NTP Software QFS®
for NetApp®

Installation Guide

Version 8.5

This guide provides a short introduction to installation and initial configuration of NTP Software QFS® for NAS, NetApp® Edition, from an administrator's perspective. Upon completion of the steps within this document, NTP Software QFS for NAS, NetApp Edition will be installed within your enterprise community. This Installation Guide applies to all NTP Software QFS for NAS, NetApp Filer® editions..

Table of Contents

Executive Summary

Thank you for your interest in NTP Software QFS® for NAS, NetApp® Edition. NTP Software QFS controls storage for millions of users worldwide. NTP Software QFS for NAS, NetApp Edition extends our best-of-breed technology to include the NetApp family of products, allowing you to manage Windows® and NAS-hosted storage as a seamless whole.

Given the architecture of your Filer, NTP Software QFS for NAS, NetApp Edition does its job remotely. Part of NTP Software QFS Family of Products, NTP Software QFS for NAS, NetApp Edition uses a connector service to create a bridge and include Filers as full participants in storage environments controlled by NTP Software QFS. In light of this fact, you will need to install the NAS connector on one of the Windows Server® 2008, Windows Server® 2008 R2, Windows Server® 2012, or Windows Server® 2016 machines in your environment. This may be an existing server or workstation, or a standalone system.

To be managed by NTP Software QFS, version 6.5 or later (excluding versions7.1.x) of the Data ONTAP® operating system is required on the Filer. If the QFS license key supports NFS, the managed Filer ONTAP version need to be 7.3 or newer. If QFS is running on Windows Server 2008 or newer, it is recommended to upgrade to ONTAP version 7.3.3 or newer.

NTP Software QFS for NAS, NetApp Edition requires the Cluster mode NetApp Filer to run Data ONTAP version 8.2 or later.

NTP Software QFS for NAS, NetApp Edition can be used to manage NetApp Filers, vFilers®, and NetApp clusters or any combination of these systems. NTP Software 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 NTP Software QFS on Windows, a login with administrator rights is needed. You will be installing four different services: the NTP Software Smart Policy Manager™ service, the NTP Software QFS service, the NAS Connector, and the NTP Software QFS Watchdog 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 NTPSoftware QFS service requires a domain user account with local administrative rights on the NetApp Filer. The NAS Connector service uses this account as well.

Your hardware should be appropriate for the services running on each machine. The connector itself and NTP Software QFS for NAS, NetApp Edition impose almost no load. on either machine.

Preparing the NetApp Filer

Preparing NetApp Filer for NTP Software QFS for NAS

NTP Software QFS for NAS, NetApp Edition requires the NetApp Filer to run Data ONTAP version 6.5 or later (excluding versions 7.1.x). If the QFS license key supports NFS, the managed Filer ONTAP version need to be 7.3 or newer. If QFS is running on Windows Server 2008 or newer, it is recommended to upgrade to ONTAP version 7.3.3 or newer. If your Filer is not running one of the supported versions, you must upgrade your operating system before you proceed. (Please refer to your Network Appliance documentation for instructions.)

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

NTP Software QFS for NAS, NetApp Edition requires the Cluster mode NetApp Filer to run Data ONTAP version 8.2 or later.

> **NOTE:** In case NTP Software QFS for NAS, NetApp Edition is running on W2k8 Server or W2k8R2 Server, the Filers' hosts file needs to include the IP address and FQDN of the machine running NTP Software QFS.

To insert the IP address and FQDN within the Filer's hosts file, perform the following steps:

1. Go to http://filername/na_admin
2. Click FilerView > Network > Manage Hosts File
3. On the Manage Hosts File page, click the Insert button.
4. On the Create a New/etc/hosts Line dialogue box, add in the IP, FQDN, and other required data of the current NTP Software QFS server machine and then click Ok.
5. On the Manage Hosts File page, click the Apply button.

Preparing NetApp Filer for NFSv4 Support

Although NTP Software QFS® does not install any components on the NetApp® server; you will need to enable NFSv4 protocol in the Data ONTAP® and disable NFSv3 to prevent its usage. Perform these steps:

1. Log on to the NetApp® server with an account that has administrative privileges.

2. To enable NFSv4 in the Data ONTAP®, enter the following command at the prompt:

   options nfs.v4.enable on
   options nfs.v4.id.domain localdomain

3. It is recommended to disable NFSv3 in the Data ONTAP® and keep only NFSv4 enabled. To do so, enter the following command:

   options nfs.v3.enable off

4. Make sure the volumes and qtrees that will be accessed using the NFS protocol have their security style set to mixed. To check that, enter the following command:

   qtree status

   The command should display something similar to the following:

   If the volume has a value under the Style column is ntfs or unix, proceed to step 5. If the volume has a value under the Style column is mixed, skip step 5 and go directly to the next section.

5. Enter the following command to set the security style to mixed (replace <path> with the actual path, as /vol/vol0 for the example shown above:

   qtree security <path> mixed

6. Open the exports file located inside the etc directory of your filer.

7. NFS exports are similar to CIFS shares. The exports file contains entries for NFS exports. For every path you wish to export, add the following line to the end of the exports file (where <path> is replaced with the actual path as in step 5):

   <path> -sec=sys,rw,anon=0

Preparing NetApp Filer for NFSv3 Support

Although NTP Software QFS® does not install any components on the NetApp® server; you will need to enable NFSv3 protocol in the Data ONTAP® and disable NFSv4 to prevent its usage. ONTAP 7.3.x or later is required for NFS support. Perform these steps:

1. Log on to the NetApp® server with an account that has administrative privileges.
2. Make sure NFSv3 is enabled in the Data ONTAP®, by entering the following command at the prompt:

   options nfs.v3.enable on
3. It is recommended to disable NFSv4 in the Data ONTAP® and keep only NFSv3 enabled. To do so, enter the following command:

   options nfs.v4.enable off
4. Follow the steps 4 through 7 in the previous section (Preparing NetApp® Filer® for NFSv4 Support).

> **NOTE**: ONTAP 7.3.3 or later is required for NFS support.

Preparing NetApp Filer for Unix-to-Windows User Mapping

For NTP Software QFS® to work with NFS protocol, Unix users should be mapped to corresponding Windows users. To do that, follow these steps:

1. Log on to the NetApp® server with an account that has administrative privileges and type the following command at the prompt. This will make sure that if the filer fails to map the operating user, their operation will be denied:

   options nfs.require_valid_mapped_uid on

2. If you have NIS or LDAP configured for your Unix users, skip to step 4. Otherwise, open the passwd file located inside the etc directory of your filer.

3. The passwd file contains entries for all Unix users that will be accessing the filer. For every Unix user, add the following entry to the end of the filer::

   <unix_name>::<unix_uid>:<unix_gid>::/:

   Example: Assume we have a Unix user with the name unixClient. This user has a UID of value 1000 and a GID with a value 1000. The added entry should look as follows:

   unixClient::1000:1000::/:

4. Open the usermap.cfg file located inside the etc directory of your filer.

5. The usermap.cfg file contains entries that specify the mappings desired for the system. Each entry specifies a pair of Windows and Unix users, separated with a mapping operator. Enter the desired mapping entries in the following format:

   [<DOMAIN_NAME>\]<WINDOWS_NAME> <MAPPING_DIRECTION> <UNIX_NAME>

   DOMAIN_NAME is the domain that the Windows user belongs to (optional).
   WINDOWS_NAME is the account name of the Windows user.
   UNIX_NAME is the name of the Unix user.
   MAPPING_DIRECTION is either ==, => or <=, for bidirectional mapping, left-to-right mapping and right-to-left mapping respectively.

   Example: Assume we have a Unix user with the name unixClient, and we want to map this Unix user to the Windows user windowsUser whose account belongs to the myDomain domain. The mapping entry should look as follows:

   myDomain\windowsUser == unixClient

For more details about user mapping and its verification, please refer to the "**Error! eference source not found.**" section.

> **IMPORTANT**: For vFilers, the mapping configuration on the vFiler must be identical to the mapping configuration on its host filer.

User Mapping Configuration

All Unix user should have corresponding mapping on the Windows domain for NTP Software QFS® to work with the NFS protocol properly. Mapping entries are stored in the usermap.cfg file on the filer. All Unix users included in the mapping mechanism should have entries in the passwd file as well if you don't have NIS or LDAP servers configured for your Unix users (refer to the "Preparing NetApp Filer for NFSv3 Support

Although NTP Software QFS® does not install any components on the NetApp® server; you will need to enable NFSv3 protocol in the Data ONTAP® and disable NFSv4 to prevent its usage. ONTAP 7.3.x or later is required for NFS support. Perform these steps:

5. Log on to the NetApp® server with an account that has administrative privileges.
6. Make sure NFSv3 is enabled in the Data ONTAP®, by entering the following command at the prompt:

   options nfs.v3.enable on
7. It is recommended to disable NFSv4 in the Data ONTAP® and keep only NFSv3 enabled. To do so, enter the following command:

   options nfs.v4.enable off
8. Follow the steps 4 through 7 in the previous section (Preparing NetApp® Filer® for NFSv4 Support).

> **NOTE**: ONTAP 7.3.3 or later is required for NFS support.

Preparing NetApp Filer for Unix-to-Windows User Mapping" section for configuration steps).

Default Mapping

Before configuring the mapping mechanism on the filer, it is better to configure (or disable) the default filer mapping. When a mapping request comes in to the filer, it is first checked against the NIS, LDAP or mapping files. If this fails, the request is checked against the default filer mapping. If the latter fails, the request is allowed or denied based on the value set for nfs.require_valid_mapped_uid (refer to the "Preparing NetApp Filer for NFSv3 Support

Although NTP Software QFS® does not install any components on the NetApp® server; you will need to enable NFSv3 protocol in the Data ONTAP® and disable NFSv4 to prevent its usage. ONTAP 7.3.x or later is required for NFS support. Perform these steps:

9. Log on to the NetApp® server with an account that has administrative privileges.

10. Make sure NFSv3 is enabled in the Data ONTAP®, by entering the following command at the prompt:

    options nfs.v3.enable on

11. It is recommended to disable NFSv4 in the Data ONTAP® and keep only NFSv3 enabled. To do so, enter the following command:

    options nfs.v4.enable off

12. Follow the steps 4 through 7 in the previous section (Preparing NetApp® Filer® for NFSv4 Support).

> **NOTE**: ONTAP 7.3.3 or later is required for NFS support.

Preparing NetApp Filer for Unix-to-Windows User Mapping" section for configuration steps).

The default filer mapping is set using the following command:

options wafl.default_nt_user [<DOMAIN_NAME>\]<WINDOWS_NAME>

DOMAIN_NAME is the domain that the Windows user belongs to (optional). WINDOWS_NAME is the account name of the Windows user.

If you wish to set the default mapping to nobody (i.e. denying the request), type two double quotes (empty string) as follows:

options wafl.default_nt_user ""

General Form

Generally, the mapping entry looks as follows in the mapping file:

[<DOMAIN_NAME>\]<WINDOWS_NAME> <MAPPING_DIRECTION> <UNIX_NAME>

DOMAIN_NAME is the domain that the Windows user belongs to (optional). WINDOWS_NAME is the account name of the Windows user. UNIX_NAME is the name of the Unix user. MAPPING_DIRECTION is either ==, => or <=, for bidirectional mapping, left-to-right mapping and right-to-left mapping respectively.

Example: Assume we have a Unix user with the name unixClient, and we want to map this Unix user to the Windows user windowsUser whose account belongs to the myDomain domain. The mapping entry should look as follows:

myDomain\windowsUser == unixClient

(Please refer to your Network Appliance™ documentation for more instructions.)

Mapping Directions

There are three mapping operators that can be used per mapping entry to define the mapping direction:

- Bidirectional Mapping (==): maps the Unix user to the Windows user, and vice versa.
- Left-to-right Mapping (=>): maps the Windows user to the Unix user.
- Right-to-left Mapping (<=): maps the Unix user to the Windows user.

> **Note:** NTP Software QFS® is not concerned with the mapping from Windows user to Unix users. Hence, the usage of left-to-right mapping direction (=>) is not needed in the mapping mechanism.

Wildcards and Symbol Conventions

The asterisk (*) is considered as a wildcard character, meaning any user. If the source contains a wildcard, this means any user will be mapped to the destination. Note that Data ONTAP® does not map explicit sources to destinations with wildcards. However, if both the source and the destination contain wildcards, the mapping is fine. The wildcard can be used in place of any of the DOMAIN_NAME, WINDOWS_ACCOUNT_NAME and UNIX_NAME with respect to the previous note.

The null string (“”) is used to specify nobody, where the mapping matches no name and rejects the user. It can be used with the asterisk as well. Examples:

maps any user belonging to the myDomain domain to the Unix user unixClient:
myDomain* => unixClient

maps any user with the name windowsUser belonging to any domain to the Unix user unixClient:
*\windowsUser => unixClient

maps any Unix user to the Windows User myDomain\windowsUser:
myDomain\windowsUser <= *

maps any user belonging to the myDomain domain to nobody
myDomain* => “”

maps any user with the name windowsUser belonging to any domain to nobody:
*\windowsUser => “”

Mounting NFS Exports on Unix Clients

NFS exports are similar to CIFS shares. To access any of your NFS exports from a Unix client machine, the export should be mounted first (refer to the " Support" section). To do that, follow the next steps:

1. Open a terminal window on your Unix client machine, and type the following commands:

   sudo mkdir /mnt/<mount_dir>
   sudo mount –t nfs4 <filer_ip_address>:<path> /mnt/<mount_dir>

   Where <mount_dir> is the name of your choice to mount the filer's path on, <filer_ip_address> is the address to the filer, and <path> it the actual path to the volume, qtree or folder you wish to mount.

   Example: The following commands will create a directory with the name myfiler and mount the path /vol/vol0/home on the filer at the IP address 10.0.0.10 to it:

   sudo mkdir /mnt/myfiler
   sudo mount –t nfs4 10.0.0.10:/vol/vol0/home /mnt/myfiler

2. If the process was successful, you should access the path stated on the filer using the following command:

   cd /mnt/<mount_dir>

   Example: Continuing the previous example, the path on the filer could be accessed using the following command:

   cd /mnt/myfiler

   To dismount the path, use the following command:

   sudo umount /mnt/<mount_dir>

   IMPORTANT: If you want to use NFSv3 protocol instead of NFSv4 protocol, just use nfs instead of nfs4 in step 1 above.

Requirements

NTP Software QFS components must meet the following minimum requirements.

NTP Software QFS for NAS, NetApp Edition Server Requirements

NTP Software QFS for NAS is installed on a server in your environment. The hardware must be suitable for our software operation, and our requirements are the minimum necessary. If your server is also hosting antivirus or other programs, your environment's requirements may be greater than those in the following list:

Hardware Specification

The following hardware components are the minimum requirements to support NTP Software QFS for NAS, NetApp Edition. If the NTP Software QFS for NAS server is also hosting antivirus or other programs, the requirements may be greater than those in the following list:

- 1 GHz CPU
- 1 GB RAM
- 150 MB free disk space
- Network interface card

Software Specification

- Windows Server® 2008 or later
- WoW 64

NetApp Filer Requirements

The NetApp Filer to which NTP Software QFS for NAS, NetApp Edition will be connected requires the following:

- Data ONTAP v. 6.5 or later (excluding versions7.1.x). If the QFS license key supports NFS, the managed Filer ONTAP version need to be 7.3 or newer. If QFS is running on Windows Server 2008 or newer, it is recommended to upgrade to ONTAP version 7.3.3 or newer.

