



DefendX Software Control-Audit for NetApp Installation Guide

Version 5.1

This guide provides a short introduction to the installation and initial configuration of DefendX Software Control-Audit™ for NAS, NetApp® Edition, from an administrator's perspective. Upon completion of the steps within this document, DefendX Software Control-Audit for NAS, NetApp Edition will be installed within your enterprise community.



Table of Contents

Executive Summary.....	3
Preparing the NetApp Filer	4
Requirements	6
Server Requirements.....	6
NetApp Filer Requirements.....	7
Before You Begin	7
Installation	8
Installing DefendX Software Smart Policy Manager	8
Installing DefendX Software Control-Audit for NAS, NetApp Edition.....	16
Installing DefendX Software Control-Audit Reports	25
Configuring Control-Audit Reports Website Security	33
Using the Configuration Wizard	44
Adding the Filer to DefendX Software Control-Audit for NAS Admin	49
About DefendX Software	52
DefendX Software Professional Services	52
Legal & Contact Information	53

Executive Summary

Thank you for your interest in DefendX Software Control-Audit™ for NAS, NetApp® Edition. DefendX Software Control-Audit monitors file and directory operations for users. DefendX Software Control-Audit for NAS, NetApp Edition extends our best-of-breed technology to include the NetApp family of products, allowing you to manage NAS-hosted storage as a seamless whole.

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

To be monitored by DefendX Software Control-Audit, version 6.5 or later (excluding version 7.1) of the Data ONTAP® operating system is required on the Filer. DefendX Software Control-Audit for NAS, NetApp Edition can be used to monitor NetApp Filers, vFilers®, and NetApp clusters or any combination of these systems. DefendX Software Control-Audit imposes no restrictions on how you organize or manage your storage. You can monitor file operations on individual paths, directories, and/or shares.

To install DefendX Software Control-Audit, a login with administrator rights is needed. You will be installing three different services: the DefendX Software Smart Policy Manager™ service, the DefendX Software Control-Audit service, and the NAS connector service.

The DefendX Software Smart Policy Manager service should be installed with a domain user account as its service account. The DefendX Software Control-Audit 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.

Preparing the NetApp Filer

DefendX Software Control-Audit for NAS, NetApp Edition requires the NetApp Filer to run Data ONTAP version 6.5 or later (excluding version 7.1). If your Filer is not running version 6.5 or later, you must upgrade your operating system before you proceed. (Please refer to your NetApp documentation for instructions.)

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

Although DefendX Software Control-Audit does not install any components on the NetApp server, you will need to enable the Data ONTAP fpolicy management service. Follow these steps:

1. Log on to the NetApp server with an account that has administrative privileges.
2. At the prompt, enter the following command: `fpolicy create DefendXSoftware_Control-Audit screen`
3. To verify that CIFS file policies are now enabled, enter the following command: `fpolicy`
4. If you want Control-Audit to record permission and owner changes for your files and directories, you will need to enable CIFS SetAttr feature of fpolicy, enter the following command:

```
fpolicy options DefendXSoftware_Control-Audit cifs_setattr on
```

Note: If you don't have any Control-Audit Policy that monitors *Permission Change* or *Owner Change* events, then you should disable CIFS SetAttr feature.

These steps create the configuration that allows DefendX Software Control-Audit to register with and manage your Filer. They must be completed before you try to configure DefendX Software Control-Audit for NAS, NetApp Edition.

NOTE: In case DefendX Software Control-Audit 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 DefendX Software Control-Audit.

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

1. Go to http://filename/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 DefendX Software QFS server machine and then click **OK**.
5. On the **Manage Hosts File** page, click the **Apply** button.

Requirements

Server Requirements

DefendX Software Control-Audit 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:

- 1 GHz CPU
- Windows Server 2008 or Later
- 1 GB RAM
- 150 MB free disk space
- Network interface card
- Internet Explorer version 6 or Later or Firefox version 2.x or Later
- IIS version 6 or 7
- Microsoft SQL Server 2005 or Later

NOTE: SP3 is recommended to be used if MS SQL server 2005 is the database server.
--

- SQL Server Reporting Services 2005 or later
- Microsoft .NET Framework 2.0
- ASP.NET AJAX 1.0
- Microsoft Report Viewer 2005 SP1 (installed along with the Report Pack)

NOTES:

The Remote Connection to the SQL Server should be enabled.

The SQL Server user should have db_datareader and execute permissions on the Control-Audit database.

The Reporting Service on the database server must grant access to the currently logged Windows user while installing the application.

NetApp Filer Requirements

The NetApp Filer to which DefendX Software Control-Audit for NAS, NetApp Edition will be connected requires the following:

- Data ONTAP v. 6.5 or later (excluding version 7.1)
- 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.

Before You Begin

Before running DefendX Software Control-Audit for NAS NetApp Edition installer, make sure you have the following ready for a smooth installation:

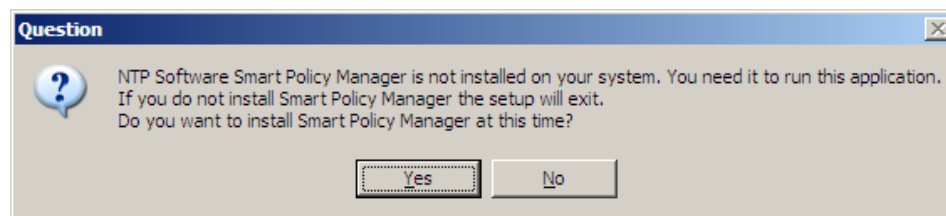
1. The Microsoft SQL Server user name and password for authentication.
2. Access to server/Filer.
3. The license key you were given when you purchased the Control-Audit product.

Installation

Prior to installing DefendX Software Control-Audit for NAS, NetApp Edition, DefendX Software recommends verifying that the installation server meets the requirements listed in the *Requirements* section of this document.

Installing DefendX Software Smart Policy Manager

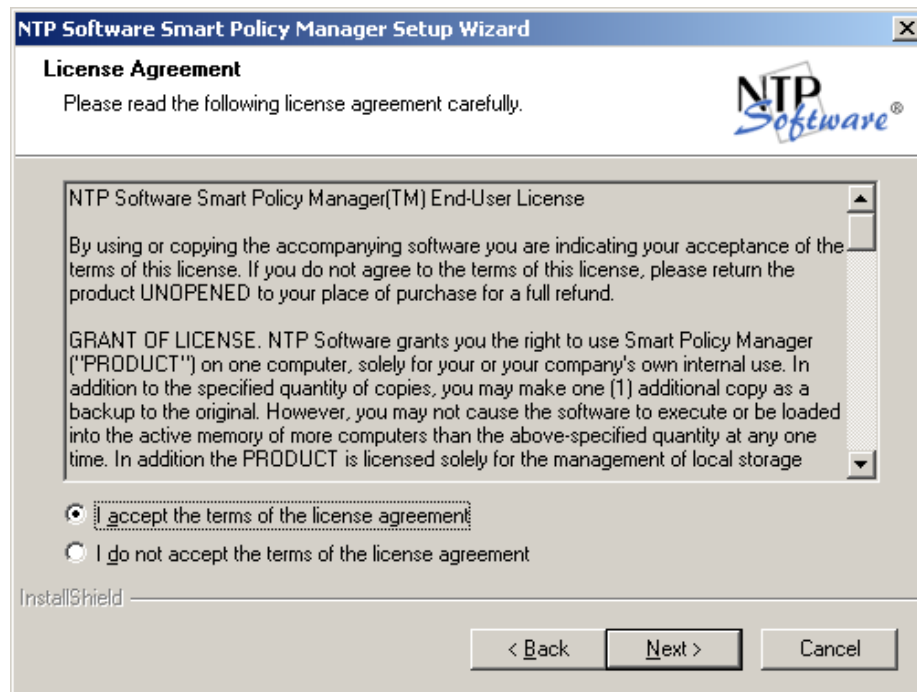
1. Log on to your server by using an account with administrator privileges.
2. Run the DefendX Software Control-Audit installer. If DefendX Software Smart Policy Manager is not installed, the following installer will launch automatically. If DefendX Software Smart Policy Manager is installed, you can skip to the section on *Installing DefendX Software Control-Audit for NAS, NetApp Edition*.



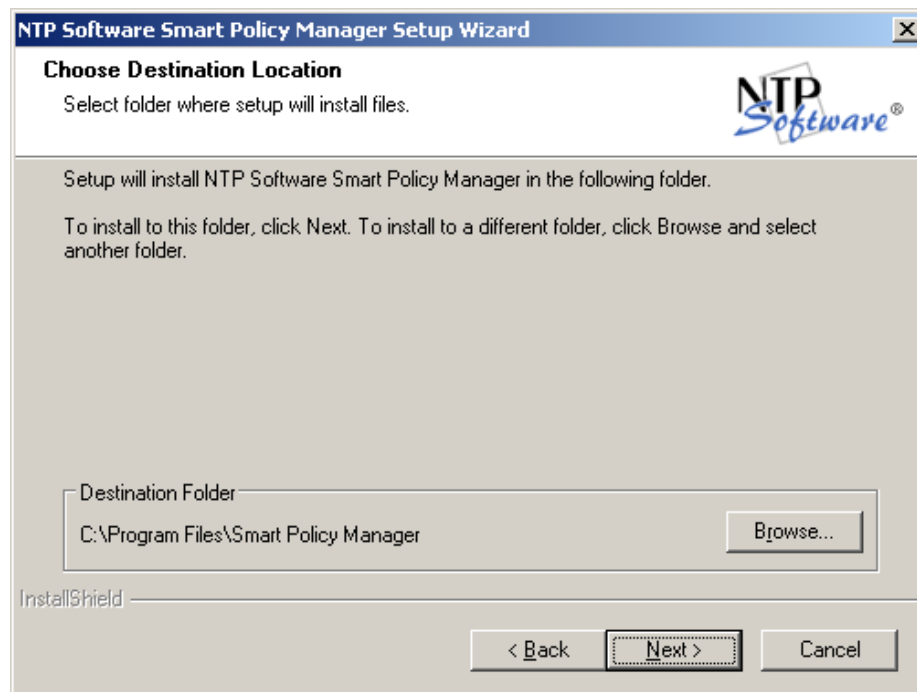
3. The DefendX Software Smart Policy Manager Installation Wizard opens. Click **Next** to begin the installation.



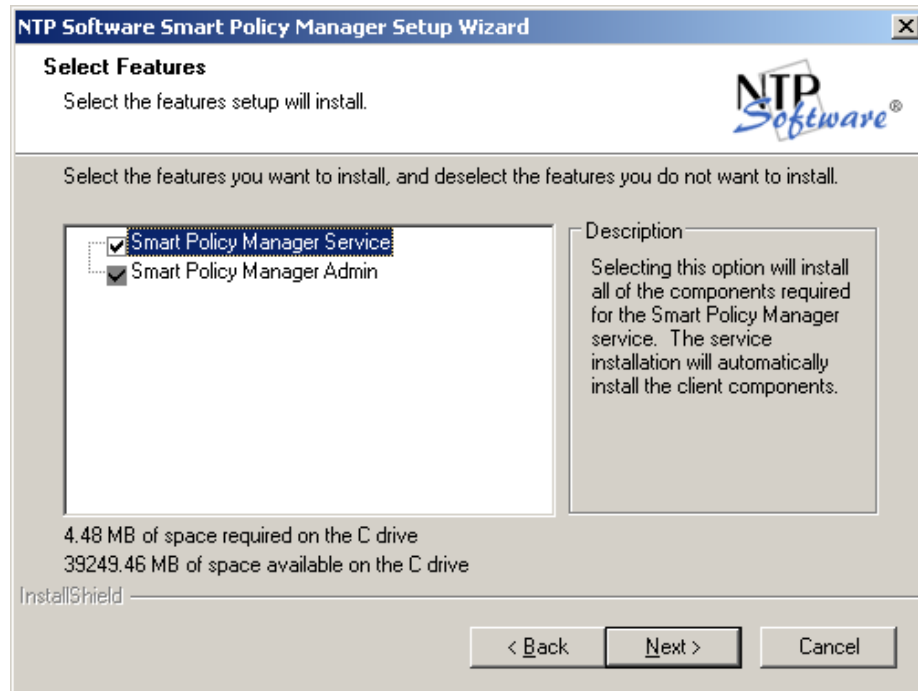
4. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



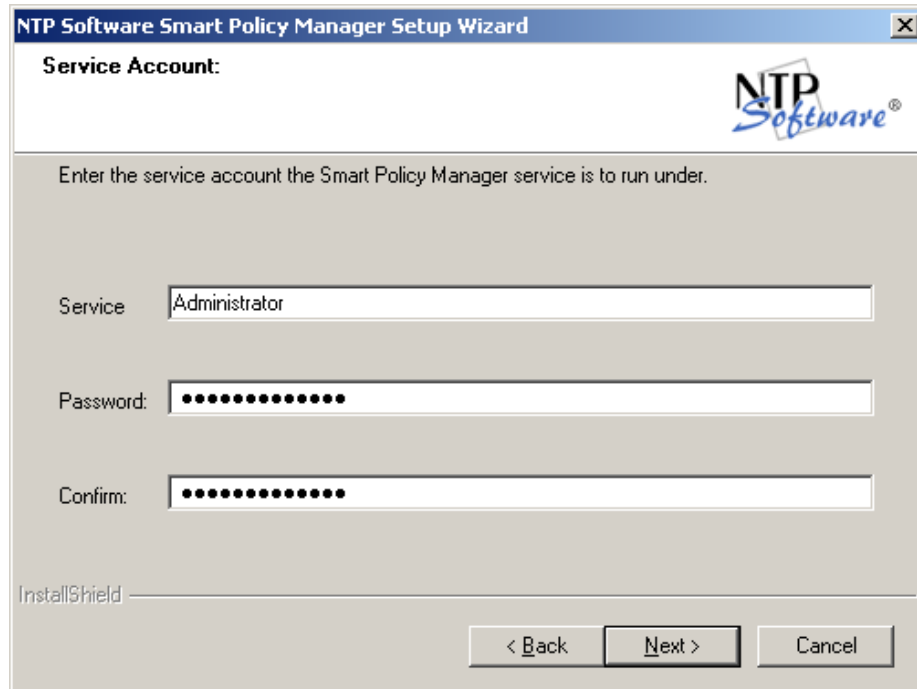
5. In the **Choose Destination Location** dialog box, click **Browse** to choose the location where you want to install DefendX Software Smart Policy Manager and then click **Next**.



