NTP Software QFS® Family of Products User Manual

Abstract

This manual details the method for using NTP Software QFS Family of Products from an administrator's perspective. Upon completion of the steps within this document, NTP Software QFS Family of Products will be used to manage your enterprise community successfully.

Rev 1.3, January 2009

Doc 5895EF

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

Doc 5895EF.

Table of Contents

Introduction

Thank you for your interest in NTP Software QFS Family of Products. NTP Software QFS controls storage for millions of users worldwide. NTP Software QFS Family of Products extends our best-of-breed technology, allowing you to manage Windows and NAS-hosted storage as a seamless whole.

Given the architecture of your NetApp® filer, IBM® N Series filer, or EMC® Celerra®, NTP Software QFS does its job remotely. Part of the QFS Family of Products, NTP Software QFS uses a connector service to create a bridge and include filers/Celerras as full participants in storage environments controlled by QFS. In light of this fact, you will need to install the NAS/EMC connector on one of the Windows 2000 or 2003 machines in your environment. This may be an existing server or workstation or a standalone system.

To be managed by QFS, version 6.5 or later of the Data ONTAP® operating system for filers or version 5.6.36.2 or later of the DART operating system for Celerras is required. NTP Software QFS Family of Products can be used to manage filers, Celerras, filer clusters and Celerra clusters, or any combination of these systems. QFS imposes no restrictions on how you organize or manage your storage. You can impose policies on individual directories, users, and/or groups of users.

Note: If you want to use email-based messaging and notifications, access to an email server is required.

To install QFS on Windows, a login with administrator rights is needed. You will be installing three different services: the NTP Software Smart Policy Manager™ service, the QFS Service, and the NAS Connector Service.

The NTP Software Smart Policy Manager service should be installed with a domain user account as its service account so that it can communicate with your mail system and other storage servers with which it may share policies. The QFS service requires a domain user account with local administrative rights on the filer or EMC Celerra. The NAS Connector Service uses this account as well.

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

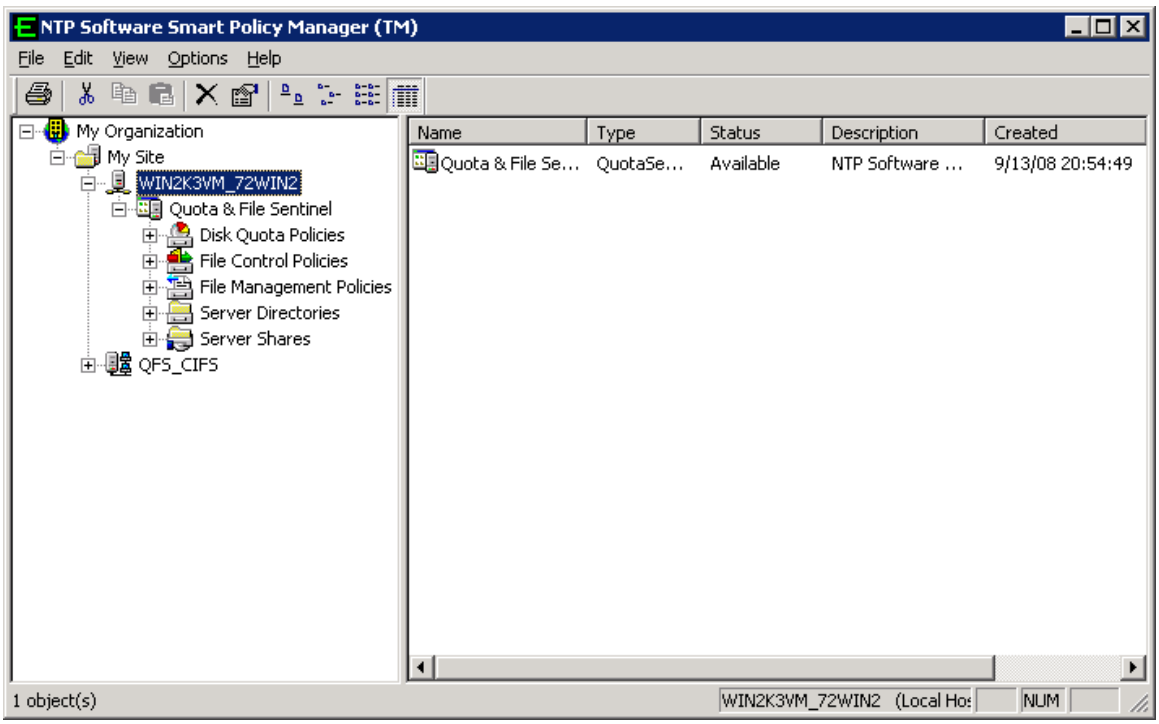
Overview of Smart Policy Manager

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's look at our underlying policy-based rules engine, Smart Policy Manager.

Smart Policy Manager allows you to organize your storage resource management 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 the following example, My Site). This is the Global Network configuration, whose container we created at installation.



Preparing NetApp Filers or IBM N Series Filers

Note: Refer to this section only if you have NetApp filers or IBM N Series filers attached to your environment. *If you do not have NetApp or IBM N Series filers, you should not apply the instructions specified in this section.*

Enabling the fpolicy Management Service (NetApp Filers)

NTP Software QFS requires NetApp filers to run Data ONTAP version 6.5 or later. If your filer is running a version prior to 6.5, you must upgrade your operating system before you proceed. (Please refer to your Network Appliance documentation for instructions.)

Although QFS does not install any components on the NetApp filer, you will need to enable the Data ONTAP fpolicy management service.

- Data ONTAP versions 7.0.6 and 7.2.2 contain a number of fixes that address stability and memory issues related to fpolicy functionality in Data ONTAP. NetApp strongly recommends that customers using fpolicy move to one of these Data ONTAP versions or higher.
- The Data ONTAP 7.1 release family is currently not supported by fpolicy.
- For more information on NetApp filers, consult NetApp Customer Support Bulletin CSB-0704-02: Fpolicy Update for Data ONTAP.

