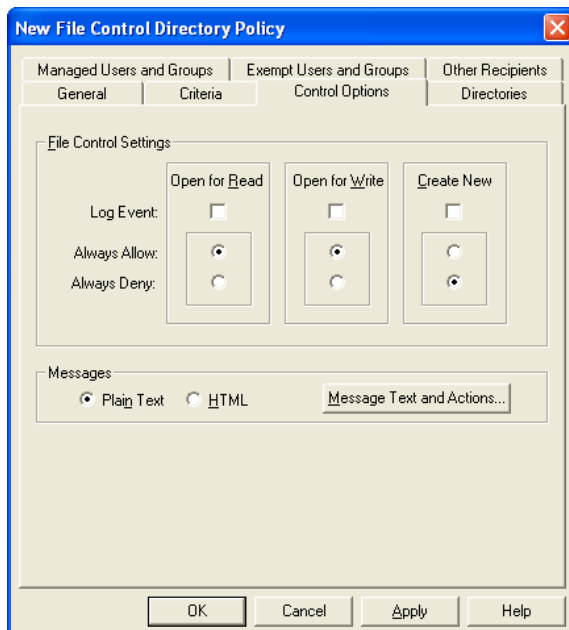
QFS is very flexible in how it can manage file access. The Log Event options enable you to register an event in the event log when this action occurs. You can use these events for auditing.

If QFS is running on the client machine, it can even talk to the user to confirm the user's intent. This is helpful in protecting against script viruses in companies where desktop automation is in use and people have valid reasons to run and/or create scripts and *.VBS files.

Doc #.

7. Click **OK** to save this policy.

The previous examples created file control policies for directories. How do you create file control policies for shares?

Creating Folder Policies Using Shares

1. Right-click File Control Policies and select **New** > **Folder Policy Using Shares**.
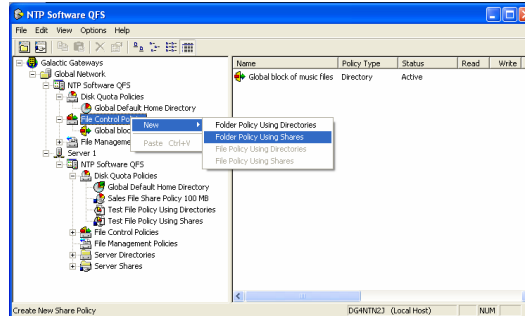
2. Click the **General** tab and specify a name and description for the new policy.
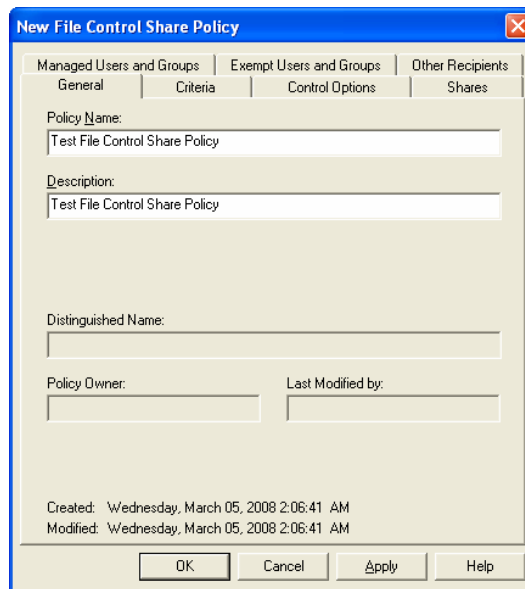
3.   Click the **Criteria** tab. Click **Add** and enter the file patterns you want to block or select a pattern from the predefined collections list.

   Note: QFS follows the normal Windows rules for specifying files with wildcards. Be sure to include the asterisk and period (*.) before the file type.

4.   Click **OK**.

Doc #.
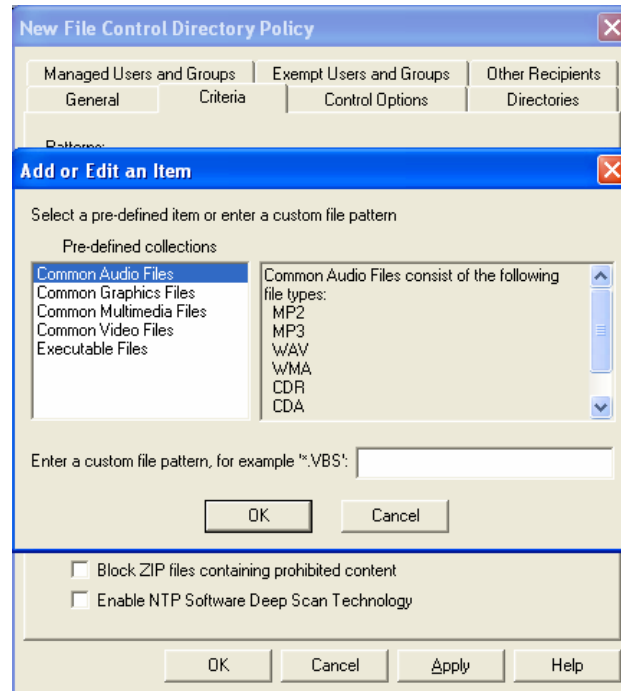
Now we need to set permissions for the file types.

5.   Click the **Control Options** tab. Since our policy is intended to prevent the creation of these files, check **Create New** and make sure that the **Always Deny** radio button is selected.
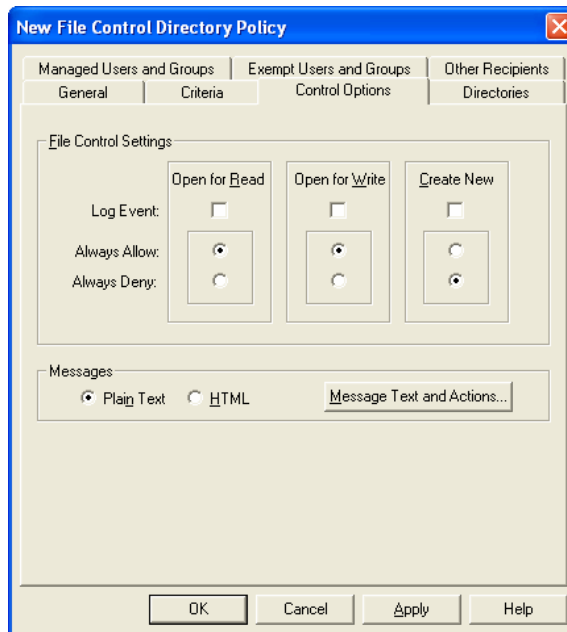
6.   We need to tell QFS which shared directory to control. Click the **Shares** tab.

7.   Click the **Add** button; then click the **Browse** button.

Doc #.

8.   From the shares on your server, select the share you want to manage; then click **OK**.
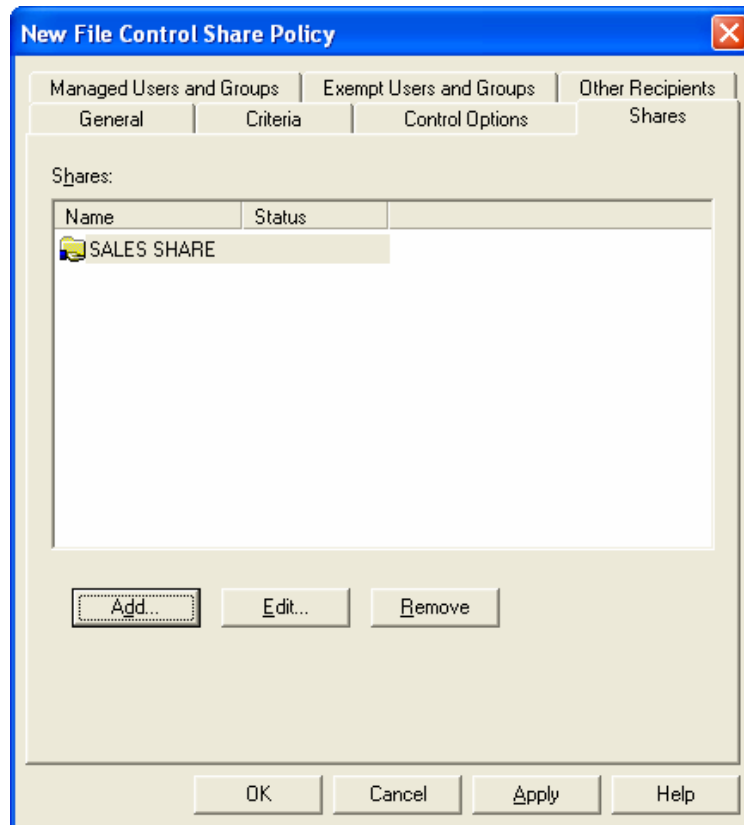
Pushing NTP Software QFS to Additional Machines

A new system is installed in two steps. First, the system needs to be in your Smart Policy Manager hierarchy, which means installing Smart Policy Manager on the target machine (if it isn't already there for another application. Then NTP Software QFS is installed.