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

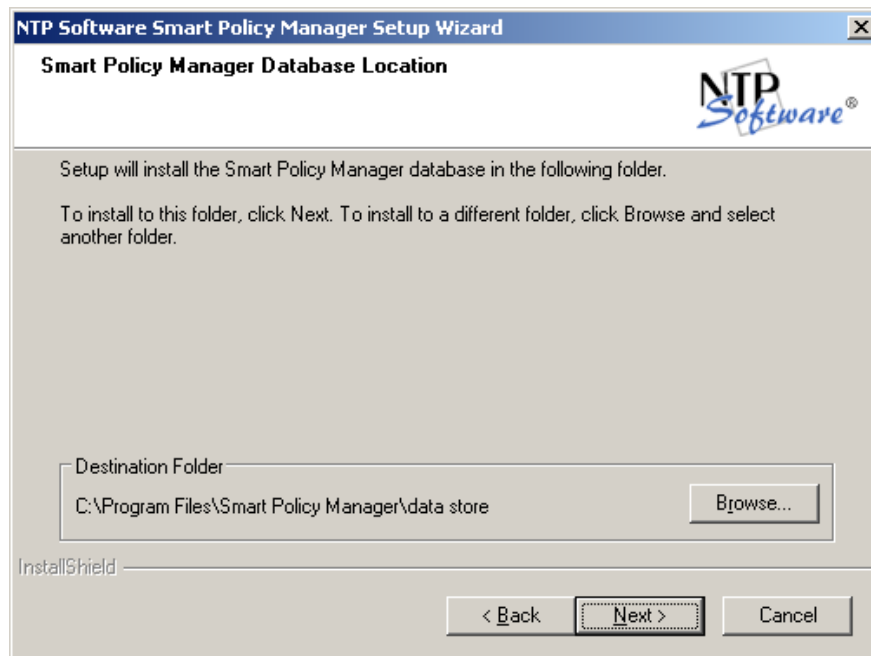


7. In the **Service Account** dialog box, when prompted for a Windows domain user account to run the DefendX Software Smart Policy Manager service, enter the username and password for a domain user account with administrative rights on the local machine. Click **Next**.

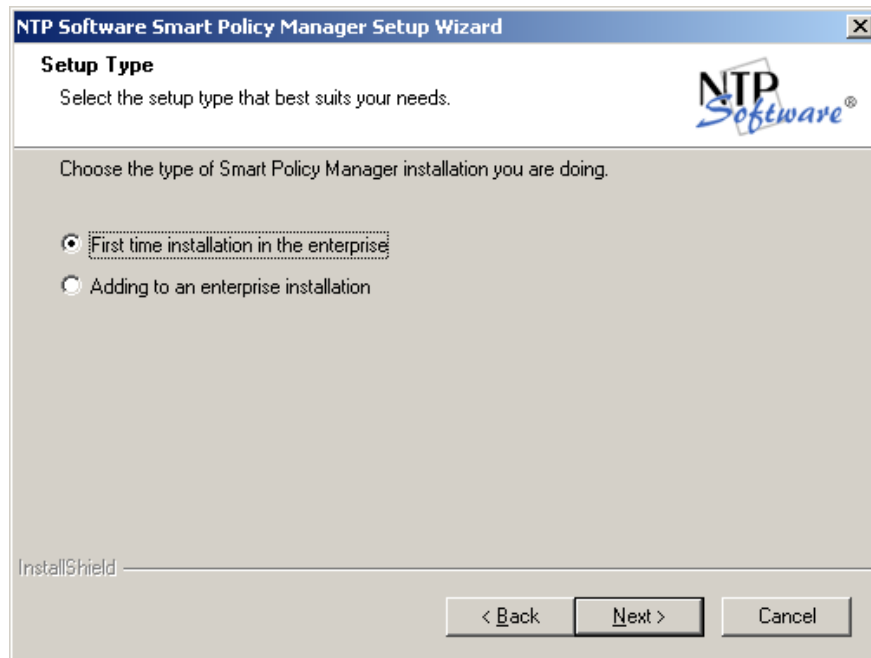


The image shows a Windows-style dialog box titled "NTP Software Smart Policy Manager Setup Wizard". The main heading is "Service Account:". Below this, there is a sub-heading "Enter the service account the Smart Policy Manager service is to run under." followed by the NTP Software logo. The dialog contains three input fields: "Service" with the text "Administrator", "Password:" with masked characters, and "Confirm:" with masked characters. At the bottom left, there is a label "InstallShield" followed by a horizontal line. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

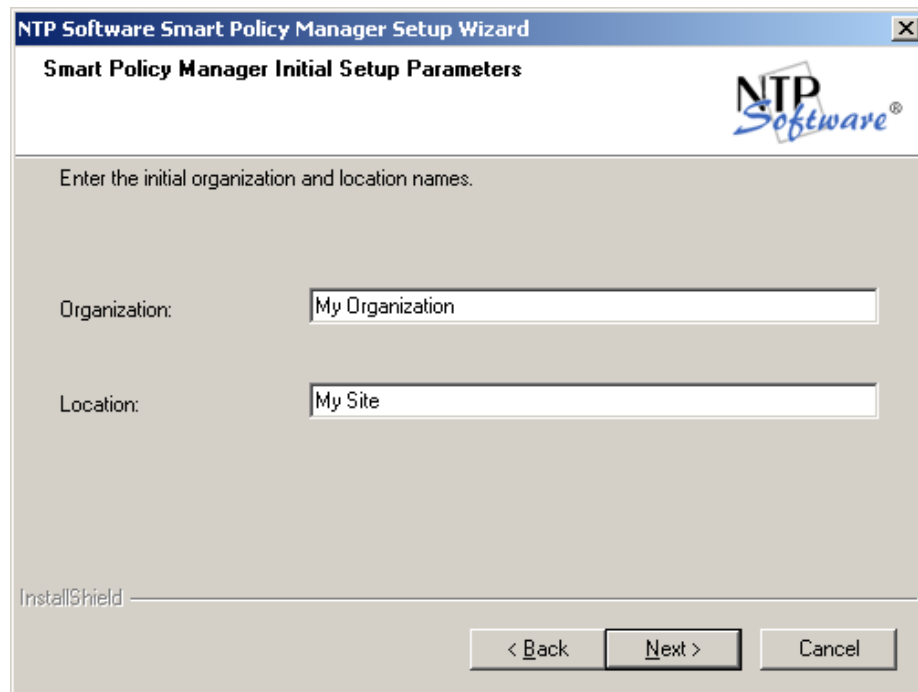
8. In the **Smart Policy Manager Database Location** dialog box, enter the directory name where you want to install the DefendX Software Smart Policy Manager database or just accept the default location. Click **Next**.



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

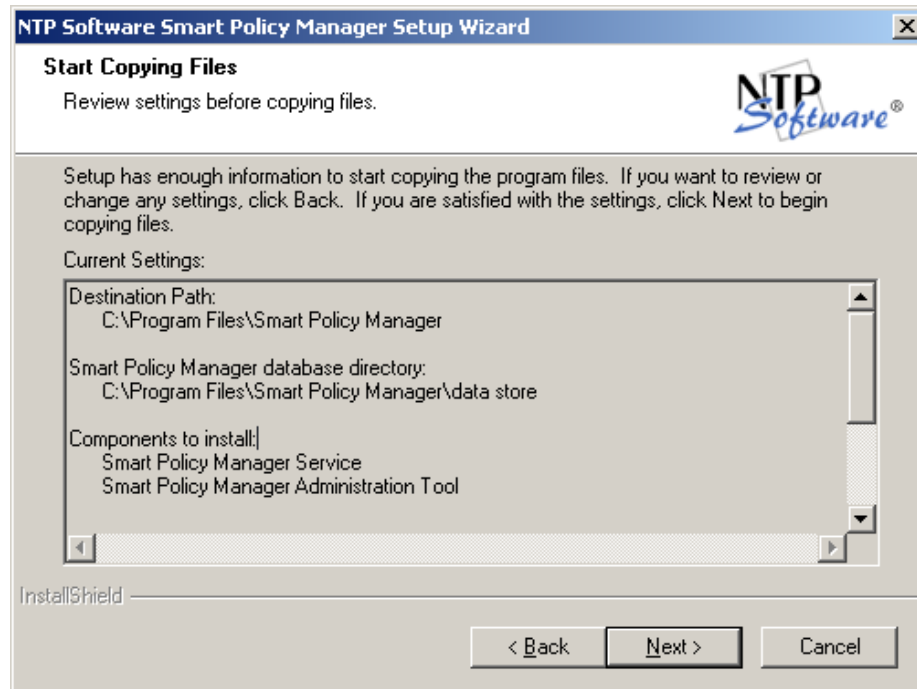


10. In the **Smart Policy Manager Initial Setup Parameters** dialog box, provide DefendX Software Smart Policy Manager with a name for your organization and a location name for this DefendX Software Smart Policy Manager instance, or accept the default settings. Click **Next**.

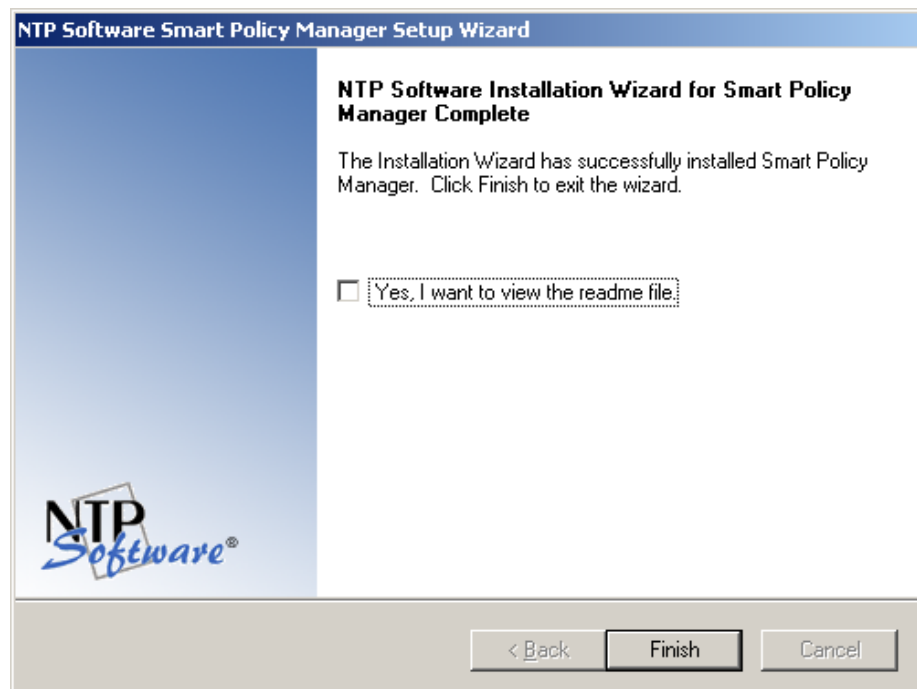


The screenshot shows a Windows-style dialog box titled "NTP Software Smart Policy Manager Setup Wizard". The main heading inside is "Smart Policy Manager Initial Setup Parameters". In the top right corner, there is a logo for "NTP Software®". Below the heading, a text prompt says "Enter the initial organization and location names." There are two input fields: the first is labeled "Organization:" and contains the text "My Organization"; the second is labeled "Location:" and contains the text "My Site". At the bottom left, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

11. 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.

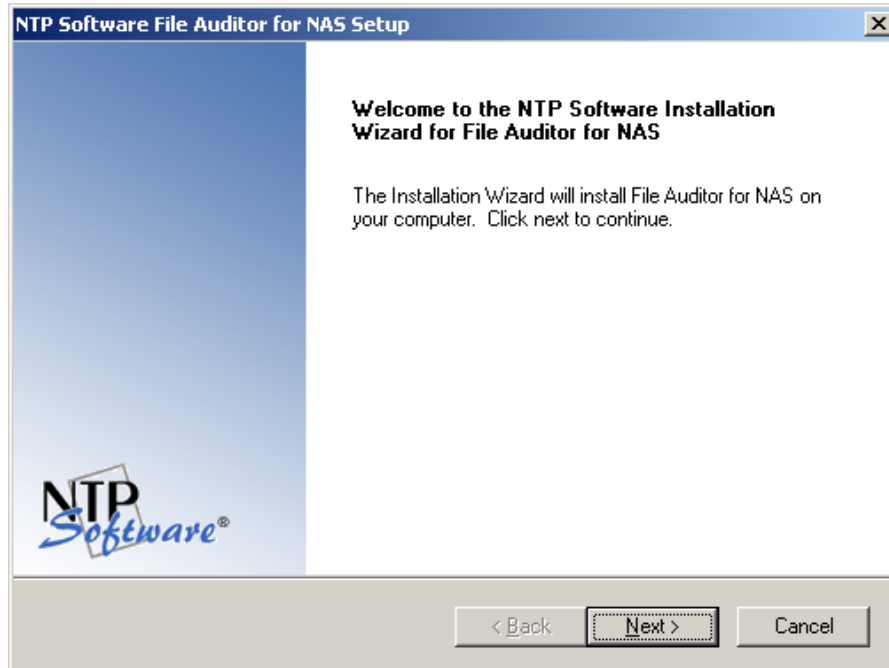


12. If you do not want to view the DefendX Software Smart Policy Manager readme file, clear the **Yes, I want to view the readme file** checkbox. When you click **Finish**, the DefendX Software Control-Audit for NAS Installer opens.

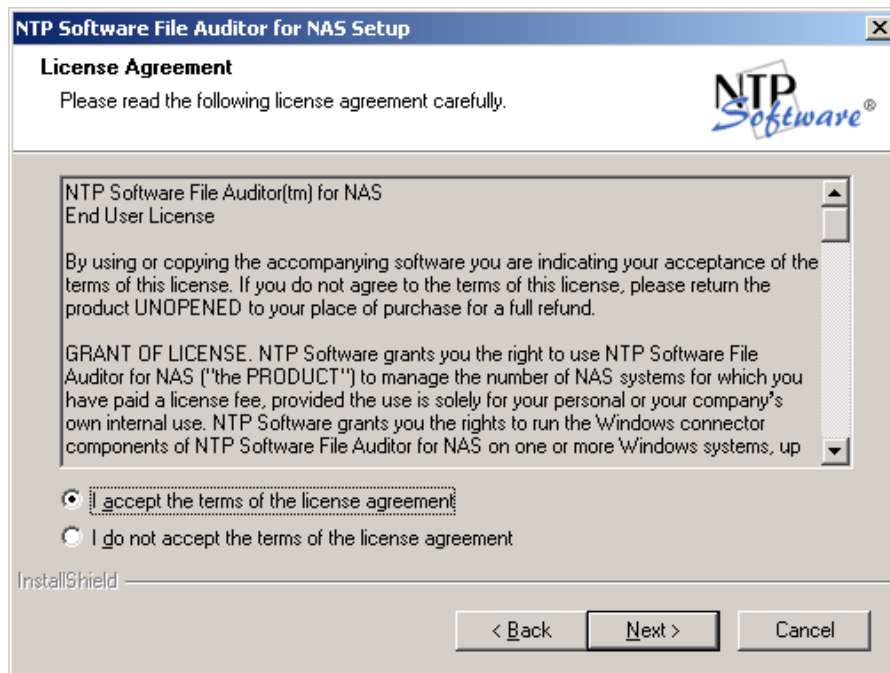


Installing DefendX Software Control-Audit for NAS, NetApp Edition

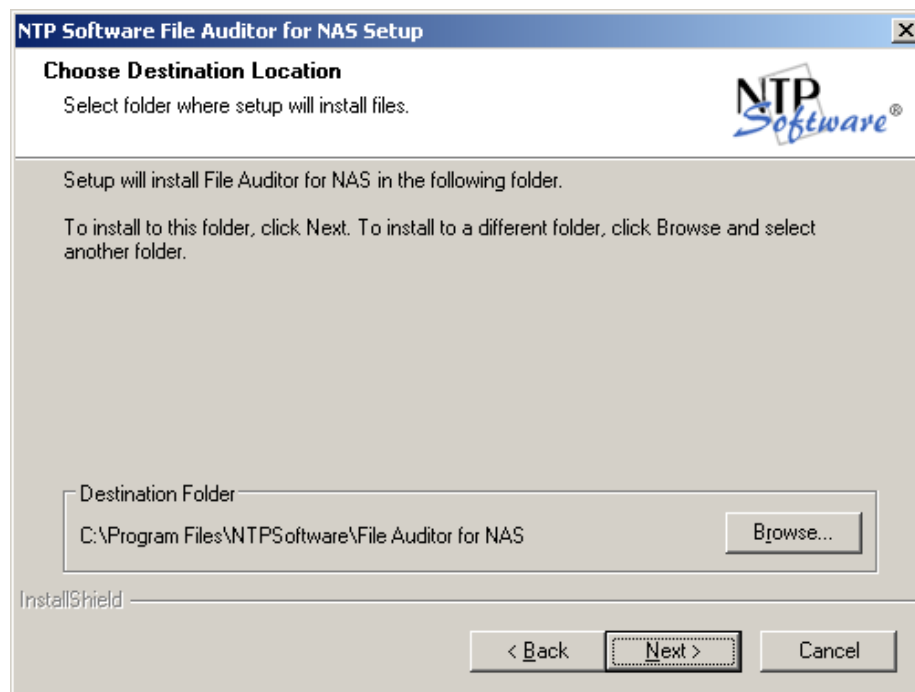
1. When the DefendX Software Control-Audit for NAS Installation Wizard opens, click **Next** to begin the installation.