Follow these steps to enable the Data ONTAP fpolicy management service:

1. Log into the NetApp filer with an account that has administrative privileges.
2. At the prompt, enter the following command:

   ```
   fpolicy create NTPSoftware_QFS screen
   ```

3. Enter the following command:

   ```
   fpolicy enable NTPSoftware_QFS
   ```

4. To verify that CIFS file policies are now enabled, enter the following command:

   ```
   fpolicy
   ```

These steps create the configuration that allows QFS to register with and manage your filer. They must be completed before you try to configure QFS. Later in this document, we will register a file policy server with the filer. No further filer administration is required.

Note: Data ONTAP versions 7.0.6 and 7.2.2 contain a number of fixes that address stability and memory issues related to fpolicy functionality in Data ONTAP. For NetApp filers, NetApp strongly recommends that customers using fpolicy move to one of these Data ONTAP versions or higher.

The Data ONTAP 7.1 release family is currently not supported with Fpolicy.

Adding Your Filer to the QFS Policy Hierarchy

Next you need to add your filer to the collection of servers being managed by QFS.

1. Run QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.
2. Right-click **My Site** and choose **New** > **Filer**.
3. You will be prompted to enter a name. The name you enter here must match the name of your NetApp or IBM filer.
4. Now that you have added your filer to the collection of servers recognized by QFS, right-click the filer you just added and select **New** > **Quota File & Sentinel Application**.

   Entries will appear under the filer for Disk Quota and File Control policies.
5. Next, we need to associate the policies you will create here with a filer. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed QFS.
6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the QFS Configuration screen.
7. Click the **NetApp Connector** tab.
8. Click the **Add** button.
9. Enter the name of your filer and click **OK**.
10. Click **OK** in the NTP Software QFS Configuration screen.

Preparing the EMC Celerra

Note: Refer to this section only if you have one or more EMC Celerras attached to your environment. *If you do not have EMC Celerras, you should not apply the instructions specified in this section.*

Preparing the QFS Windows Machine

Follow the steps below to prepare the Windows machine to host QFS:

1. Before installing NTP Software QFS, you have to make sure that Celerra Event Enabler (CEE) version 4.2 or later is appropriately installed and configured in your environment. Contact EMC for further information on this configuration.
2. NTP Software QFS requires the EMC Celerra to run DART version 5.6.36.2 or later. If your Celerra is not running version 5.6.36.2 or later, you must upgrade your operating system before you proceed. (Refer to your EMC documentation for instructions.)
3. After installing the Celerra Event Enabler on the QFS machine, you need to specify the software with which the CEE will register. To do this, set **ntp** for the following key:

   HKEY_LOCAL_MACHINE\SOFTWARE\EMC\Celerra Event Enabler\CEPP\CQM\Configuration\EndPoint

Preparing the EMC Celerra for QFS Management

For any Celerra that will be managed by QFS, once the server is started and has mounted its root filesystem, go to the .etc directory and create the cepp.conf file (if it does not exist). You have to edit this file to include your CEPP pool description.

Note: The cepp.conf file must contain at least one line defining the pool of CEPP servers. If the line is too long, you can add \ at the end of each line:

```
pool name=<poolname> servers=<IP addr1>|<IP addr2>|... \
preevents=<event1>|<event2>|....\
postevents=<event3>|<event4>|.. \
posterrevents=<event5>|<event6>|... \
option=ignore or denied \
reqtimeout=<time out in ms> \ retrytimeout=<time out in ms>
```

Notes

- Each event can include one or more (or all) of the following events:
  - OpenFileNoAccess
  - OpenFileRead
  - OpenFileWrite
  - CreateFile
  - CreateDir
  - DeleteFile
  - DeleteDir
  - CloseModified
  - CloseUnmodified
  - RenameFile
  - RenameDir
  - SetAclFile
  - SetAclDir
- Postevents and posterrevents are not supported in QFS. We recommend turning them off to improve performance. Dropping those two fields from the CEPP will stop the Celerra from generating events of those types.
- At least one event, one pool, and one server per pool must be defined.

Recommended timeout values:

- The recommended value for *reqtimeout* is 5000.
- The recommended value for *retrytimeout* is 750.

Follow these steps to edit the cepp.conf file:

1. Log into the Celerra control station as su.
   a. Type **mount server_2:/ /mnt2** to mount the root filesystem. (Create /mnt2 if it does not exist, and replace **server_2** with your server name if you are configuring a different server.)
   b. Type **cd /mnt2/.etc** and look for the file cepp.conf. Create the file if it does not exist.
   c. Use vi to edit the cepp.conf file. Edit the *servers* field to use the IP address of the machine running QFS. The result should look something like this:

      ```
      pool name=cqm servers=10.30.3.57 preevents=* option=ignore
      reqtimeout=5000 retrytimeout=750
      ```

2. Type **.server_config server_2 -v "cepp stop"** and press Enter.
3. Type **.server_config server_2 -v "cepp start"** and press Enter.

   Note: Replace **server_2** with the name of the server you want to configure.

These steps create the configuration that allows QFS to register with and manage your Celerra. They must be completed before you try to configure QFS.

Adding a Celerra to the QFS Policy Hierarchy

Next, you need to add your EMC Celerra to the collection of servers being managed by QFS.

1. Run QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.
2. Right-click **My Site** and choose **New** > **EMC Celerra**.
3. You will be prompted to enter a name. The name you enter here must match the name of your EMC Celerra.
4. Now that you have added your EMC Celerra to the collection of servers recognized by QFS, right-click the EMC Celerra you just added and select **New** > **Quota & File Sentinel Application**.

   Entries will appear under the EMC Celerra for disk quota and file control policies.
5. Next, you need to associate the policies you will create here with an EMC Celerra. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed QFS.
6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the QFS Configuration screen.
7. Click the **EMC Connector** tab.
8. Click the **Add** button.
9. Enter the name of your EMC Celerra, the control station IP, username, and password, and then click **OK**.
10. Click **OK** in the NTP Software QFS Configuration screen.

