DefendX Software

DefendX Software Control-Audit for Hitachi

Installation Guide

Version 5.1

This guide details the method for the installation and initial configuration of DefendX Software Control-Audit™ for NAS, Hitachi Edition, from an administrator's perspective. Upon completion of the steps within this document, DefendX Software Control-Audit for NAS, Hitachi Edition will be installed within your enterprise community.

Table of Contents

Executive Summary

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

Given the architecture of your Hitachi NAS Server, DefendX Software Control-Audit for NAS, Hitachi Edition does its job remotely. DefendX Software Control-Audit for NAS, Hitachi Edition uses a connector service to create a bridge and include Hitachi NAS Servers as full participants in storage environments monitored by DefendX Software Control-Audit. In light of this fact, you will need to install the Hitachi connector on one of the Windows Server® 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, the NOS operating system is required on the Hitachi NAS Server. DefendX Software Control-Audit for NAS, Hitachi Edition can be used to manage Hitachi NAS Servers and clusters or any combination of these systems. DefendX Software Control-Audit imposes no restrictions on how you organize or manage your storage. You can impose policies on individual directories, users, and/or groups of users.

To install DefendX Software Control-Audit on Windows, logging on 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 DefendX Software Control-Audit Hitachi 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 Hitachi NAS Server. The Hitachi Connector service uses this account as well.

Your hardware should be appropriate for the services running on each machine. The connector itself and DefendX Software Control-Audit for NAS, Hitachi Edition imposes almost no load on either machine.

Preparing the Hitachi NAS Server

To prepare the HNAS Server, the following must be taken into consideration:

1. For each EVS (Virtual Server) that is managed by DefendX Software Control-Audit, at least one CIFS server name must be created and must join the same domain as the Control-Audit machine.

2. The logon account used to register with the Hitachi NAS Server (the account that will be assigned to the DefendX Software Control-Audit service) needs to be a member of the Hitachi NAS Server's local group Backup Operators. This can be added from the Hitachi NAS Server Command Line Interface (CLI) using the following command:

   ```
   localgroup add "Backup Operators"
   <FQDomainName\AccountName>
   ```

3. The File-Filtering feature must be enabled in the EVS. To enable the File-Filtering feature, use the following command:

   ```
   fsm set allow-defendx-file-filtering true
   ```

Preparing the DefendX Software Control-Audit Windows Machine

To prepare the DefendX Software Control-Audit Machine, you need to add HOSTS and LMHOSTS file entries that include the IP address and the CIFS server name of the EVS. The IP address should be the address of the dedicated network.

Requirements

DefendX Software Control-Audit for NAS, Hitachi Edition Server Requirements

DefendX Software Control-Audit for NAS is installed on a server in your environment. The hardware components of this server 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.

Hitachi NAS Server Requirements

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

- NOS operating system version 6.1.1684.18 or later.
- Network interface card

NOTE: It is strongly recommended that two network adapters be installed on both the Hitachi NAS Server and the Windows Server. The connection between the two servers 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, Hitachi 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.

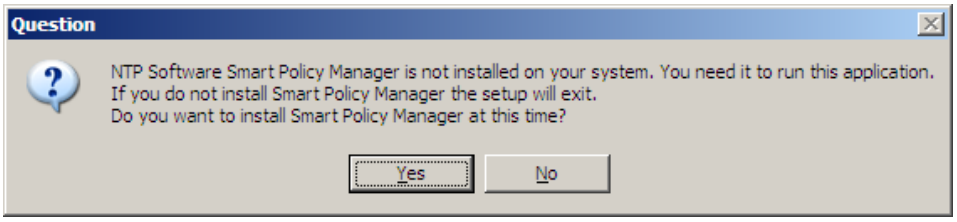
Installation

Prior to installing DefendX Software Control-Audit for NAS, Hitachi Edition, it is highly recommended to verify that the installation server meets the requirements listed in the *Requirements* section of this document.

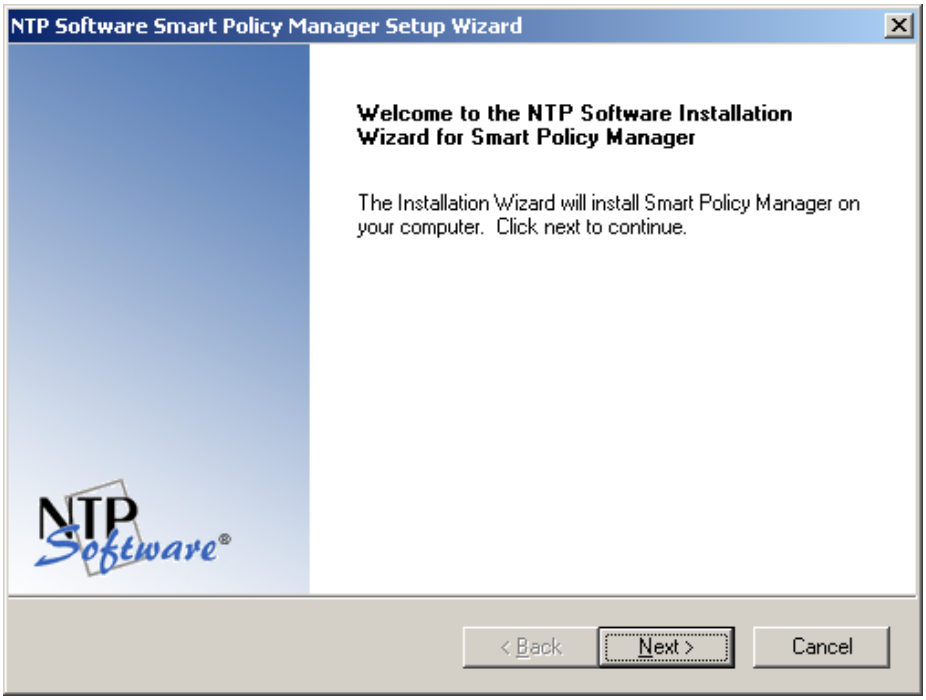
Installing DefendX Software Smart Policy Manager

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

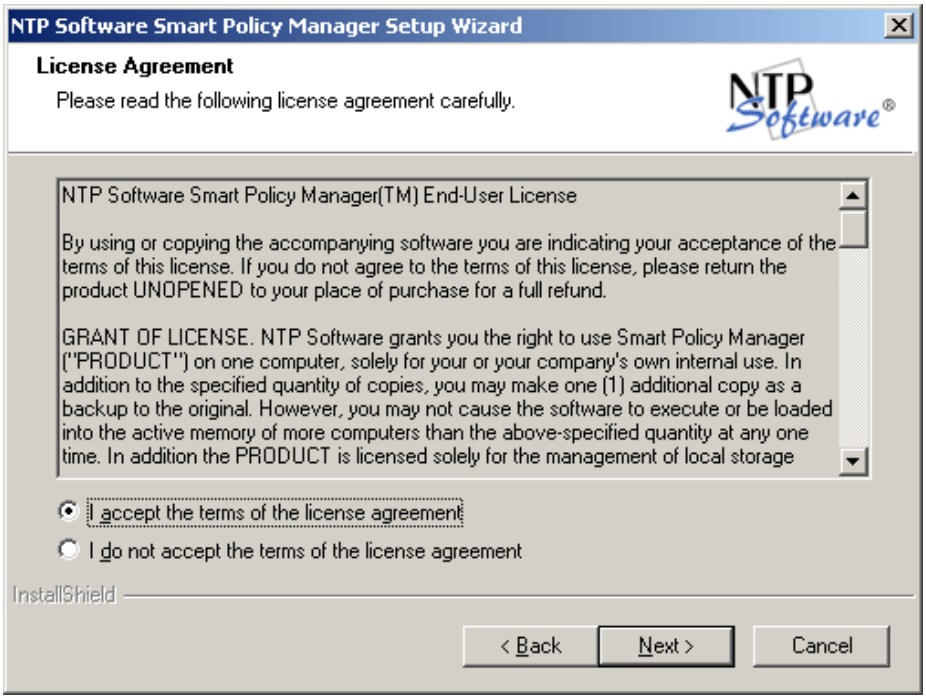
2. Run the DefendX Software Control-Audit installer. If DefendX Software Smart Policy Manager is not installed, the following installer will launch automatically. If DefendX Software Smart Policy Manager is installed, you can skip to the section on Installing DefendX Software Control-Audit for NAS, Hitachi Edition.