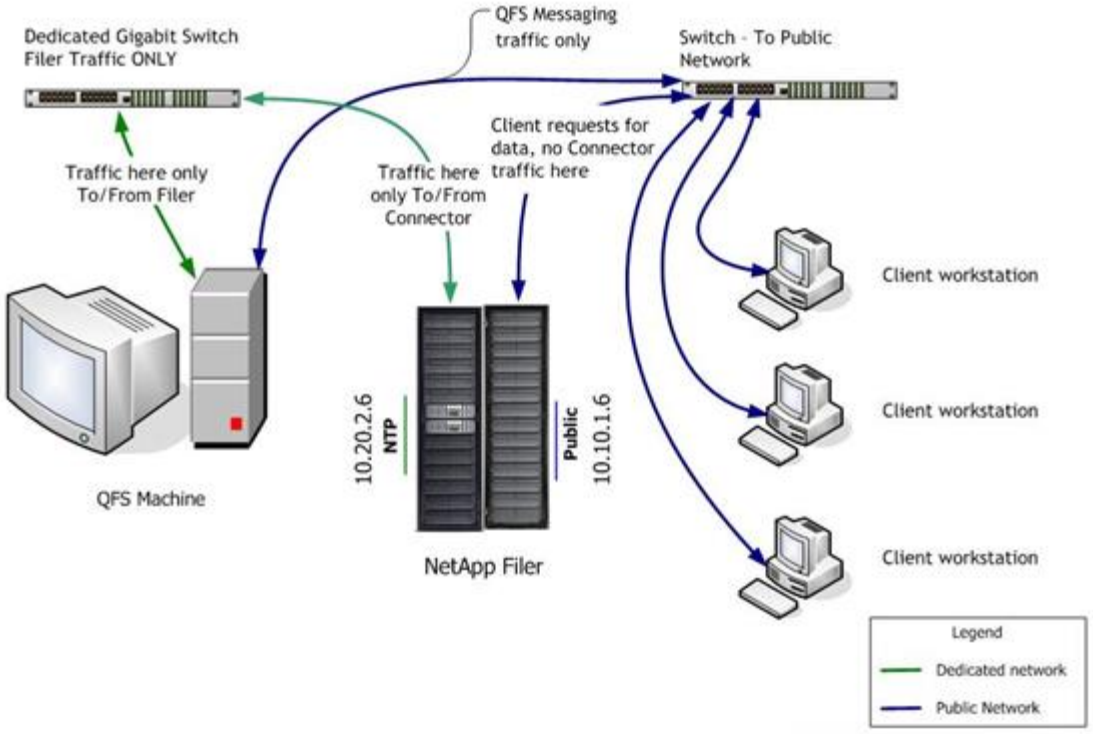
- NTP Software QFS for NAS, NetApp Edition requires the Cluster mode NetApp Filer to run Data ONTAP version 8.2 or later.

- Network interface card

> **NOTE:** It is strongly recommended that two network adapters be installed in both the Filer and Windows server. The connection between the server and Filer should be a dedicated connection (i.e., separate from the public network connection). Using a single network adapter will greatly increase the time required to process data, and may cause excessive delays in the environment.

Network Configuration

NTP Software QFS for NAS, NetApp Edition Installation Best Practice



IMPORTANT: One network connection on the NTP Software QFS machine should be configured as a dedicated and direct connection between the Windows host and the NetApp Filer.

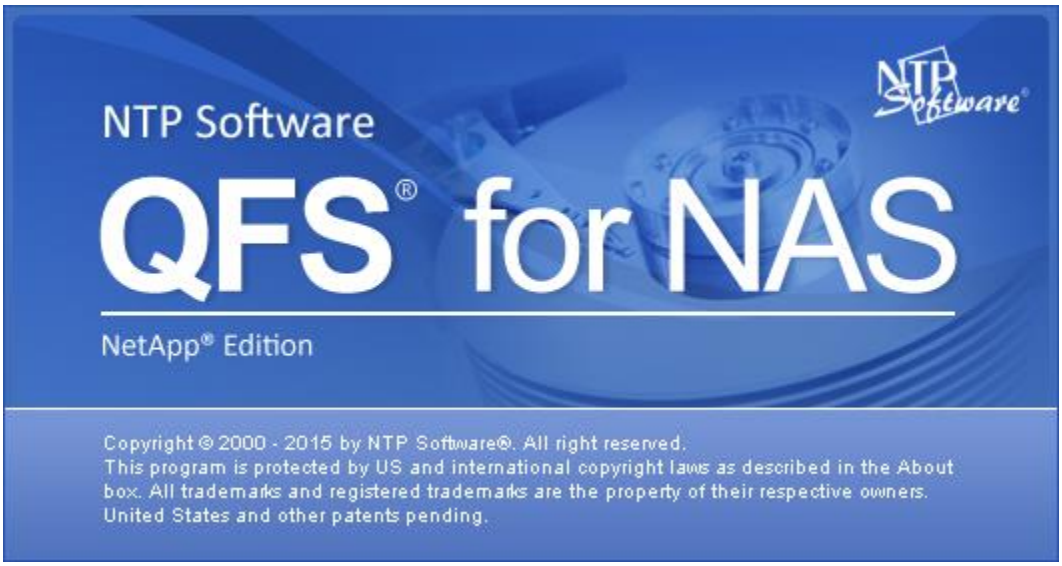
Installation

Prior to installing NTP Software QFS for NAS, NetApp Edition, NTP Software recommends verifying that the installation server meets the requirements listed in the Requirements section of this document.

Installing NTP Software Smart Policy Manager™

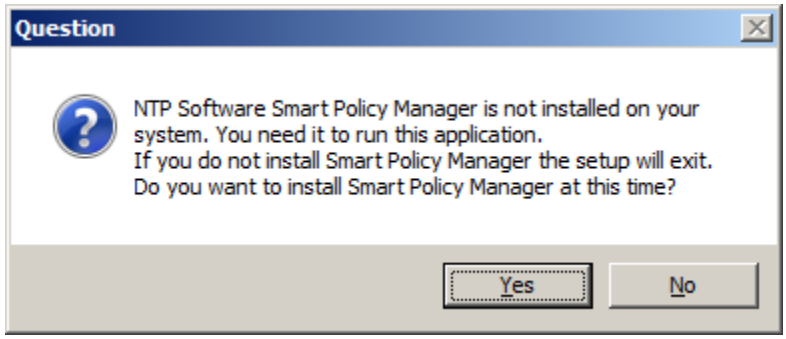
1. Log on to your server by using an account with administrator privileges.

2. Run the NTP Software QFS installer. If NTP Software Smart Policy Manager™ is not installed, the following installer will launch automatically.

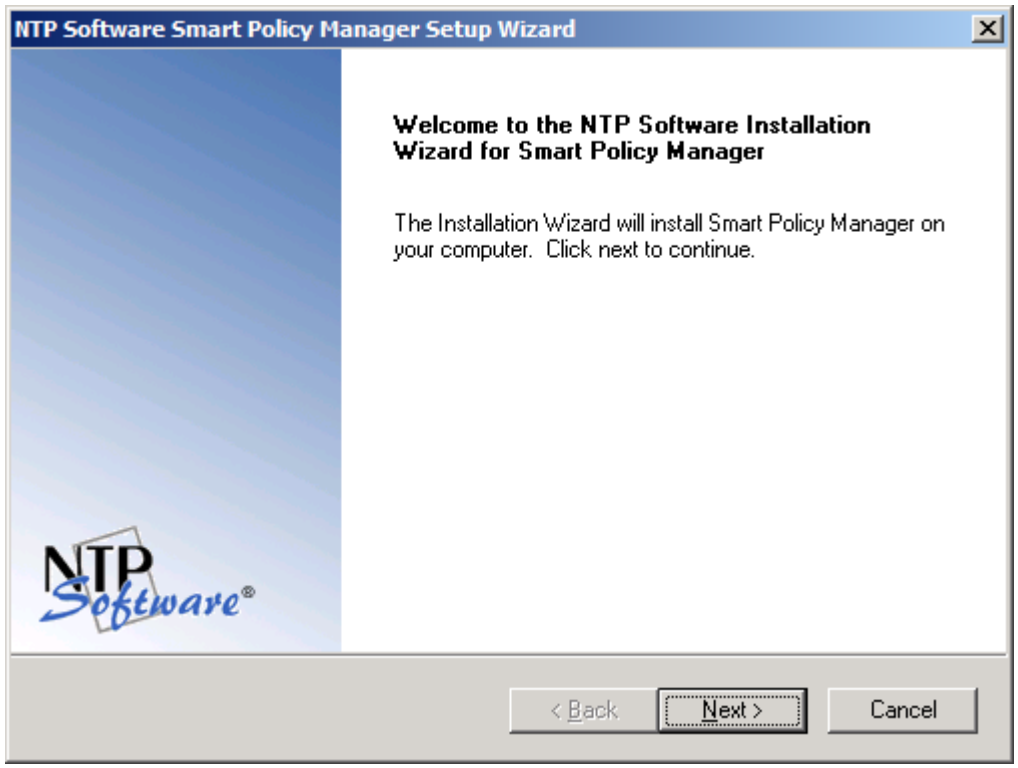


If NTP Software Smart Policy Manager is installed, you can skip to the section on Installing NTP Software QFS for NAS, NetApp Edition.

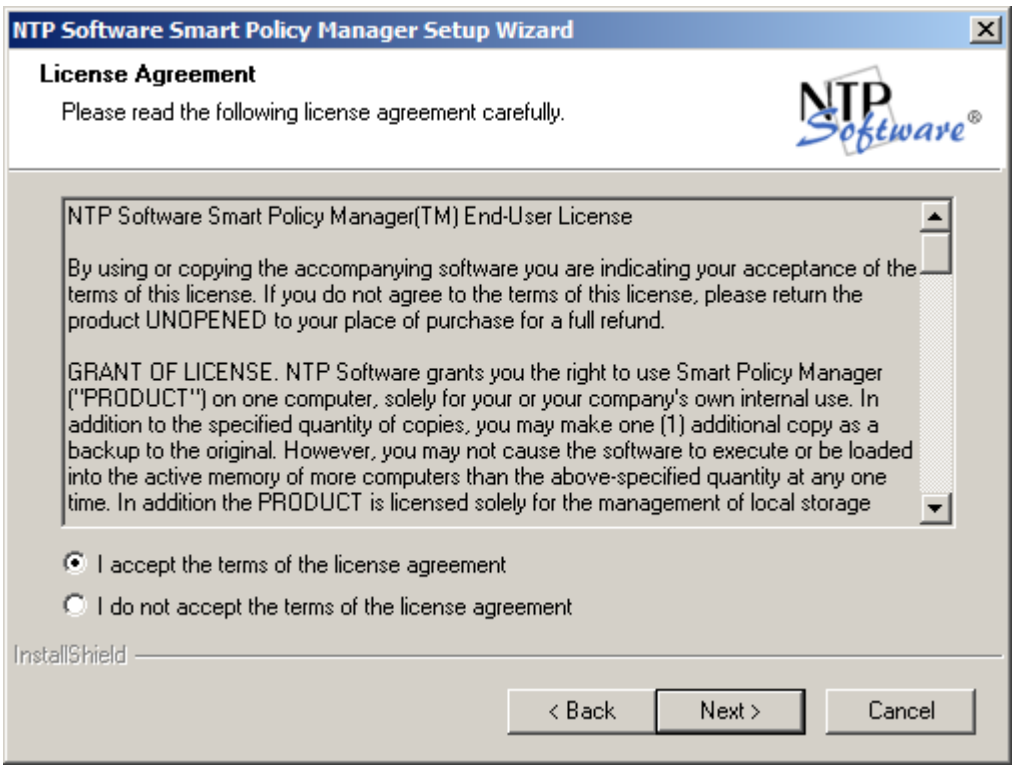
3. When prompted to install NTP Software Smart Policy Manager, click the **Yes** button.



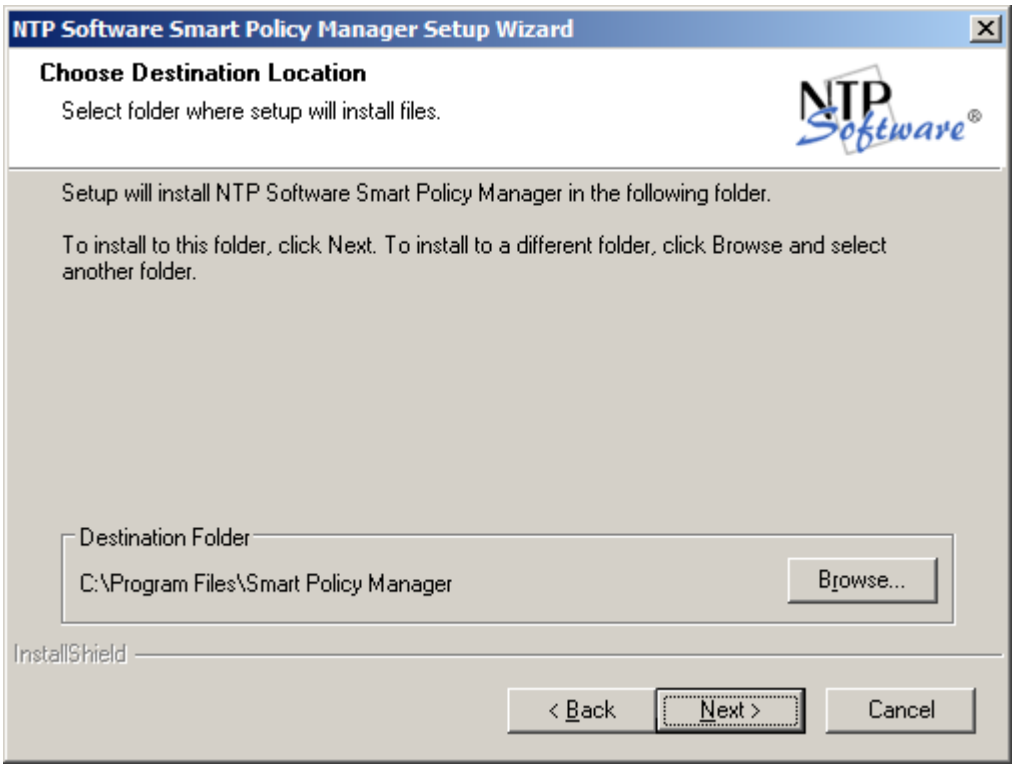
4. The **NTP Software Smart Policy Manager Installation Wizard** opens. Click **Next** to begin the installation.