You are ready to move on and create some policies.

Setting the QFS Application Properties

1. Right-click **Quota & File Sentinel** under the main Windows server.
2. Click **Properties** on the pop-up menu.
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's 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.
7. 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.
8. 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.

Policy Creation

This section outlines standard QFS procedures for creating policies.

Note: When testing policies you have created, perform the tests from an independent machine that is *not* running QFS.

Let's walk through creating a few typical policies. For EMC, two policy types are available: disk quota policies and file control policies. We will show an example of each.

Creating Disk Quota Policies

This section walks you through creating a typical disk quota policy. We will create a quota policy for all your user home directories in a typical server configuration. 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 NTP Software Smart Policy Manager hierarchy view, locate the server/filer/Celerra you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **Quota & File Sentinel** to expand the policy types.
2. Right-click **Disk Quota Policies** and select **New** > **Folder Policy Using Directories**.
3. In the **New Policy** dialog box, click the **General** tab. Enter a name and a description for your new policy.

4. Click the **Quota** tab, select **Absolute Quota Limit**, enter **50 MB** as the limit, click **Deny Writes at 100% of quota**, and leave **Overdraft** unchecked for this example.

   Note: In a production environment, it is a best practice to implement a 10% overdraft.

5. Click the **Thresholds** tab to view the thresholds for this quota policy. Notice that one threshold is already set up: **At Quota 100%**. Adding more thresholds is as simple as clicking **Add** and filling in the percentage information for that threshold.

   As space is consumed, these thresholds serve as triggers for various actions. Each threshold can send email or pop-up messages to the triggering user, the NTFS owner of the file, and/or to any other group or individual (network administrators, the Help Desk, and so on). A threshold can also run a third-party process; for example, running a virus scan on the file in question, or starting an archive to tape.

   QFS lets you create up to 200 threshold levels for each policy. Common choices for additional levels are 75%, 85%, and 95%. As users hit each of these levels, you can customize your messages to suggest that users delete some files or contact the Help Desk and request a quota increase before their ability to save new documents runs out. It is also possible to integrate QFS with your intranet or automated workflow and process the limit increase automatically.

6. Double-click the **At Quota 100%** threshold. The **Threshold Properties** dialog box for that threshold level appears. If you configured QFS for email earlier, select the checkbox for email to the triggering user.

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

   The **Threshold Commands** tab allows you to specify a program, script, or batch (.BAT) file that will run when the threshold is reached.

7. After you have chosen the appropriate settings for email and messages, click **OK** to return to the **New Policy** dialog box.

8. Click the **Directories** tab. Click the **Add** button and type ***<physical path of the Celerra\subdirectory>*** or type the appropriate directory name followed by a backslash and asterisk (*).

   Note: By default, this quota applies to all users. You can verify this fact by clicking the **Managed Users and Groups** tab.

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

9. Click **OK** to close the **New Policy** dialog box. QFS will create the new quota directory policy, which will be inherited by all systems from this point down in your hierarchy.

Creating File Screening Policies

This section shows you how to create a file screening policy. Perhaps your company has a corporate policy that forbids downloading music files from the Internet. To help the staff comply with this policy, let's create a file screening policy that prohibits creating music files on the server.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server/filer/Celerra you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **Quota & File Sentinel** to expand the policy types.

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

3. The **New File Policy** dialog box opens. Give your policy a name and description.

4. Click the **Criteria** tab. Then click **Add** and enter the file patterns you want to block (for example, ***.AVI**, ***.MP3**, ***.MPG**, ***.MP2**, and ***.VBS**).

   Note: Be sure to include the asterisk and period (***.**) when you specify a file type.

   QFS follows the normal Windows rules for wildcard file specifications. For example, enter ***.MP?** to include .MP3, .MP2, .MPG, etc. — all music files.

   This tab also includes two options, **Block Zip files containing prohibited content** and **Enable NTP Deep Scan Technology**, which enable the administrator to decide how thoroughly files are scanned for the policy. See the following sections of this document for more detailed information on these features.

5. Click **OK** to return to the **New File Policy** dialog box.

6. Click the **Directories** tab. Click the **Add** button and either type **vol****users*** or type the appropriate directory name followed by a backslash and asterisk (*).

7. Click the **Control Options** tab. Since our policy is to prevent the creation of these files, select the radio button labeled **Always Deny** under the options **Open for Read**, **Open for Write**, and **Create New**.

   By default, user accounts with Administrator privileges are exempt from any policy you create. If you want to change this setting, click the **Exempt Users and Groups** tab, select the **Administrators** entry, and click **Remove**.

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

Creating File Management Policies

This section walks you through creating a file management policy. Your company may have a corporate policy that allows your employees to store files in a central or shared location. As an administrator, you are responsible for maintaining the data stored in this location, which includes deleting old or obsolete data. Let's create a file management policy that automatically manages aged files.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server/filer/Celerra you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **Quota & File Sentinel** to expand the policy types.
2. Right-click **File Management Policy** and select **New** > **Folder Policy Using Directories**.
3. The **New File Policy** dialog box opens. Give your policy a name and description.
4. Click the **Criteria** tab. Set the aspects of the policy: file patterns to remove, age of the files, size, and archive status. You can also select a specific action to take for the files; for example, allowing audit, quarantine, or removal when the policy is triggered. Specify when to enforce the policy and whether it will be applied retroactively to files created before the policy.
5. Click the **Alerts** tab. As desired, turn on alerts for the quarantine and deletion of files. Once the alert is enabled, you have the option of enabling email (if the email server has been configured).
6. Click **OK** to save the policy.

Viewing Directories

This section shows how you can view all the directories that are located on a certain server, filer, or Celerra.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server, filer, or Celerra containing directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.
2. Click the plus sign next to **Quota & File Sentinel**.
    a. For the Windows server, click the plus sign next to **Server Directories** to view the folders located on that server.
    b. For the filer, click the plus sign next to **Filer Directories** to view the volumes located on that filer.