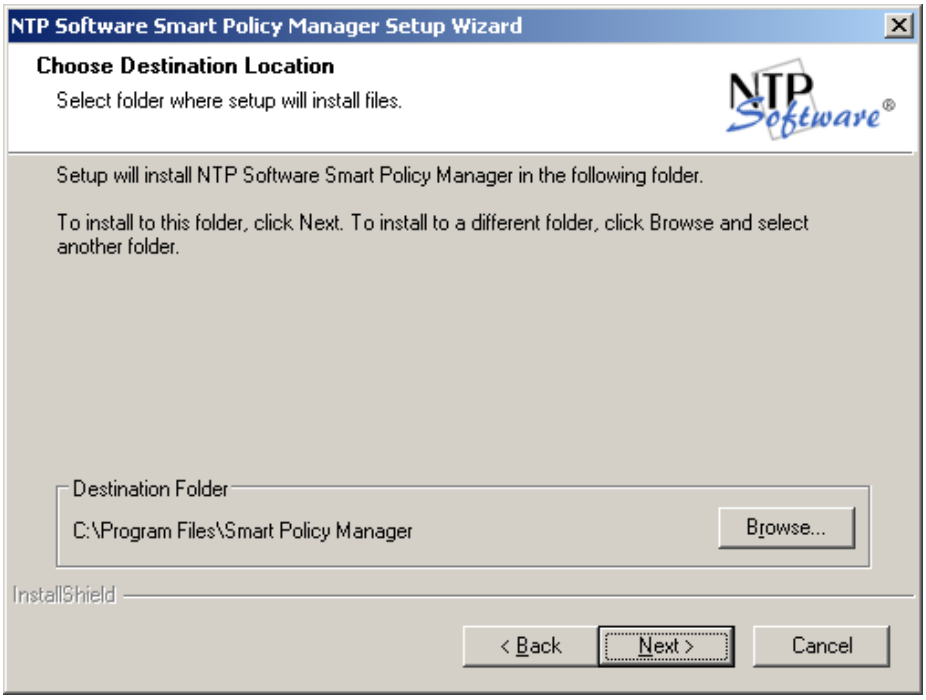
3. The DefendX Software Smart Policy Manager Installation Wizard opens. Click **Next** to begin the installation.



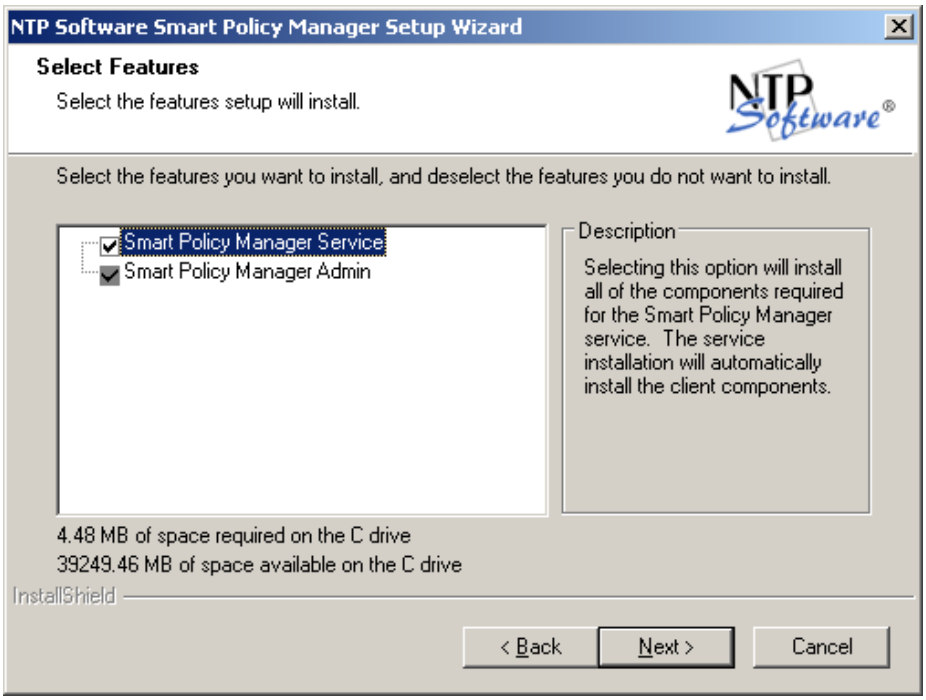
4. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



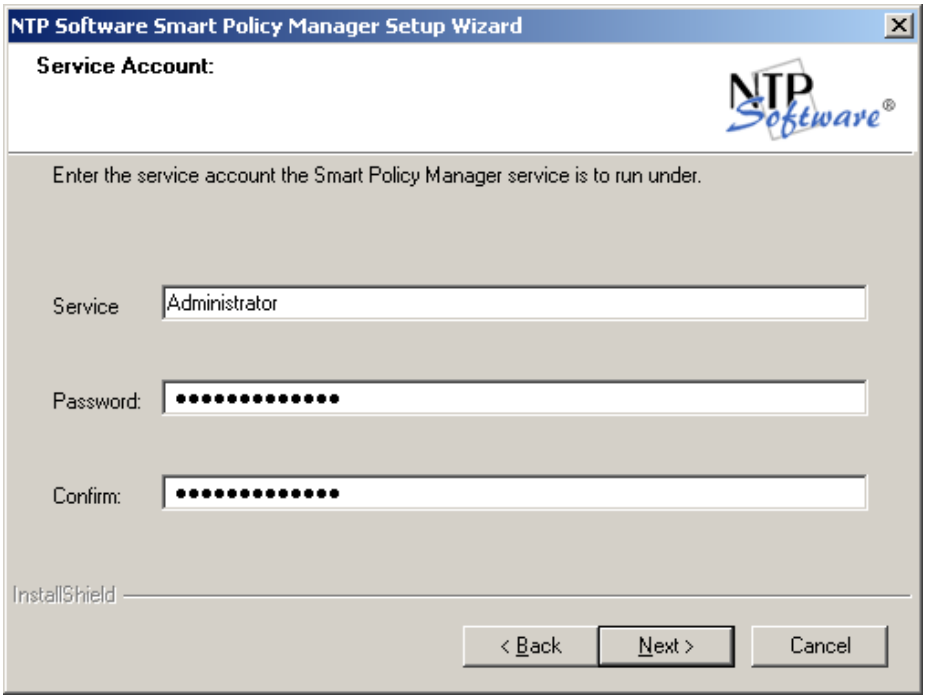
5. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Smart Policy Manager and then click **Next**.



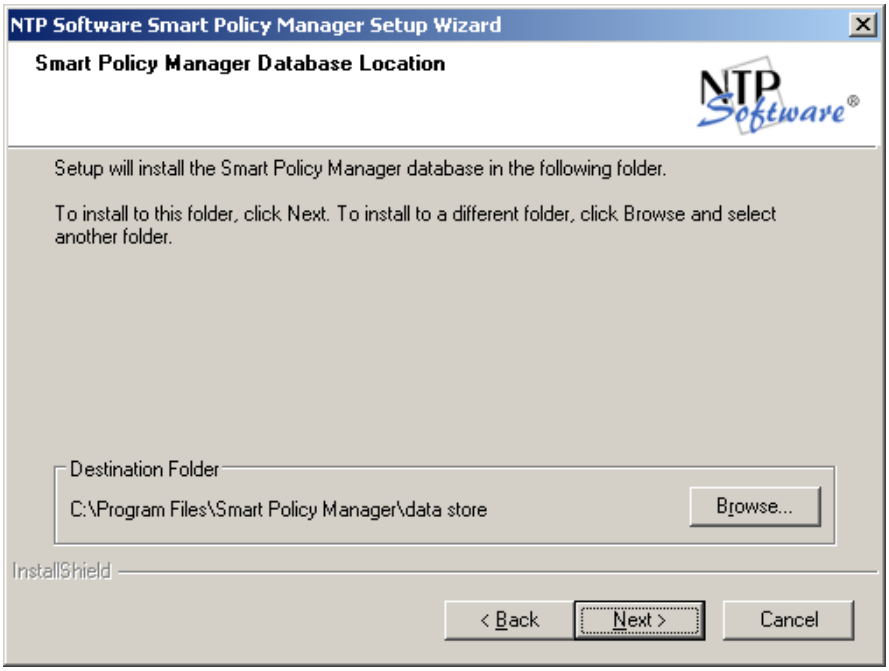
6. In the **Select Features** dialog box, select the components you want to install and then click **Next**.