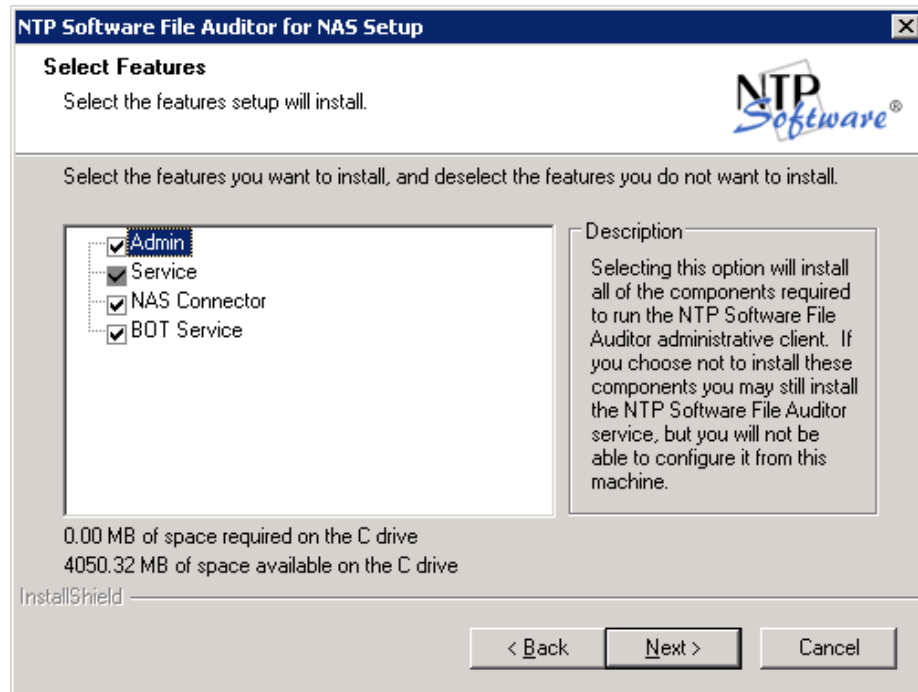
2. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



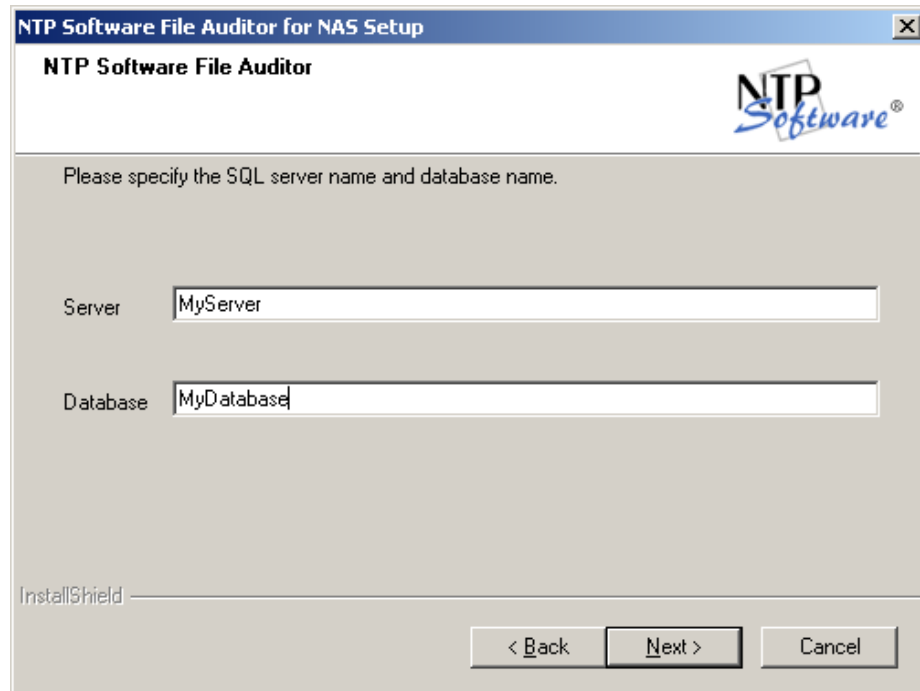
3. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Control-Audit and then click **Next**.



4. In the **Select Features** dialog box, select the components to be installed on the local machine. The **Admin** component allows administration of the DefendX Software Control-Audit service. The **NAS Connector** component is required if this machine will need to communicate with a Filer for file and directory operations monitoring purposes. The BOT Service component is required if you wish to have the Business Overwatch Tasks Service & its configuration interface.

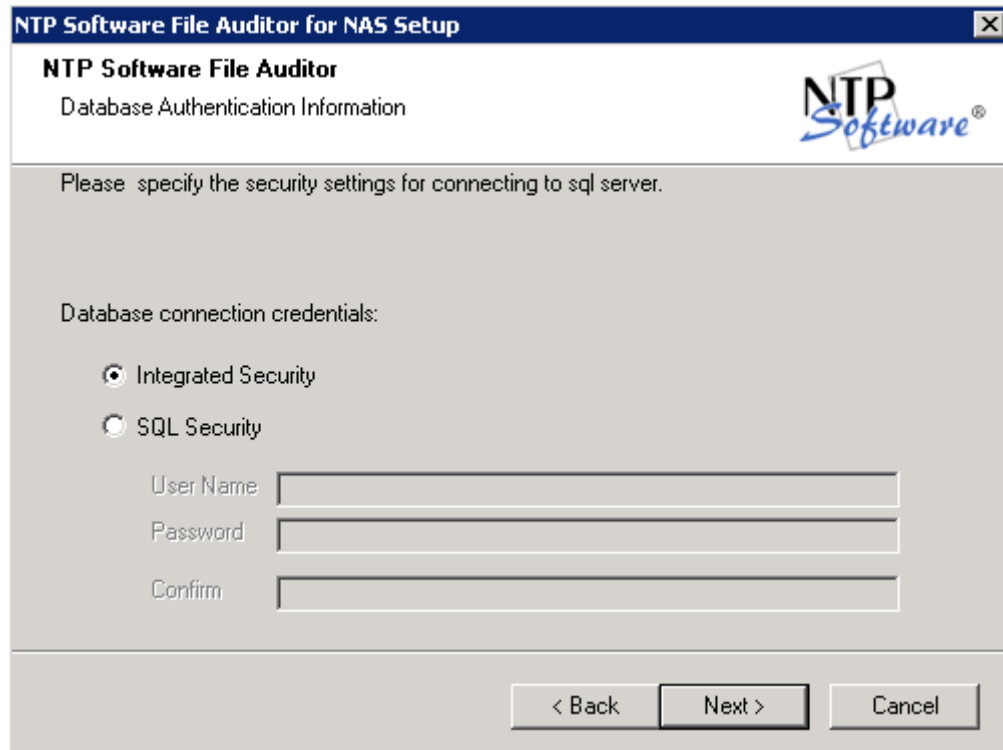


5. In the **DefendX Software Control-Audit** dialog box, provide your SQL Server name and your database name.

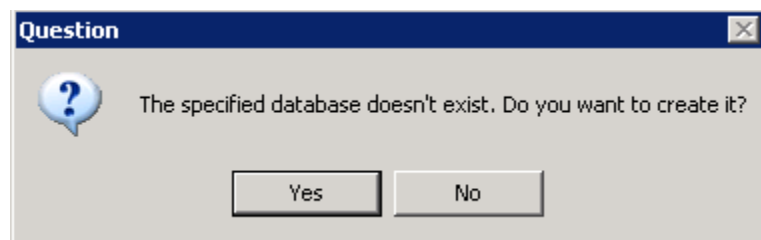


The screenshot shows a Windows-style dialog box titled "NTP Software File Auditor for NAS Setup". The dialog has a blue header bar with the title and a close button. Below the header, the text "NTP Software File Auditor" is displayed on the left, and the "NTP Software" logo is on the right. The main area of the dialog contains the instruction "Please specify the SQL server name and database name." followed by two text input fields. The first field is labeled "Server" and contains the text "MyServer". The second field is labeled "Database" and contains the text "MyDatabase". At the bottom left of the dialog, the text "InstallShield" is visible. At the bottom right, there are three buttons: "< Back", "Next >", and "Cancel".

6. In the **DefendX Software Control-Audit** dialog box, specify the security setting to be used to connect to the SQL Server for database and tables creation.

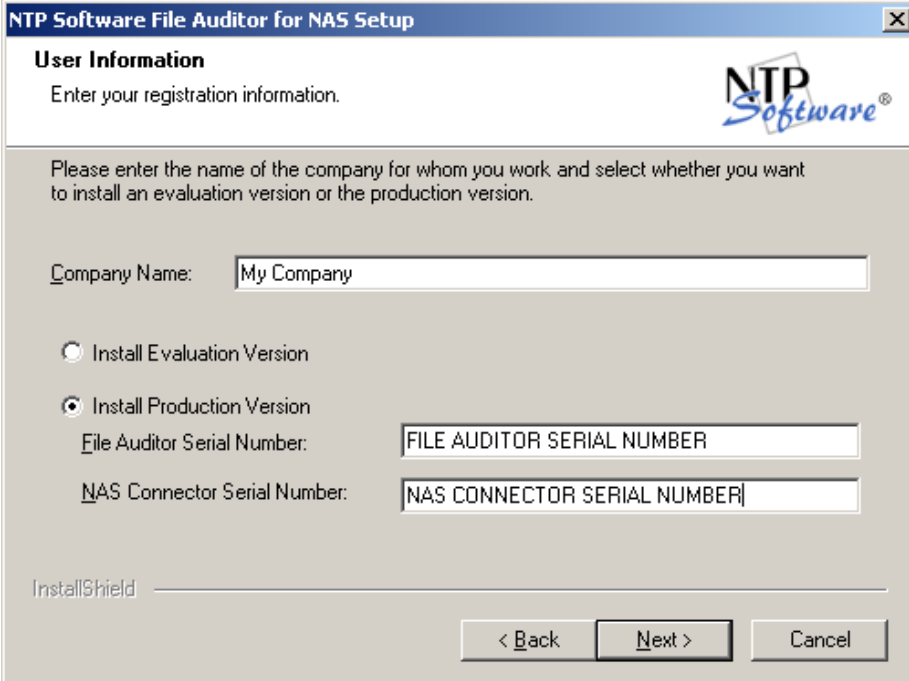


If the database doesnot exist, the below question dialog will be displayed. Click the **Yes** button. If you wish to create the database yourself, run the SQL Scripts in the Control-Audit for NAS installation folder after the setup is complete. The script file is "Control-Audit DB Schema and User Script.sql".



NOTE: If you are upgrading from Control-Audit 2.2 or older versions, the installer will prompt for upgrading the database. Alternatively, you can run the upgrade script manually; the script file "Control-Audit DB Upgrade Script.sql" is located in the Control-Audit installation directory after the setup is complete.

7. In the **User Information** dialog box, provide your company name. Select the **Install Evaluation Version** option if you wish to try the evaluation version of the software. Otherwise, please insert your DefendX Software Control-Audit and NAS Connector serial numbers. Click **Next**.



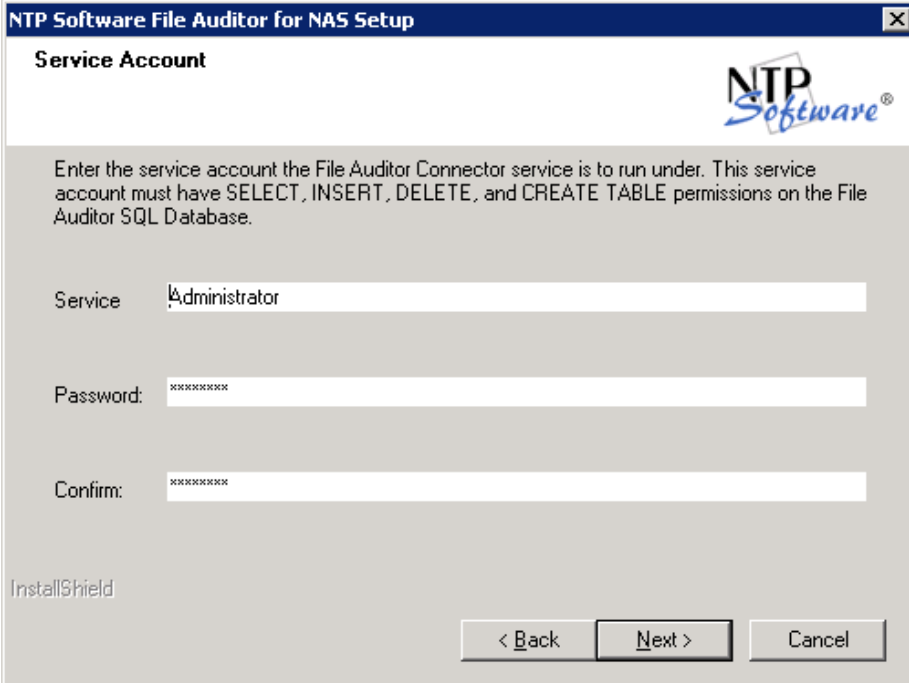
The dialog box is titled "NTP Software File Auditor for NAS Setup". It has a "User Information" section with the instruction "Enter your registration information." and the NTP Software logo. Below this, it says "Please enter the name of the company for whom you work and select whether you want to install an evaluation version or the production version." There is a text field for "Company Name" containing "My Company". Two radio buttons are present: "Install Evaluation Version" (unselected) and "Install Production Version" (selected). Below the radio buttons are two text fields: "File Auditor Serial Number" containing "FILE AUDITOR SERIAL NUMBER" and "NAS Connector Serial Number" containing "NAS CONNECTOR SERIAL NUMBER". At the bottom left is the "InstallShield" logo. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