       Note: You can view that feature if you have a NetApp or IBM N Series filer attached to the Quota & File Sentinel application.
    c. For the Celerra, click the plus sign next to **Celerra Directories** to view a list of the mount path(s) of the file system(s) that can be accessed through the CIFS Server.

       Note: You can view that feature if you have an EMC Celerra attached to the Quota & File Sentinel application.

Viewing Shares

This section shows how you can view all the shared directories located on a certain server, filer, or Celerra.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server, filer, or Celerra with shared directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.
2. Click the plus sign next to **Quota & File Sentinel**.
    a. For the Windows server, click the plus sign next to **Server Shares** to view the shared folders located on that server.
    b. For the filer, click the plus sign next to **Filer Directories** to view the volumes located on that filer.

       Note: You can view that feature if you have a NetApp or IBM N Series filer attached to the Quota & File Sentinel application.
    c. For the Celerra, click the plus sign next to **Celerra Shares** to view the shared folders located on that CIFS Server.

       Note: You can view that feature if you have an EMC Celerra attached to the Quota & File Sentinel application.

NTP Software DeepScan

A powerful feature of NTP Software QFS is NTP Software DeepScan®. This technology allows the administrator to specify whether to use the default scan for file extensions or scan more deeply for header information to determine the true nature of a file.

Before selecting **Enable Deep Scan Technology** on the **Criteria** tab in the New File Policy dialog box, it is important that you understand how this function will affect your data and user community.

NTP Software DeepScan uses file header information to determine the type of file. Even if the file *Sunshine on My Shoulder.mp3* is renamed *Sunshine on My Shoulder.txt*, it will be seen and controlled as an audio (.MP3) file. Likewise, *Lion.jpg* may be renamed to *Lion.txt*, but it still will be seen and controlled as a .JPG file. DeepScan does this by looking at the file type. A .JPG file is in JPEG image format, so it will not matter whether the file has the extension .JPG, .JPEG, or .TXT.

Note: The file types detected by the NTP Software DeepScan technology are .EXE, .AVI, .GIF, .JPEG, .MPEG audio, MS office, text (Unicode and ANSI), .TIFF, .WAV, and .ZIP.

Some notable items regarding the DeepScan operation:

- **Windows Media Video (.WMV)**. Due to proprietary information unreleased by Microsoft, QFS cannot determine this type of file with DeepScan. It is not included when you select the Common Video Files option. Even with DeepScan disabled, however, QFS manages .WMV format files by extension.
- **Microsoft Office files.** Microsoft Office applications store documents as OLE structured storage files (known as *compound files*). Microsoft Office recognizes Office files regardless of extension (.PST, .DOC, .XLS, etc.), and they are all treated as the same file type. This characteristic prevents QFS from being able to block .PST files while allowing .DOC files, for example, when DeepScan is enabled. The .DOC file is seen as the same file type as the blocked .PST file and is also blocked. If the administrator adds .DOC to managed files, QFS will also manage other Office files in the same manner.
- **Text files.** When forming your file control strategy, bear in mind that a .VBS or .BAT file is a text format file. With DeepScan enabled, QFS will manage them (and similar text-file extensions) in the same manner as .TXT files.

To enable NTP Software DeepScan, follow these steps:

1. In the NTP Software Smart Policy Manager hierarchy view, locate the filer or Celerra you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **Quota & File Sentinel** to expand the policy types.
2. Expand the **File Control Policies**. Then right-click the desired file control policy and select **Properties**.
3. Click the **Criteria** tab. Check the **Enable NTP Deep Scan Technology** option to control how thoroughly files are scanned for the policy.

NTP Software Zip Scan

Another powerful feature of NTP Software QFS is NTP Software Zip Scan™. If this option is selected, QFS looks for managed file types inside compressed files with the .ZIP extension. For example, entering the **.MP3** file type and selecting **Block Zip files containing prohibited content** on the **Criteria** tab in the **New File Policy** dialog box will block files named .MP3 within a .ZIP file.

Blocking .ZIP files is performed by examining the list of contents for the .ZIP file. With current technology, adding a third level of scanning could negatively impact file operations. When polling the industry, we found that most customers were not particularly concerned with renamed files within .ZIP files because users would find using those renamed files to be cumbersome enough to outweigh any benefits they would gain.

To enable NTP Software Zip Scan, follow these steps:

1. In the NTP Software Smart Policy Manager hierarchy view, locate the filer or Celerra you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to **Quota & File Sentinel** to expand the policy types.
2. Expand the **File Control Policies**. Right-click the desired file control policy and select **Properties**.
3. Click the **Criteria** tab. Check the **Block Zip files containing prohibited content** option to specify how thoroughly files are scanned for the policy.

End User Support Infrastructure (EUSI)

NTP Software 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 about what constitutes a quota violation, and to assist users in fixing the problem.

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:

- **NTP Software QFS Email Templates.** Install these components on the same server as NTP Software QFS.
- **NTP Software QFS HelpSite™.** This collection of web pages describes what each quota policy violation means. Its purpose is to help users understand why they were notified about a quota violation, to reduce the amount of time administrators spend answering these simple questions.
- **End User Support Infrastructure website.** This site allows users to see what policy they violated, request policy changes, and clean up their drives.

The NTP Software QFS HelpSite, EUSI 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. By default, the directories are named HelpSite and EndUserSupportWebSite. 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, use the following addresses:

  `http://10.10.2.40`

  `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.