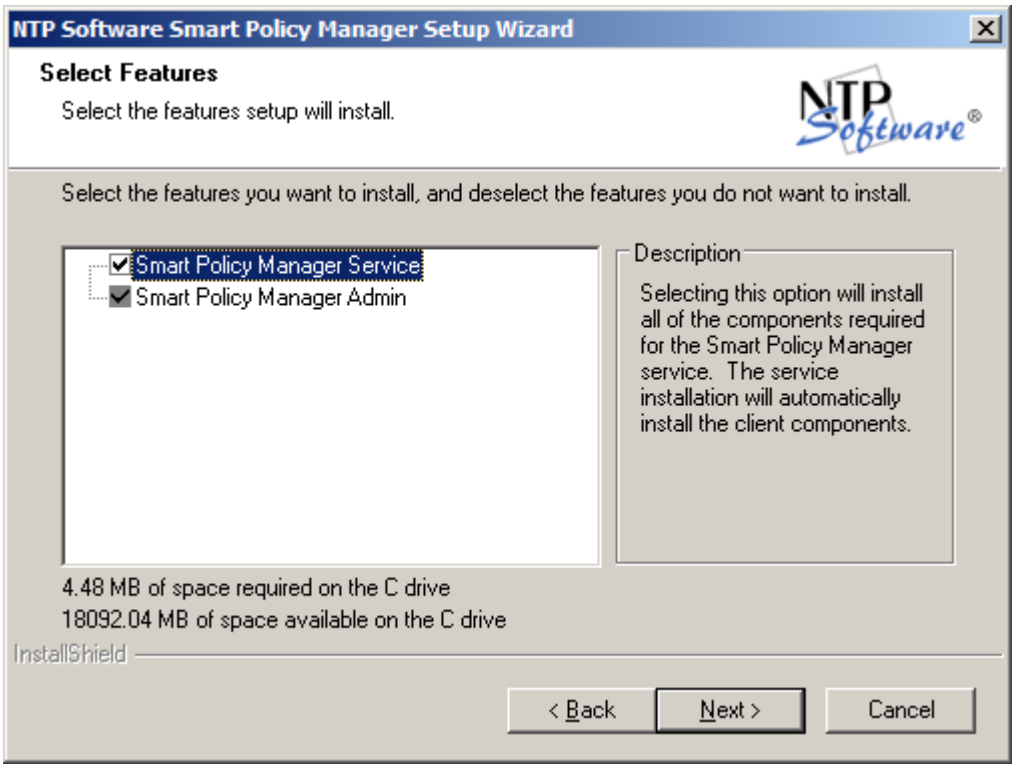
5. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



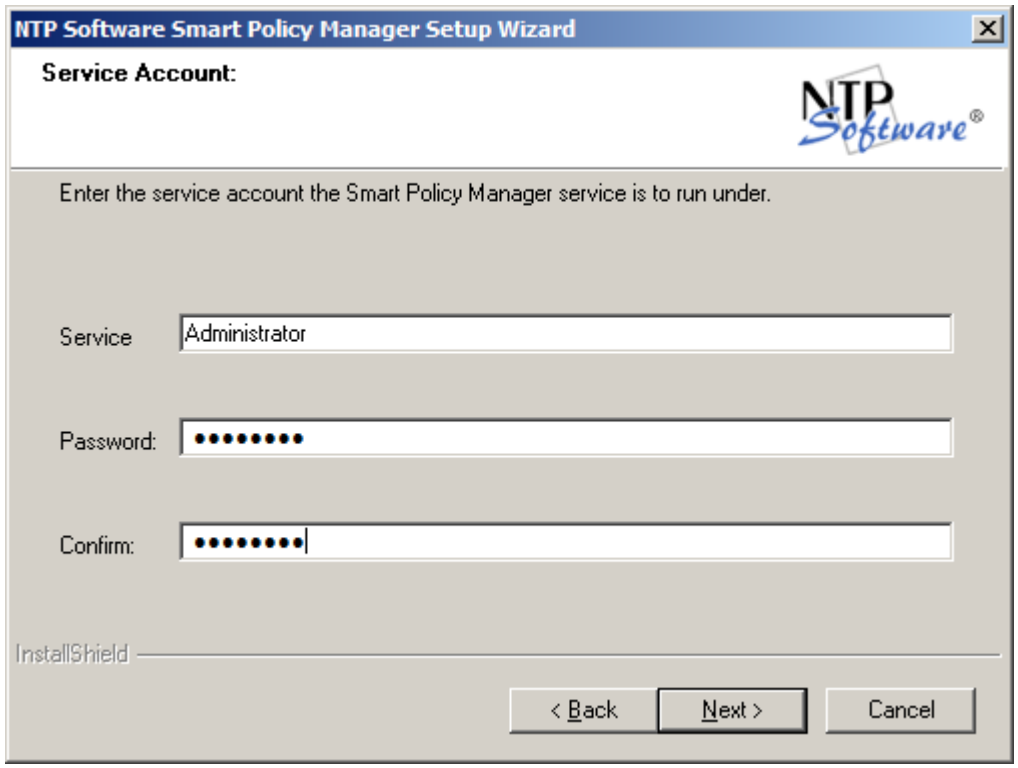
6. In the **Choose Destination Location** dialog box, click **Browse** to choose the location where you want to install NTP Software Smart Policy Manager, and then click **Next**.



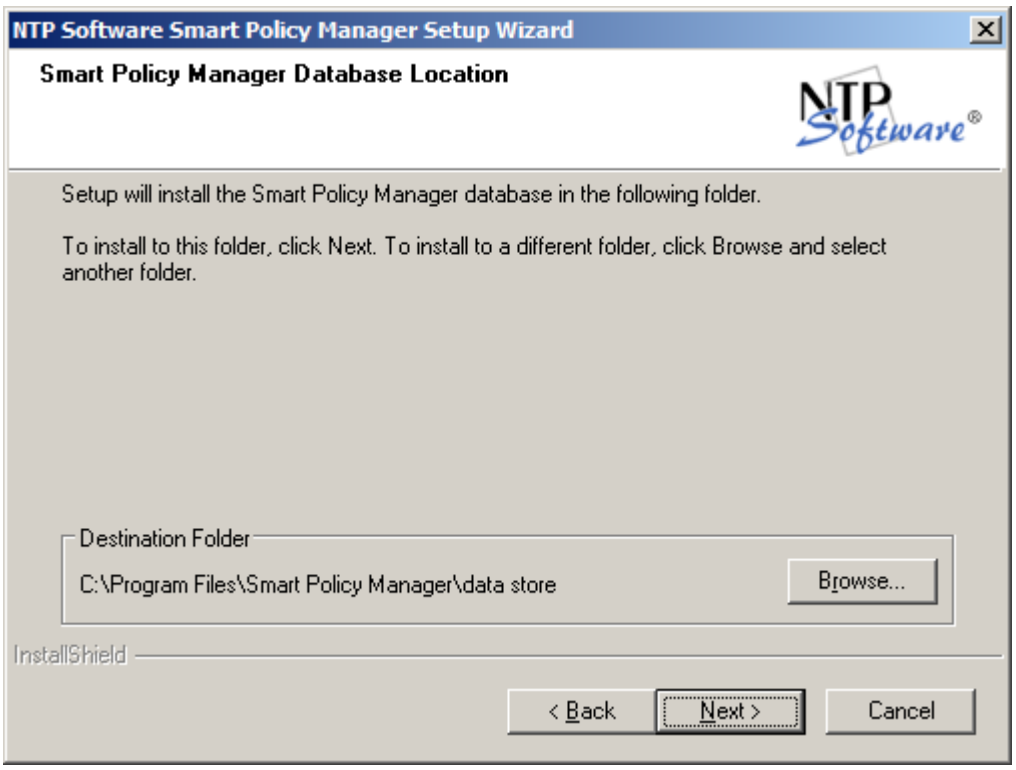
7. In the **Select Features** dialog box, select the components you want to install, and then click **Next**.



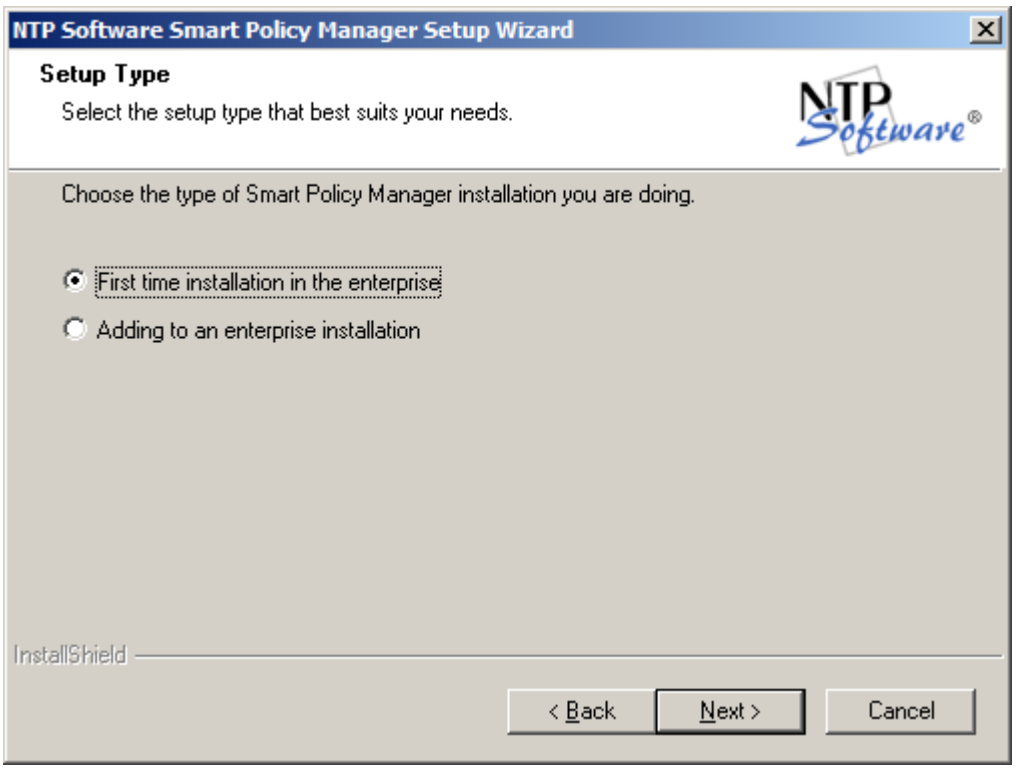
8. In the **Service Account** dialog box, when prompted for a Windows domain user account to run the NTP Software Smart Policy Manager service, enter the username and password for a domain user account with administrative rights on the local machine. Click **Next**.



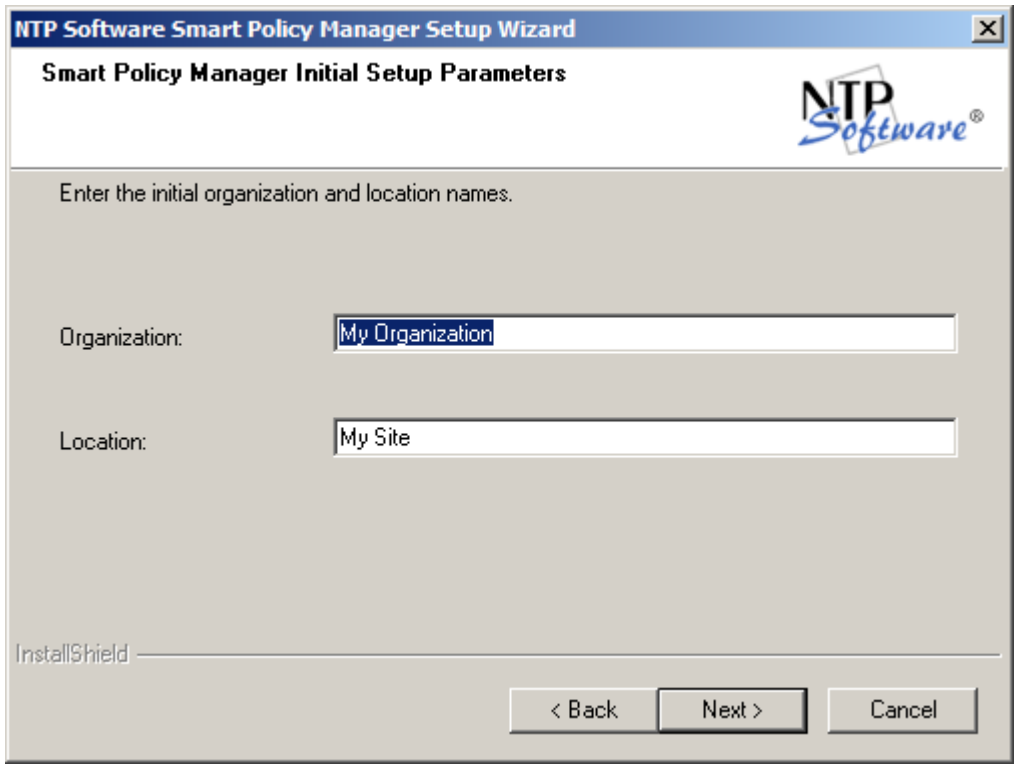
9. In the **Smart Policy Manager Database Location** dialog box, enter the directory name where you want to install the NTP Software Smart Policy Manager database, or just accept the default location. Click **Next**.



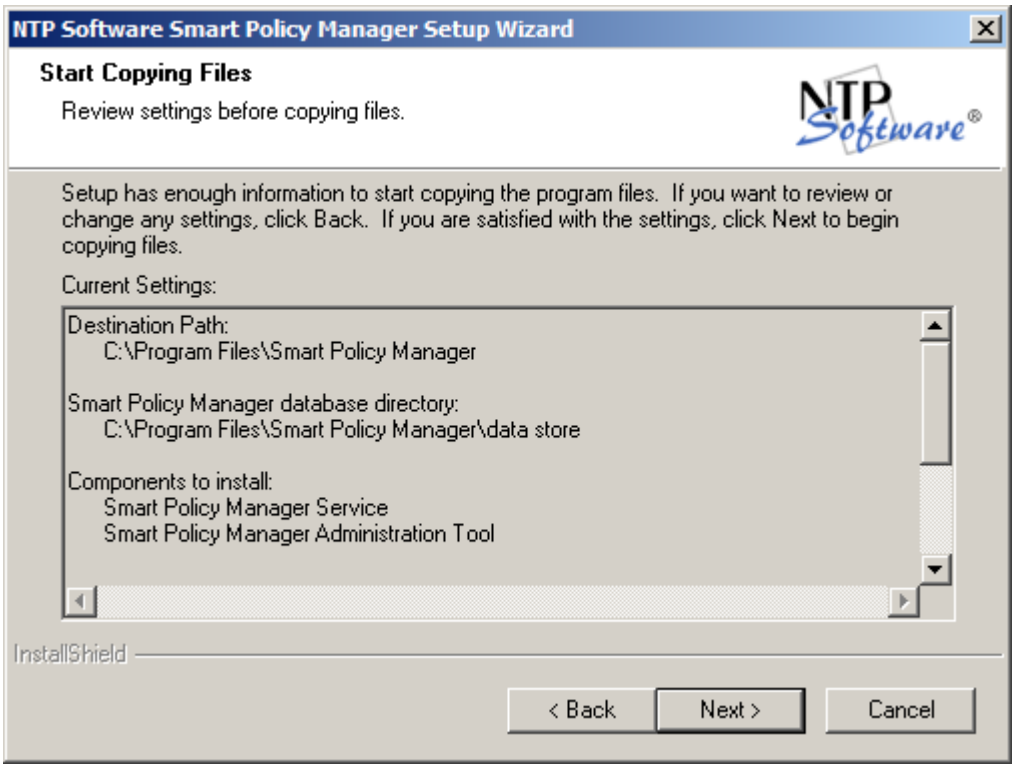
10. In the **Setup Type** dialog box, select the NTP Software Smart Policy Manager installation type for your environment. If installing to a new environment with no prior NTP Software Smart Policy Manager installations, click **Next**. If installing in an environment where NTP Software Smart Policy Manager is already running, choose **Adding to an enterprise installation** and click **Next**.