8. In the **Account Type** dialog box, specify the account type to be used. Click **Next**.



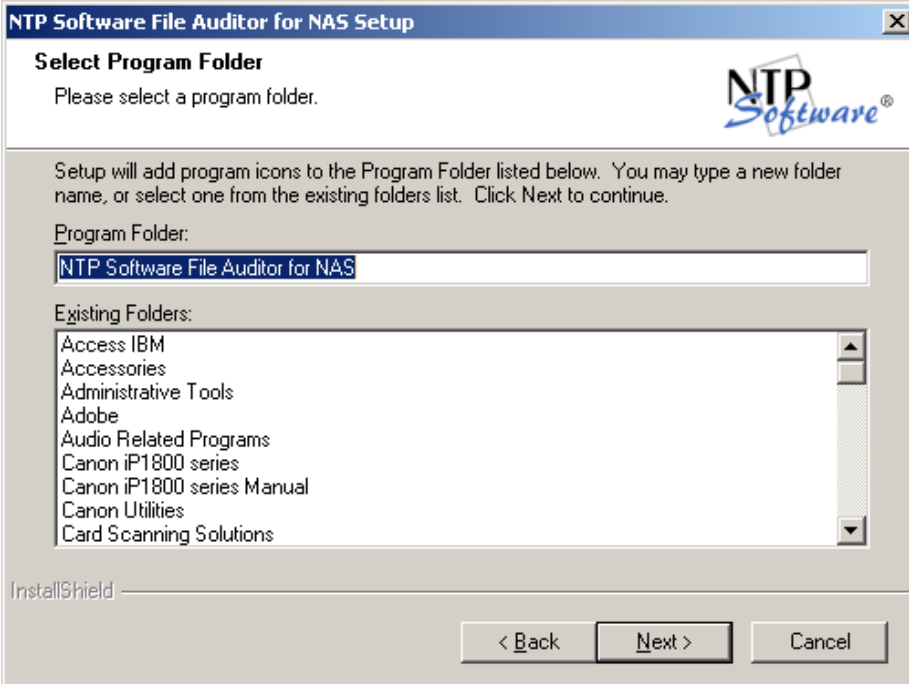
The dialog box is titled "NTP Software File Auditor for NAS Setup". It has an "Account Type" section with the instruction "Please specify the type of account to use." and the NTP Software logo. Below this, it says "The File Auditor service can run as a specified account or the built-in system account." There are two radio buttons: "Specify an account to use." (selected) and "Use the built-in system account. The following features are disabled:" (unselected). The disabled features list includes: "The ability to specify UNC paths in policies.", "Active Directory/LDAP email address lookups.", and "User account lookups across multiple domains." At the bottom left is the "InstallShield" logo. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

9. In the **Service Account** dialog box, when specifying an account, enter a username with local administrative privileges. This account will be used to log in and monitor file operations. Click **Next**.



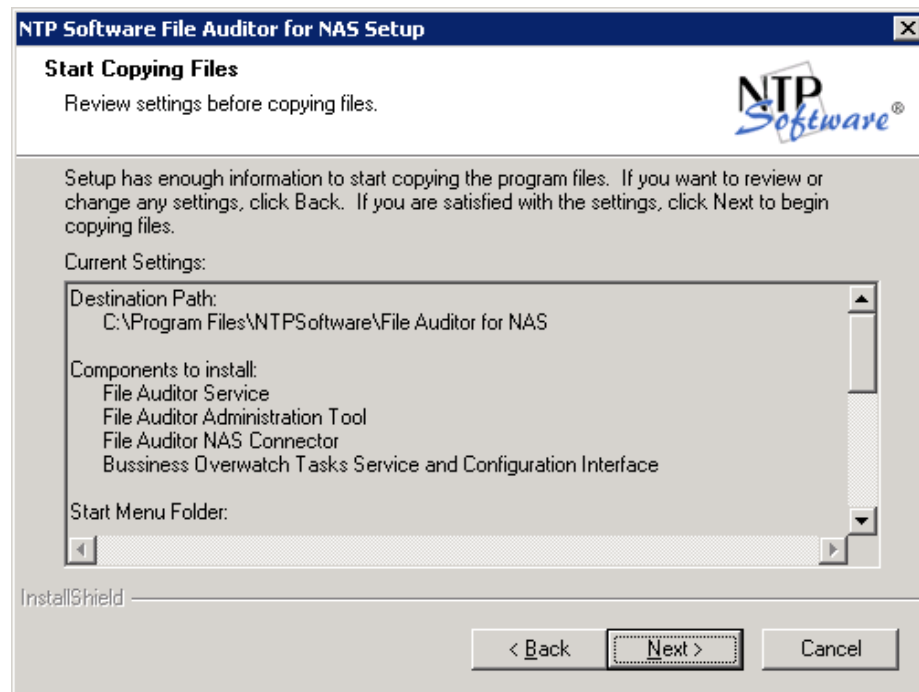
The dialog box is titled "NTP Software File Auditor for NAS Setup" and has a sub-header "Service Account". It includes the NTP Software logo. The main text states: "Enter the service account the File Auditor Connector service is to run under. This service account must have SELECT, INSERT, DELETE, and CREATE TABLE permissions on the File Auditor SQL Database." There are three input fields: "Service" with the text "Administrator", "Password:" with masked characters "xxxxxxx", and "Confirm:" with masked characters "xxxxxxx". At the bottom left is the "InstallShield" logo, and at the bottom right are three buttons: "< Back", "Next >", and "Cancel".

10. In the **Select Program Folder** dialog box, select the program folder to host the DefendX Software Control-Audit for NAS startup group. Click **Next**.

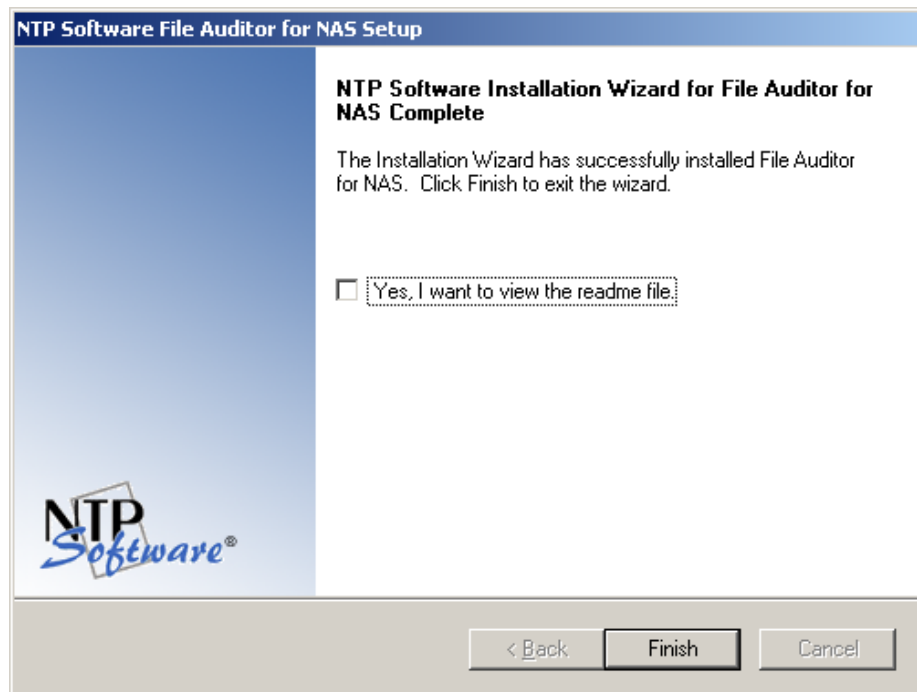


The dialog box is titled "NTP Software File Auditor for NAS Setup" and has a sub-header "Select Program Folder". It includes the NTP Software logo. The main text states: "Please select a program folder. Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue." There are two input areas: "Program Folder:" with the text "NTP Software File Auditor for NAS" and "Existing Folders:" with a list box containing the following items: "Access IBM", "Accessories", "Administrative Tools", "Adobe", "Audio Related Programs", "Canon iP1800 series", "Canon iP1800 series Manual", "Canon Utilities", and "Card Scanning Solutions". At the bottom left is the "InstallShield" logo, and at the bottom right are three buttons: "< Back", "Next >", and "Cancel".

11. In the **Start Copying Files** dialog box, review your components, NAS Connector and BOT Service information. Click **Back** to make any changes; otherwise, click **Next** to begin copying the files.



12. If you do not want to view the DefendX Software Control-Audit for NAS readme file, clear the **Yes, I want to view the readme file** checkbox. When you click **Finish**, the DefendX Software Control-Audit for NAS, NetApp Edition Configuration Wizard will open.



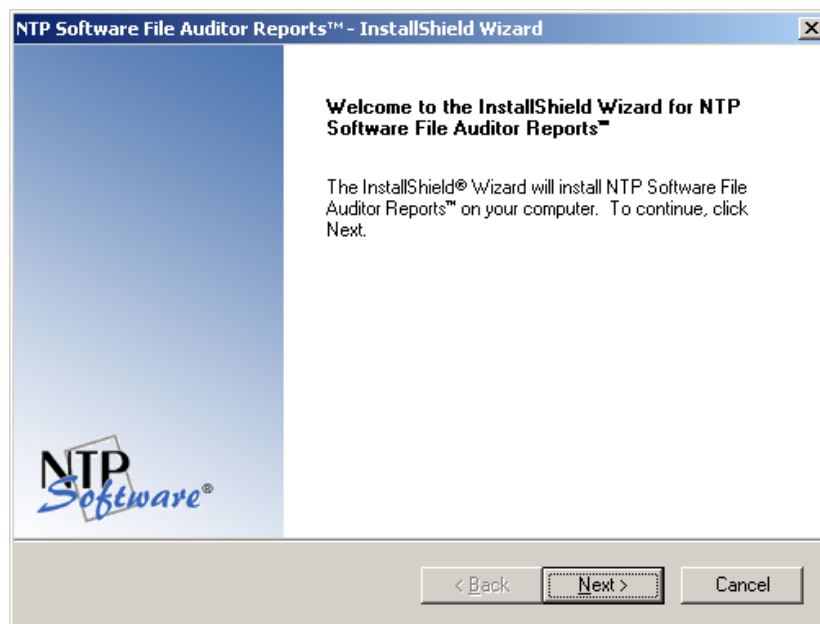
13. Once you click finish, the NetApp Configuration Wizard will be displayed.

Installing DefendX Software Control-Audit Reports

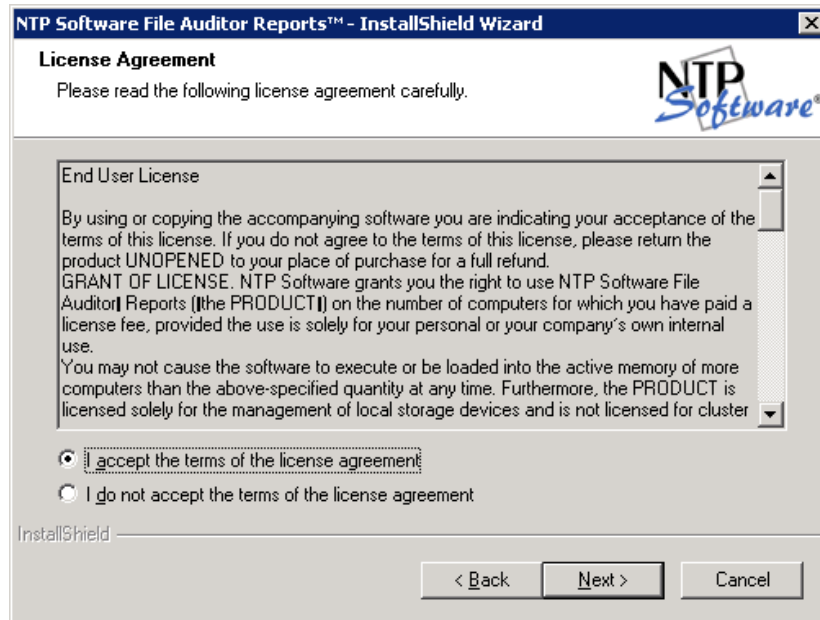
1. When the DefendX Software Control-Audit Reports Wizard opens, click **Next** to begin the installation.

NOTE: The user installing the Control-Audit Reports must be assigned the Content Management role. To assign a user the Content Management role, perform the following steps:

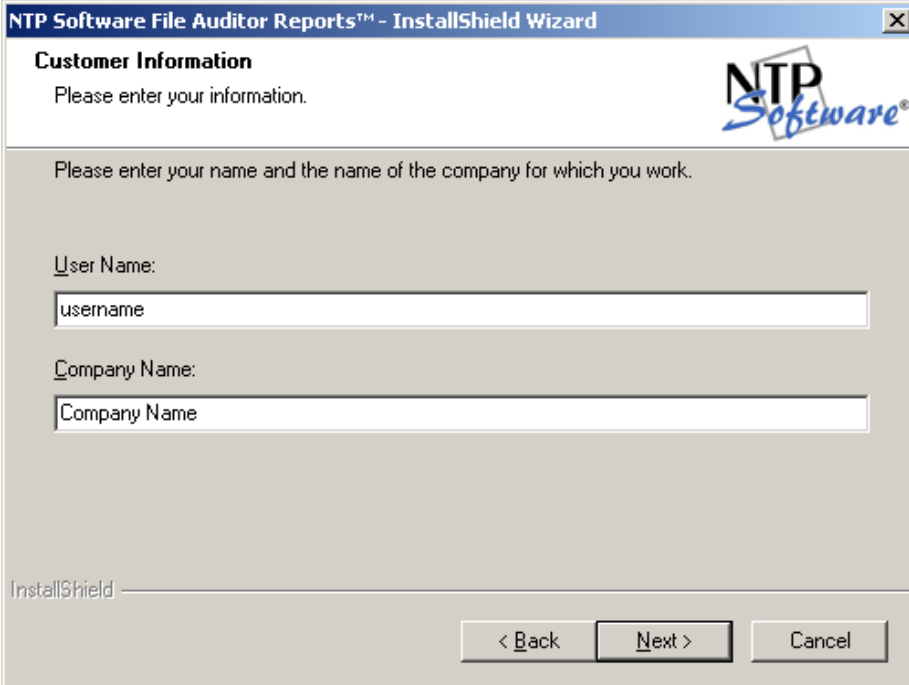
1. Open SQL Server Reporting Services URL on the host machine – example: [http://[SQLReportingHostMachine]/Reports].
2. Navigate to the **Properties** tab.
3. Navigate to the **Security** tab.
4. Create a new Role by clicking **New Role Assignment** or edit an already existing Group or User.



2. 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.



3. In the **Customer Information** dialog box, provide your user name and the company name. Click **Next**.



NTP Software File Auditor Reports™ - InstallShield Wizard

Customer Information

Please enter your information.

Please enter your name and the name of the company for which you work.