NTP Software QFS Email Templates

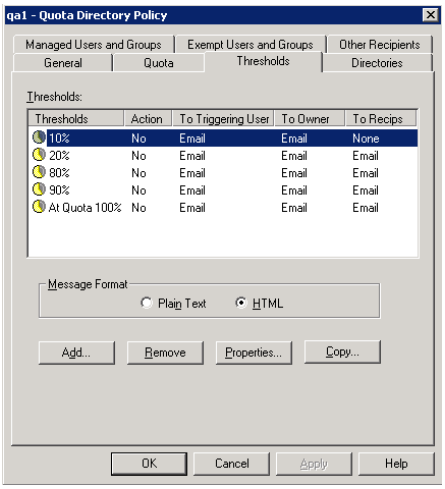
NTP Software QFS Email Templates are preformatted HTML email messages that can be imported easily into NTP Software QFS. The following email templates are provided:

- **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 message might indicate a prohibited extension (such as .MP3) or some other blocking reason specified in the QFS policy.
- **OverQuota.** Indicates that a user's action has caused his or her storage to exceed quota. This particular message contains links to both the 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, see the NTP Software QFS documentation for valid keys.
- **FileRemoval.** Indicates that a particular file of a user has been removed by a file removal policy.

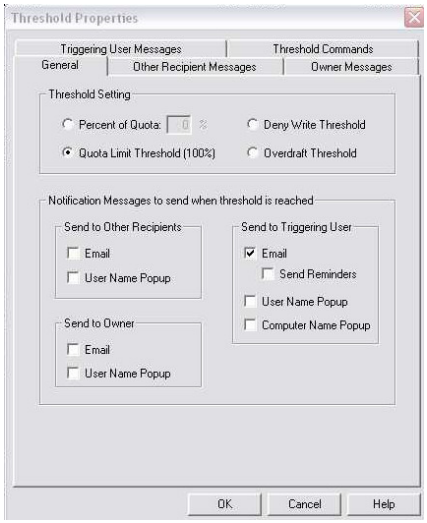
Note: When installing the QFS Email Templates, it is very important that you specify URLs for the QFS HelpSite and the End User Support Infrastructure website. The default web pages have placeholders for these URLs. If you do not specify the addresses, the email templates will not function as designed.

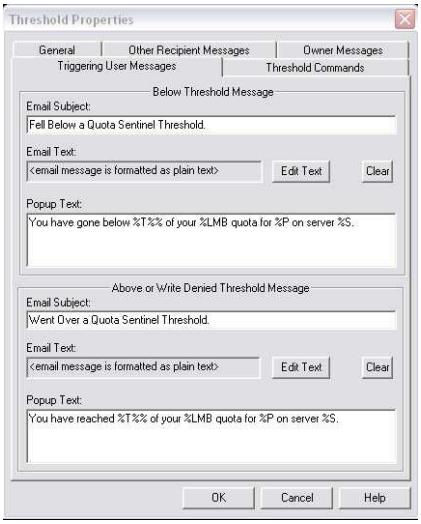
Adding an Email Template to QFS

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.

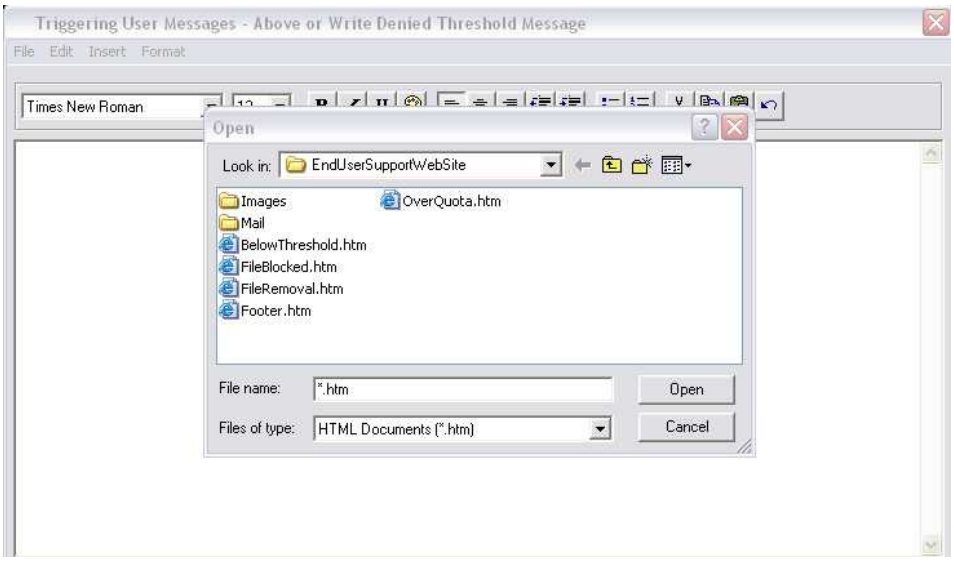


3. Select **HTML** as the message format and then click the **Properties** button.
4. In the Threshold Properties dialog box, you can customize messages for each type of recipient. For this example, we only want to send email to the user who triggered the quota. In the **Send to Triggering User** section of the dialog box, select **Email** as the notification method.
5. Click the **Triggering User Messages** tab.





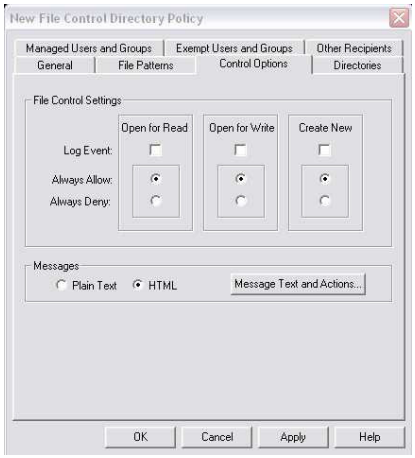
6. In the section **Above or Write Denied Threshold Message**, click the **Edit Text** button to open a text editor. In the text editor, choose **File** > **New** to remove all existing text.
7. Choose **Insert** > **File**. Browse to the directory where the End User Support Infrastructure website was installed and open the file **OverQuota.htm**.