Pushing Smart Policy Manager to another System

1. In the left pane, right-click the container **Global Network** and select **New** > **Server** from the pop-up menu.
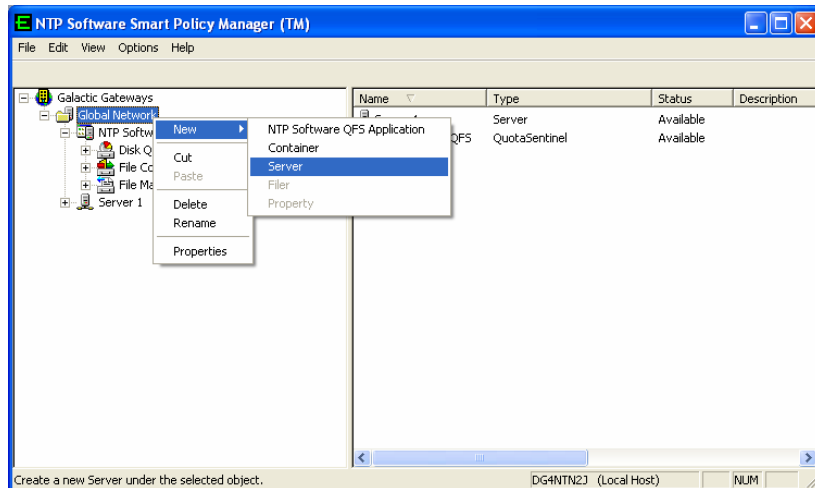
2. In the New Server dialog box, enter the name of the destination server where you want QFS to be installed. Click **OK**.

3. A message box warns you that the remote computer doesn't have Smart Policy Manager installed. Click **Yes** to install Smart Policy Manager on the remote computer. The installation begins.

4. When you're prompted for the drive on the target machine where you want Smart Policy Manager to be installed, select the correct drive (C: in most cases) and click **Next**.

5. When prompted for a Smart Policy Manager service account and password, enter the appropriate information for your network. Select the login domain from the dropdown and enter the account as shown.

6. When you've entered all the required information, click **Finish**.

Doc #.

7. The new server appears in the tree view of your SMART POLICY MANAGER hierarchy. Right-click the new target server and select **New** > **NTP Software QFS** to "push" (remotely install) QFS to the target server.
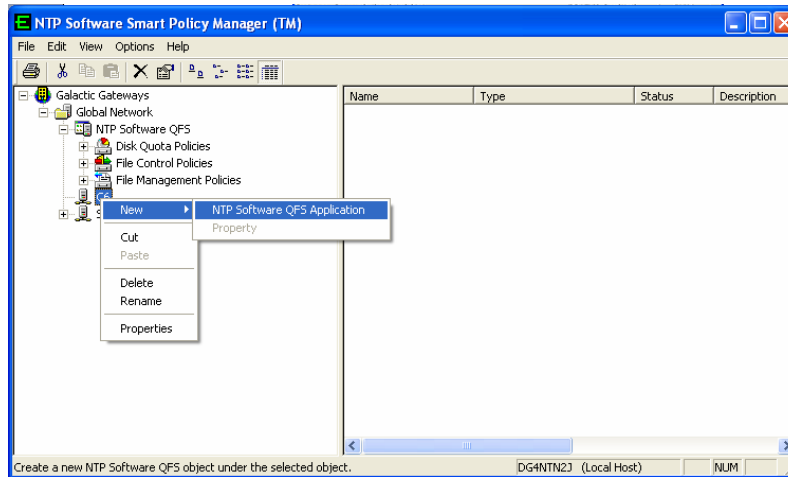
8. In the New Application dialog box, enter any desired comments in the description field; then click **OK**.

> It might be useful to enter a comment such as *Pushed on 7/6 by Sally Smith*. This way, administrators who come after you can determine when and how the software was installed.
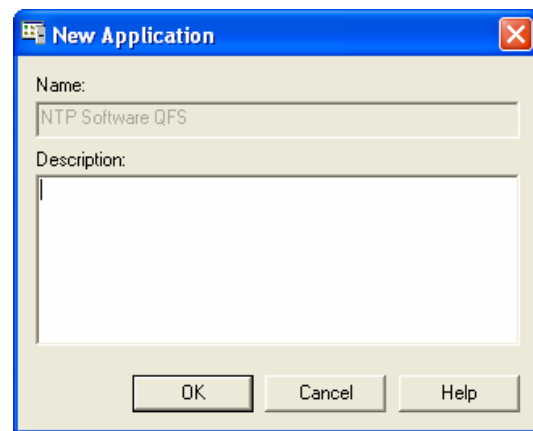
9. When the confirmation message appears, select **Yes** to begin the installation.

Doc #.
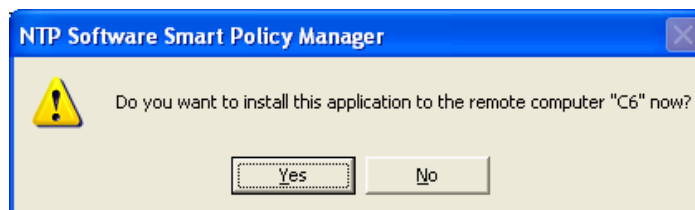
10. You'll be asked to choose the drive that should be used on the remote machine. In general, you should make the same choice as in step 4.

11. The component selection dialog box appears. Choose the appropriate setting and click **Next**.

    Note: When you push the Admin components, they're delivered to the target system, but not installed in the program menu. However, they still exist in Add/Remove Programs.

    Fill in the service account information as you did in step 5, and then click **Finish**.

12. When the success message appears, click **OK**.

    You should see the new QFS application in the left pane as an application, under the target server to which you just pushed (remotely installed) it.

    See how easy it is to install QFS to machines throughout your enterprise?

Doc #.

Reports and System Performance

QFS has several reporting options for your convenience. We'll briefly discuss and demonstrate each option so you can evaluate them.

QFS Admin Reports

QFS comes installed with a built-in reporting module called *QFS Admin Reports*. To access it and run reports, follow these steps:

1. Click the Windows Start button and then select Programs > NTP Software QFS > NTP Software QFS Admin Reports.

2. The NTP Software Report Wizard appears. Select **Create a report from a report template** and then click **Next**.

<table>
<tr>
<td>
Reports can contain any of the information available to QFS. The report templates are preconfigured for common scenarios.
</td>
<td>

</td>
</tr>
</table>
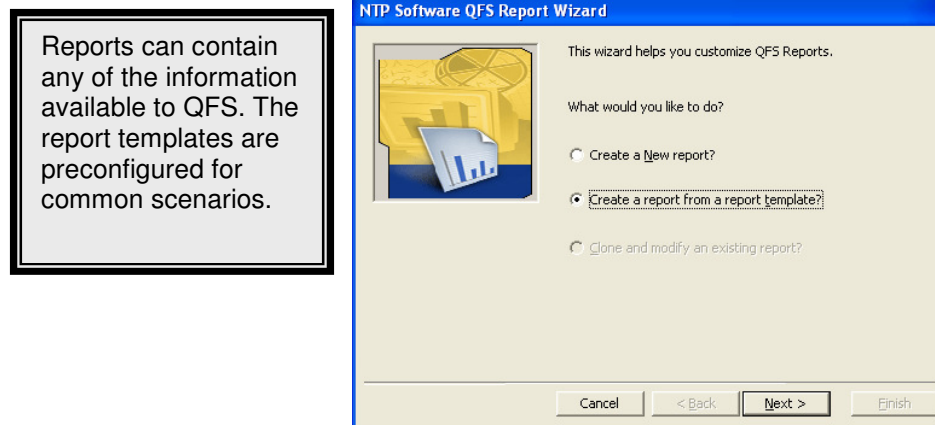
3. When prompted to select a report type, click **All Active Quota Policies** and then click **Next**.