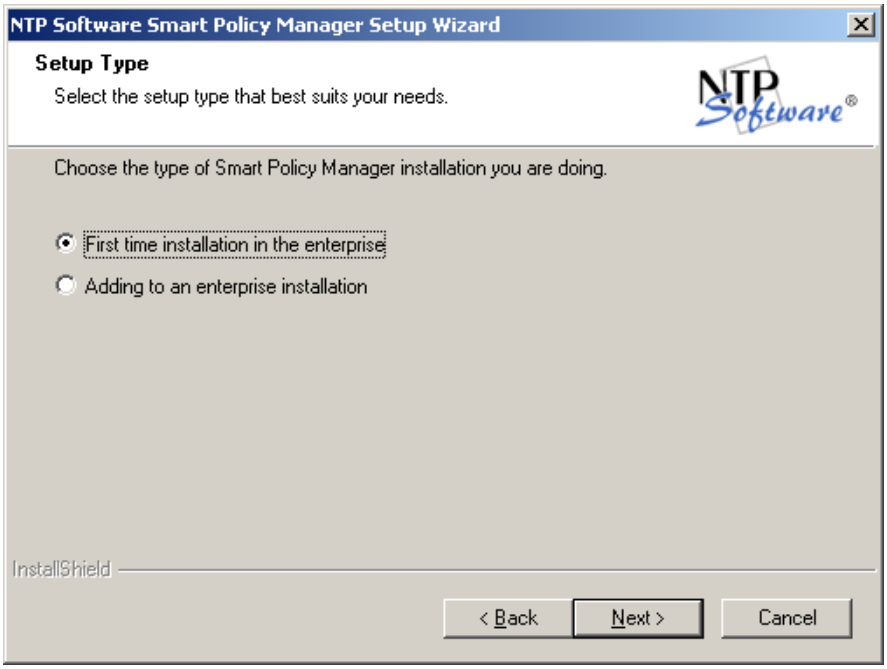
7. In the **Service Account** dialog box, when prompted for a Windows domain user account to run the DefendX Software Smart Policy Manager service, enter the username and password for a domain user account with administrative rights on the local machine. Click **Next**.



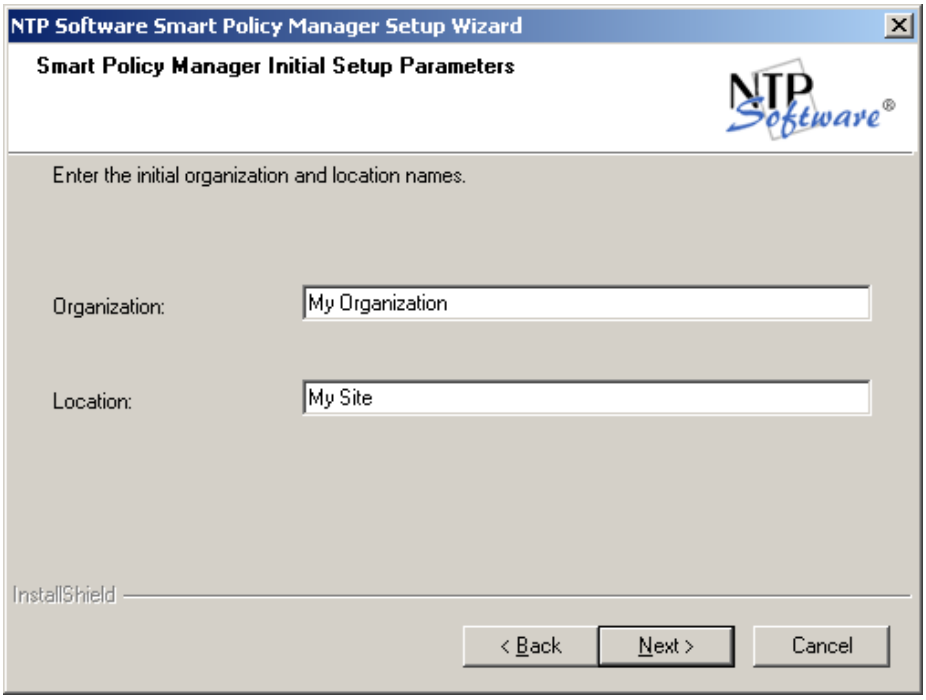
8. In the **Smart Policy Manager Database Location** dialog box, enter the directory name where you want to install the DefendX Software Smart Policy Manager database or just accept the default location. Click **Next**.



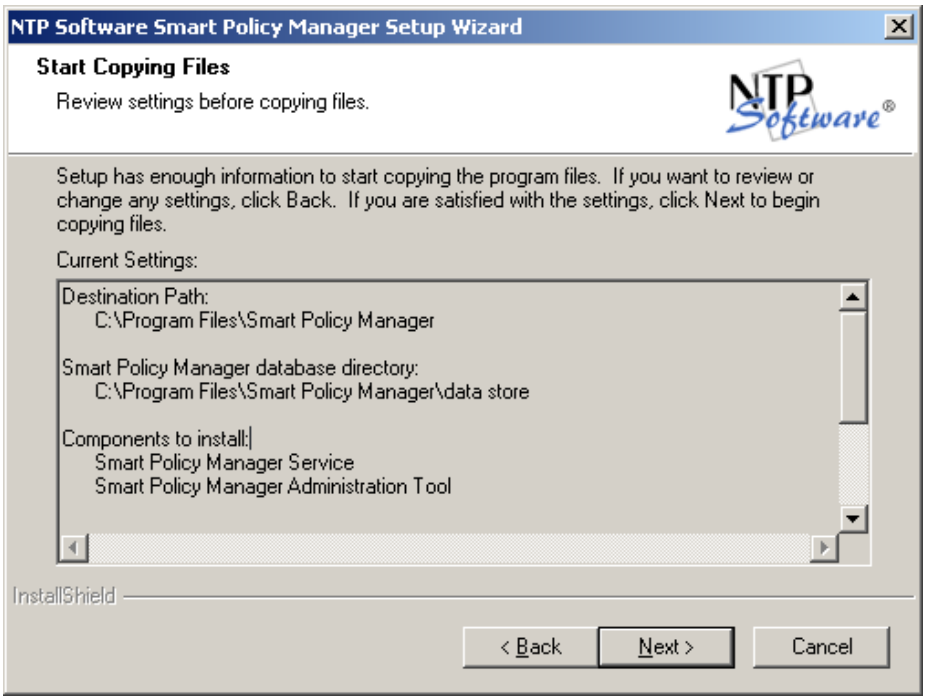
9. In the **Setup Type** dialog box, select the DefendX Software Smart Policy Manager installation type for your environment. If installing to a new environment with no prior DefendX Software Smart Policy Manager installations, click **Next**. If installing in an environment in which DefendX Software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



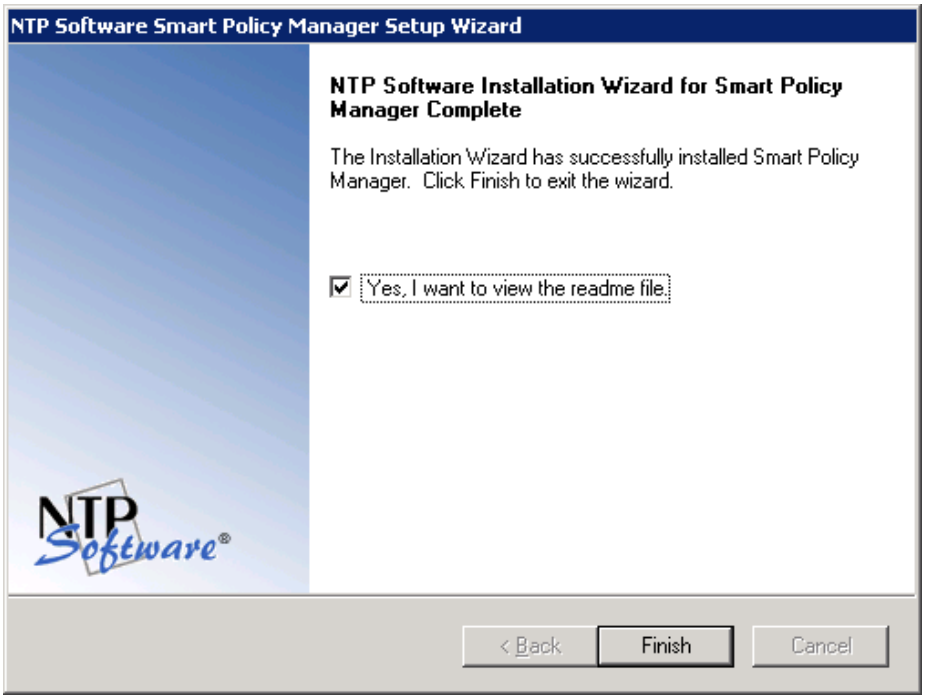
10. In the **Smart Policy Manager Initial Setup Parameters** dialog box, provide DefendX Software Smart Policy Manager with a name for your organization and a location name for this DefendX Software Smart Policy Manager instance, or accept the default settings. Click **Next**.



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.