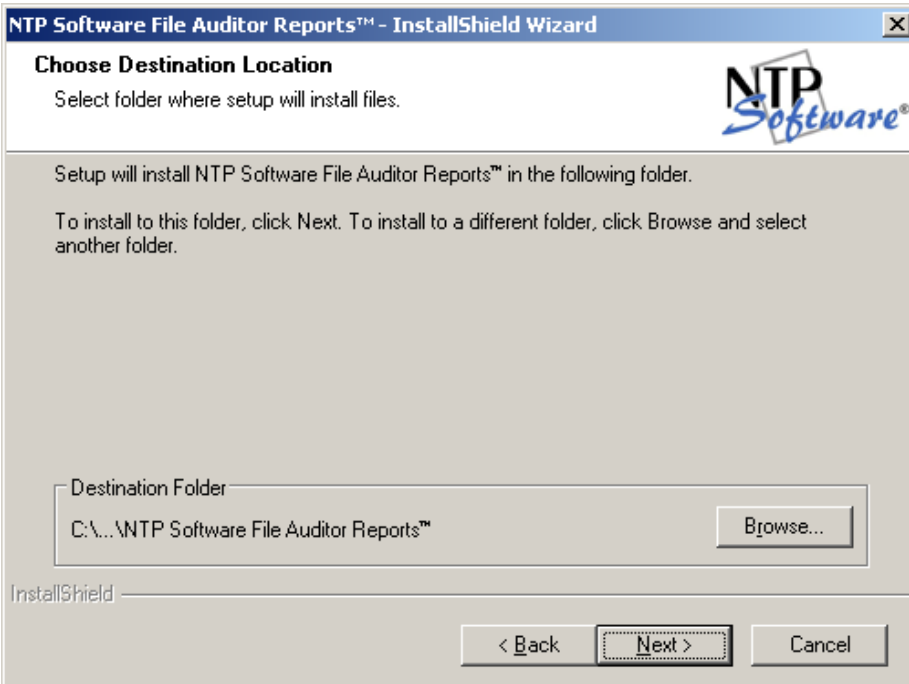
User Name:
username

Company Name:
Company Name

InstallShield

< Back Next > Cancel

4. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Control-Audit Reports and then click **Next**.



NTP Software File Auditor Reports™ - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install NTP Software File Auditor Reports™ in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

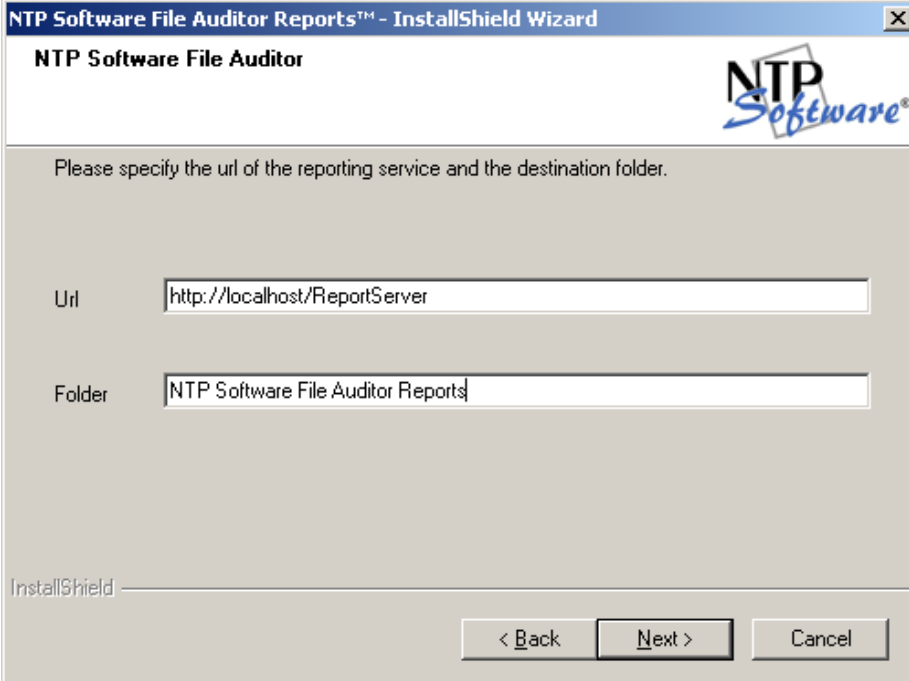
Destination Folder
C:\...\NTP Software File Auditor Reports™

Browse...

InstallShield

< Back Next > Cancel

5. In the **DefendX Software Control-Audit** dialog box, specify the URL of the reporting service and the destination folder. Click **Next**.



NTP Software File Auditor Reports™ - InstallShield Wizard

NTP Software File Auditor

Please specify the url of the reporting service and the destination folder.

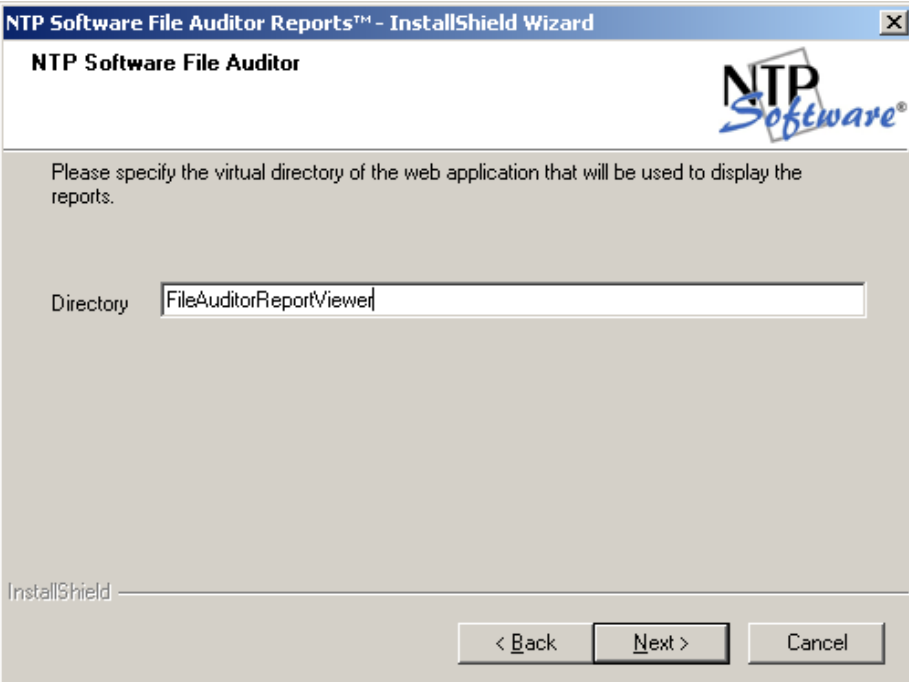
Url:

Folder:

InstallShield

< Back Next > Cancel

6. In the **DefendX Software Control-Audit** dialog box, specify the web application virtual directory. Click **Next**.



NTP Software File Auditor Reports™ - InstallShield Wizard

NTP Software File Auditor

Please specify the virtual directory of the web application that will be used to display the reports.

Directory:

InstallShield

< Back Next > Cancel

7. In the **DefendX Software Control-Audit** dialog box, specify the SQL Server name and the database name hosted on the SQL Server. Click **Next**.

NTP Software File Auditor Reports™ - InstallShield Wizard

NTP Software File Auditor

Please specify the SQL database server name and database name.

Server: (local)

Database: FileAuditor

< Back Next > Cancel

8. In the **DefendX Software Control-Audit** dialog box, specify the security setting to connect to the SQL Server database. Click **Next**.

NTP Software File Auditor Reports™ - InstallShield Wizard

NTP Software File Auditor

Please specify the security settings for connecting to sql server.

☐ Integrated Security

☒ SQL Security

User Name: FAReportingUser

Password: [masked]

Confirm: [masked]

< Back Next > Cancel

NOTES:

Control-Audit has a default user "Control-AuditReportingUser" and default password "Control-AuditReporter2010" that you can use or change.

If the **SQL Security** setting was selected, the user should have at least the db_datareader, db_datawriter, and execute permissions.

For Historical Data feature to function properly under the **SQL Security** setting, "Control-AuditReportingUser" user should have ADMINISTER BULK OPERATIONS permission to the database, along with ALTER and INSERT permissions to the HistoricalOperations and HistoricalDACLS tables. Control-Audit Installer attempts to set these permissions during installation.

If the **Integrated Security** setting was selected, the Control-Audit Reports data source will use the website's Application Pool identity to access Control-Audit database. Please refer the section "Configuring Control-Audit Reports website security".

To change the Control-Audit Reports data source, you need to do the following:

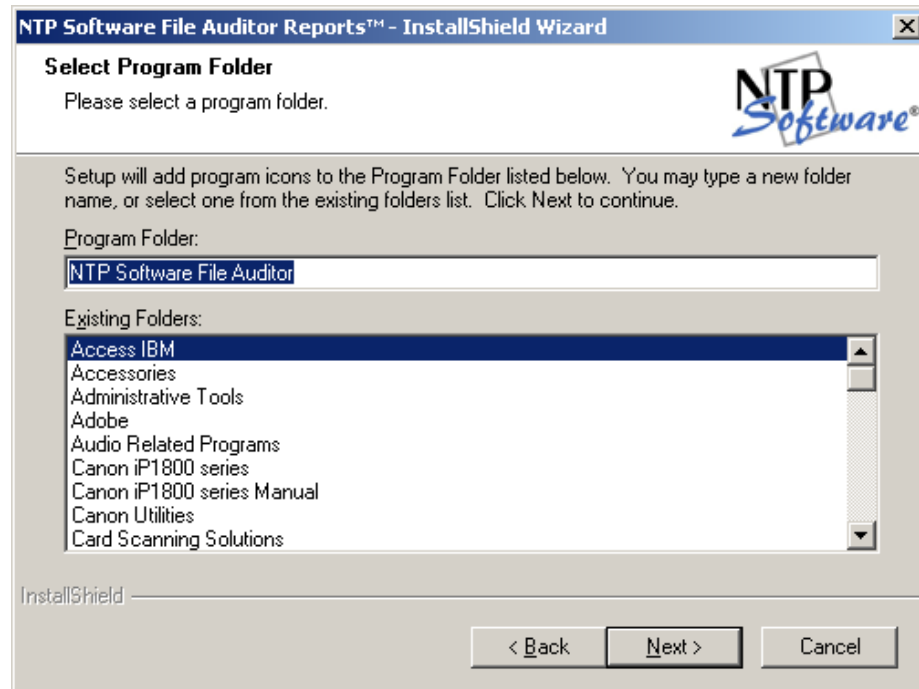
1. Open SQL Server Reporting Services Manager URL on the host machine [http://[SQLReportingHostMachine]/Reports].
2. Open the **DefendX Software Control-Audit Reports** folder, or the reports folder specified in the installation.
3. Open **DFXPOps**.
4. Select the needed reports data source,

The network users who should run the reports must be assigned to the browser role on reporting Service reports. To give a user or group access to the reports, you need to do the following:

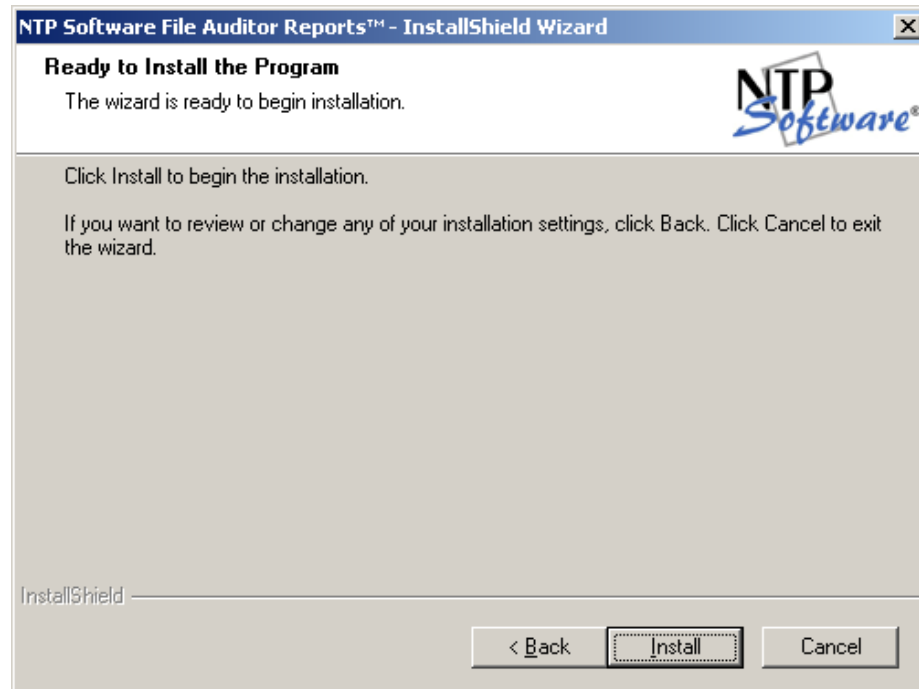
1. Open SQL Server Reporting Services Manager URL on the host machine [http://[SQLReportingHostMachine]/Reports].
2. Open the **DefendX Software Control-Audit Reports** folder, or the reports folder specified in the installation.
3. Open the **Properties** top tab, then select **Security** left tab.
4. Click on **New Role Assignment**.
5. Write the user or group name, select the Browser role, then click **OK**.

9. If the **Please upgrade to SP3** dialog box was displayed, click **OK**.

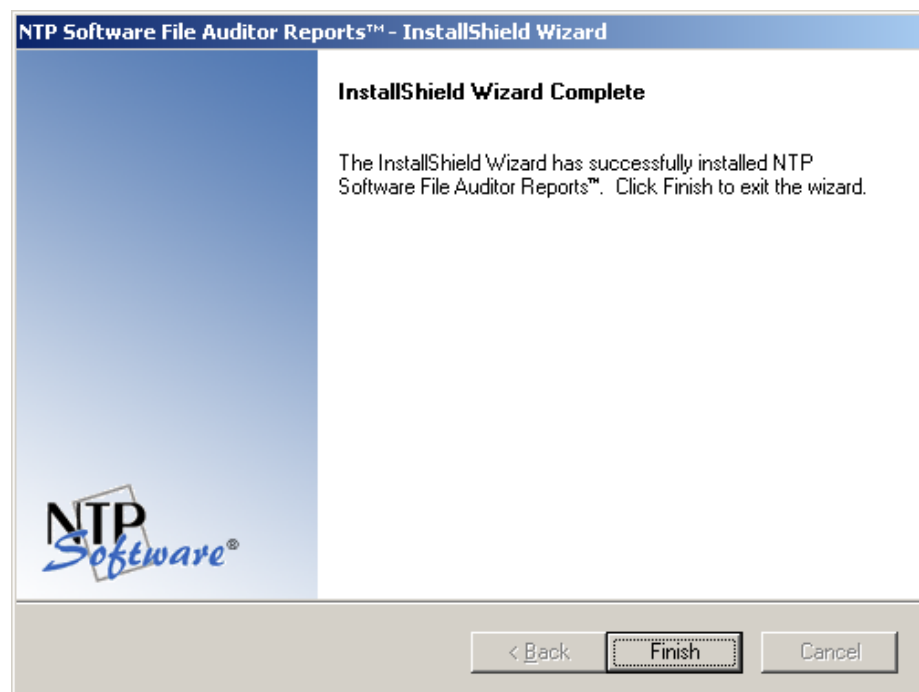
10. In the **Select Program Folder** dialog box, select the program folder to host the DefendX Software Control-Audit Reports startup group. Click **Next**.



11. In the **Ready to Install the Program** dialog box, click **Back** to make any changes; otherwise, click **Install** to begin copying the files.