Doc #.

4.   Select the server(s) for which you want reports. Click the right-arrow (**>**) button to add the selected server(s) to this report and then click **Next**.
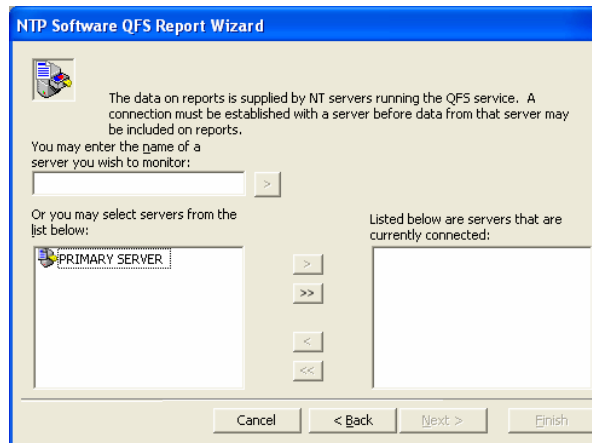
5.   Click **Finish** to begin generating the report. The report automatically appears onscreen when complete. When you close the report, you're asked whether you want to save it; if so, specify the desired location.

Creating a New Report

This feature provides the functionality to design a required report.

1. Click the Windows Start button and then select Programs > NTP Software QFS > NTP Software QFS Admin Reports.

2. The NTP Software Report Wizard appears. Select **Create a New report** and then click **Next**.

3. Specify a name and title for your report and then click **Next**.
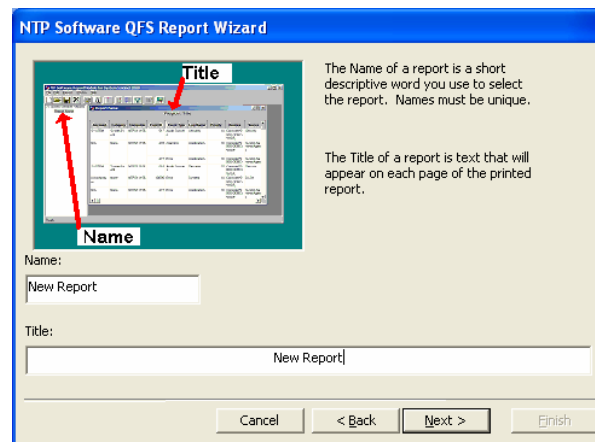
4. Select the server(s) for which you want reports and then click **Next**.

5. Click the right-arrow (**>**) button to add to the selected server(s) to this report.

Doc #.
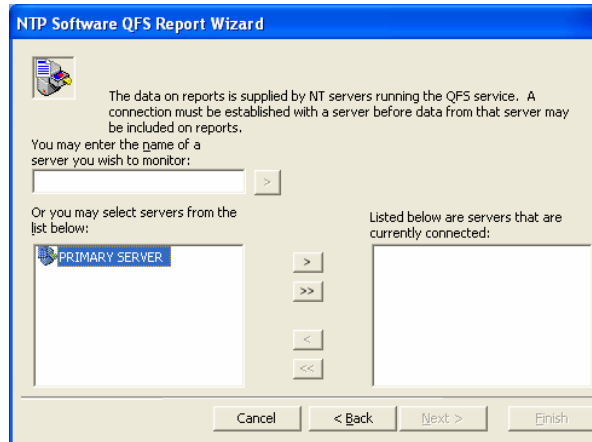
6.   Choose the columns you want to add to your report.

7.   Sort the columns, as you want to view them in the report. Click **Next**.
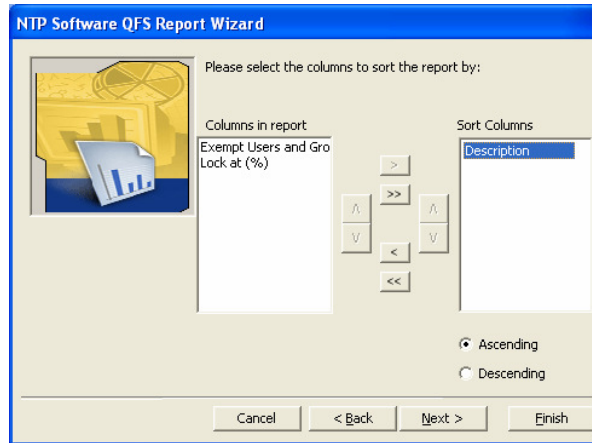
8.   Use the combo boxes to add filters to restrict the data that appears on your report (see image, right). Click **Next**.

9.   Your report is ready to be displayed. Click **Finish**.

End User Support Infrastructure (EUSI) Installation

End User Support Infrastructure (EUSI) is an integrated component of NTP Software's QFS application. EUSI contains several utilities to aid network administrators in informing users of exactly what a quota violation is and to assist in fixing the problem.

Installing EUSI

To install End User Support Infrastructure, insert the CD and select the installation option from the install interface. Follow the prompts to install the various components:

- **QFS Email Templates.** Install these components on the same server as NTP Software QFS.
- **QFS HelpSite.** This collection of web pages describes what each quota policy violation means. The purpose is to help users understand why they were notified about a quota violation, to cut back on the amount of time administrators spend answering these simple questions.
- **End User Support Infrastructure website.** This site allows the user to see what policy he or she violated, request a change in the policy, and clean up his or her drive.
- **Storage Investigator.** Users can download this .CAB file from the EUSI website. To download the .CAB file, the user must be an administrator on his or her local machine. If the user isn't an admin, the installation and registration of the Storage Investigator must be done by the administrator, using the included .MSI file.

The QFS HelpSite, End User Support Infrastructure website, and Storage Investigator components should be installed on an intranet web server. The QFS Email Templates component should be installed on the server where NTP Software QFS is installed.

Three dialog boxes are of particular importance in the installation process:

- **Virtual Directory.** When the QFS HelpSite and End User Support Infrastructure website are installed on a web server, the installation creates virtual directories. The directories are named HelpSite and NTPSCustomerServiceSite. You can change these default names in the Virtual Directory dialog box.
- **Hosting URL.** Use this dialog box to specify the URL of the web server that hosts the QFS HelpSite and End User Support Infrastructure website; for example, http://10.10.2.40 or http://intranetserver. This address is used by the QFS Email Templates component to access the websites.
- **E-mail Options.** In this dialog box, the Recipient is the mailbox to which quota change requests should be sent. One feature of the End User Support Infrastructure website is the capability for users to email requests for quota policy changes. The SMTP Server is the address of the email server to use.

QFS Email Templates

QFS Email Templates are preformatted HTML email messages that can easily be imported into NTP Software QFS. The following email templates are provided:

- **BelowThreshold.** Indicates that the user has gone below quota and is now allowed to save things to the share name again.
- **FileBlocked.** Indicates that a particular file was blocked from being stored on a network share. This might indicate a prohibited extension (.MP3, for example) or some other blocking reason specified in the QFS policy.

Doc #.

- • **OverQuota.** Indicates that a user's action has caused his or her storage to exceed quota. This particular email message contains links to both QFS HelpSite and the End User Support Infrastructure website. The OverQuota email message automatically passes the server and share name of the drive on which the quota was violated. To change this setting, review the NTP Software QFS documentation for valid keys.