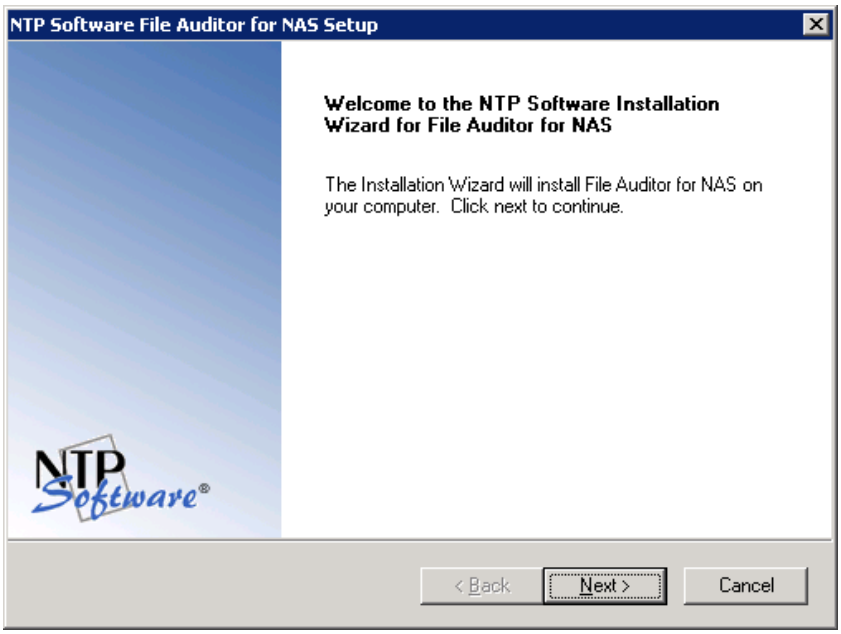
12. If you want to view the DefendX Software Smart Policy Manager readme file, check the **Yes, I want to view the readme file** checkbox. Then click **Finish**.



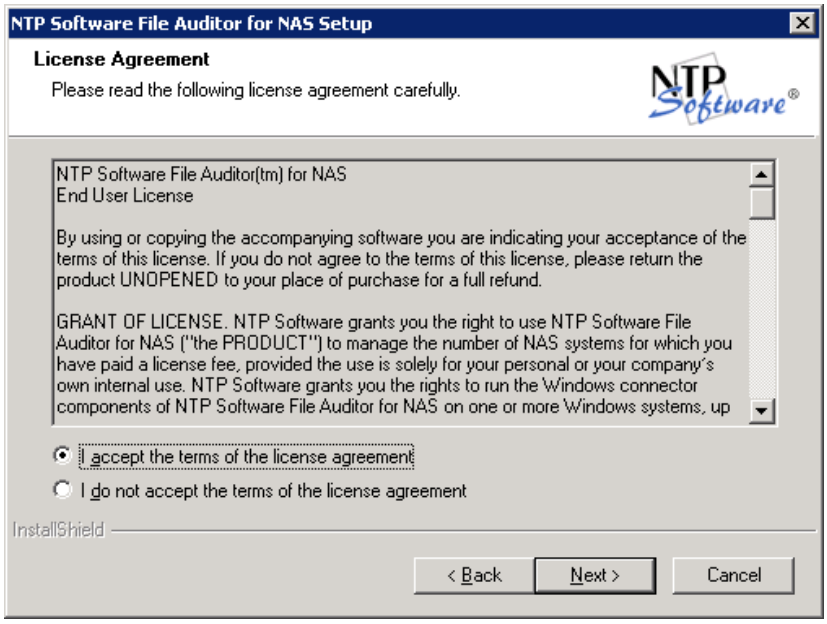
Installing DefendX Software Control-Audit for NAS, Hitachi Edition

1. If you have followed the steps in the Installing DefendX Software Smart Policy Manager section, you will be directed to the next step automatically.

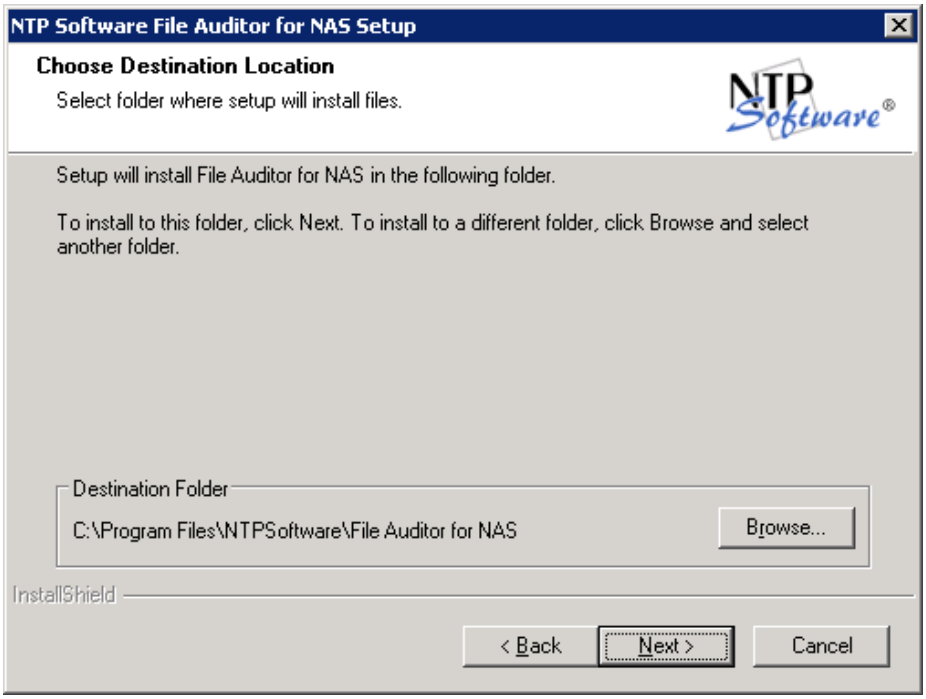
2. When the DefendX Software Control-Audit for NAS Installation Wizard opens, click **Next** to begin the installation.



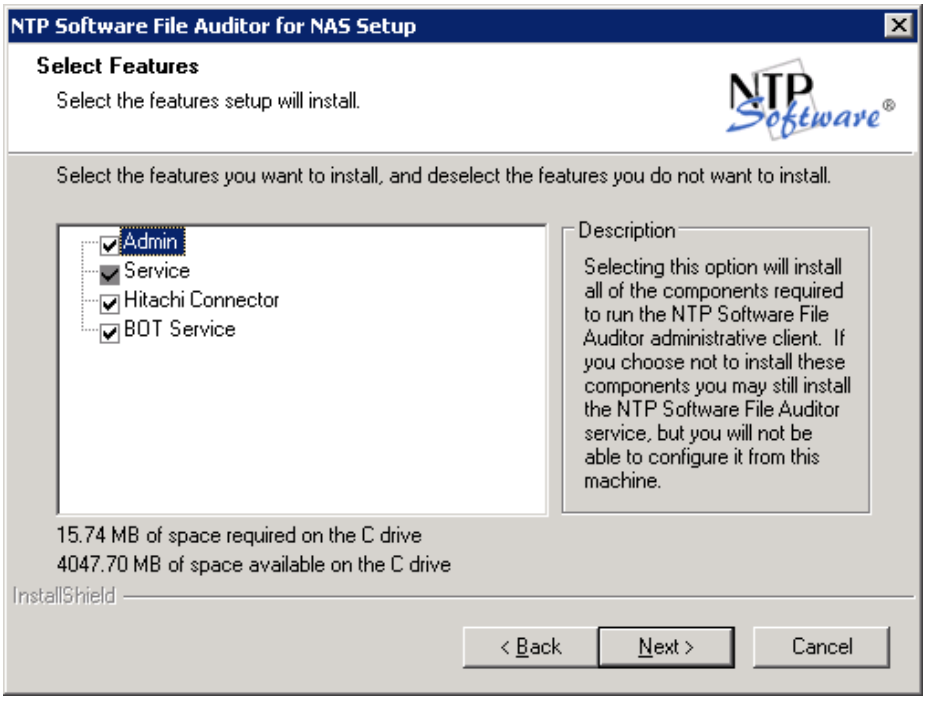
3. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