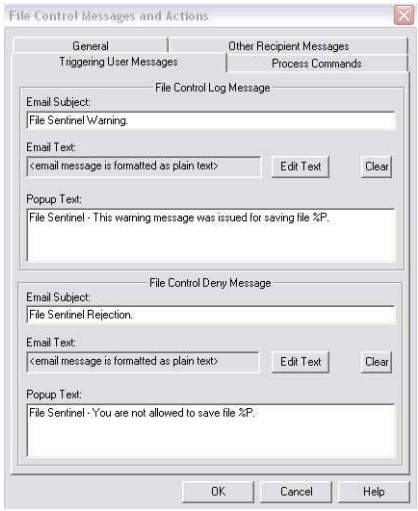
8. Click File, Save & Close
9. Click **OK** as needed to exit the dialog boxes. Now, when a user goes over quota, he or she will receive an email message explaining that the quota limit has been reached on that server.

Specifying a File Control Message

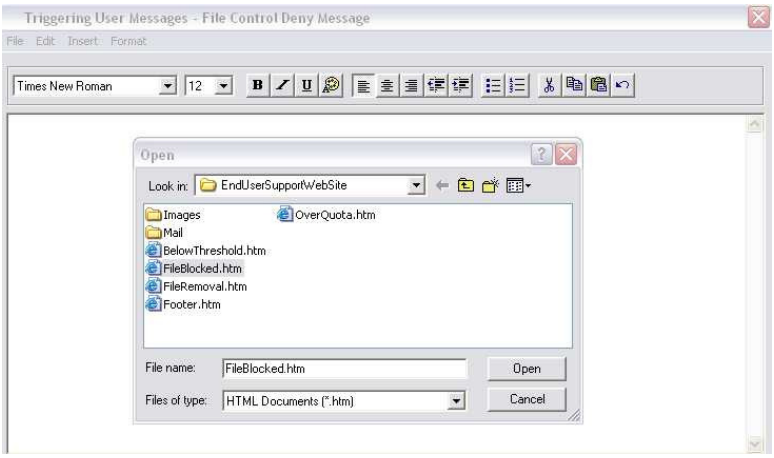
1. After creating a file control directory policy, click the **Control Options** tab in the **New File Control Directory Policy** dialog box.
2. In the **Messages** section of the dialog box, select **HTML**. Then click the **Message Text and Actions** button.



3. 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.
4. 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.



5. In the text editor, choose **File** > **New** to remove all existing text.
6. Choose **Insert** > **File**. Browse to the directory where the End User Support Infrastructure website was installed and open the file **FileBlocked.htm**.



7. Click File, Save & Close
8. Click **OK** as needed to exit the dialog boxes. Now, when a user tries to copy a blocked file, he or she will receive an email message.

NTP Software QFS HelpSite

The NTP Software 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.

End User Support Infrastructure 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 NTP Software QFS Email Templates files. During the installation of End User Support Infrastructure, you will 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 is 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.

For more information on configuring Storage Investigator, see *NTP Software Storage Investigator Parameters Reference*, ID #5073EF. For more information on using Storage Investigator, see *NTP Software Storage Investigator User Guide*, ID #5071EF.

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 is not 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 does not have Smart Policy Manager installed. Click **Yes** to install Smart Policy Manager on the remote computer. The installation begins.
4. When you are 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 drop-down list and enter the account.
6. When you have entered all the required information, click **Finish**.
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**.
9. When the confirmation message appears, select **Yes** to begin the installation.
10. You will 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 are 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.

QFS Admin Reports

NTP Software QFS has several reporting options for your convenience. We will briefly discuss and demonstrate each option so that you can evaluate them. QFS comes installed with a built-in reporting module called QFS Admin Reports. To access it and run reports, follow these steps:

1. Click **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin Reports**.
2. The NTP Software Report Wizard appears. Select **Create a report from a report template** and then click **Next**.
3. When prompted to select a report type, click **All Active Quota Policies** and then click **Next**.
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 are asked whether you want to save it; if so, specify the desired location.

Configuration Wizard

1. Click **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Configuration Wizard**.
2. Click the **View Pre-Wizard Checklist** button and gather the required information before continuing. Click **Next**.
3. Enter the name of your filer or Celerra. Click **Next**.
4. If you do not want to send email notifications to users when a quota status changes, uncheck the **Yes! We do want email notifications enabled** checkbox. Specify which email system your environment uses. Click **Next**.
5. Enter the name of your Active Directory server. (Enter a second server, if desired.) Click the **Test Active Directory Lookup** button and test at least one email address to verify connectivity. Then click **Next**.
6. Enter the SMTP gateway, the SMTP domain, and the email address to use for notifications. Enter any password(s) required for your environment. Click **Test Mail Settings** to verify that the information is correct. Then click **Next**.
7. Click the **Create a Local Policy** button to see how to link the filer or Celerra to QFS. Review the remaining information by clicking through the buttons in the lower half of the dialog box. When finished, click **Close**.

   Note: The NTP Software QFS for NAS Configuration Wizard is also available via the menu. Click **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Configuration Wizard**.

Command-Line Interface

NTP Software provides administrators with the option to perform user administration tasks through the 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.

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 removal 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.
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

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not 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

Parameter Name	Description
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

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes.

AddFileRemovalPolicy

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

Syntax

AddFileRemovalPolicy <targetserver> <policy> <type>

Parameters

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the file removal 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.

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

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not 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

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. Username pop-up.

abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reaches 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

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 is very important that you specify all the parameters for messages. If you do not 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

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reaches 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 is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

AddPolicyDescription

Adds a description to a given policy.

Syntax

AddPolicyDescription <targetserver> <policy> <description>

Parameters

Parameter Name	Description
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

Parameter Name	Description
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* 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

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. 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

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 is very important that you specify all the parameters for messages. If you do not 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

Parameter Name	Description
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

Parameter Name	Description
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 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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not 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

Parameter Name	Description
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 is very important that you specify all the parameters for messages. If you do not 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

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	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 is very important that you specify all the parameters for messages. If you do not 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

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not need to put a semicolon at the end.

RemoveFilePatterns

Removes file patterns from a file control policy.