- • **FileRemoval.** Indicates that a particular file of a user has been removed by a file migration policy.

Note: When installing the QFS Email Templates, it's very important that you specify the URLs of the QFS HelpSite and the End User Support Infrastructure website. The default web pages include placeholders for these URLs. If you don't specify these URLs, the email templates won't function as designed.

Adding an Email Template to QFS

1. Open the NTP Software QFS admin tool. Select the policy to which you want to add email; then choose **File** > **Properties**.

2. Click the **Thresholds** tab.

3. Select **HTML** in the **Message Format** section of the dialog box.

4. Click the **Properties** button.
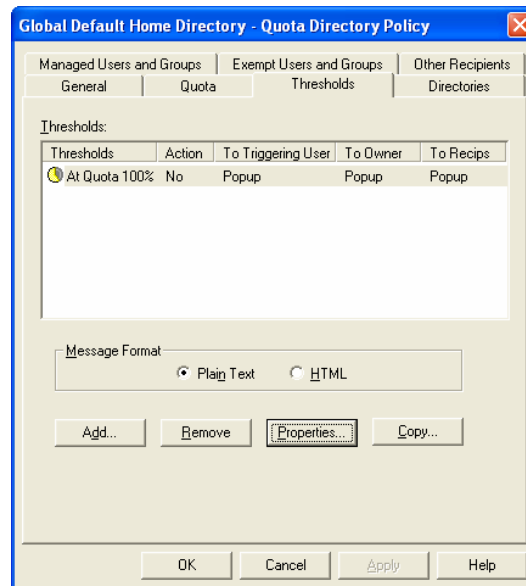
5. In the Threshold Properties dialog box, you can customize messages for each recipient. For this example, we're sending email only to the user who triggered the quota policy. In the **Send to Triggering User** section of the dialog box, select **Email** as the notification method.
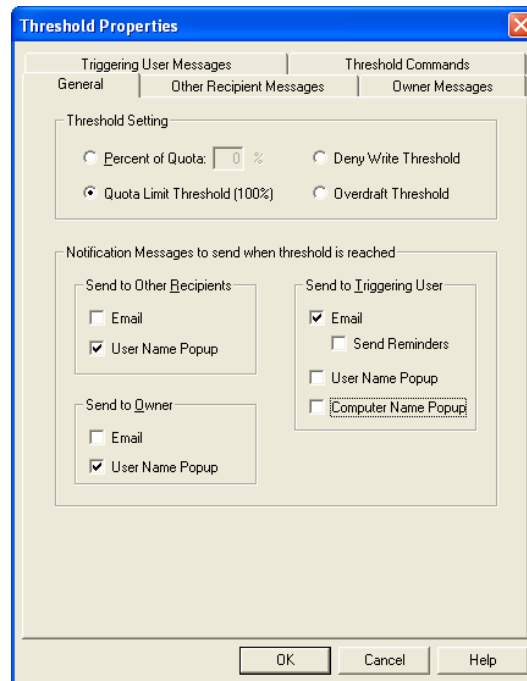
6. Click the **Triggering User Messages** tab. In the section **Above or Write Denied Threshold Message**, click the **Edit Text** button to open a text editor.
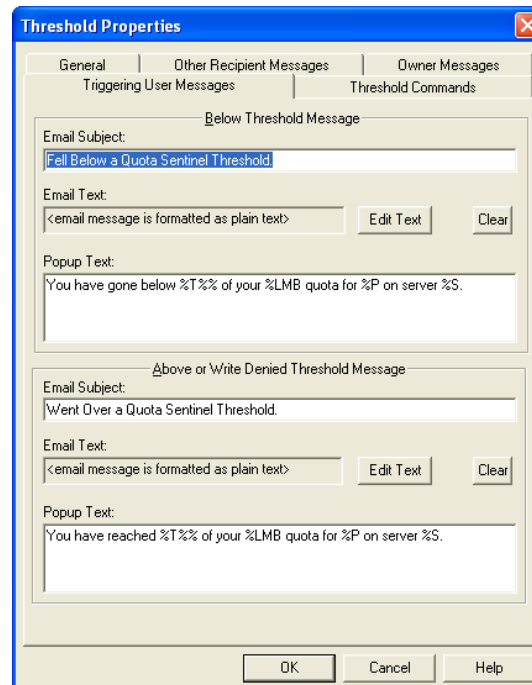
7. In the text editor, choose **File** > **New** to remove all existing text.

8. Choose **Insert** > **File**. Browse to the directory where the End User Support Infrastructure website was installed and open the file **OverQuota.HTM**.

9. Edit the htm as desired and click **File**, then **Save & Close** to exit the dialog boxes. Now, when a user goes over quota, he or she will receive an email message explaining that the quota limit has been reached on that server.

Specifying a File Control Message

1. In the tree view (left pane), expand the **Global Network** container and then expand the **NTP Software QFS** application.

2. Right-click **File Control Policies** and select **New** > **Folder Policy Using Directories**. (If necessary, refer to the earlier discussion of how to create file control policies.)

3. In the New File Control Directory Policy dialog box, click the **Control Options** tab. In the **Messages** section of the dialog box, select **HTML**. Then click the **Message Text and Actions** button.

Doc #.
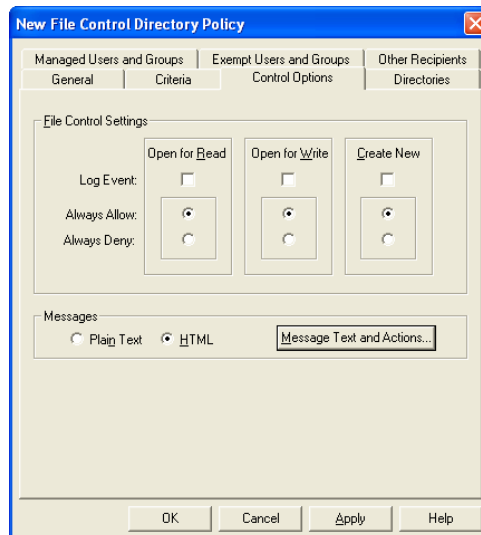
4.   In the File Control Messages and Actions dialog box, click the **General** tab and select **Email** as the notification method in the **Send to Triggering User** section of the dialog box.
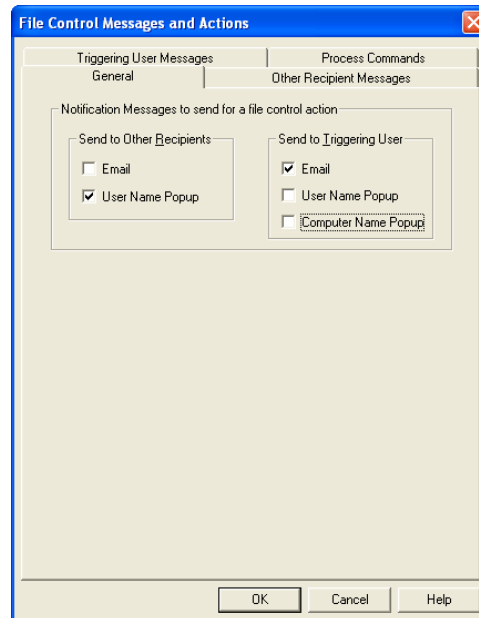
5.   Click the **Triggering User Messages** tab. In the **File Control Deny Message** section of the dialog box, click the **Edit Text** button to open a text editor.
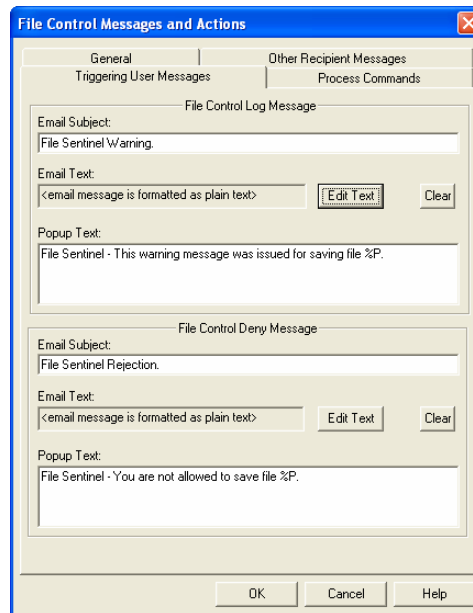
6. In the text editor, choose **File** > **New** to remove all existing text.