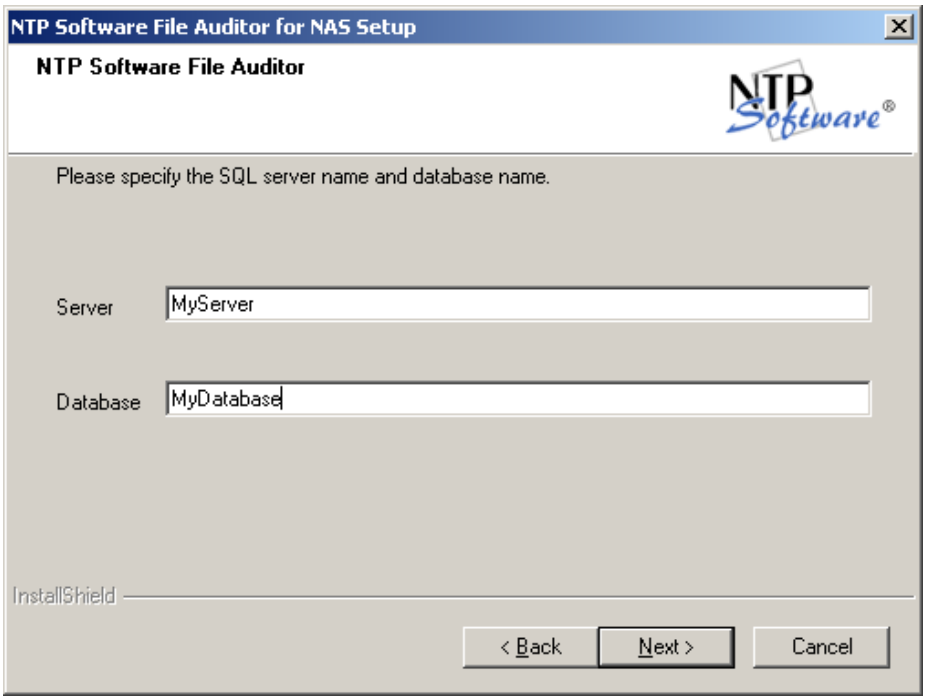
4. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Control-Audit and then click **Next**.



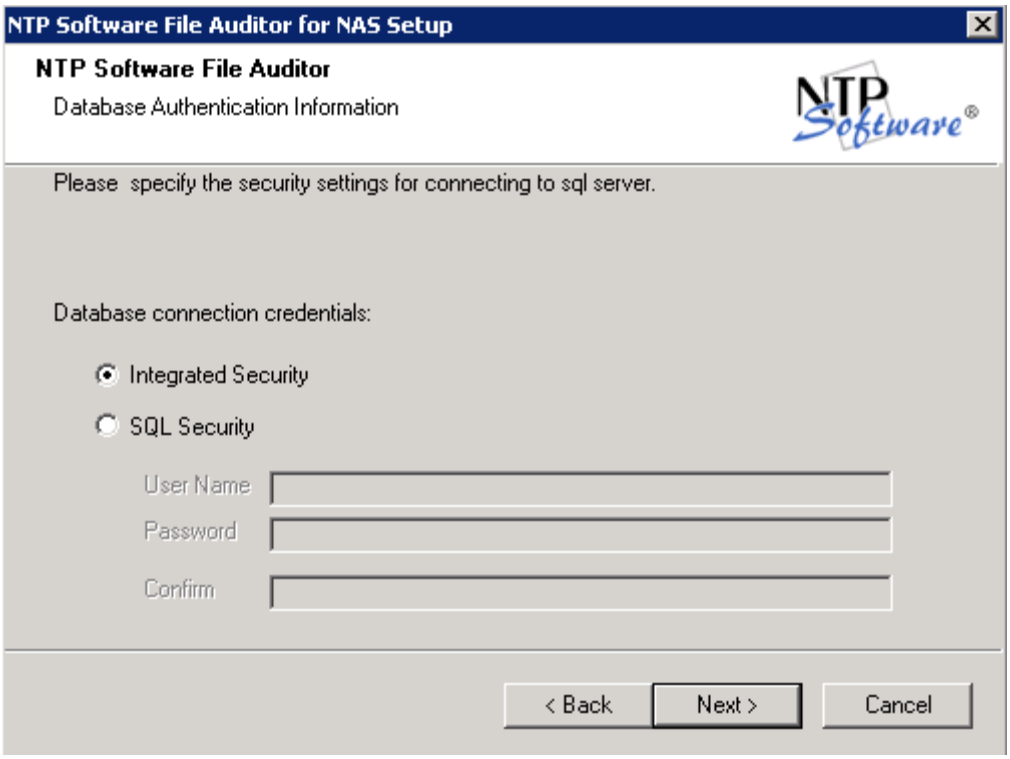
5. In the **Select Features** dialog box, select the components to be installed on the local machine. The **Admin** component allows for administration of the DefendX Software Control-Audit service. The **Hitachi Connector** component is required if this machine will need to communicate with a Hitachi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



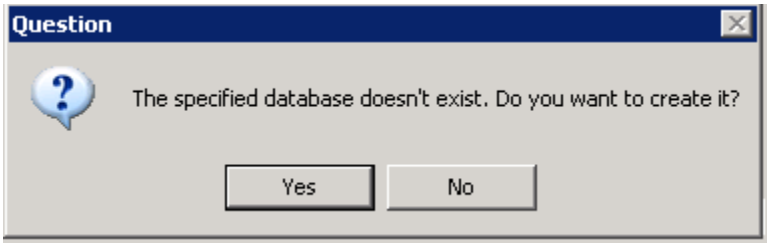
6. In the **DefendX Software Control-Audit** dialog box, provide your SQL Server name and your database name.



7. 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.

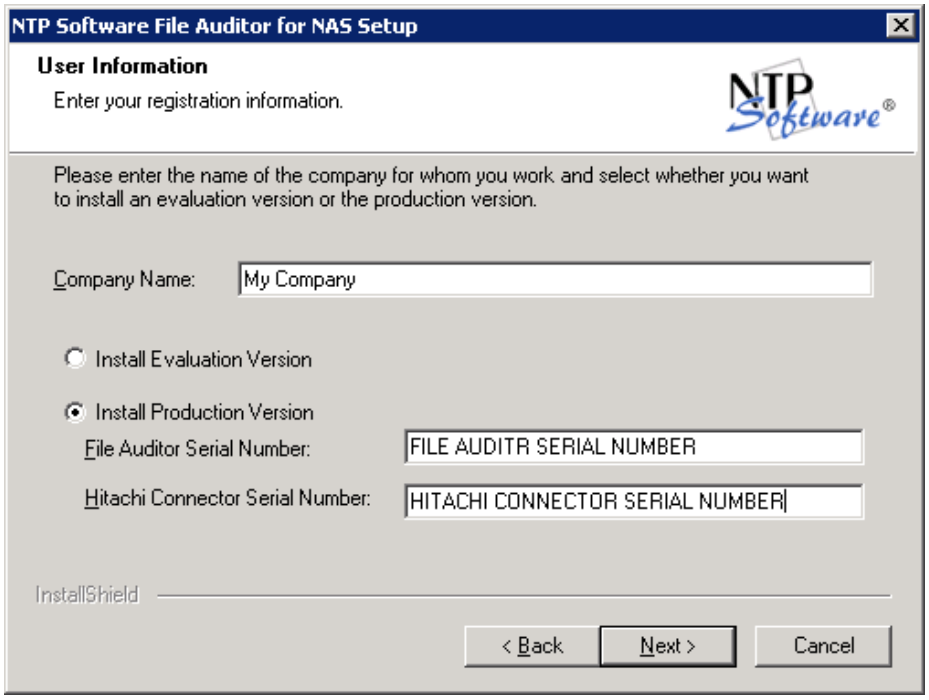


If the database doesnot exist, the question dialog below will be displayed. Click the **Yes** button. If you wish to create the database yourself, run the SQL Scripts in the Control-Audit for NAS installation folder after the setup is complete. The script file is "Control-Audit DB Schema and User Script.sql".