Syntax

RemoveFilePatterns <targetserver> <policy> <patterns>

Parameters

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not have to put a semicolon at the end.

RemoveOtherRecipients

Removes other recipients from the recipient list.

Syntax

RemoveOtherRecipients <targetserver> <policy> <users>

Parameters

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not need to put a semicolon at the end.

RemovePolicy

Removes a policy from the QFS configuration.

Syntax

RemovePolicy <targetserver> <policy>

Parameters

Parameter Name	Description
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

Parameter Name	Description
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

Parameter Name	Description
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 is very important that you specify the list enclosed in double quotes. **Note:** If you have only one user in the list, you do not need to put a semicolon at the end.

RemoveThreshold

Removes a threshold from the policy.

Syntax

RemoveThreshold <targetserver> <policy> <thresholdvalue>

Parameters

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

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

Parameter Name	Description
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

Parameter Name	Description
targetserver	Level of the policy.
policy	Name of the policy.
flag	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

Parameter Name	Description
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 removal policy.

Syntax

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

Parameters

Parameter Name	Description
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.

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

Parameter Name	Description
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

Parameter Name	Description
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>

Parameters

Parameter Name	Description
targetserver	Level at which the policy needs to be created within the EASE 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.

Appendix: Installing QFS in Clustered Environments

Notes

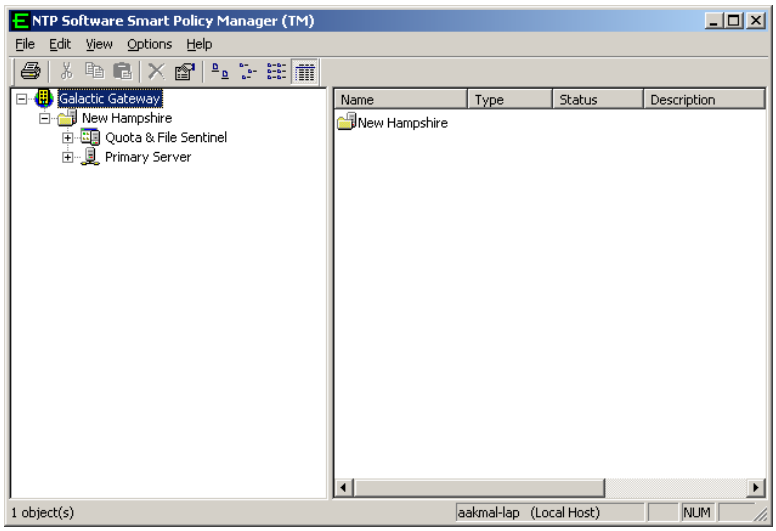
- QFS requires a manual setup by an administrator for clustered environments.
- The Connector service can be started on the servers on which QFS was installed; however, in the QFS user interface, the filer or Celerra is assigned to only one server node and must be reassigned manually from a previously assigned node.
- A filer or Celerra cannot communicate with more than one QFS server at a time.

Installing QFS in Clustered Environments

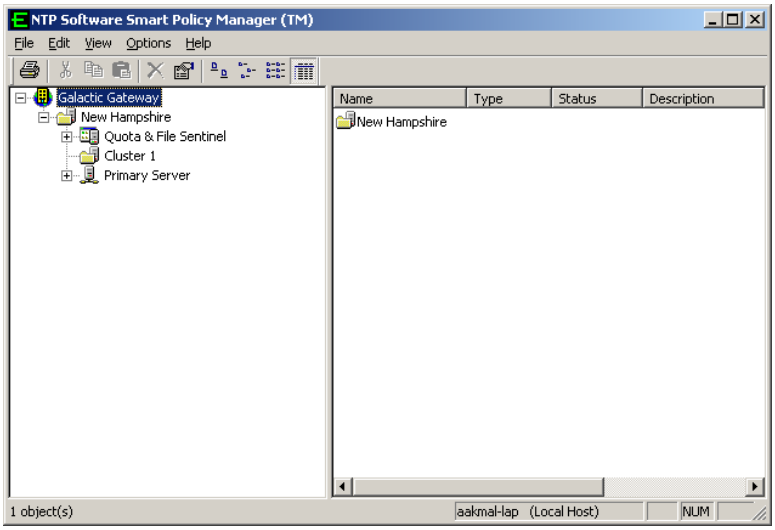
Follow these steps:

1. Install NTP Software QFS on a server as described in *NTP Software QFS for NAS, EMC Edition Quick Start Guide*, ID #6051EF.
2. After QFS is installed successfully, open QFS to find the global container (in this example, Galactic Gateway) 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.



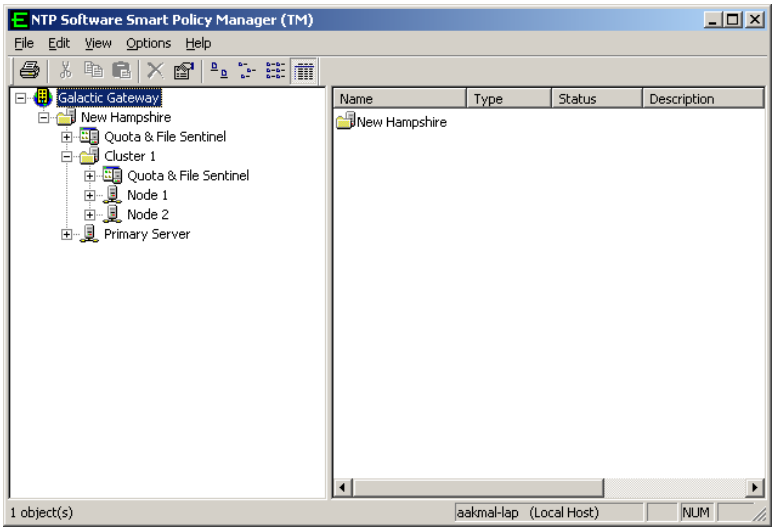
4. Right-click the site container (New Hampshire in this example) and select **New** > **Container** from the pop-up menu to create your cluster container. Give the new container the name of the cluster. In the example, we have used Cluster 1 as the name.