7. Choose **Insert** > **File**. Browse to the directory where the End User Support Infrastructure website was installed and open the file **FileBlocked.HTM**.
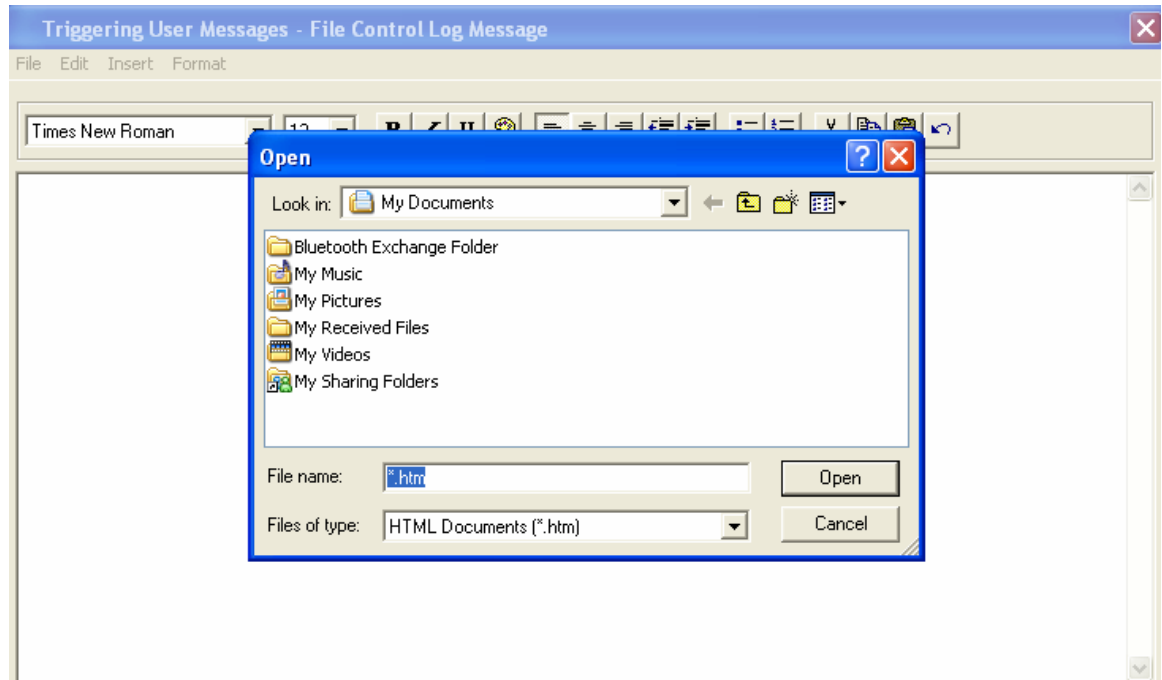
8. Edit the htm as desired and click **File**, then **Save & Close** to exit the dialog boxes. Now, when a user tries to copy a blocked file, he or she will receive an email message.

Doc #.

QFS HelpSite

The QFS HelpSite provides web pages that answer the most basic questions about QFS policies and violations. The idea is to take this burden away from the network administrator and put the information in one central place. The QFS Email Templates contain links to the QFS HelpSite so that, when a user triggers a QFS policy, he or she can quickly obtain information about the policy and how to fix the problem.

The QFS HelpSite should be installed on a local web server. The installation process takes care of creating the virtual directory within IIS.

EUSI Website

This website contains pages that allow the user to do the following:

- Download Storage Investigator for cleaning up the user's directories.
- Email the network administrator, requesting a change to the user's policy.

The website is accessible from the QFS Email Templates files. During the installation of End User Support Infrastructure, you'll be prompted for the name of the virtual directory that should be created. This component should be installed on a web server.

Storage Investigator

Storage Investigator is a tool to help users clean up their shares and directories in order to avoid violating storage policies. Storage Investigator shows all files sorted by various criteria, such as the following:

- Largest files
- Oldest files
- Duplicate files
- Aged files
- Extensions

Storage Investigator is an ActiveX control that's set up to download from CleanupFiles.Asp in the End User Support Infrastructure website. Due to the nature of ActiveX controls, the user must be an administrator on the local machine to download and register the ActiveX control. For environments where users are not administrators on their local machines, an .MSI file is provided. This file can be used with Active Directory or other tools to "push" an installation of Storage Investigator to each machine. Once the Storage Investigator ActiveX control is installed and registered, users can run the control.

Doc #.

Command-Line Interface

The command-line interface enables administrators to automate routine tasks within NTP Software QFS for Windows. Utilizing the command-line interface, an administrator can write a series of commands in a batch file, which can be scheduled to run at regular intervals. With the batch file running, the command-line interface functions as if commands were being entered manually.

Usage

The command-line interface uses the following command structure:

QFSCMD <command> <EASE hierarchy path> <command parameters>

<command>	Specifies the name of the command.
EASE hierarchy path	An optional parameter that defines where in the EASE hierarchy the command will apply. By default, all commands apply to the local machine as it appears in the SMART POLICY MANAGER hierarchy.

Example:

```
EASE://My Organization\My Site\W2KCONN\Quota & File Sentinel
```

<command parameters>	A variable number of command-specific parameters. See the following reference section for details of the parameters for each command.

Example:

```
C:\QFS_CLI\QfsCmd.exe AddQuotaPolicy "EASE://My Organization\My
Site\W2KCONN\Quota & File Sentinel" cli_aqp_03 DIR
```

Note: When using the command-line console with batch (.BAT) files, the percent sign (%), if used, must be doubled (for example, `90%%`).

The following sections provide a complete list of supported commands and parameters.

Doc #.

Quick Reference

The following table briefly describes the commands for policy manipulation. See the Command Reference for a complete alphabetical listing of all of the commands, with parameters and descriptions.

Command	Description
AddQuotaPolicy	Adds a new quota policy.
AddFileControlPolicy	Adds a new file control policy.
AddFileRemovalPolicy	Adds a new file migration policy.
RemovePolicy	Removes a policy.
AddPolicyDescription	Adds a description for a policy.
AddTargetUsers	Adds users or groups to the list of users governed by a policy.
RemoveTargetUsers	Removes users or groups from the list of users governed by a policy.
AddExemptUsers	Adds users to the list of users exempt from a policy.
RemoveExemptUsers	Removes users from the list of users exempt from a policy.
AddTargetPath	Adds directories or share paths to the list of paths governed by a policy.
RemoveTargetPath	Removes directories or share paths from the list of paths governed by a policy.
SetAlwaysEnforce	Sets the flag indicating whether a policy is always to be enforced.
SetQuotaLimit	Sets the quota limit for a policy.
AddUserThreshold	Adds a user threshold.
AddOwnerThreshold	Adds a quota threshold for the owner of the file.
AddRecipientThreshold	Adds a quota threshold for recipients.
AddOtherRecipientThreshold	Adds a quota threshold for other recipients.
AddThresholdCommand	Adds a threshold command.
RemoveThreshold	Removes a threshold from a policy.

Doc #.

AddOtherRecipients	Adds other recipients to a list.
RemoveOtherRecipients	Removes other recipients from a list.
AddFilePatterns	Adds file patterns for a file blocking policy.
RemoveFilePatterns	Removes file patterns from a file blocking policy.
SetFileControlOptions	Sets the control options for a file blocking policy.
SetEmailMessageFormat	Sets the format for email messages.
SetSmtpConfiguration	Sets SMTP configuration parameters.
SetFileRemovalCriteria	Sets the lifetime for a file removal policy.
SetQuotaDenyWriteLevel	Sets the level at which a quota denies file writes.