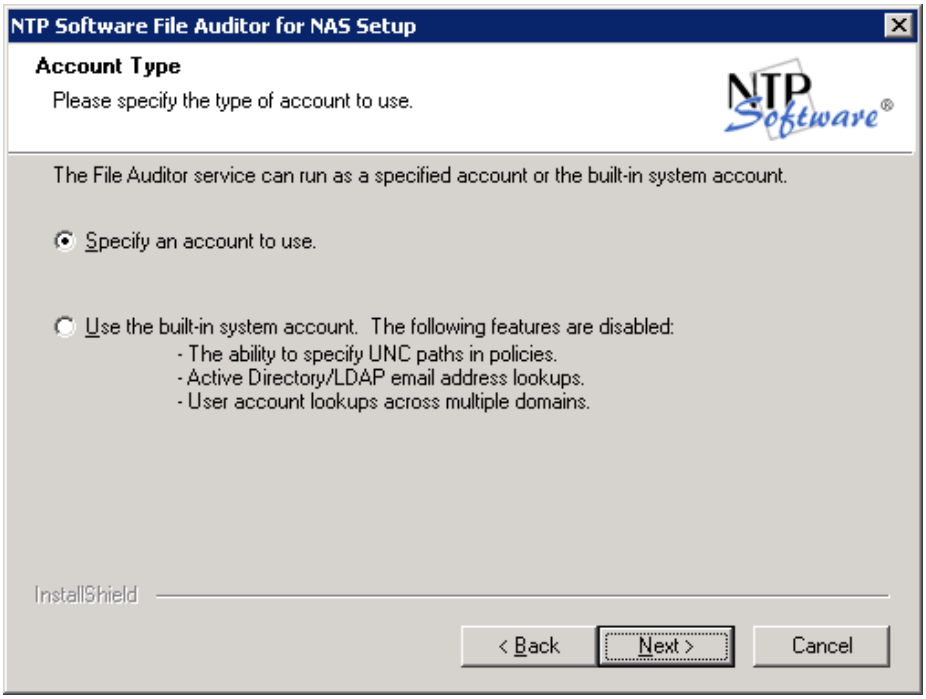


NOTE: If you are upgrading from Control-Audit 2.2 or older versions, the installer will prompt for upgrading the database. Alternatively, you can run the upgrade script manually; the script file "Control-Audit DB Upgrade Script.sql" is located in the Control-Audit installation directory after the setup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

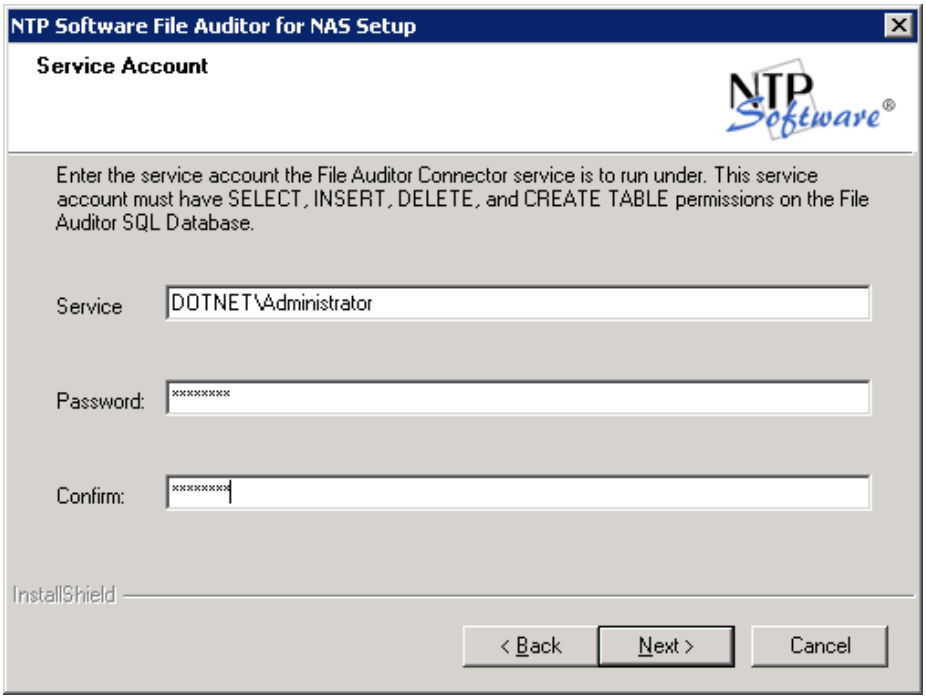
8. In the **User Information** dialog box, provide your company name. Select the **Install Evaluation Version** option if you wish to try the evaluation version of the software. Otherwise, please insert your DefendX Software Control-Audit and Hitachi Connector serial numbers. Click **Next**.



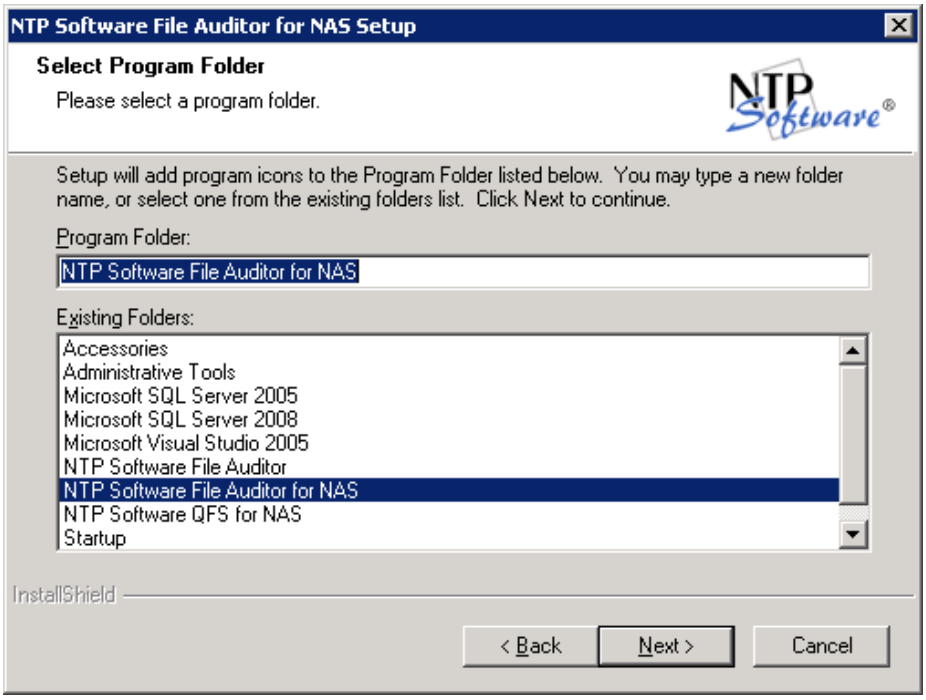
9. In the **Account Type** dialog box, specify the account type to be used. Click **Next**.



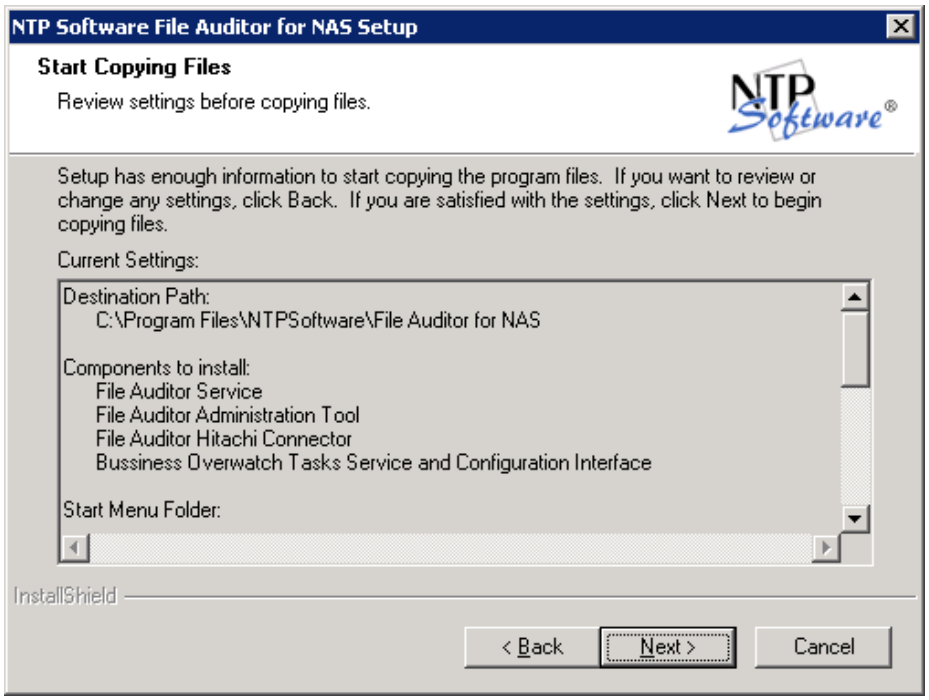
10. In the **Service Account** dialog box, when specifying an account, enter a username with local administrative privileges. This account will be used to log in and monitor file and directory operations. Click **Next**.