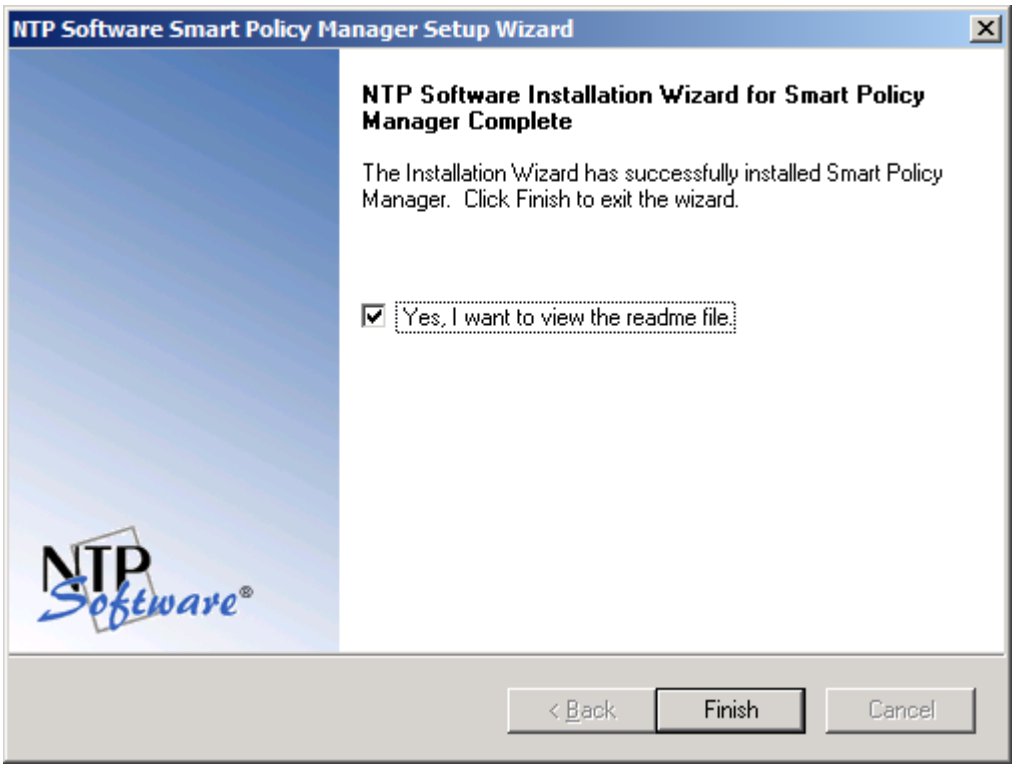
11. In the **Smart Policy Manager Initial Setup Parameters** dialog box, provide NTP Software Smart Policy Manager with a name for your organization and a location name for this NTP Software Smart Policy Manager instance, or accept the default settings. Click **Next**.



12. In the **Start Copying Files** dialog box, review your configuration information. Click **Back** to make any changes; otherwise, click **Next** to begin copying the files.

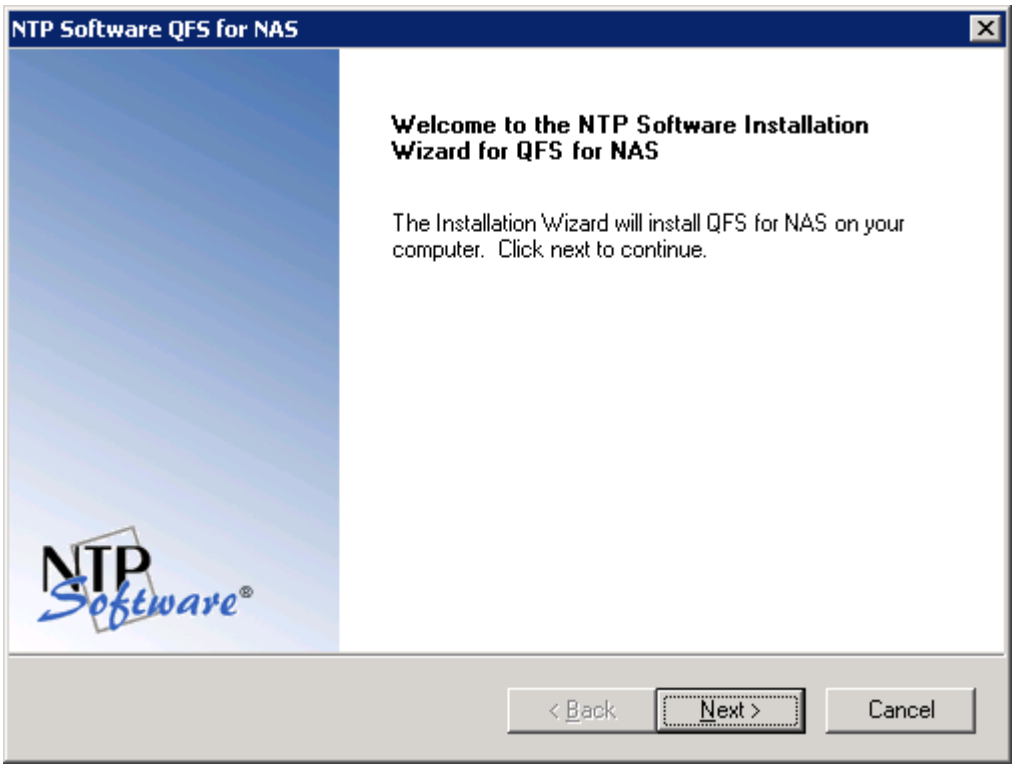


13. If you want to view the NTP Software Smart Policy Manager readme file, check the **Yes, I want to view the readme file** checkbox, and then click **Finish**.

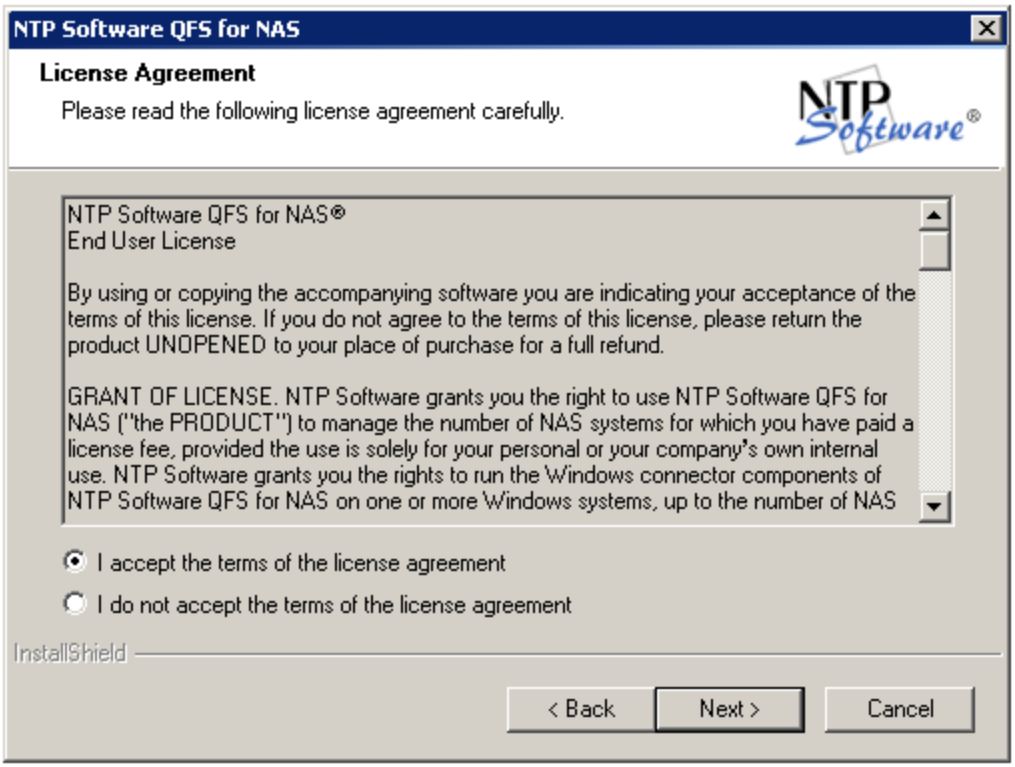


Installing NTP Software QFS for NAS

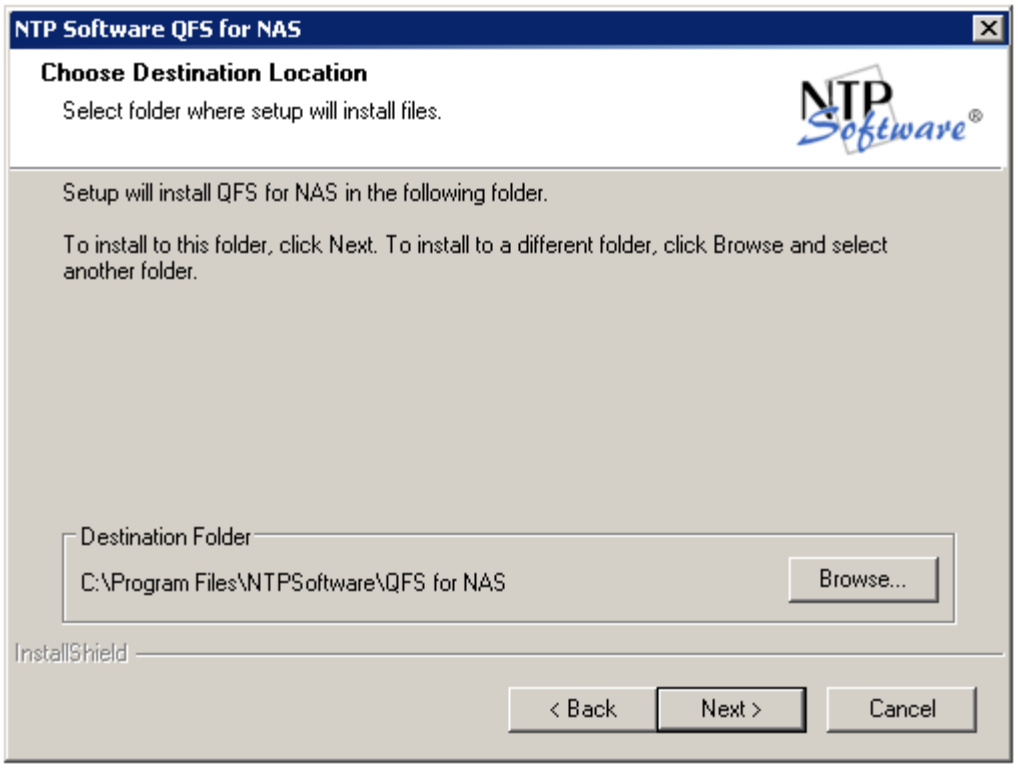
1. When the **NTP Software QFS for NAS** setup wizard opens, click **Next** to begin the installation.



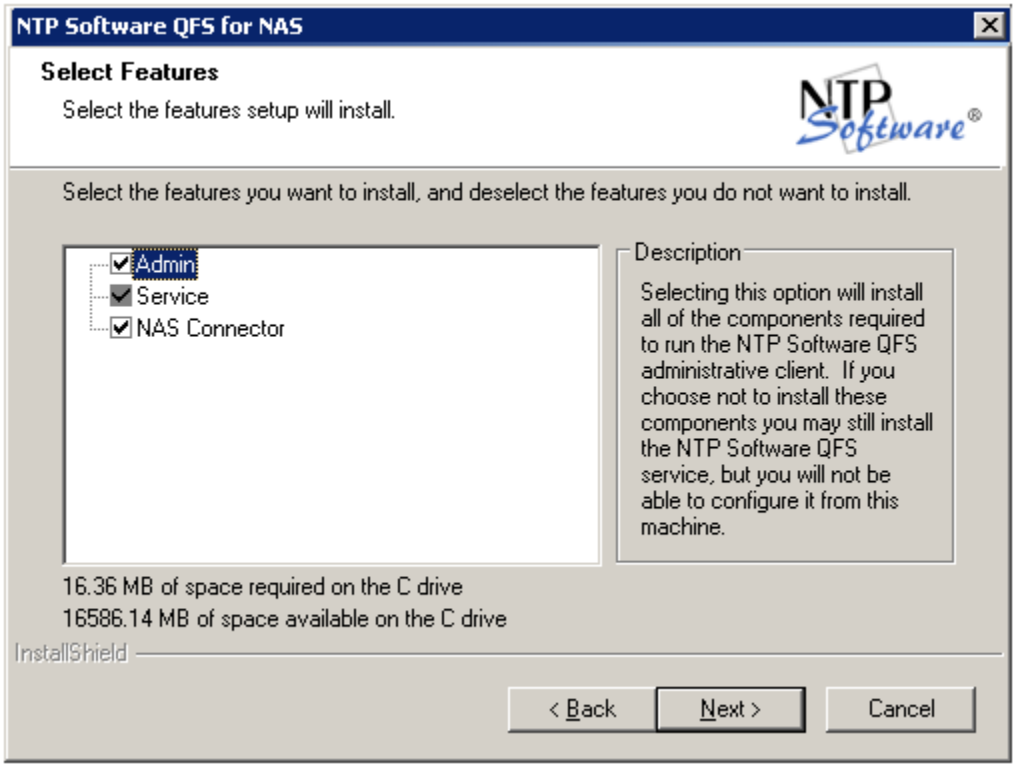
2. Read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



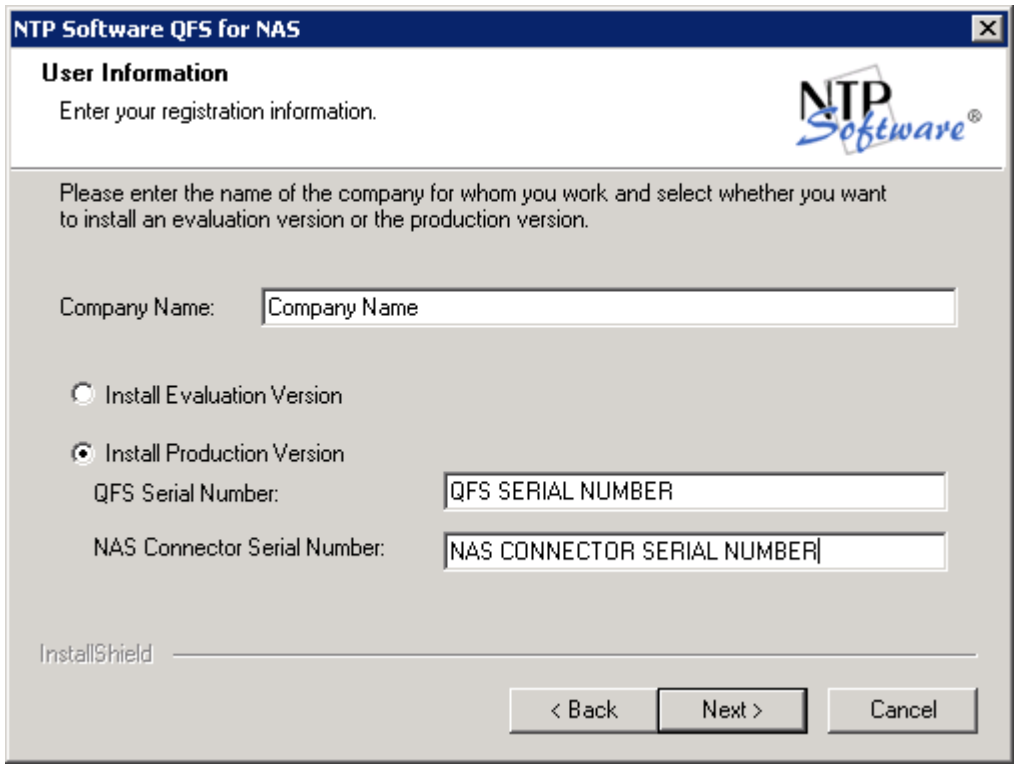
3. Choose the location where you want to install NTP Software QFS and then click **Next**.