12. You have successfully installed the DefendX Software Control-Audit Reports. Click **Finish**.



Configuring Control-Audit Reports Website Security

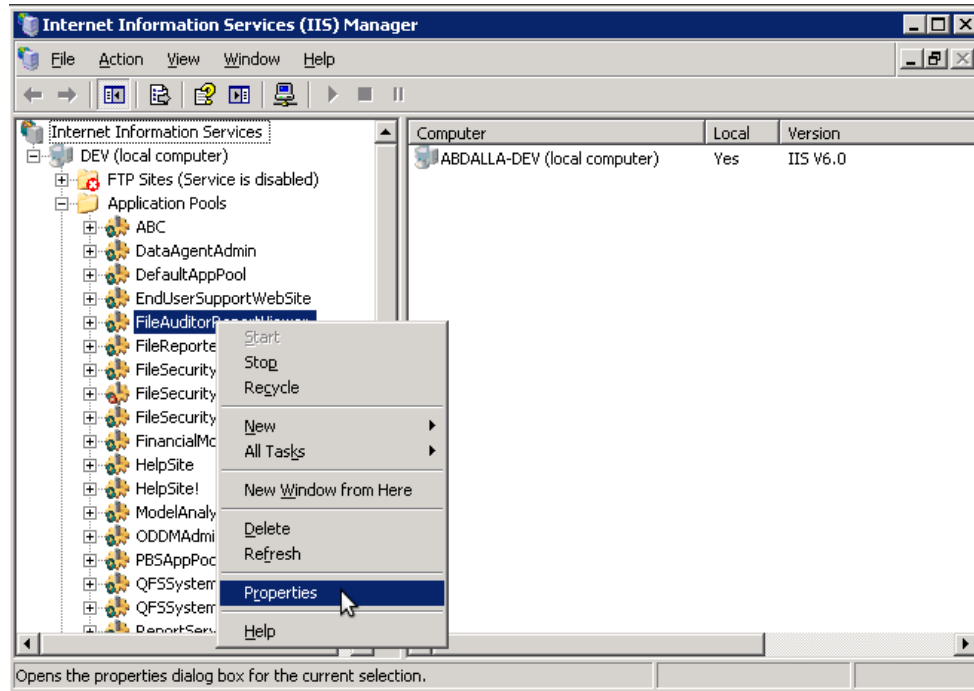
For Historical Data feature to function properly under the Integrated Security setting, The Windows user account who will recall the historical data should have ADMINISTER BULK OPERATIONS permission to the database, along with ALTER and INSERT permissions to the HistoricalOperations and HistoricalDACLS tables.

This section will help you configure Control-Audit Reports website to user integrated security authentication to operate with DefendX Software ODDM and Microsoft SQL Server.

1. Create a domain user account to be assigned to Control-Audit Reports website.
2. In SQL Server, create a login for that user and grant the user the following privileges to Control-Audit database:
 - a. db_datareader
 - b. db_datawriter
 - c. EXECUTE.
3. If you will use Control-Audit ODDM Archiving feature, you must grant the user the following privileges as well:
 - a. ADMINISTER BULK OPERATIONS permission to Control-Audit database.
 - b. ALTER and INSERT permissions to the HistoricalOperations and HistoricalDACLS tables.
 - c. Read and Change permissions to a share on an DefendX Software ODDM Primary server.
4. Configure Control-Audit Reports Viewer website application pool to use the user account you created. The following section will describe how to assign a user account to an application pool in IIS6 or IIS7.

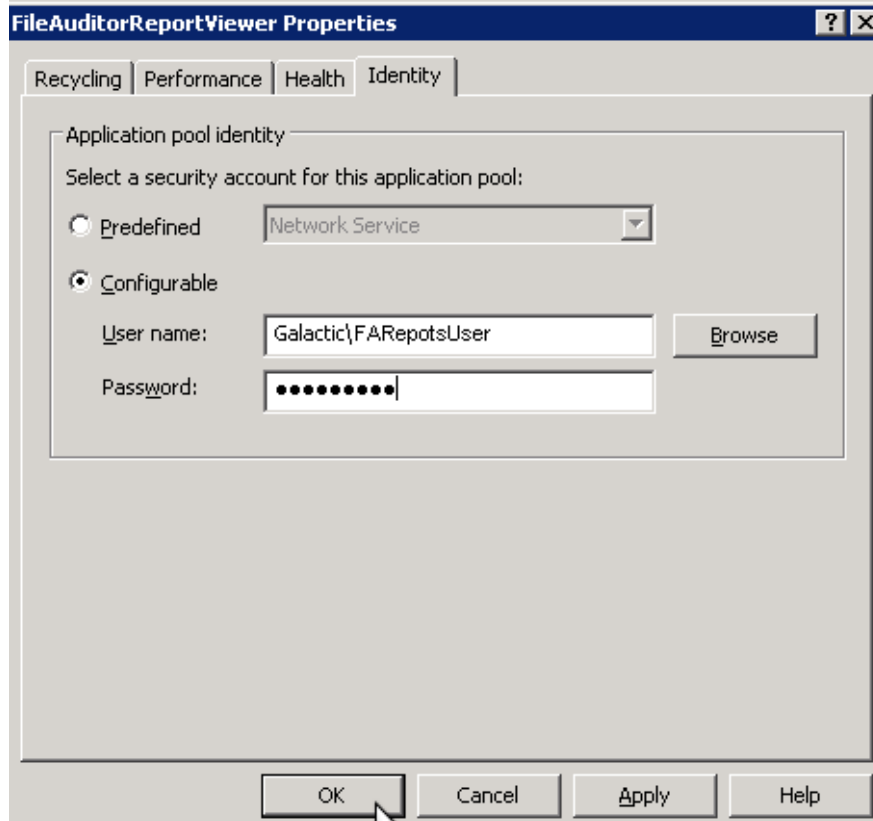
To assign a User Account to an Application Pool in IIS 6, please follow the following:

1. Open Internet Information Services (IIS) Manager console from Administrative Tools.
2. Right-click on the DFXReportViewer application pool and click Properties.

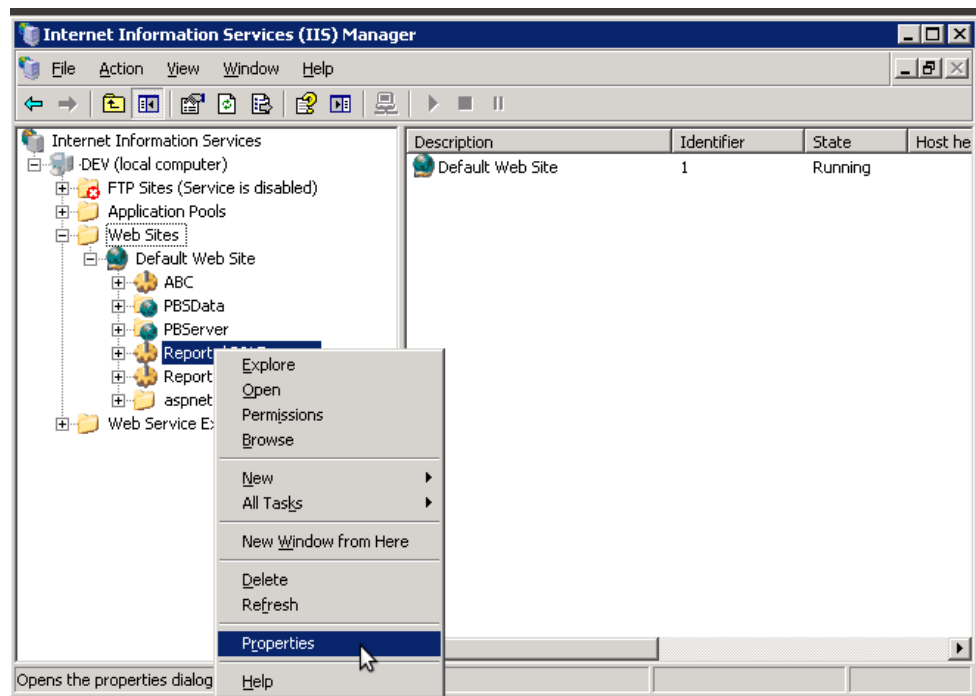


3. In the **Identity** tab, select **Configurable**.

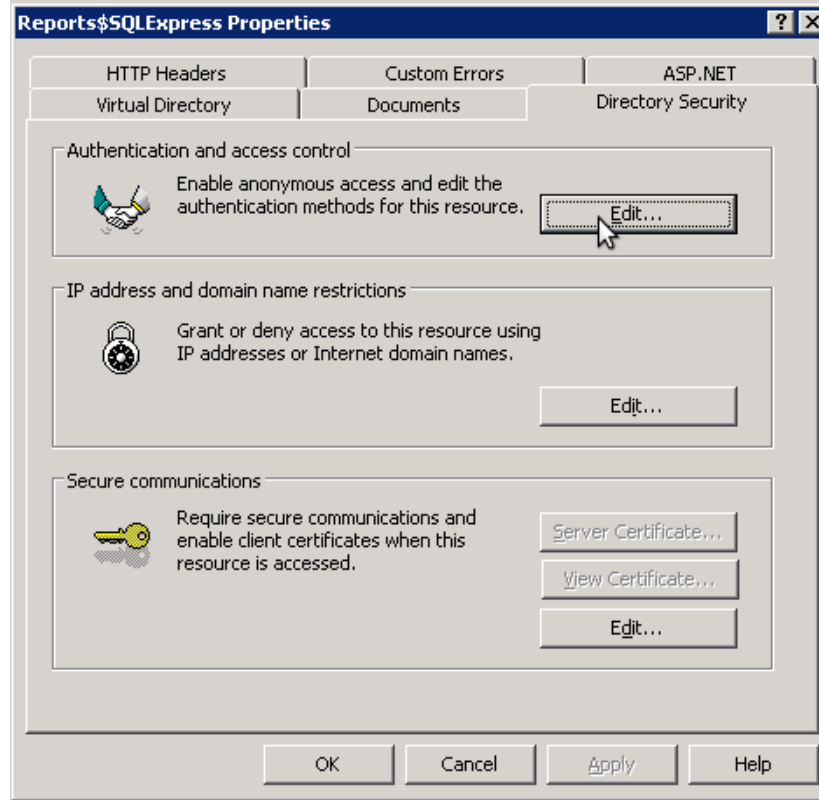
4. Enter the account details, then click **OK**.



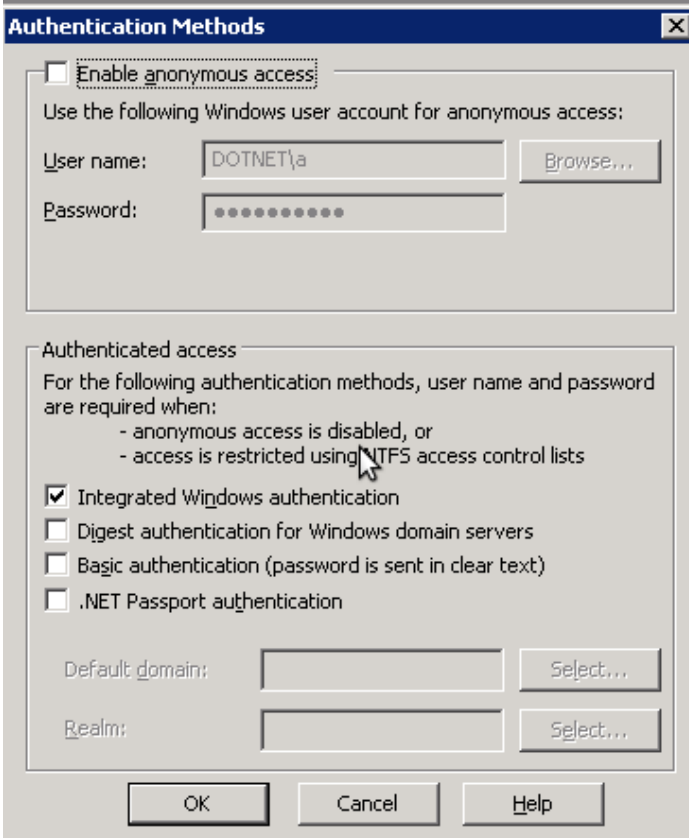
5. Open the DFXReportViewer website properties.



6. In the **Directory Security** tab, under **Authentication and access control**, click **Edit**.



7. Disable all authentication methods except **Integrated Windows Authentication**.



The image shows a Windows-style dialog box titled "Authentication Methods". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into two main sections. The top section is for "Anonymous access" and contains a checkbox labeled "Enable anonymous access:" which is currently unchecked. Below this checkbox is a text label "Use the following Windows user account for anonymous access:". Underneath this label are two input fields: "User name:" with the text "DOTNET\administrator" and a "Browse..." button to its right, and "Password:" with a masked password field (represented by dots). The bottom section is titled "Authenticated access" and contains a text label "For the following authentication methods, user name and password are required when:". Below this label are two bullet points: "- anonymous access is disabled, or" and "- access is restricted using NTFS access control lists". There are four checkboxes in this section: "Integrated Windows authentication" (checked), "Digest authentication for Windows domain servers" (unchecked), "Basic authentication (password is sent in clear text)" (unchecked), and ".NET Passport authentication" (unchecked). At the bottom of the dialog are three buttons: "OK", "Cancel", and "Help".

Authentication Methods

☐ Enable anonymous access:

Use the following Windows user account for anonymous access:

User name: DOTNET\administrator Browse...

Password:

Authenticated access

For the following authentication methods, user name and password are required when:

- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☒ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

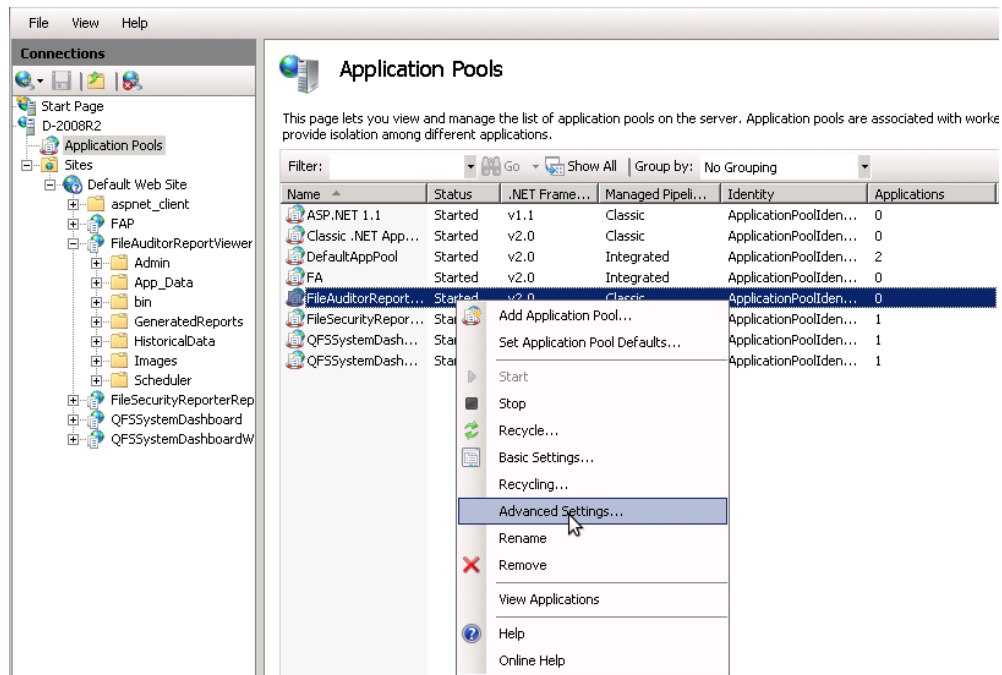
Default domain: Select...

Realm: Select...

OK Cancel Help

To assign a User Account to an Application Pool in IIS 7, please perform the following steps:

1. Open IIS from the control panel and choose the DFXReportViewer application pool.
2. Right-click and choose **Advanced Settings**.