Command Reference

AddExemptUsers

Adds a specific user or list of users to the policy's exempt user list.

Syntax

AddExemptUsers <targetserver> <policy> <account>

Parameters

targetserver   Level of the policy.

policy   Name of the policy.

users   List of user or group accounts, separated by semicolons.

Result

Exempt users <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

AddFileControlPolicy

Creates a new file control policy and adds it to the QFS configuration.

Syntax

AddFileControlPolicy <targetserver> <policy> <type>

Parameters

targetserver   Level of the policy.

policy   Name of the file control policy to add.

type	DIR — Directory policy.
	SHARE — Share policy.

Result

File control policy <policy> successfully added or a text message describing the error encountered.

Remarks

The new policy is created at the level specified by the first parameter. If <targetserver> is left blank, the policy is created under the local server's NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

AddFilePatterns

Adds file patterns for a file control policy.

Syntax

AddFilePatterns <targetserver> <policy> <patterns>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
patterns	List of file patterns, separated by semicolons.

Result

File patterns <patterns> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes.

AddFileRemovalPolicy

Creates a new file migration policy and adds it to the QFS configuration.

Syntax

AddFileRemovalPolicy <targetserver> <policy> <type>

Parameters

targetserver	Level of the policy.
policy	Name of the file migration policy to add.
type	DIR — Directory policy.
	SHARE — Share policy.

Result

File removal policy <policy> successfully added or a text message describing the error encountered.

　　　　　　　　Doc #.

Remarks

The new policy is created at the level specified by the first parameter. If *targetserver* is left blank, the policy is created under the local server's NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

AddOtherRecipients

Adds other recipients to the recipient list.

Syntax

AddOtherRecipients <targetserver> <policy> <users>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Recipients <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

AddOtherRecipientThreshold

Adds a quota threshold for other recipients.

Syntax

AddOtherRecipientThreshold <targetserver> <policy> <thresholdvalue> <thresholdtype> <abovesubject> <abovemessage> <aboveemail> <belowsubject> <belowmessage> <belowemail>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	1 — Email notification.
	2 — Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.

Doc #.

belowemail	Body of email notification message showing user has gone below threshold.

Result

Other recipient threshold added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It's very important that you specify all the parameters for messages. If you don't want to set any particular message, specify an empty value enclosed in double quotes.

AddOwnerThreshold

Adds a quota threshold for the owner of a file.

Syntax

AddOwnerThreshold <targetserver> <policy> <thresholdvalue> <thresholdtype> <abovesubject> <abovemessage> <aboveemail> <belowsubject> <belowmessage> <belowemail>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	1 — Email notification.
	2 — Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

Owner threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It's very important that you specify all the parameters for messages. If you don't want to set any particular message, specify an empty value enclosed in double quotes.

AddPolicyDescription

Adds a description to a given policy.

Doc #.

Syntax

AddPolicyDescription <targetserver> <policy> <description>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
description	Description to be assigned to the policy.

Result

Policy description <description> successfully added to policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

AddQuotaPolicy

Creates a new quota policy and adds it to the QFS configuration.

Syntax

AddQuotaPolicy <targetserver> <policy> <type>

Parameters

targetserver	Level of the policy.
policy	Name of the quota policy to add.
type	DIR — Directory policy.
	SHARE — Share policy.

Result

Quota policy <policy> successfully added or a text message describing the error encountered.

Remarks

The new policy is created at the level specified by the first parameter. If <targetserver> name is left blank, the policy is created under the local server's NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

AddRecipientThreshold

Adds a recipient threshold for the given policy.

Syntax

AddRecipientThreshold <targetserver> <policy> <thresholdvalue> <thresholdtype> <abovesubject> <abovemessage> <aboveemail> <belowsubject> <belowmessage> <belowemail>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.

　　　　　　　　Doc #.

thresholdtype	1 — Email notification.
	2 — User name pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

Recipient threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It's very important that you specify all the parameters for messages. If you don't want to set any particular message, specify an empty value enclosed in double quotes.

AddTargetPath

Adds one or more specific directories or share paths to the list of paths governed by the policy.

Syntax

AddTargetPath <targetserver> <policy> <path>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
path	List of folder paths, separated by semicolons.

Result

Target path <path> successfully added to the target path <path> or a text message describing the error encountered.

Remarks

The target path(s) must be surrounded by double quotes ("") if the path contains a space.

AddTargetUsers

Adds a specific user or group to the list of users governed by the policy.

Syntax

AddTargetUsers <targetserver> <policy> <users>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.

Doc #.

users   List of user or group accounts, separated by semicolons.

Result

Target users <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

AddThresholdCommand

Adds a threshold command to be executed when the user goes above or below threshold value.

Syntax

AddThresholdCommand <targetserver> <policy> <thresholdvalue> <abovecommand> <belowcommand>

Parameters

targetserver   Level of the policy.

policy   Name of the policy.

thresholdvalue   Threshold value at which the threshold will be triggered.

abovecommand   Command to be executed when user goes above threshold.

belowcommand   Command to be executed when user goes below threshold.

Result

Threshold command successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It's very important that you specify all the parameters for messages. If you don't want to set any particular message, specify an empty value enclosed in double quotes.

AddUserThreshold

Adds a user threshold to the policy.

Syntax

AddUserThreshold <targetserver> <policy> <thresholdvalue> <thresholdtype> <abovesubject> <abovemessage> <aboveemail> <belowsubject> <belowmessage> <belowemail>

Parameters

targetserver   Level of the policy.

policy   Name of the policy.

thresholdvalue   Threshold value at which the threshold will be triggered.

thresholdtype   1 — Email notification.

                   2 — Username pop-up.

3 — Computer name pop-up.

abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

User threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It's very important that you specify all the parameters for messages. If you don't want to set any particular message, specify an empty value enclosed in double quotes.

RemoveExemptUsers

Removes a specific user or list of users from the policy's exempt user list.

Syntax

RemoveExemptUsers <targetserver> <policy> <users>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Exempt users <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

RemoveFilePatterns

Removes file patterns from a file control policy.

Syntax

RemoveFilePatterns <targetserver> <policy> <patterns>

Parameters

targetserver	Level of the policy.

> policy   Name of the policy.

> patterns   List of file patterns, separated by semicolons.

Result

File patterns <patterns> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't have to put a semicolon at the end.

RemoveOtherRecipients

Removes other recipients from the recipient list.

Syntax

RemoveOtherRecipients <targetserver> <policy> <users>

Parameters

> targetserver   Level of the policy.

> policy   Name of the policy.

> users   List of user or group accounts, separated by semicolons.

Result

Other recipients <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

RemovePolicy

Removes a policy from the QFS configuration.

Syntax

RemovePolicy <targetserver> <policy>

Parameters

> targetserver   Level of the policy.

> policy   Name of the policy.

Result

Policy <policy> successfully removed or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

RemoveTargetPath

Removes one or more specific directories or share paths from the list of paths governed by the policy.

Syntax

RemoveTargetPath <targetserver> <policy> <path>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
path	List of folder paths, separated by semicolons.

Result

Policy <policy> successfully removed or a text message describing the error encountered.

Remarks

The target path(s) must be surrounded by double quotes ("") if the path contains a space.

RemoveTargetUsers

Removes a specific user or group from the list of users governed by the policy.

Syntax

RemoveTargetUsers <targetserver> <policy> <users>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Target users <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It's very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you don't need to put a semicolon at the end.

RemoveThreshold

Removes a threshold from the policy.

Syntax

RemoveThreshold <targetserver> <policy> <thresholdvalue>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.

Doc #.

Result

Threshold successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0.

SetAlwaysEnforce

Sets the flag indicating whether the policy is always to be enforced.

Syntax

SetAlwaysEnforce <targetserver> <policy> <flag>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
flag	0 — Policy is not always enforced.
	1 — Policy is always enforced.

Result

Always Enforce Flag successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetEmailMessageFormat

Specifies the format of the threshold email message.

Syntax

SetEmailMessageFormat <targetserver> <policy> <format>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
format	0 — Plaintext format.
	1 — Rich text format.