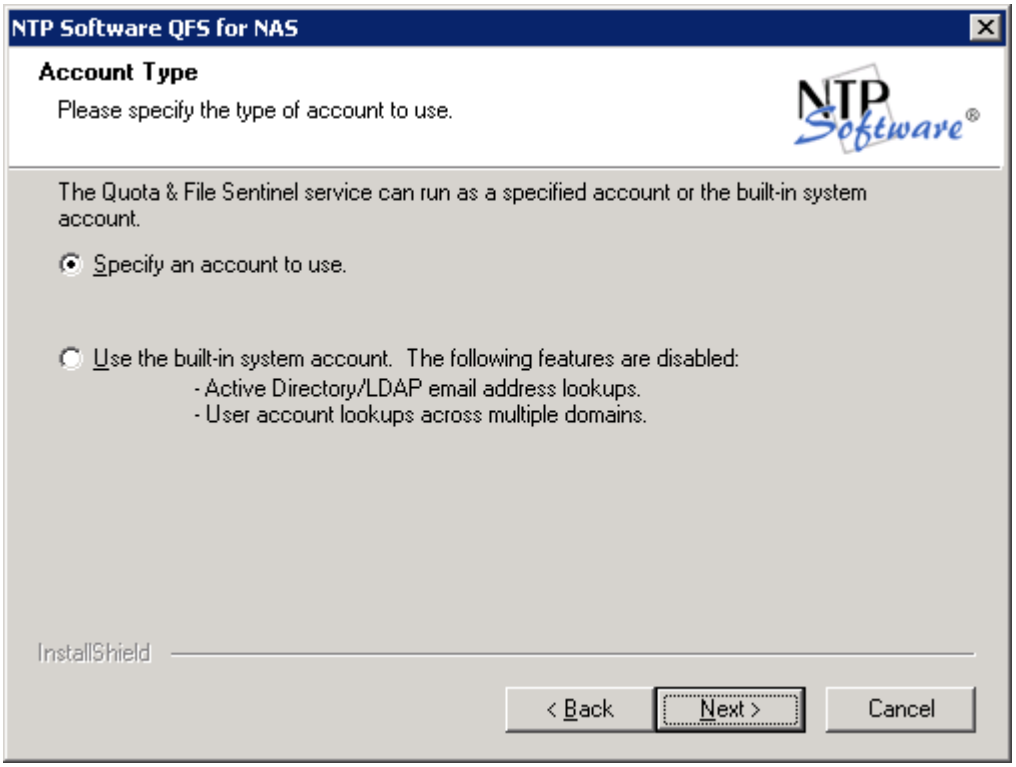
4. Select the components to be installed on the local machine. The Admin component allows administration of the NTP Software QFS service. The NAS Connector component is required if this machine will need to communicate with a Filer for quota management purposes.



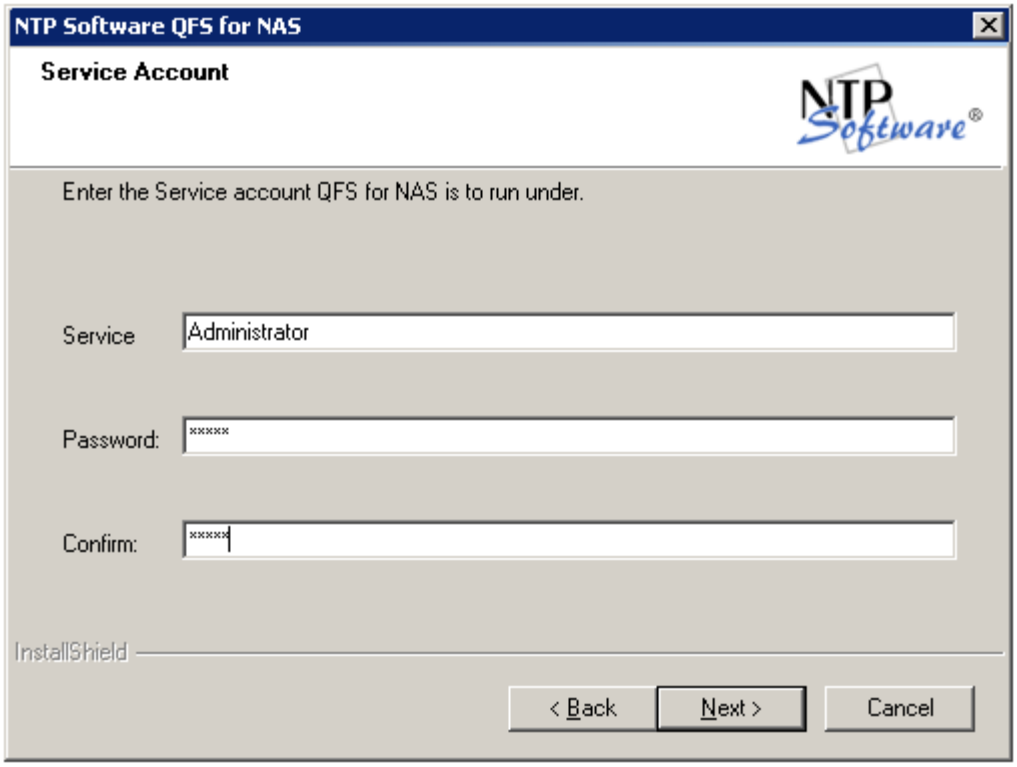
5. Provide your company name, the serial number for NTP Software QFS, and the serial number for the NAS Connector. Click **Next**.



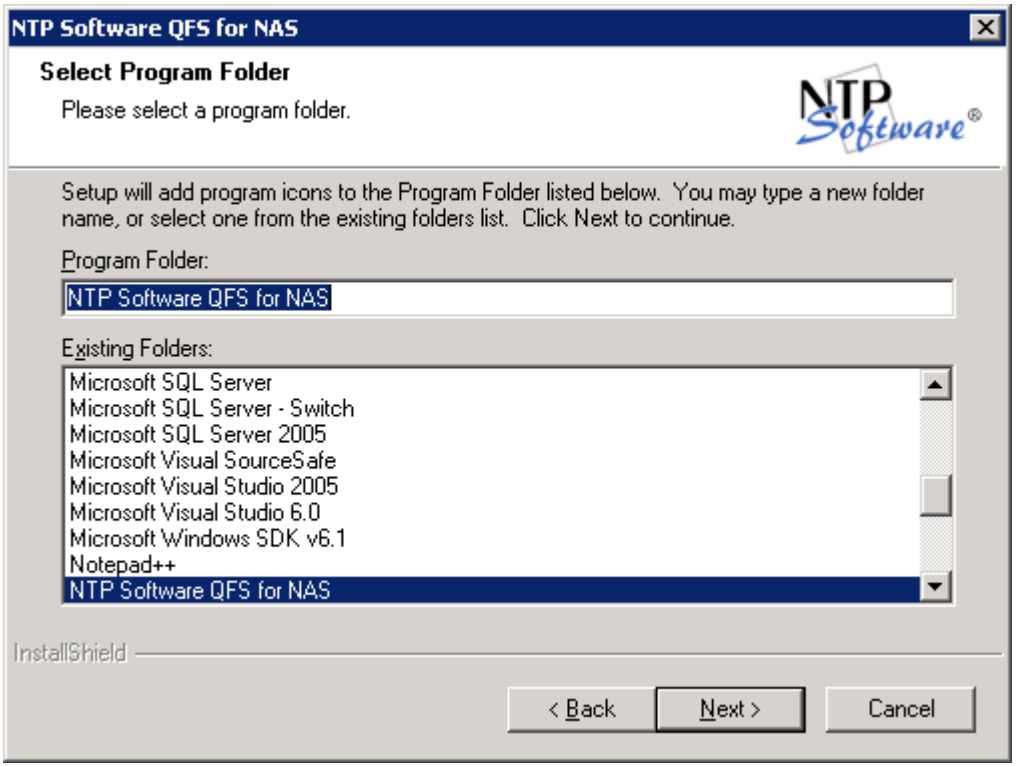
6. Specify the account type to be used. Click **Next**.



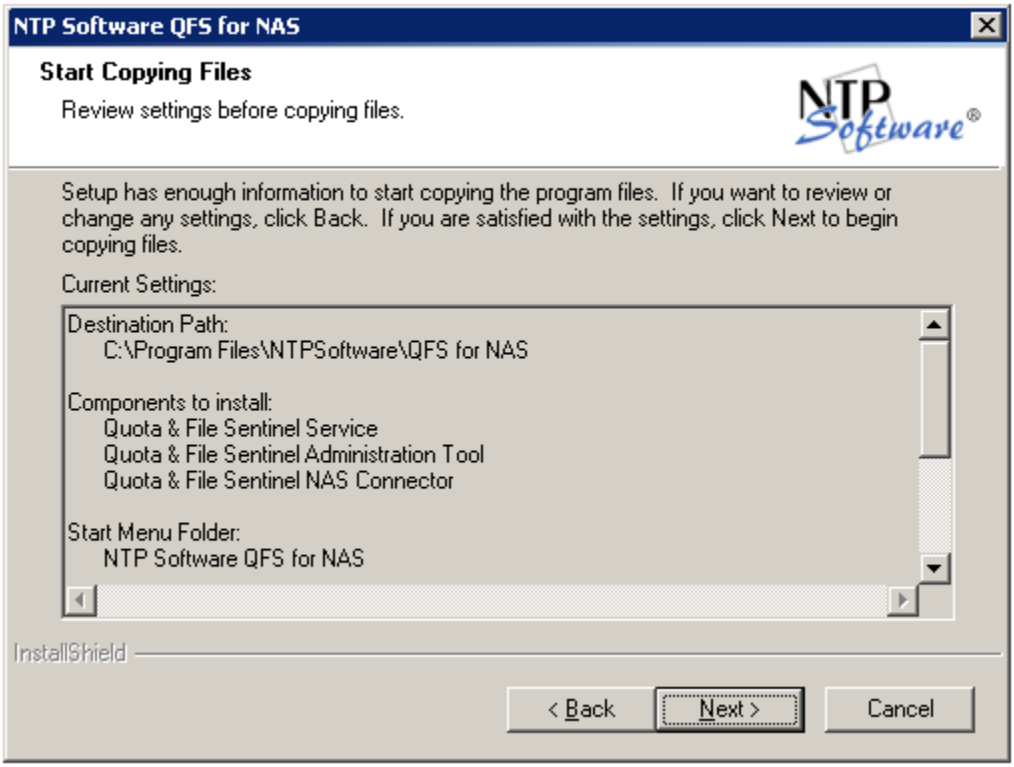
7. On specifying an account, enter a username with local administrative privileges. This account will be used to log on to and enforce quotas. Click **Next**.



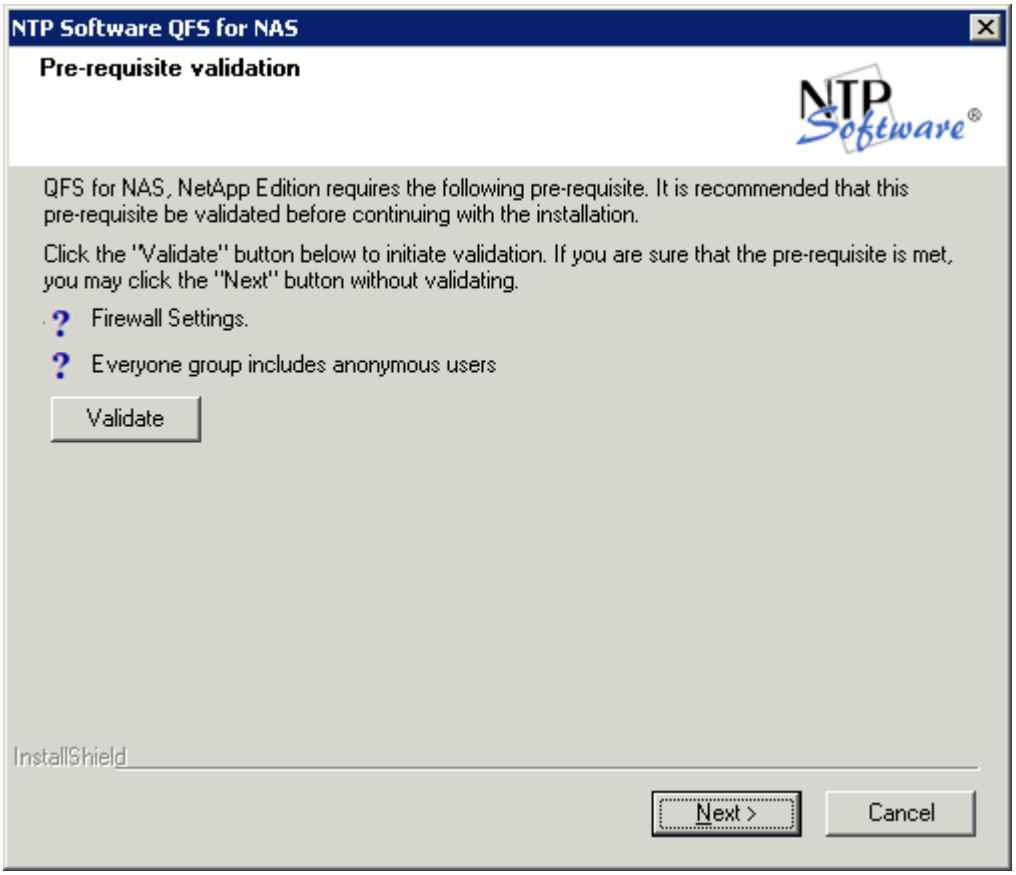
8. Specify an installation directory. Click **Next**.



9. Review your components and NAS connector information. Click **Back** to make any changes; otherwise, click **Next** to begin copying the files.



10. Click the **Validate** button to validate the **Firewall Settings** and **Everyone group includes anonymous users** pre-requisites. If you are sure that the prerequisite setting is met, you may click **Next** without running the validation.



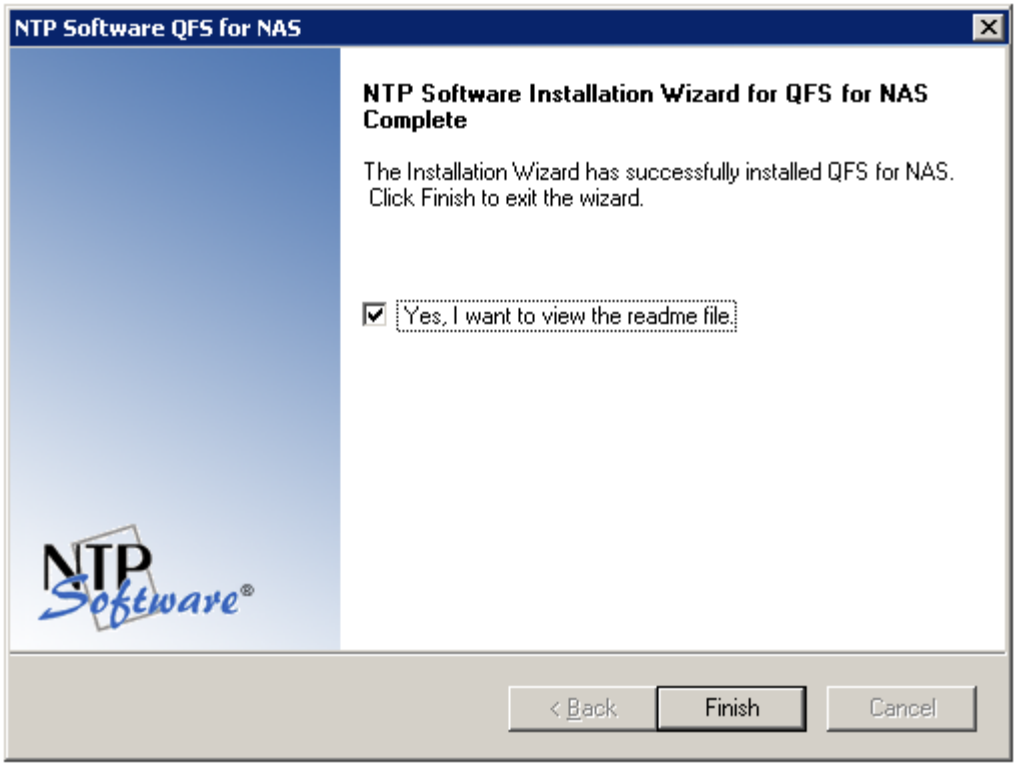
NOTES

- You can click the **Next** button without clicking the **Validate** button and thereby skipping the validation of the pre-requisites.
- If the **Validate** button is not clicked before clicking the **Next** button, a **Yes/No** warning message box will be displayed asking you either to proceed with the installation without validation or not. You are prompted to choose either Yes or No as follows:

  If **Yes** is clicked, you will be allowed to proceed to the next installer step.