3. Change the default app pool created to the user you need.

Advanced Settings

(General)

.NET Framework Version	v2.0
Enable 32-Bit Applications	False
Managed Pipeline Mode	Classic
Name	FileAuditorReportViewer
Queue Length	1000
Start Automatically	True

CPU

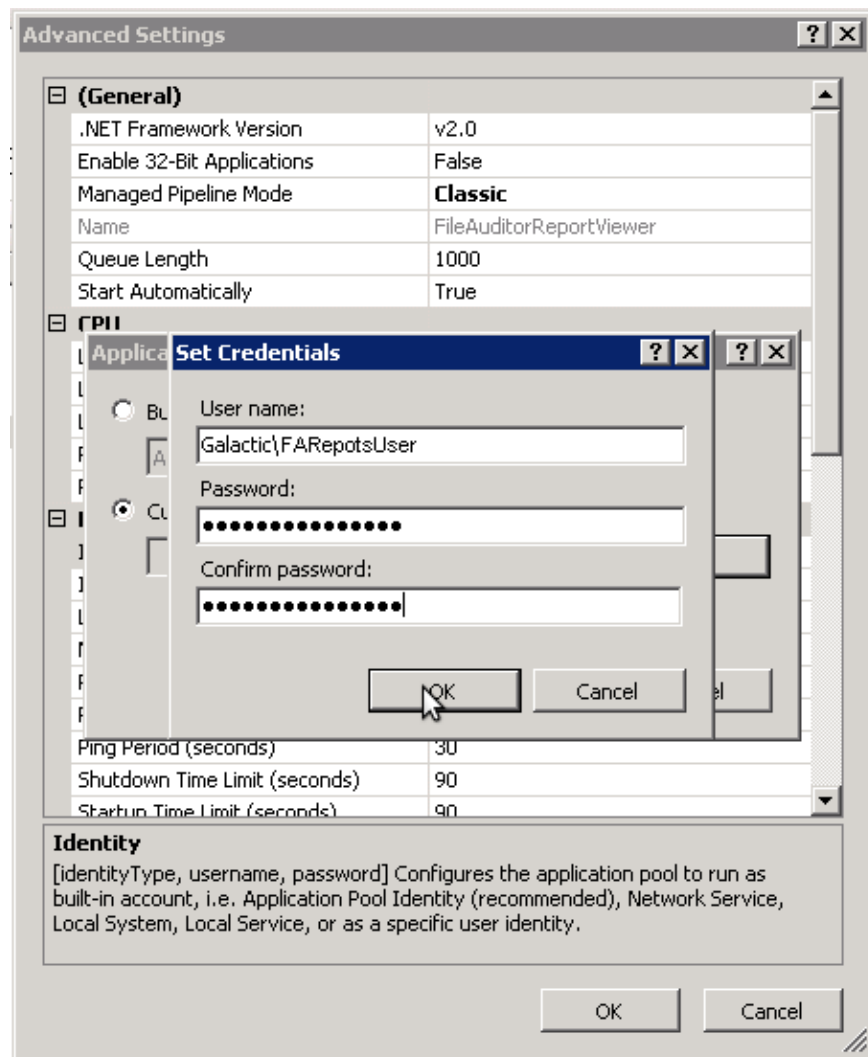
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295

Process Model

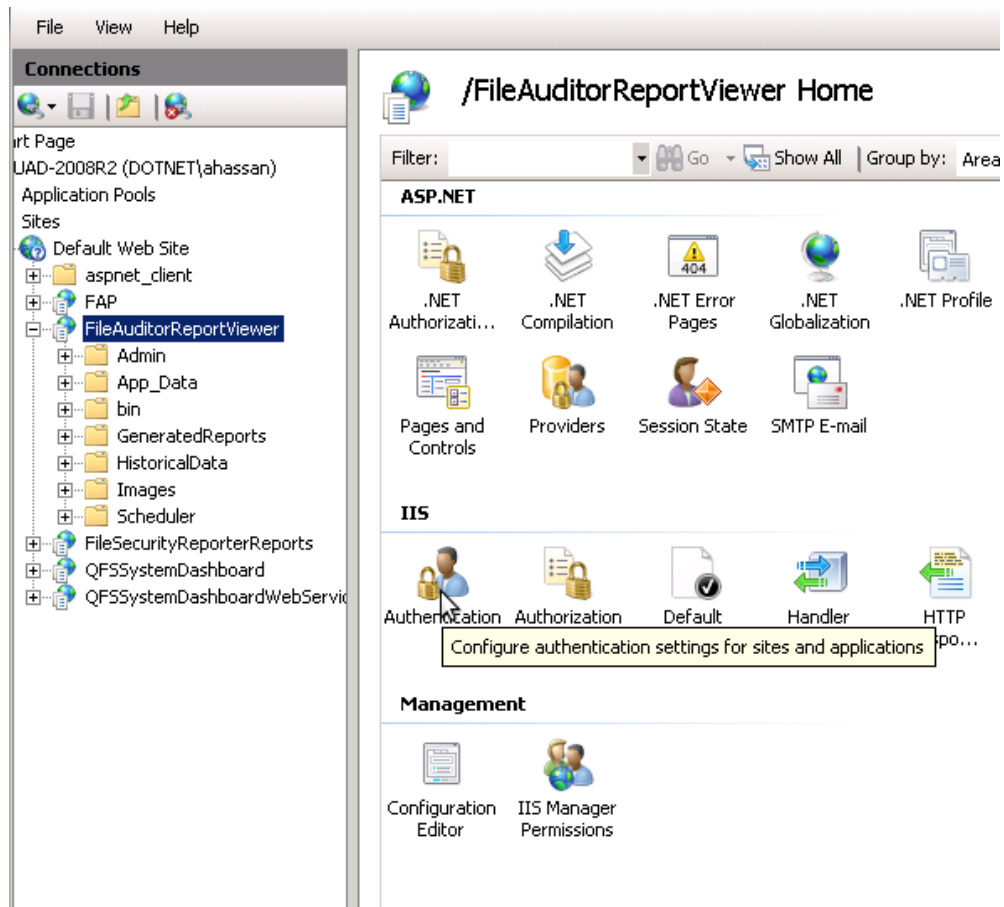
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	20
Load User Profile	False
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

Identity
[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Network Service, Local System, Local Service, or as a specific user identity.

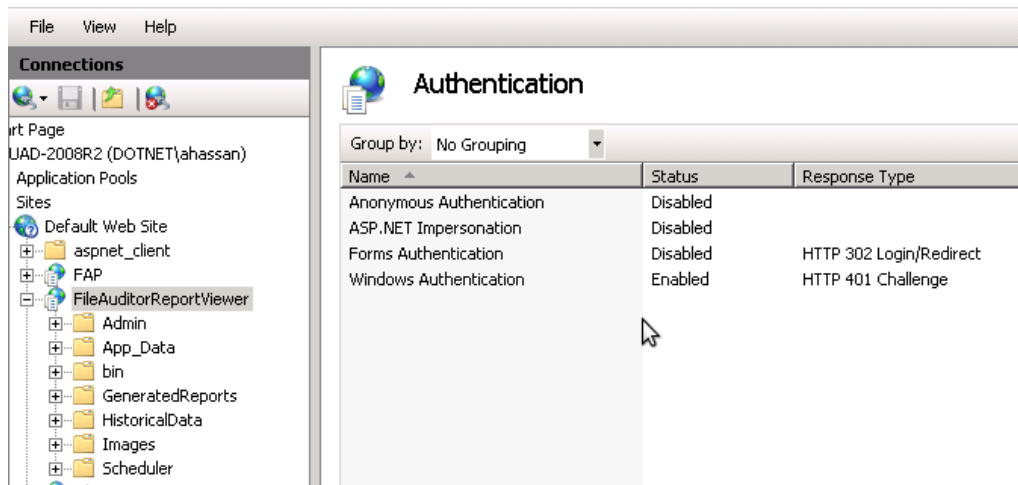
OK Cancel



4. In IIS, choose the DFXReportViewer website and open the Authentication view.

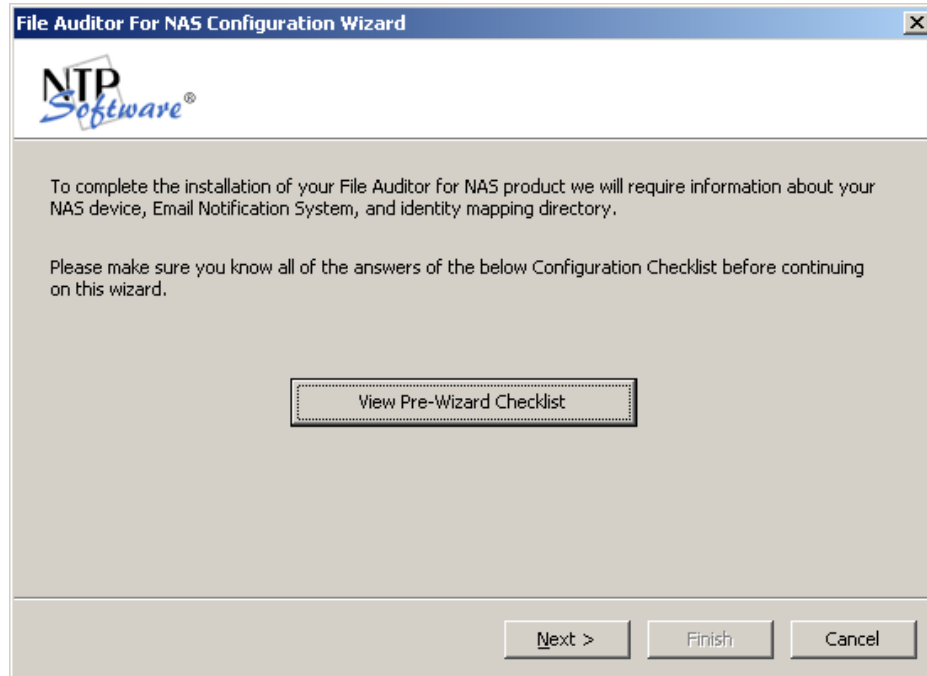


5. Disable all authentication methods except **Windows Authentication**.

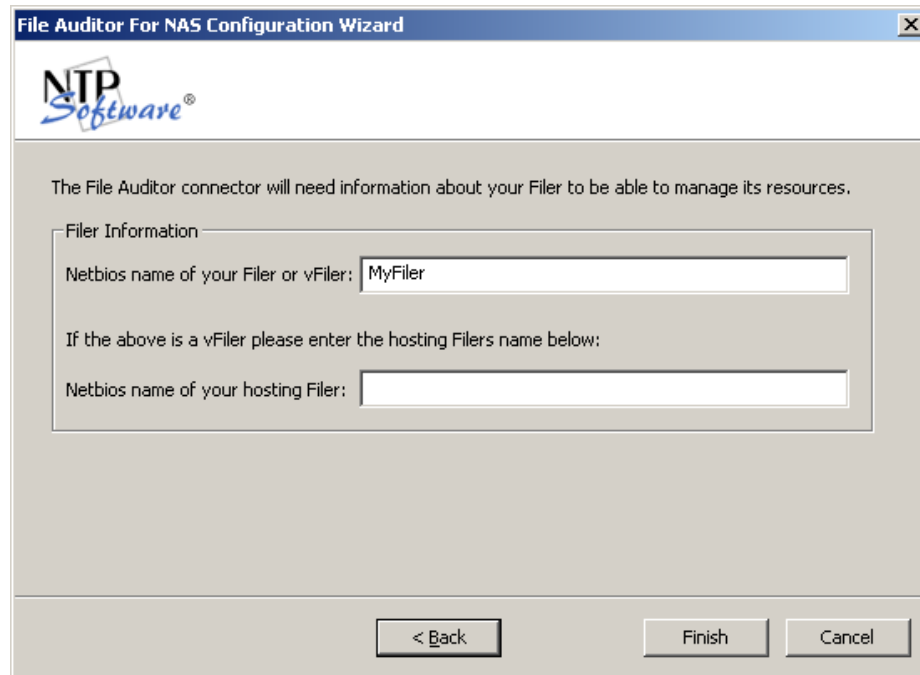


Using the Configuration Wizard

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



2. Enter the name of your Filer or vFiler. If using a vFiler, enter the name of the hosting Filer. Once finished, click **Finish**.



The File Auditor connector will need information about your Filer to be able to manage its resources.

Filer Information

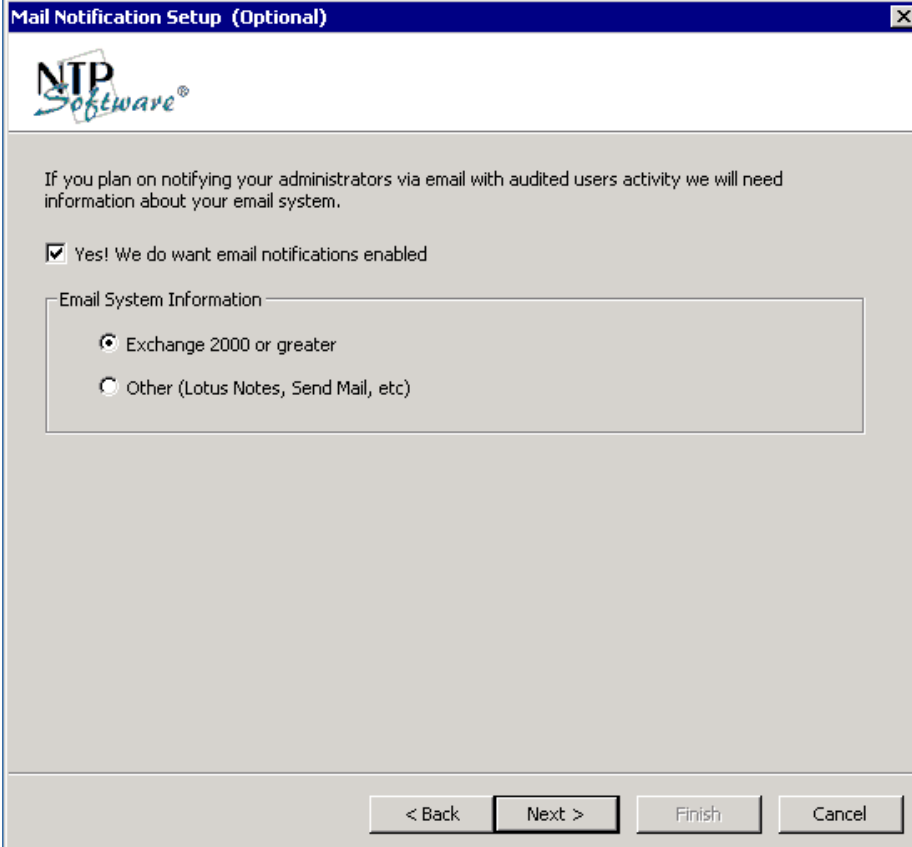
Netbios name of your Filer or vFiler:

If the above is a vFiler please enter the hosting Filers name below:

Netbios name of your hosting Filer:

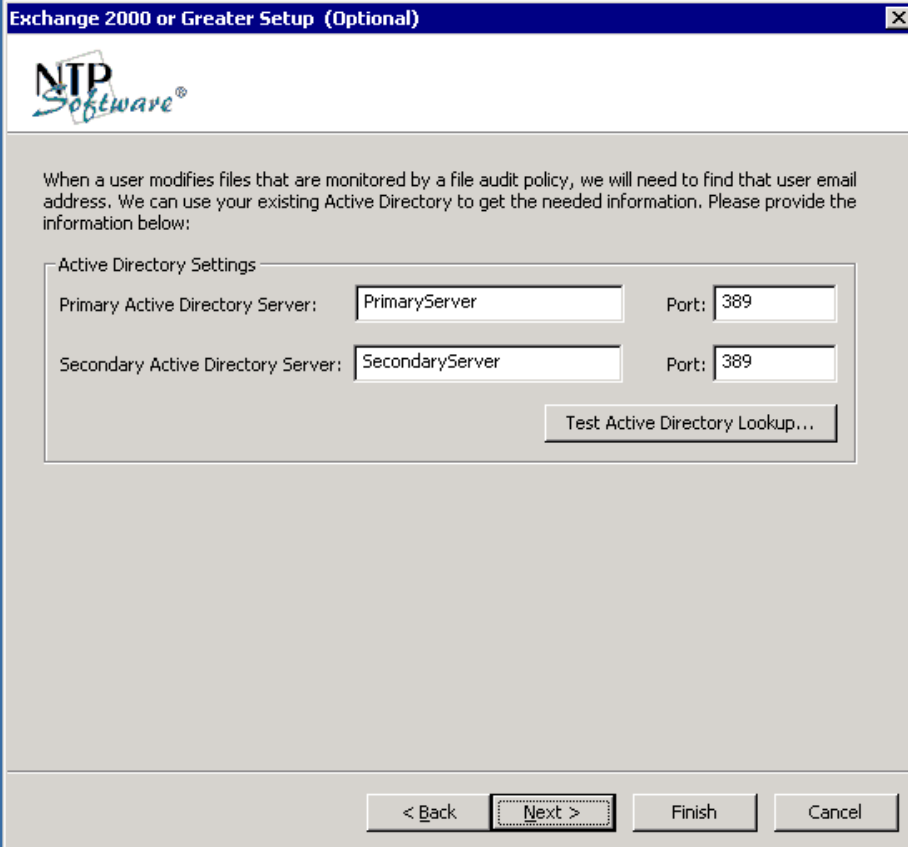
< Back Finish Cancel

3. Check the **Yes! We do want email notifications enabled** option if you wish to notify your administrators about audited users' activities. Specify the email system that your environment uses and click **Next**.



The image shows a Windows-style dialog box titled "Mail Notification Setup (Optional)". At the top left is the "NTP Software" logo. Below the logo, the text reads: "If you plan on notifying your administrators via email with audited users activity we will need information about your email system." There is a checked checkbox labeled "Yes! We do want email notifications enabled". Below this is a section titled "Email System Information" containing two radio button options: "Exchange 2000 or greater" (which is selected) and "Other (Lotus Notes, Send Mail, etc)". At the bottom of the dialog are four buttons: "< Back", "Next >", "Finish", and "Cancel".

4. Enter the name of your primary active directory server; enter a secondary active directory server if you wish. Click the **Test Active Directory Lookup** and test one email address to verify connectivity.



The image shows a Windows-style dialog box titled "Exchange 2000 or Greater Setup (Optional)". The title bar is blue with a close button on the right. Below the title bar is the NTP Software logo. The main area contains a text block explaining the need for Active Directory information. Below this is a section titled "Active Directory Settings" which contains two rows of input fields. The first row is for the "Primary Active Directory Server" with the text "PrimaryServer" and a "Port" field with "389". The second row is for the "Secondary Active Directory Server" with the text "SecondaryServer" and a "Port" field with "389". To the right of these fields is a button labeled "Test Active Directory Lookup...". At the bottom of the dialog are four buttons: "< Back", "Next >" (which is highlighted with a dashed border), "Finish", and "Cancel".

Exchange 2000 or Greater Setup (Optional)

NTP Software®

When a user modifies files that are monitored by a file audit policy, we will need to find that user email address. We can use your existing Active Directory to get the needed information. Please provide the information below:

Active Directory Settings

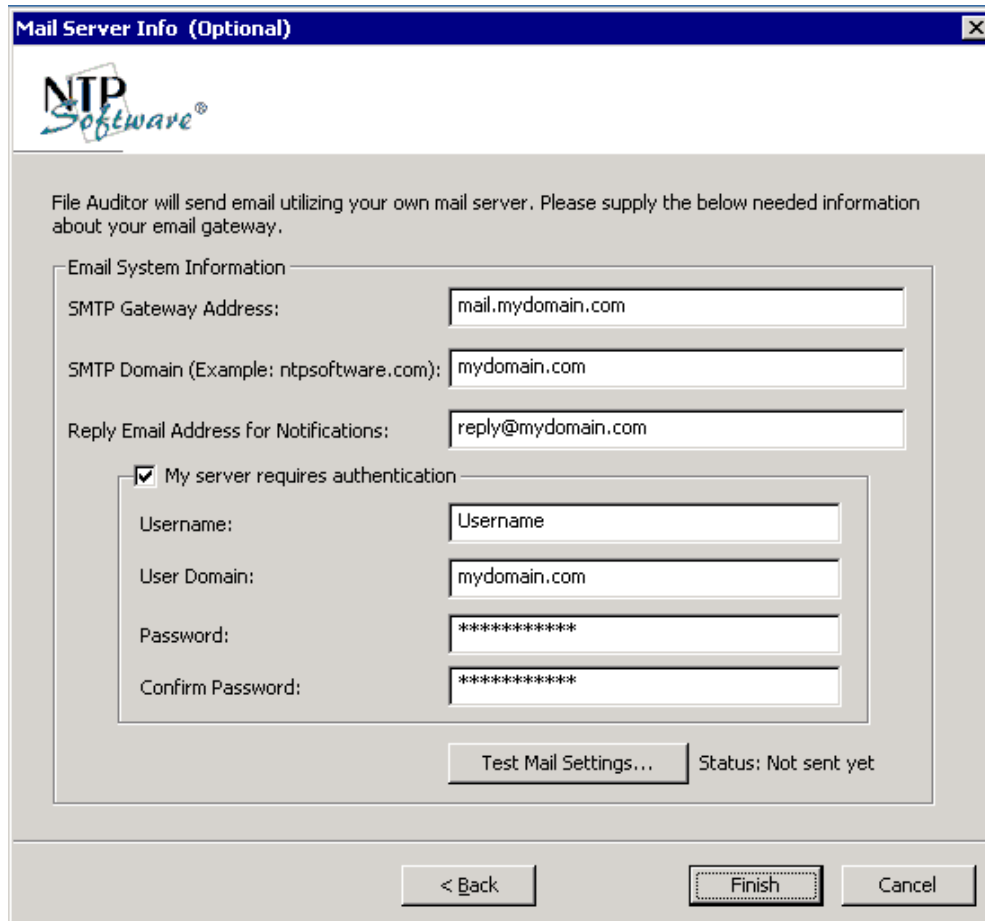
Primary Active Directory Server: PrimaryServer Port: 389

Secondary Active Directory Server: SecondaryServer Port: 389

Test Active Directory Lookup...

< Back Next > Finish Cancel

5. Specify your email gateway information. Click the **Test Mail Settings** to verify the correctness of the information provided. Click **Finish**.

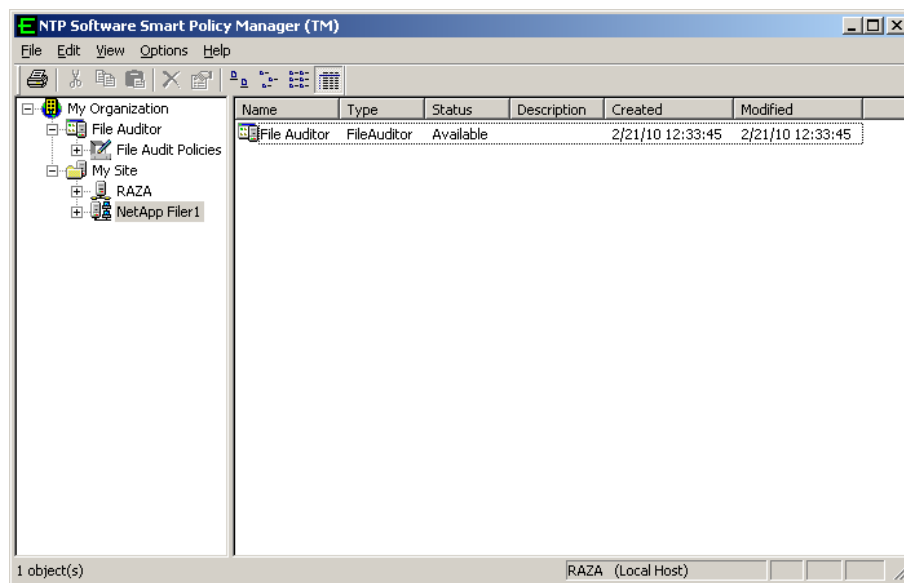


The image shows a Windows-style dialog box titled "Mail Server Info (Optional)". At the top left is the "NTP Software" logo. Below the title bar, a message states: "File Auditor will send email utilizing your own mail server. Please supply the below needed information about your email gateway." The main area is titled "Email System Information" and contains several input fields: "SMTP Gateway Address" with the value "mail.mydomain.com", "SMTP Domain (Example: ntpsoftware.com):" with the value "mydomain.com", and "Reply Email Address for Notifications:" with the value "reply@mydomain.com". Below these is a checked checkbox labeled "My server requires authentication". This checkbox is followed by a sub-section with four fields: "Username:" (containing "Username"), "User Domain:" (containing "mydomain.com"), "Password:" (containing "*****"), and "Confirm Password:" (containing "*****"). To the right of the authentication fields is a "Test Mail Settings..." button and a "Status: Not sent yet" label. At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

Adding the Filer to DefendX Software Control-Audit for NAS Admin

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

1. Click **Start > All Programs > DefendX Software Control-Audit for NAS > DefendX Software Control-Audit 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 DefendX Software Control-Audit is installed.



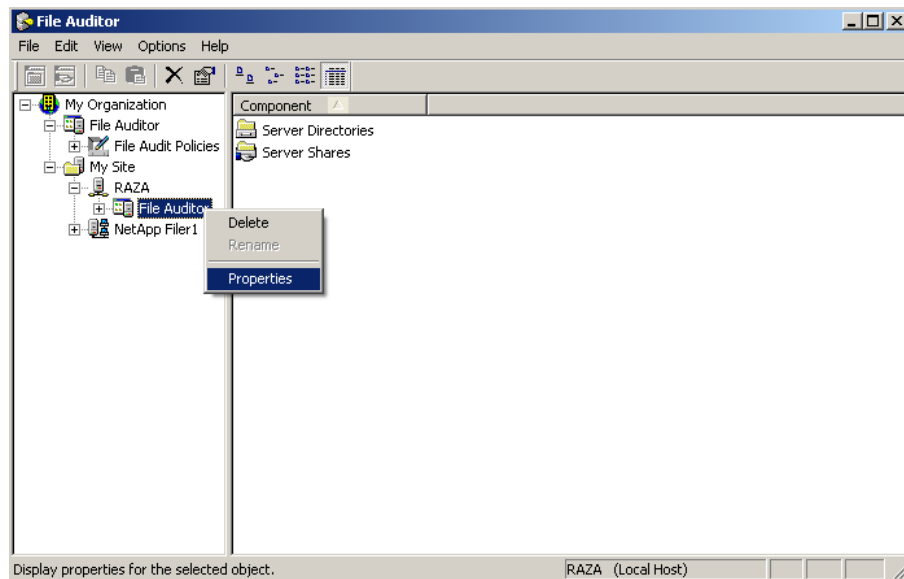
Right-click on a container node, then select **New > Filer** to add the filer to the tree.

You need to add the Filer to the NAS Connector tab by providing the Control station IP, UserName, and Password and then restarting the service.

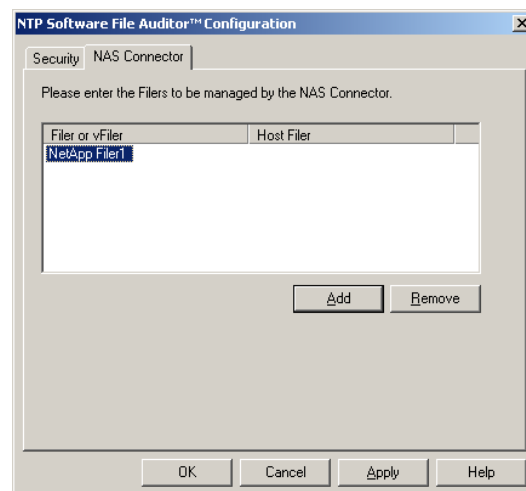
The NetApp filer will be listed in the Control-Audit Admin left panel tree view.

This allows a company with multiple Filers and multiple Control-Audit Servers to control which Control-Audit Server will manage which Filer.

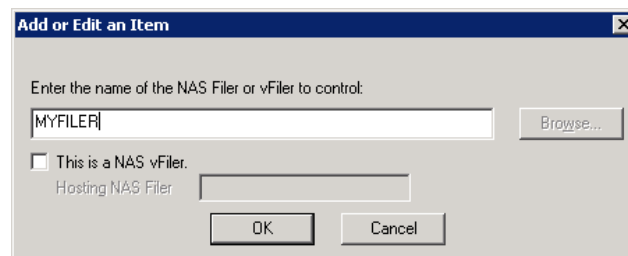
3. In the left pane, expand the server on which DefendX Software Control-Audit is installed and right-click **Control-Audit**. From the pop-up menu, choose **Properties**.



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



5. Enter the name of your Filer or vFiler. If using a vFiler, select the **This is a NAS vFiler** checkbox, then enter the Hosting NAS Filer name. Click **OK**.



To verify that the Filer has been associated with DefendX Software Control-Audit, 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_fa (file screening) is enabled.

File screen servers          P/S Connect time (dd:hh:mm)  Reqs   Fails
-----
10.30.3.25      \\MAZROUH-DEV    Pri    02:00:21             4086    0

ServerID: 2      IDL Version: 1    SMB Request Pipe Name: \ntapfrq
Options enabled: size-and-owner

Operations monitored:
File open,File create,File rename,File close,File delete
Directory rename,Directory delete,Directory create
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.
```

About DefendX Software

DefendX Software helps organizations secure their critical business files and maximize the value of their enterprise file storage resources. From comprehensive intelligence, modeling, costing and chargeback to seamless file movement, protection and archiving, DefendX provides industry-leading capabilities to eliminate waste and align the value of files with the storage resources they consume. With DefendX, important file locations and the users who access them can be monitored to provide governance, protect against theft and enforce compliance policies. For more than 20 years, DefendX Software has been helping public and private sector customers around the world save money and eliminate risk every day.

DefendX Software Professional Services

DefendX 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 DefendX Software Representative at 800-390-6937.

Legal & Contact Information

The information contained in this document is believed to be accurate as of the date of publication. Because DefendX Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of DefendX Software, and DefendX Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. DEFENDX SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

DefendX Software and other marks are either registered trademarks or trademarks of DefendX Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

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

DefendX Software
119 Drum Hill Road, #383
Chelmsford MA 01824
Phone: 1-800-390-6937
E-mail: info@DefendX.com
Web Site: <http://www.DefendX.com>

Copyright © 2020 DefendX Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Doc#DFX1283EF