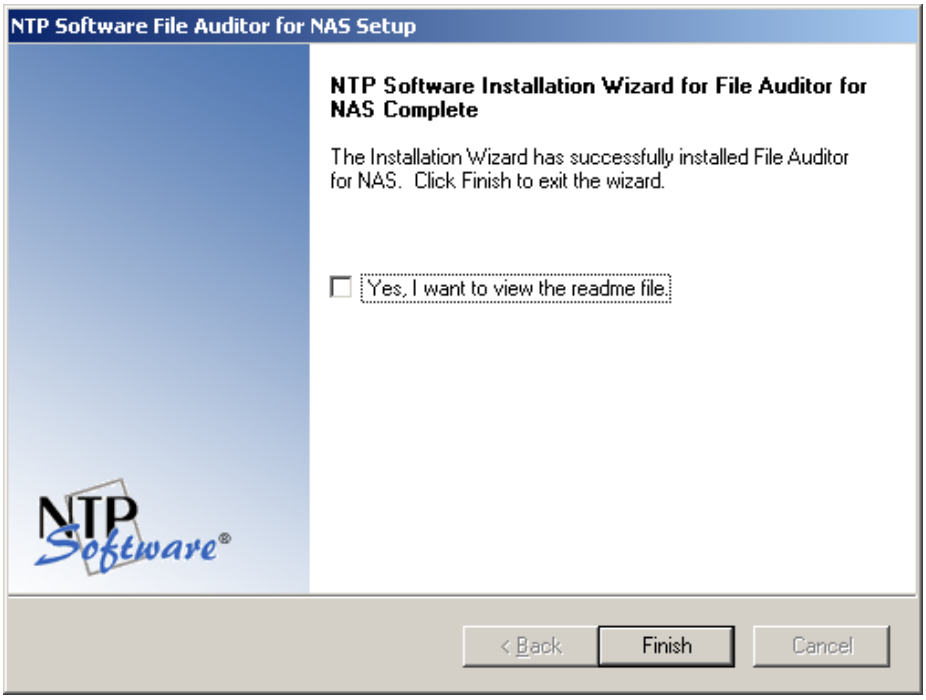
11. In the **Select Program Folder** dialog box, select the program folder to host the DefendX Software Control-Audit for NAS startup group. Click **Next**.



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



13. 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, Hitachi Edition Configuration Wizard will open.



14. Once you click Finish, the Hitchi EVS Configuration Wizard will be displayed.

Installing DefendX Software Control-Audit Reports, Hitachi Edition

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

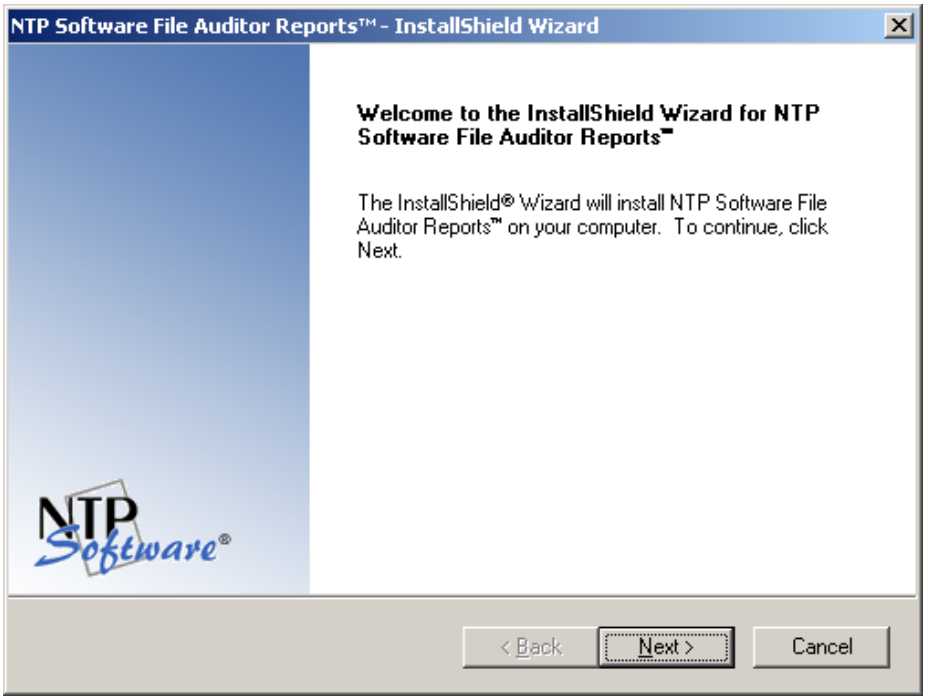
NOTE: The user installing the Control-Audit Reports must be assigned the Content Management role. To assign a user the Content Management role; follow the following steps:

a. Open SQL Server Reporting Services URL on the host machine – example: [http://[SQLReportingHostMachine]/Reports].

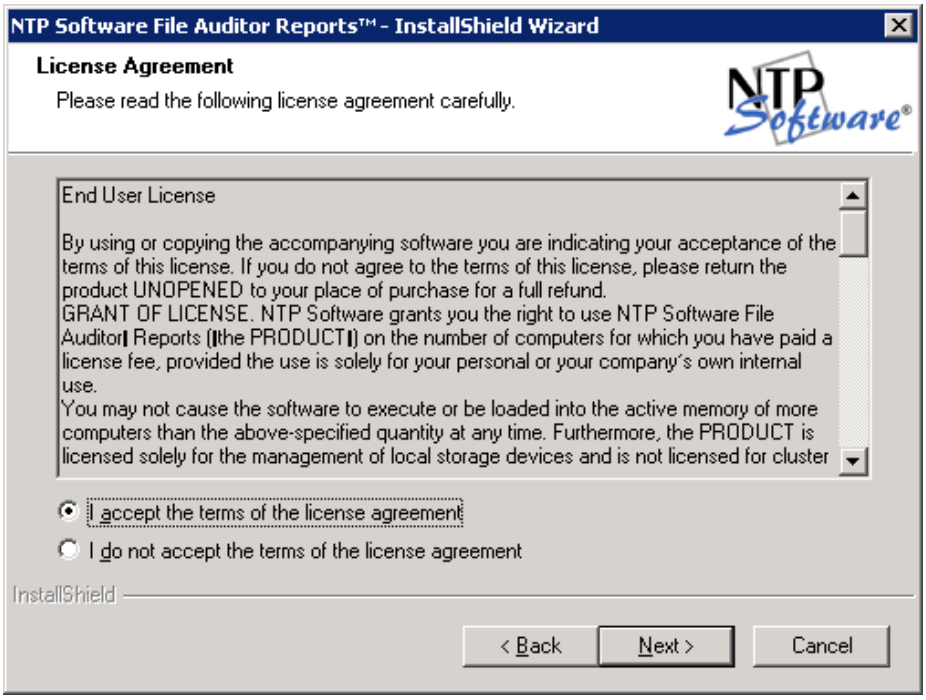
b. Navigate to the **Properties** tab.

c. Navigate to the **Security** tab.

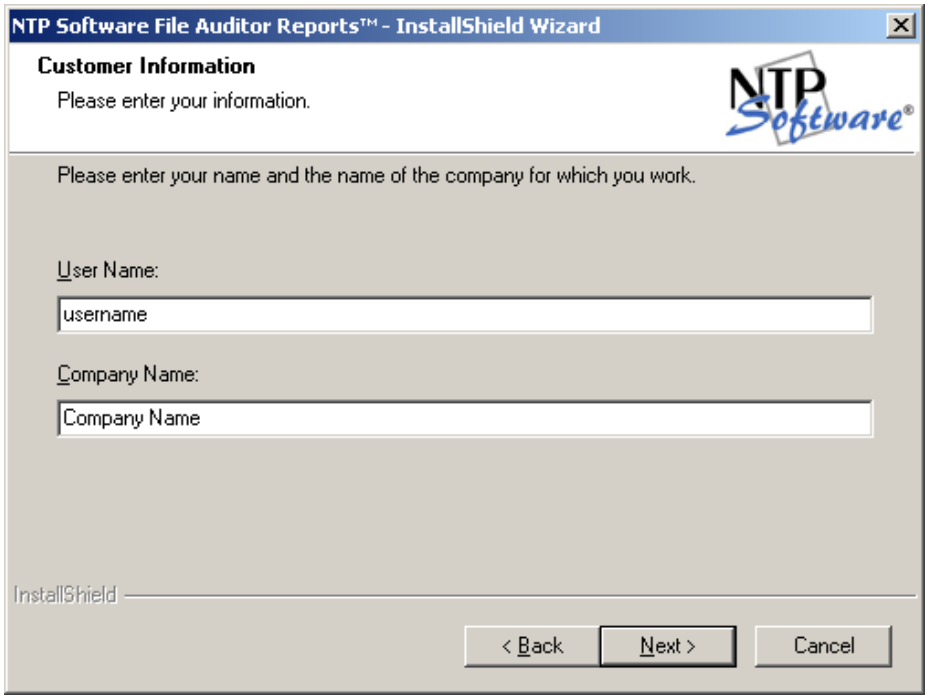
d. Create a new Role by clicking **New Role Assignment** or edit an already existing Group or User.