5. Right-click the cluster container (Cluster 1 in this example) and select **New** > **Quota & File Sentinel Application** from the pop-up menu.

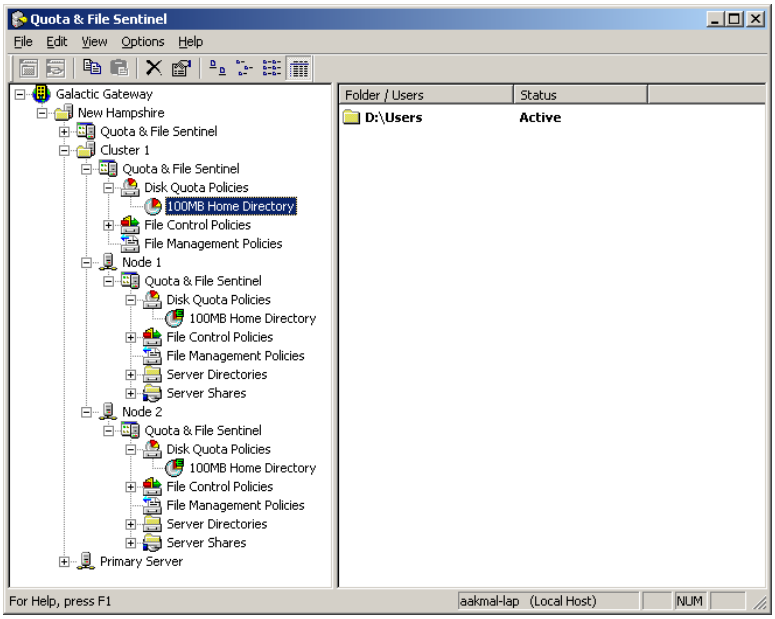
6. It is necessary to install QFS manually on each server you want to add to the tree (Node 1 and Node 2 in this example). Choose the option **Adding to an enterprise installation** during the local NTP Software Smart Policy Manager installation on each node, and point to the first QFS server.

7. 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 Quota & File Sentinel application, as shown here.



8. Click the plus sign (+) next to the QFS 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.

   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.

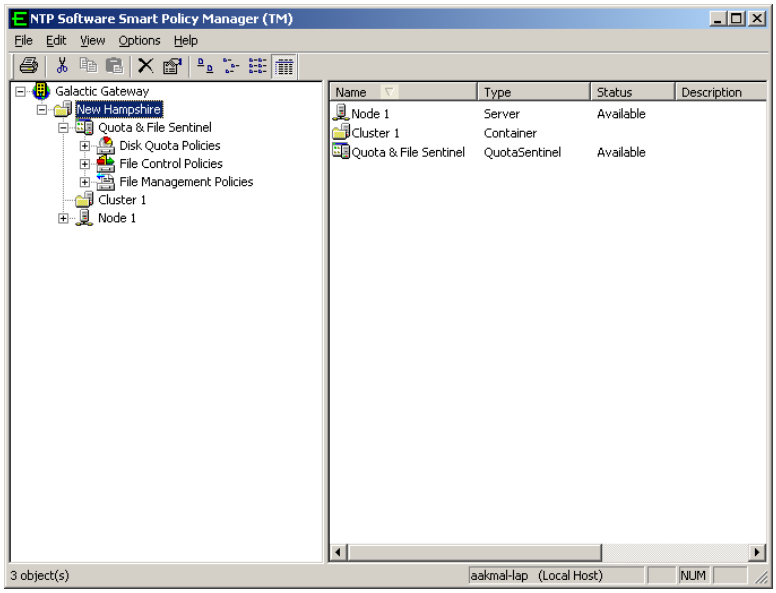


Installing NTP Software QFS onto a Node Server

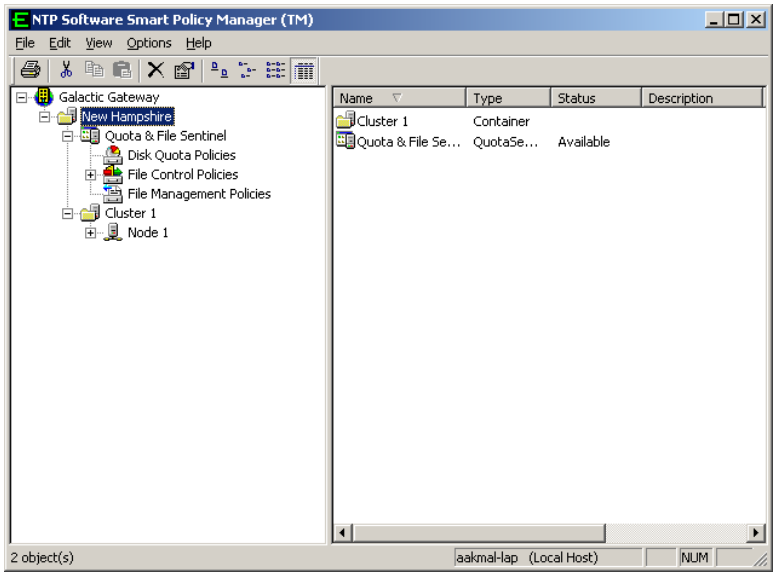
This feature enables administrators to group servers, filers, and Celerras logically to reflect their organizational physical structure, creating policies under a node that can be inherited by all the machines of that node.

Follow these steps:

1. It is necessary to install QFS manually on each of the added nodes (in this example, on Node 1). Choose the option **Adding to an enterprise installation** during the local NTP Software Smart Policy Manager installation.
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** > **Quota & File Sentinel Application** from the pop-up menu.
5. To view the global (cluster) policies, click the plus sign (+) next to the QFS application you have just added.



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

About NTP Software

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

NTP Software Professional Services

For further assistance with NTP Software 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