  If **No** is clicked, you will be returned to the same installer step.
- If the **Validate** button is clicked, the pre-requisites will be validated
-

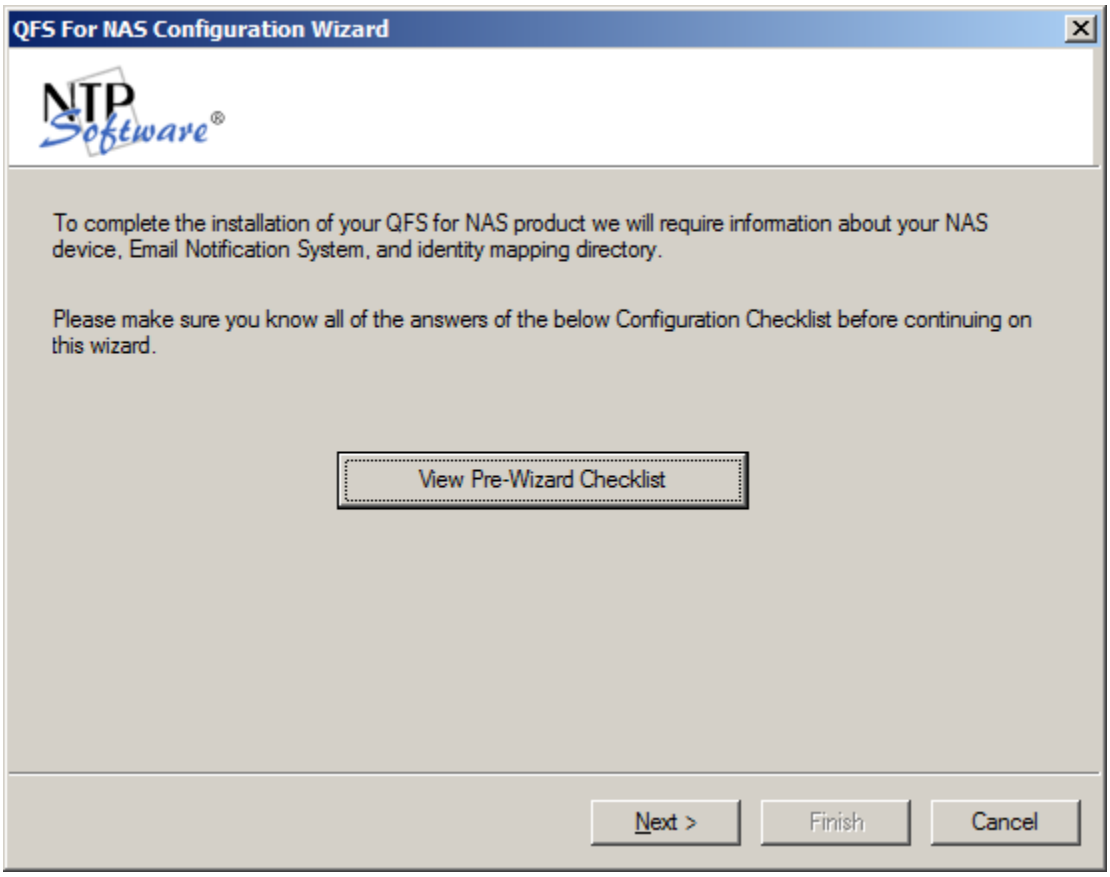
11. If you do not want to view the NTP Software QFS for NAS readme file, clear the **Yes, I want to view the readme file** checkbox. When you click **Finish**, the **NTP Software QFS for NAS, NetApp Edition configuration wizard** will open.



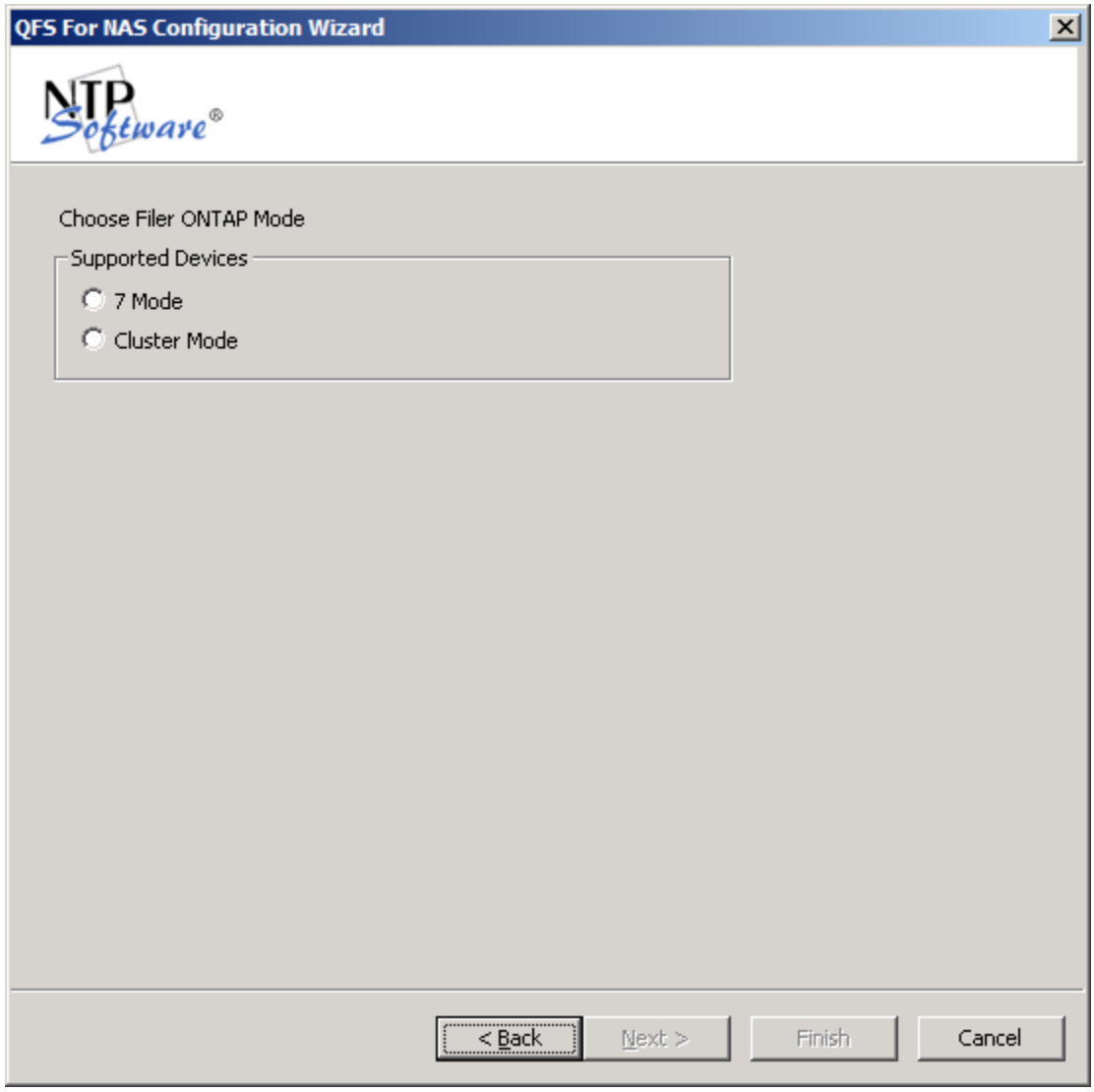
Using the NTP Software QFS for NAS Configuration Wizard

1. Click **Start** > **All Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Configuration Wizard.**

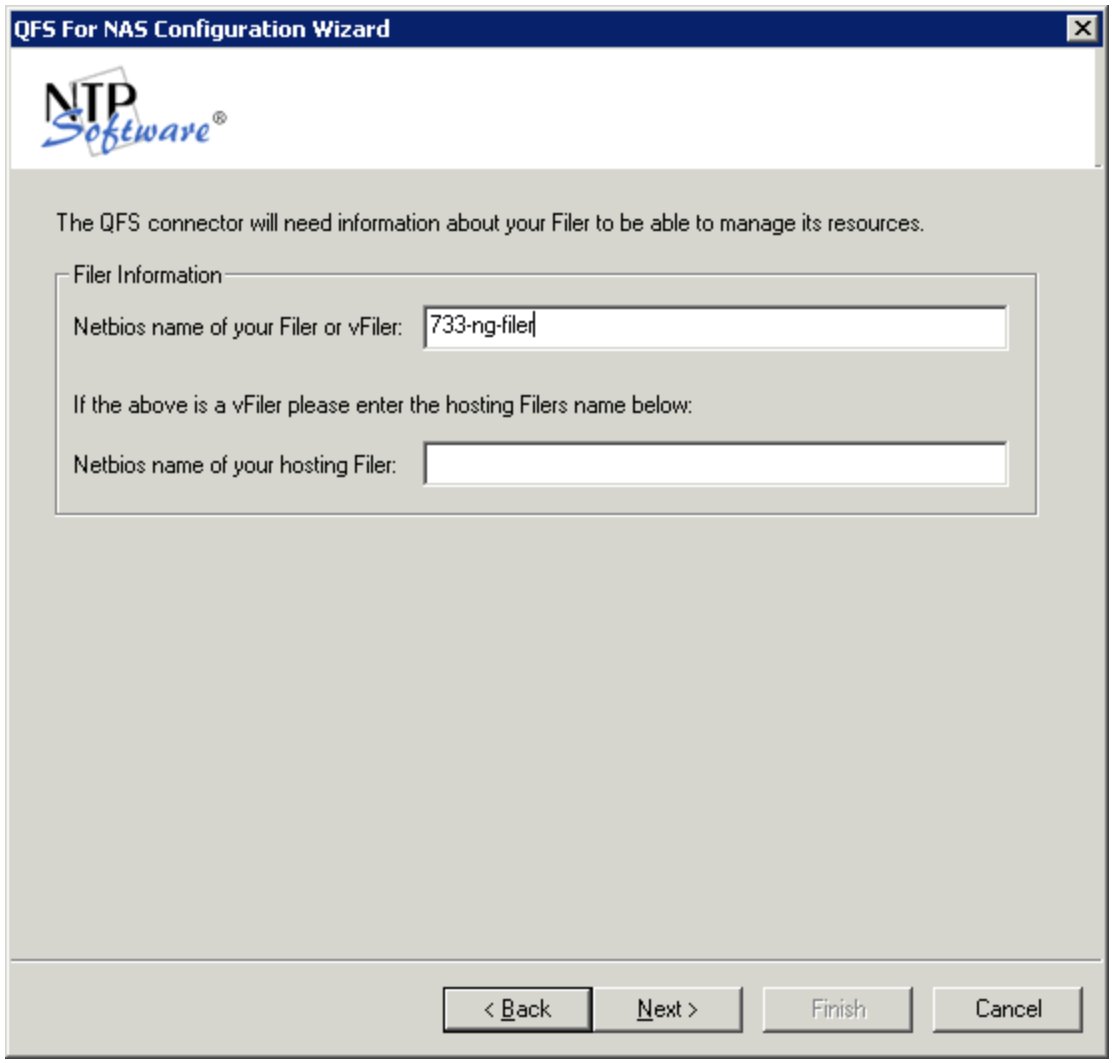
2. Click the **View Pre-Wizard Checklist** button and gather the required information before continuing. Click **Next**.



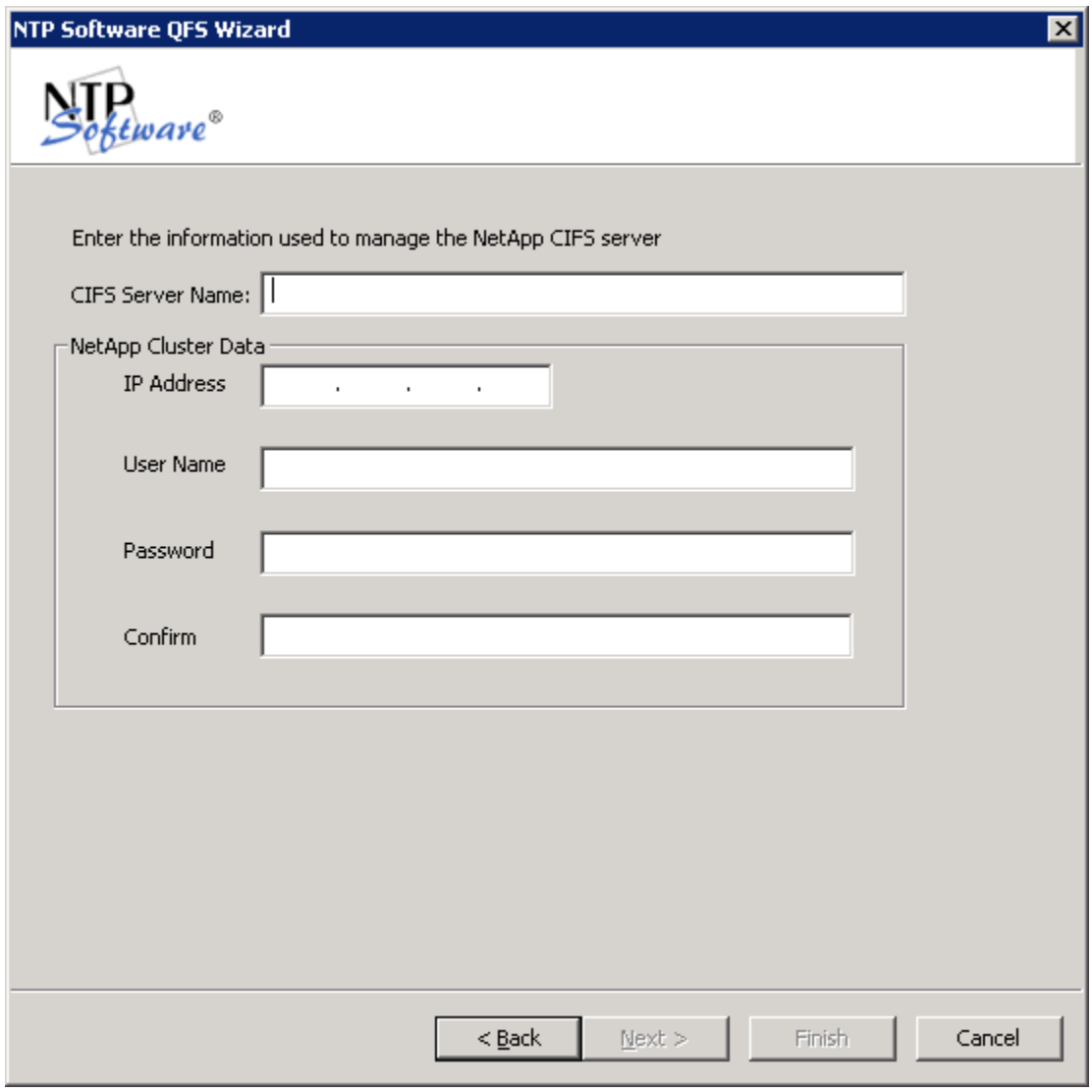
3. Choose the Filer ONTAP mode; click either **7-mode or cluster-mode**. Click **Next**.