Result

Email message format successfully set to <format> or a text message describing the error encountered.

Remarks

None.

SetFileControlOptions

Sets the control options for a file control policy.

Syntax

SetFileControlOptions <targetserver> <policy> <rwoption> <croption>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
rwoption	Option for the read/write flag:
	0 — Allow read/write.
	1 — Log event for read/write.
	2 — Deny read/write.
croption	Option for the file creation flag:
	0 — Allow create.
	1 — Log event for create.
	2 — Deny file creation.

Result

File control options successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetFileRemovalCriteria

Sets criteria for a file migration policy.

Syntax

SetFileRemovalCriteria <targetserver> <policy> <durationtype> <duration> <deletepreexisting>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
durationtype	0 — Hours.
	1 — Days.
	2 — Weeks.
	3 — Months.
duration	Duration value. Should be greater than 0 and less than 65535.
deletepreexisting	0 — Do not delete existing files.
	1— Delete existing files.

Result

File removal criteria successfully set for the policy <policy> or a text message describing the error encountered.

Doc #.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetQuotaDenyWriteLevel

Sets the level at which writes will be denied.

Syntax

SetQuotaDenyWriteLevel <targetserver> <policy> <level>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
level	Percentage level at which to deny writes. Must be between 0 and 200.

Result

Quota 'Deny Write Level' for policy <policy> successfully set to <level> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetQuotaLimit

Sets the quota limit for the policy.

Syntax

SetQuotaLimit <targetserver> <policy> <limit>

Parameters

targetserver	Level of the policy.
policy	Name of the policy.
limit	Quota limit value, in megabytes (MB). This value should be greater than 0.

Result

Quota limit successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetSmtpConfiguration

Sets the SMTP configuration parameters for *targetserver*.

Syntax

SetSmtpConfiguration <targetserver><inheritemailconfiguration> <enable/disable> <smtpserver> <smtpdomain> <senderaddress> <senderpassword>

Doc #.

Parameters

targetserver	Level at which the policy needs to be created within the Smart Policy Manager hierarchy.
inheritemailconfiguration	0 — Do not inherit email configuration.
	1 — Inherit email configuration.
enable/disable	0 — Enable.
	1 — Disable.
smtpserver	SMTP server name or IP address.
smtpdomain	Domain for SMTP server.
senderaddress	Email address to be set in the To field of the email message.
senderpassword	Password for the sender's address.

Result

(SMTP) configuration set successfully or a text message describing the error encountered.

Remarks

None.

Doc #.

Appendix: Installing QFS in Clustered Environments

Installing NTP Software QFS in a Clustered Environment

1. Install NTP Software QFS as described earlier.

2. After QFS is successfully installed, open QFS to find the global container (in this example, Galactic Getaways) 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 this example, New Hampshire) in the second tier of the hierarchy.

    Notice the installation server (in this example, Primary Server) in the third tier of the hierarchy. The QFS application is also in the third tier.
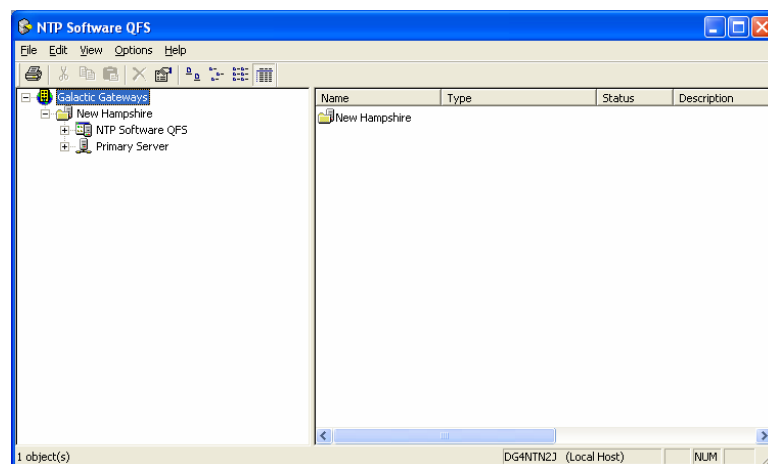

4. Right-click the site container (New Hampshire in this example) and select **New** > **Container** from the pop-up menu to create your cluster container. Give the new container the name of the cluster. In the example, we've used Cluster 1 as the name.

Doc #.
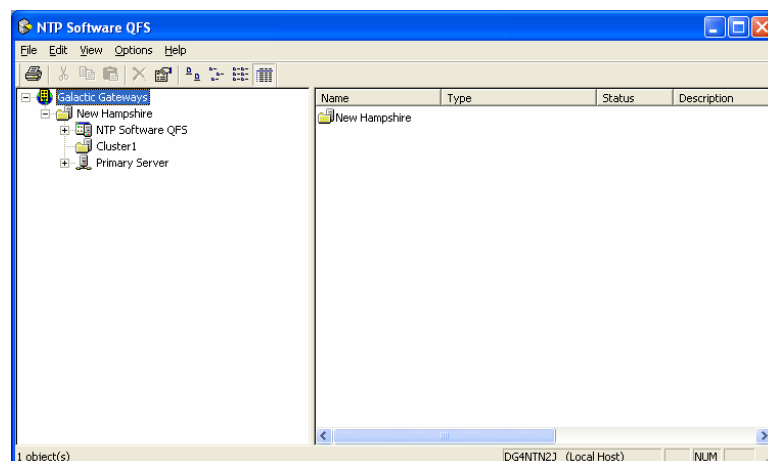
5. Right-click the cluster container (Cluster 1 in this example) and select **Add** > **NTP Software QFS Application** from the pop-up menu.

6. To initiate the "push" installation of NTP Software QFS to the node servers, right-click the cluster container and select **Add** > **Server** from the pop-up menu. You will then have the ability to select or manually enter each existing node server name.
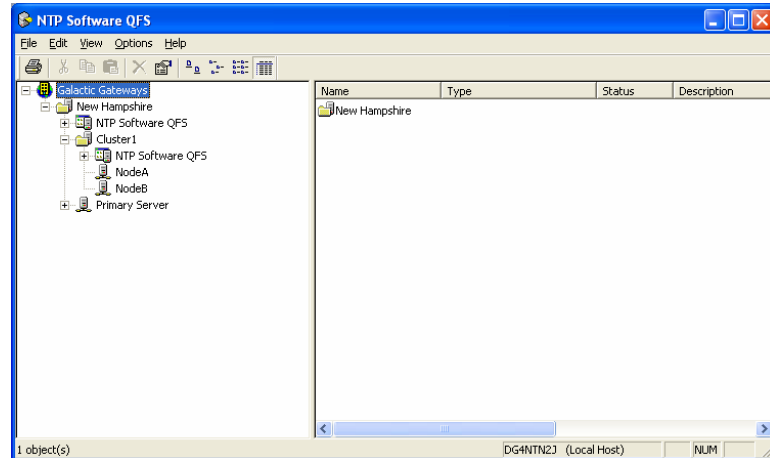
7. Click the plus sign (+) next to the QFS application you've just added, to view the global (cluster) policies. Create all policies within this application that will be applied to both nodes; they'll be propagated automatically to all nodes within the container.


Doc #.

80
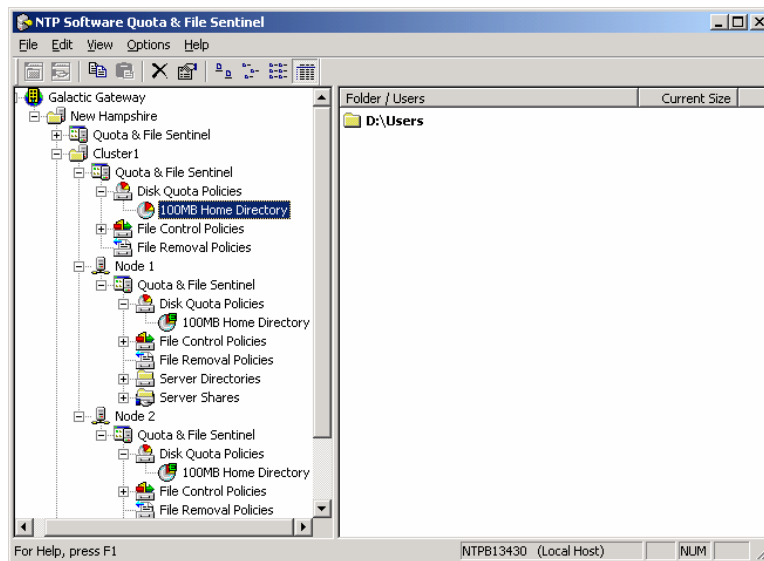
In the following example, the global 100MB policy is propagated; the replicated policies are denoted by the green *E* on the icon within each node.