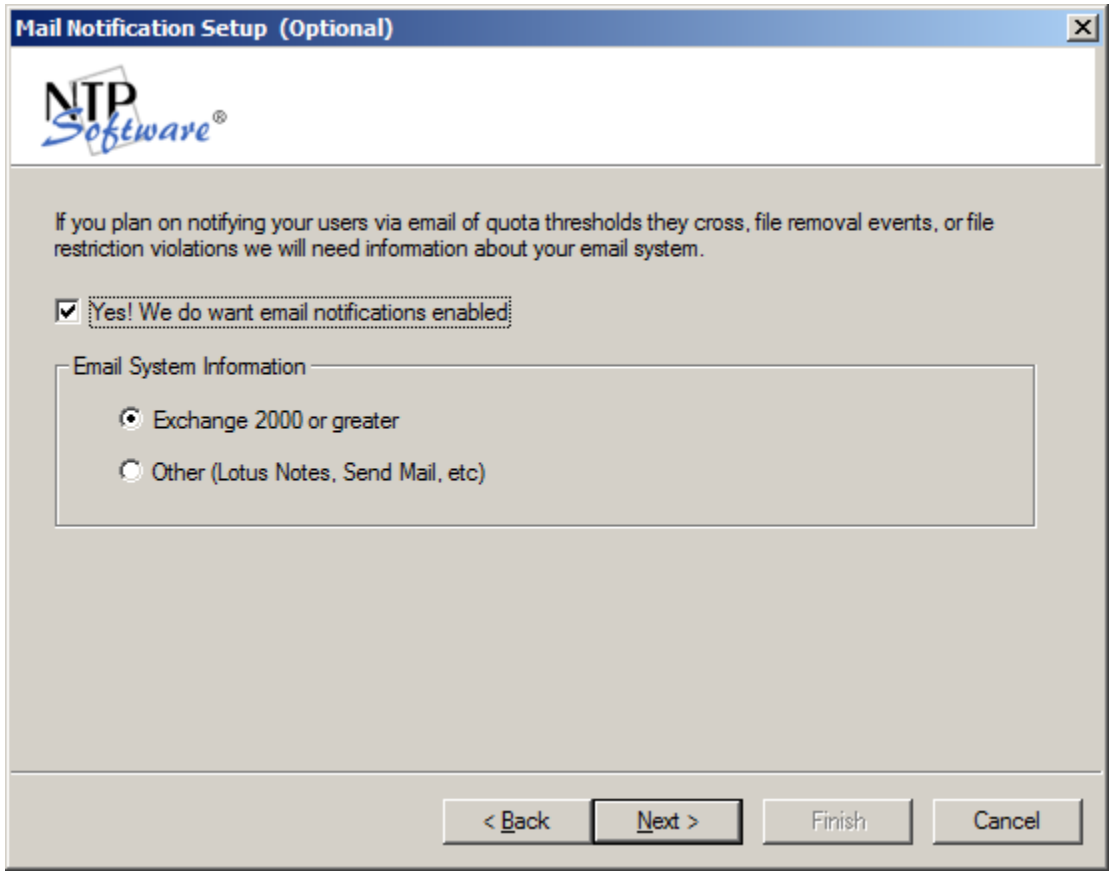
4. For 7-mode filers, enter the name of your Filer or vFiler in the first text box. If you're using a vFiler, enter the name of the hosting Filer in the second text box.



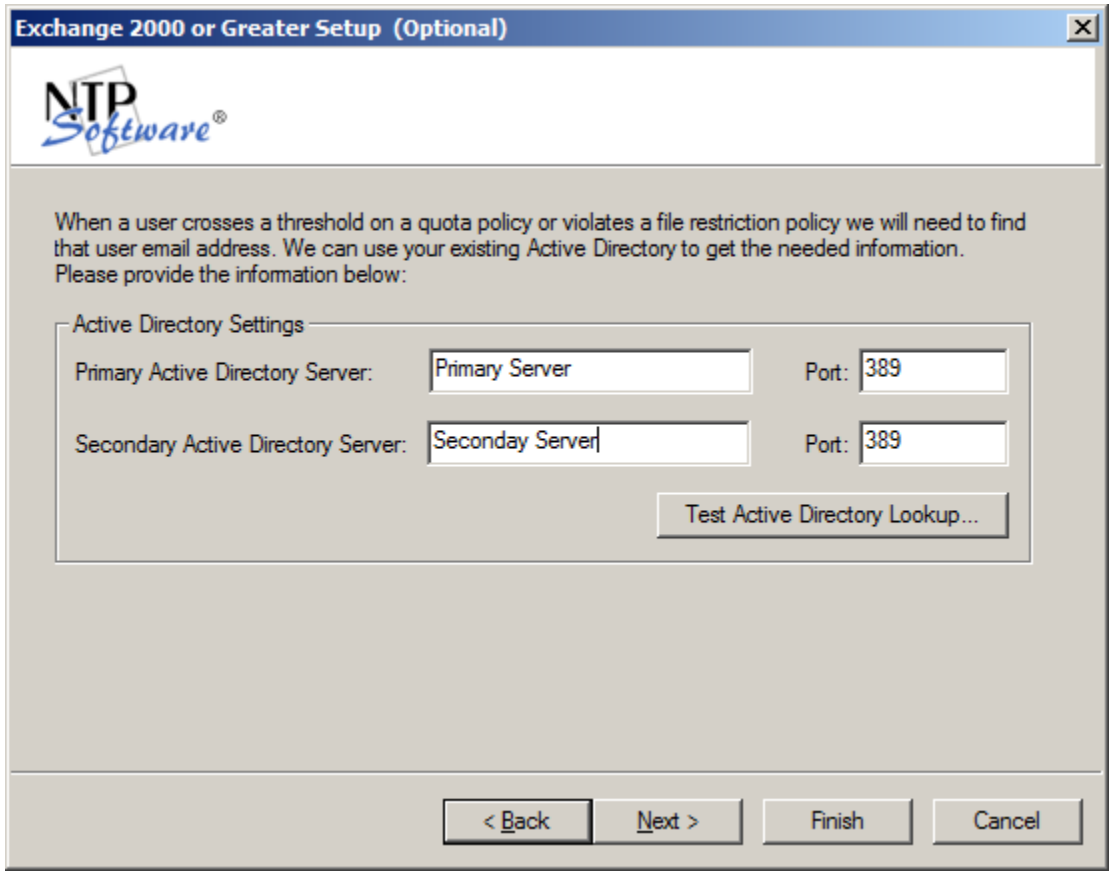
5. For cluster-mode filers, enter the name of your CIFS server, cluster IP address, user name and password for account on the cluster that has permission to execute some ONTAPI APIs required by QFS. For more details about that user account, please read the Appendix section about “Assign Permissions to User Account to Execute cDOT APIs”. Click **Next**.



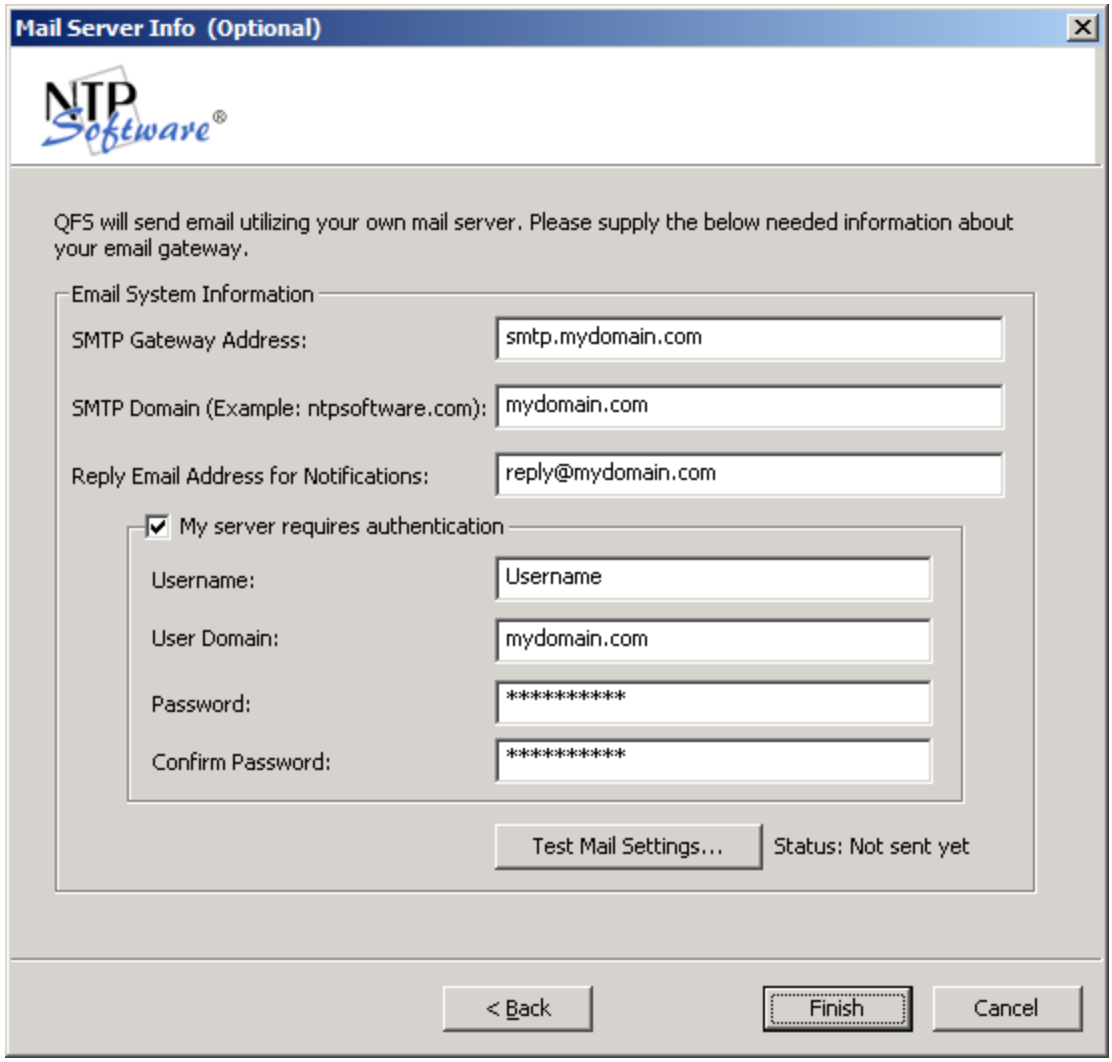
6. If you do not want to send email notifications to users when a quota status changes, clear the **Yes! We do want email notifications enabled** checkbox. Select which email system your environment uses. Click **Next**.



7. Enter the name of your Active Directory server. (Optional: 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**.



8. Enter the SMTP gateway, the SMTP domain, and the email address to use for notifications. If your SMTP server requires authentication, enter the required username, domain, password and confirm password to be used to authenticate with your SMTP server. Click **Test Mail Settings** to verify that the information is correct. Then click **Finish**.

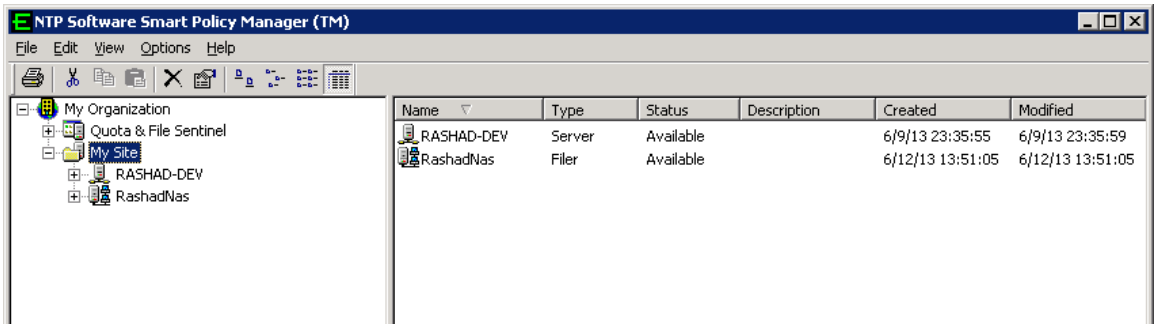


Adding the Filer to NTP Software QFS for NAS Admin

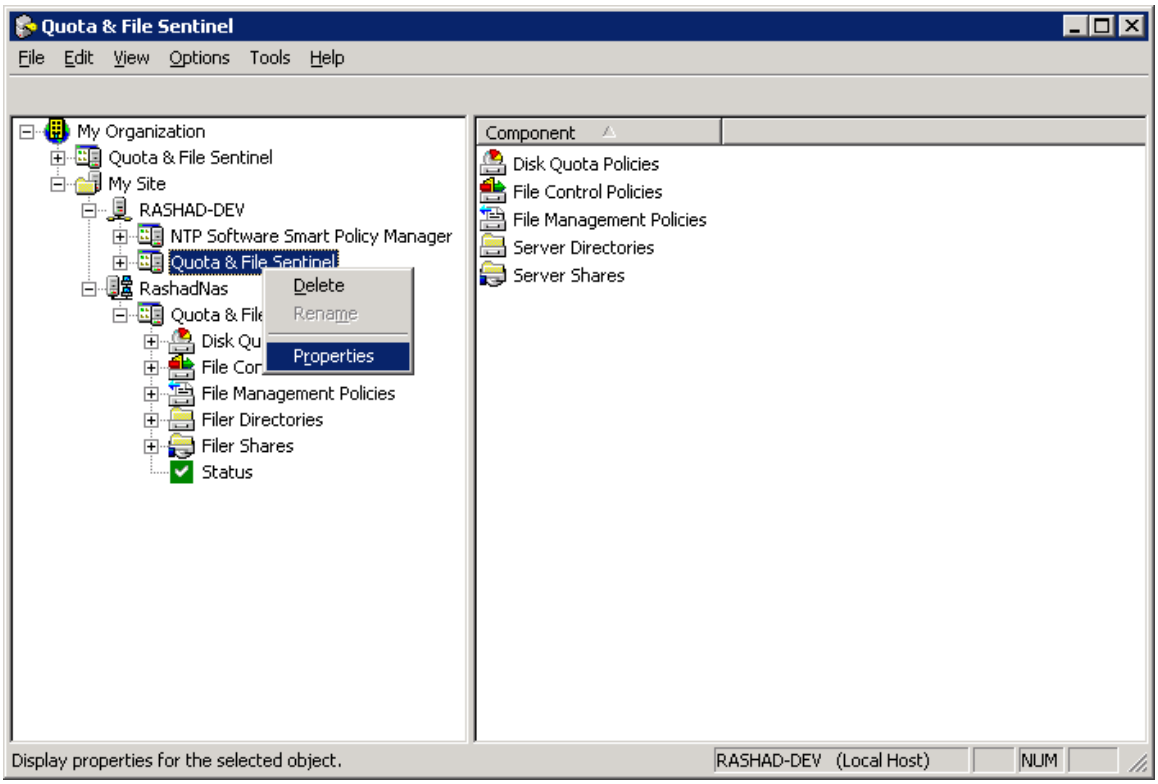
Before you can use NTP Software QFS for NAS, the Filer must be added to the NTP Software Smart Policy Manager hierarchy. Follow these steps to add the Filer:

1. Click **Start** > **All Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.

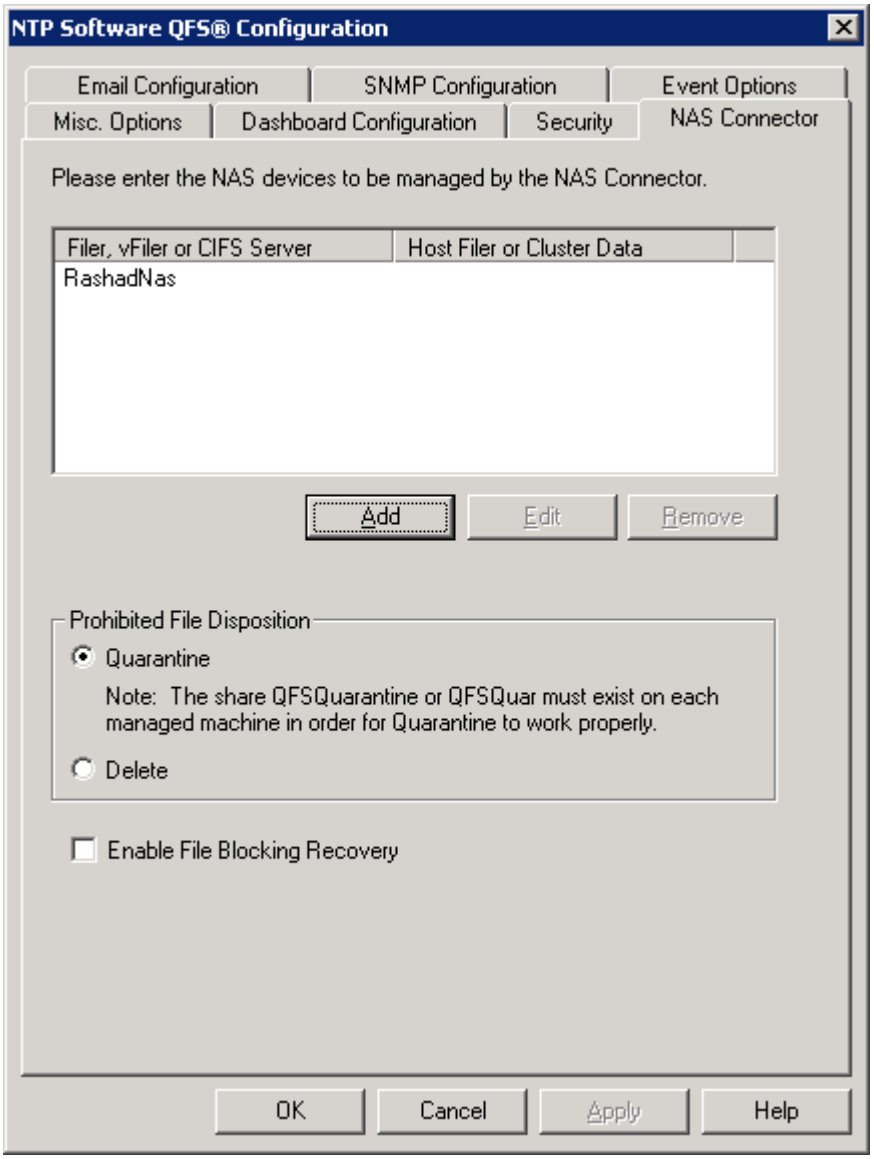
2. In the hierarchy presented, expand the location name you entered earlier. The default location is My Site. Your Filer is listed in the right pane, below the server on which NTP Software QFS is installed.



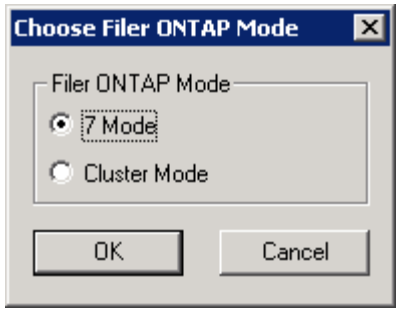
3. In the left pane, expand the server on which NTP Software QFS is installed and right-click **Quota & File Sentinel**. From the pop-up menu, choose **Properties**.



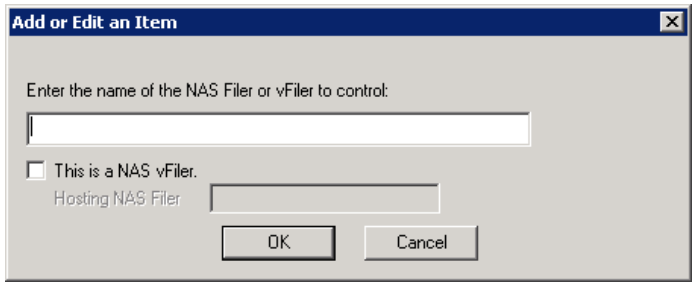
4. Click the **NAS Connector** tab. Your Filer should be listed; if it is not, click **Add**.



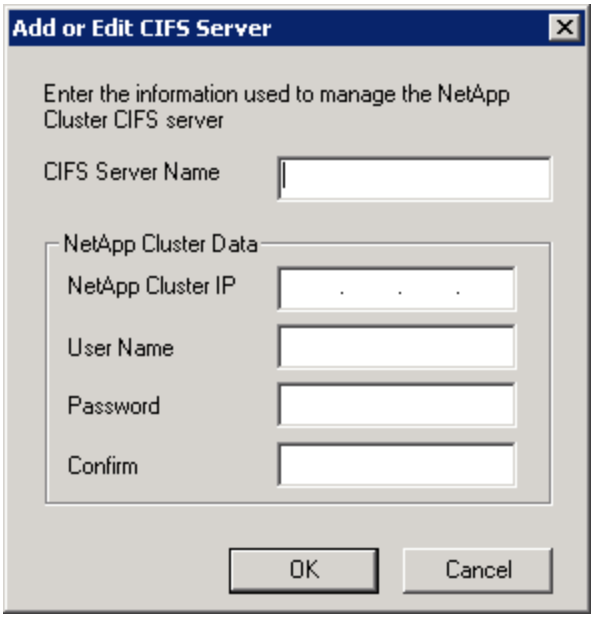
5. Choose Filer ONTAP mode; click 7-mode or cluster-mode. Click **Next**.



6. For 7-mode filers, enter the name of your Filer or vFiler. If you're using a vFiler, select the "**This is a NAS vFiler**" checkbox, then enter the Hosting NAS Filer name. Click **OK**.

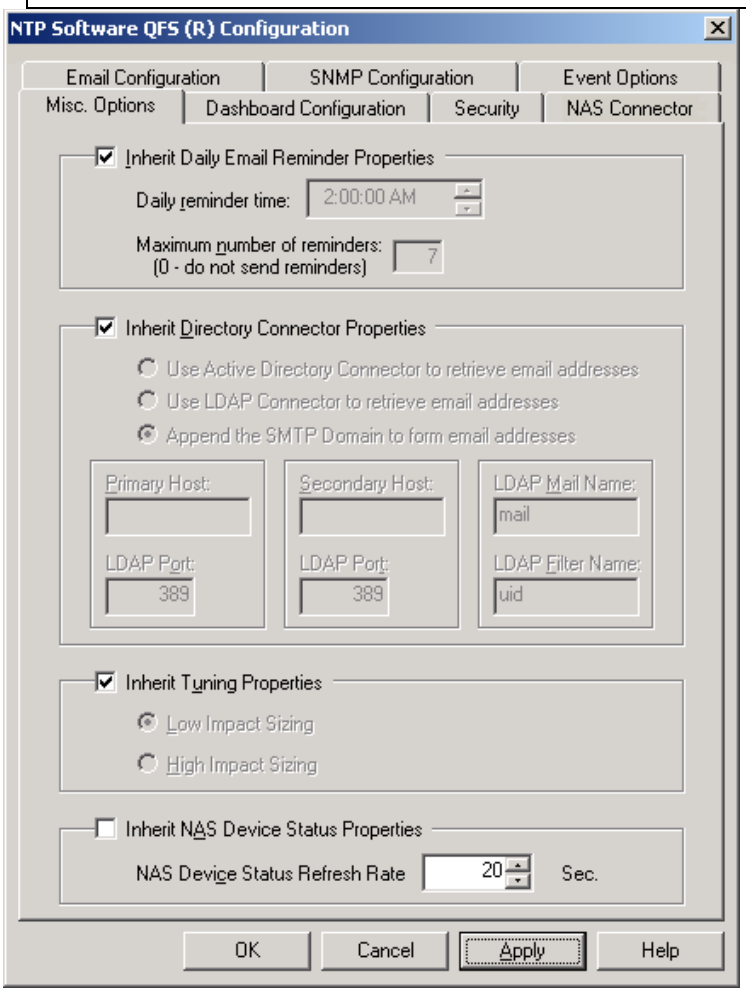


7. For cluster-mode filers, enter the name of your CIFS server, , cluster IP address, user name and password for account on the cluster that has permission to execute some ONTAPI APIs required by QFS. For more details about that user account, please read the Appendix section about “Assign Permissions to User Account to Execute cDOT APIs”. Click **Next**.



8. To configure the NAS device status refresh rate, click the **Misc**. **Options** tab in the **Quota and File Sentinel properties** dialog. The default refresh rate is 30 seconds while the minimum rate is 10 seconds and the maximum rate is 3600 seconds.

> **NOTE**: The refresh rate can be inherited from the global "Quota and File Sentinel" node in QFS hierarchy.



Verifying Registration with the Filer

To verify that the 7-mode Filer has been associated with NTP Software QFS, follow these steps:

1. Log on to the Filer.
2. Run **fpolicy** to view fpolicy settings.

   Your Filer and the associated policies should be displayed.

```
File policy NTPSoftware_QFS (file screening) is enabled.

File screen servers              P/S Connect time (dd:hh:mm)  Reqs    Fails
-------------------------------------------------------------------------------
 10.30.3.52      \\RASHAD-DEV     Pri    02:18:54                0        0

Operations monitored:
File open,File create,File rename,File close,File delete
Directory rename,Directory delete
 Above operations are monitored for CIFS only

List of extensions to screen:
 ???

List of extensions not to screen:
 Extensions-not-to-screen list is empty.
```

To verify that the cluster-mode Filer has been associated with NTP Software QFS, follow these steps:

1. Log on to the Filer.
2. Run **fpolicy show-engine –vserver *<vserver name of your managed CIFS server>*** to view fpolicy settings.

   The vserver name of your CIFS server and the associated policies should be displayed with **Server Status** appears as **connected**.

```
dev-tap82F-cm5::> fpolicy show-engine -vserver vs1-rashad74
  (vserver fpolicy show-engine)
                                  FPolicy           Server          Server
Vserver Policy Name   Node        Server            Status          Type
------- ------------- ----------- ----------------- --------------- -----------
vs1-rashad74                                        connected       primary
        NTPSoftware_  dev-tap82F-  10.20.2.121
        QFS           cm5-01
```

Appendix:

Enabling Data ONTAP fPolicy Management Service

A. In 7-Mode

Perform the following steps to enable the Data ONTAP fpolicy management service:

1. Log on to 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 NTP Software QFS to register with and manage your Filer. They must be completed before you try to configure NTP Software QFS. Later in this document, we will register a file policy server with the Filer. No further Filer administration is required.

B. In Cluster Mode

Perform the following steps to enable the Data ONTAP fpolicy management service:

1. Log on to the NetApp server with an account that has administrative privileges.
2. At the prompt, enter the following commands:

   fpolicy policy event create -vserver <*vserver name*> -event-name **NTPSoftware_QFSEVT** -protocol cifs -file-operations close, create, create_dir, rename, rename_dir, delete, delete_dir, read, write, open

   fpolicy policy external-engine create -vserver <*vserver name*> -engine-name **NTPSoftware_QFSENG** -primary-servers <*QFS connector machine IP addresses separated by comma*> -port <*unused dynamic port number*> -extern-engine-type synchronous -ssl-option no-auth

   fpolicy policy create -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -events **NTPSoftware_QFSEVT** -engine **NTPSoftware_QFSENG** -is-mandatory false -allow-privileged-access yes -privileged-user-name <*QFS connector service domain user account, in the format NetBiosName\UserName*>

   fpolicy policy scope create -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -shares-to-include "*" -volumes-to-include "*"

   fpolicy enable -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -sequence-number <*unused sequence number*>

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

   fpolicy show -vserver <*vserver name*>

NOTES:

- QFS will create and enable fpolicy automatically for the managed CIFS Server on the cluster-mode Filer using default sequence number 1. Since sequence number cannot duplicate.
- QFS will fail to enable fpolicy on cluster-mode Filer if the sequence number is used by another fpolicy on the same VServer.
- QFS will create a registry value named "***<CifsServerName>*_FPolicySeqNum**" inside the connector registry key, with default value 1. If QFS failed to enable fpolicy due to a redundant sequence number, then the user can configure this registry value to any unused sequence number, and run the **Diagnose** process on the managed CIFS server from QFS Admin (on the CIFS server Status node).
- The **Diagnose** process will try to enable the fpolicy automatically using the new sequence number configured in registry.

Assign Permissions to User Account to Execute cDOT APIs

In order to manage CIFS server on a cDOT filer, you need to provide user name and password for a Unix user on the cDOT filer with specific permissions. The following steps show how to create a Unix user on the cDOT filer, and how to assign this user account the required permissions to manage CIFS servers on that cDOT filer:

1. Create Unix user on the cDOT filer:
   - unix-user create -vserver *<vserver name>* -user *<user name>* -id *<user id>* -primary-gid *<primary group id>* -full-name *<user full name>*
2. Create the required role that contains the required permissions:

   Note: The role name specified in all of the following commands must be the same, in order to assign this one role at the end to the Unix user you just created by the command above.

   - security login role create -role *<role name>* -cmddirname "network interface show" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "version" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "volume show" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "vserver show" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "vserver cifs show" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy policy" -access all -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy show-engine" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy show" -access readonly -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy enable" -access all -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy disable" -access all -query ""
   - security login role create -role *<role name>* -cmddirname "vserver fpolicy engine-connect" -access all -query ""
   - security login role create -role *<role name>* -cmddirname "vserver name-mapping" -access all -query ""

- security login role create -role *<role name>* -cmddirname "vserver services unix-user show" -access readonly -query ""

3. Assign the role you created in step #2 to the user you created in step #1:

   - security login create -username *<user name>* -application ontapi -authmethod password -role *<role name>*

   Note: When you execute the command above, the filer will ask you to enter, and confirm, a password for that user. The password you enter here will be used along with the user name in QFS Admin/Wizard UI, when you are adding the CIFS server to be managed by QFS.

About NTP Software

NTP Software is the leading worldwide provider of software solutions for controlling file data across a global infrastructure or at a single site with individual systems. NTP Software delivers a single solution across the entire data storage environment all the way down to the individual user and supports most popular file data storage models and brands. NTP Software products reduce the cost and complexity associated with the exponential growth of unstructured data. NTP Software has been chosen to control file data for the majority of Fortune 1000 companies and thousands of customers in private and public sectors by providing leadership through superior products, services, and experience.

NTP Software Professional Services

NTP Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your NTP Software Representative at 603-622-4400.

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 installation guide is for informational purposes only. NTP SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

NTP Software and other marks 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 products and technologies described in this document may be protected by United States and/or international patents.

NTP Software

119 Drum Hill Road #383

Chelmsford, MA 01824

Phone: 1-603-622-4400

E-mail: info@ntpsoftware.com

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