Installing NTP Software QFS on a Node Server

The best-practice method of installing QFS into a cluster environment is to perform the first installation on a standalone server and then "push" the installation to the cluster nodes, using the Smart Policy Manager technology.

If the first installation must be done directly onto a node (see the following image), you can simply create a cluster container and then drag the node server into it and create your policies as noted.
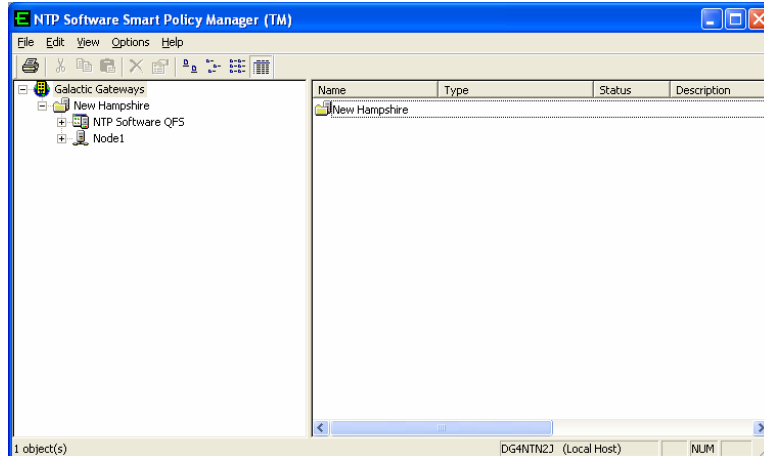

1. Right-click the site container and select **New** > **Container** from the pop-up menu to create a container for the cluster. Give the new container the cluster name.

Doc #.
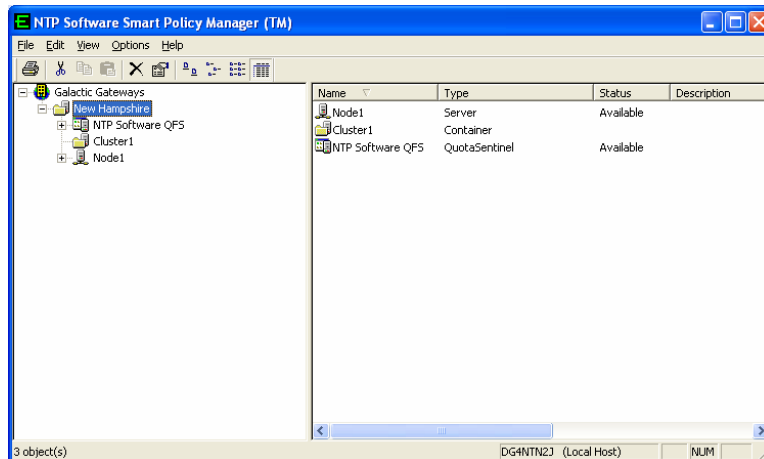
2. Click the existing server (node) and, while holding down the mouse button, drag-and-drop the server onto the cluster container to move the server into the cluster hierarchy.
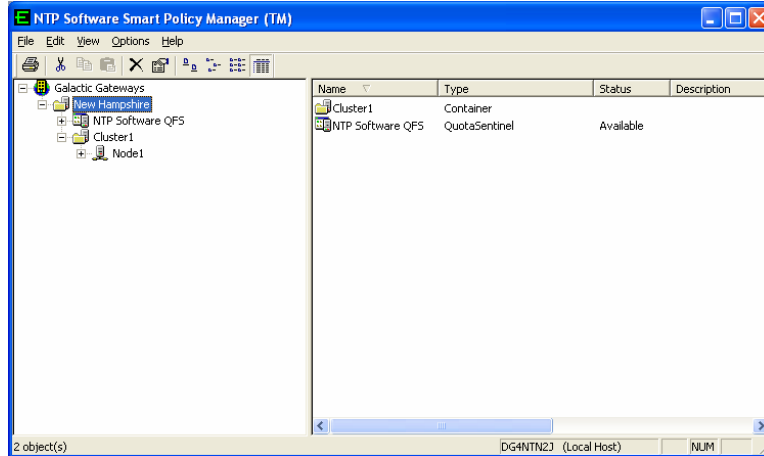

3. Right-click the cluster container and select **New** > **NTP Software QFS Application** from the pop-up menu.

4. To "push" QFS to each additional node, right-click the cluster container and select **New** > **Server**. You'll be asked to verify that you want to push the installation to the server.
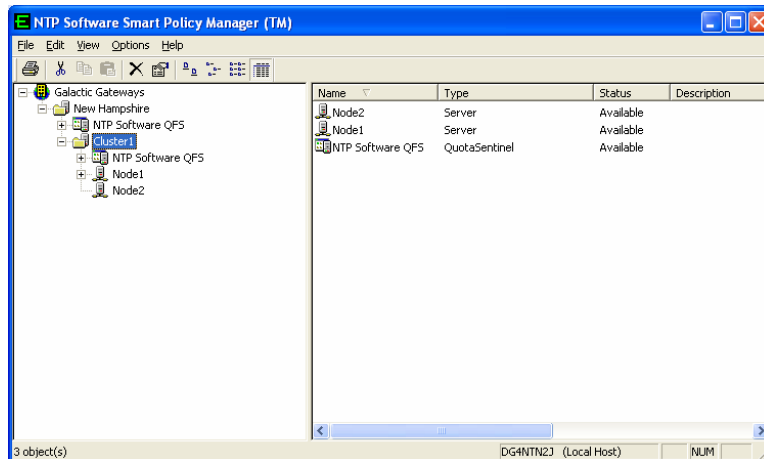
5. To view the global (cluster) policies, click the plus sign (+) next to the QFS application you've just added.

   Create all policies within this application that will be applied to both nodes, and they'll be propagated down automatically to all nodes within the container. In this example, the global 100MB policy is propagated; the replicated policies are denoted by the green *E* on the icon within each node.
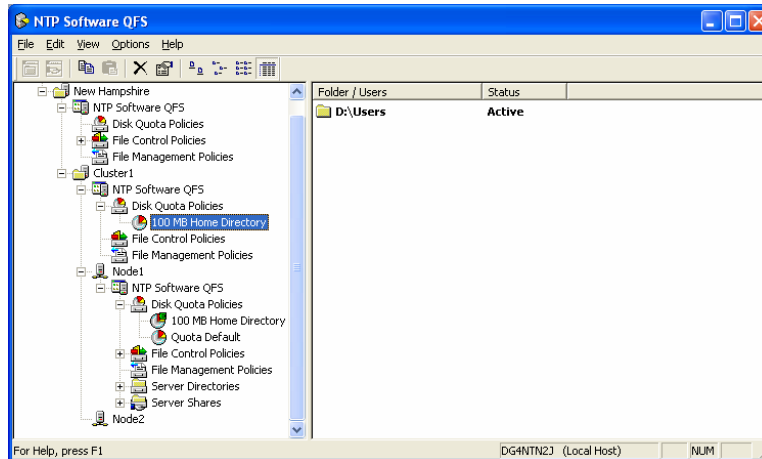
About NTP Software

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 QFS 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 Northwest Blvd. #136
Nashua, NH 03063-4066
Toll-free: 800-226-2755
International: 1-603-622-4400
Website: www.ntpsoftware.com

Doc #.