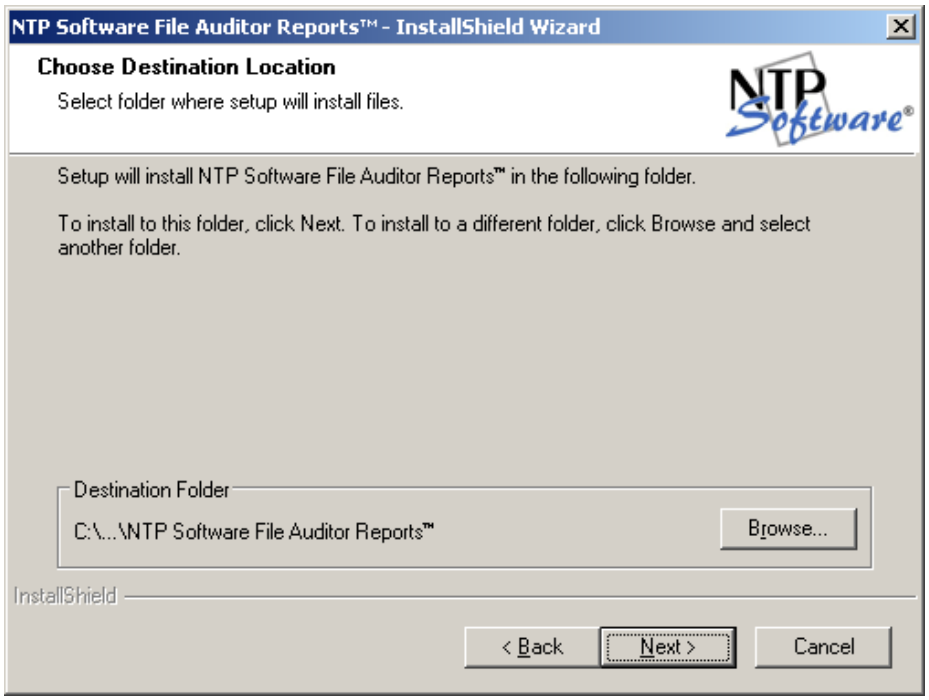
2. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



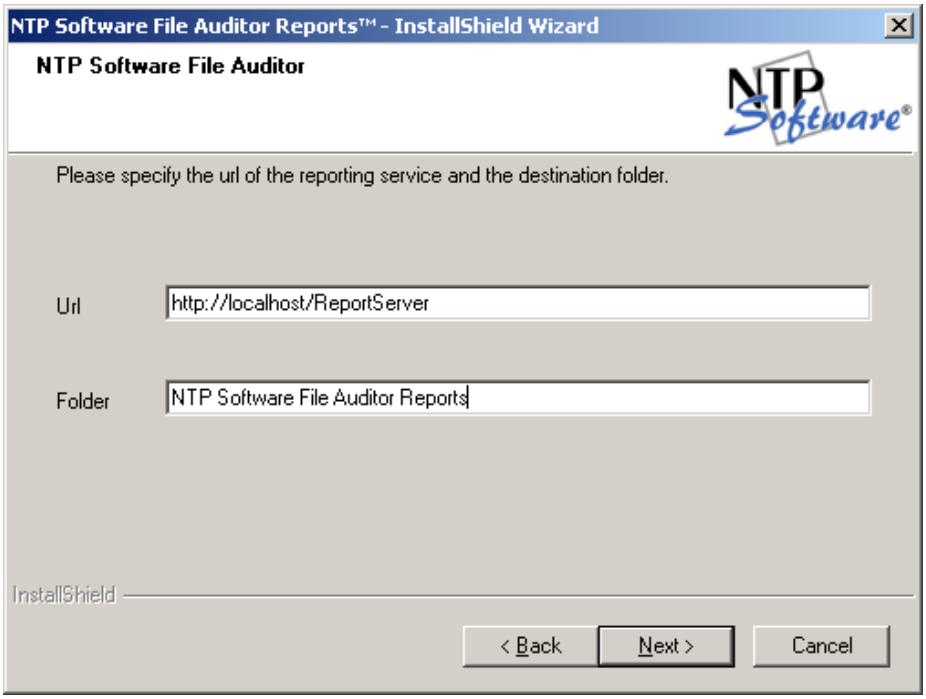
3. In the **Customer Information** dialog box, provide your user name and the company name. Click **Next**.



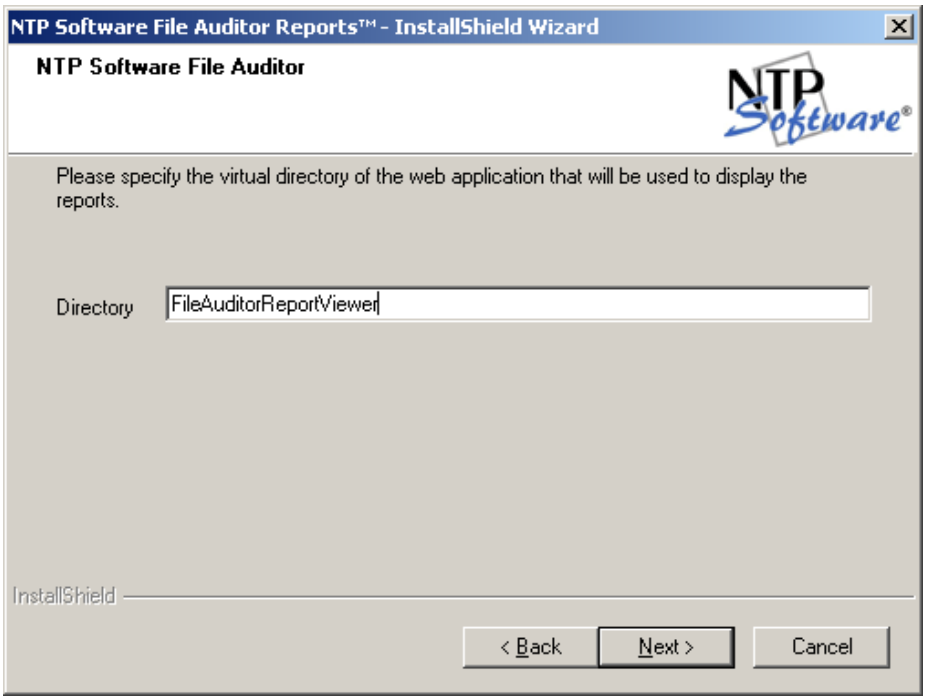
4. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Control-Audit Reports and then click **Next**.



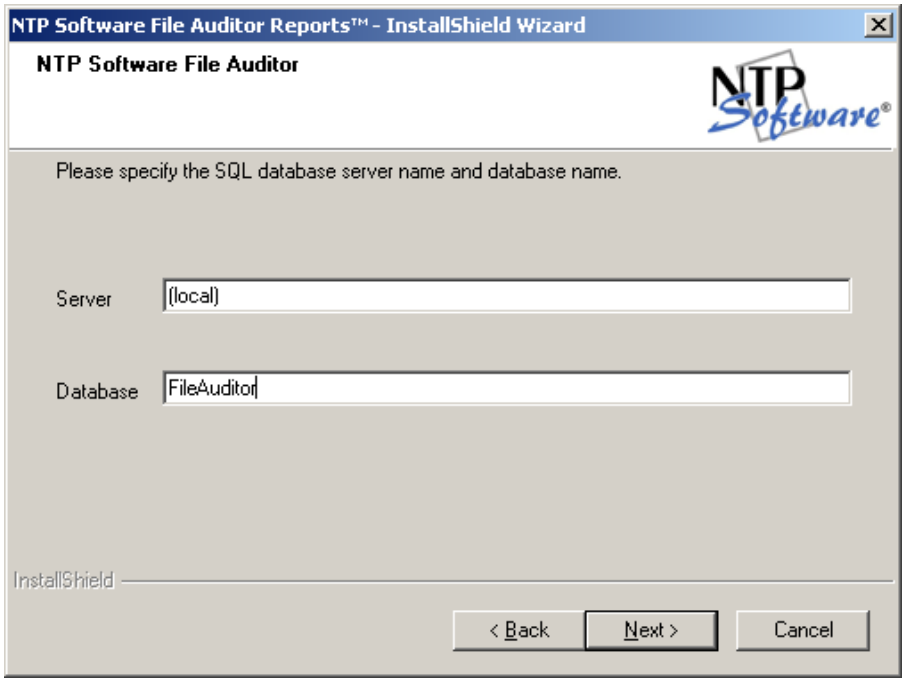
5. In the **DefendX Software Control-Audit** dialog box, specify the URL of the reporting service and the destination folder. Click **Next**.



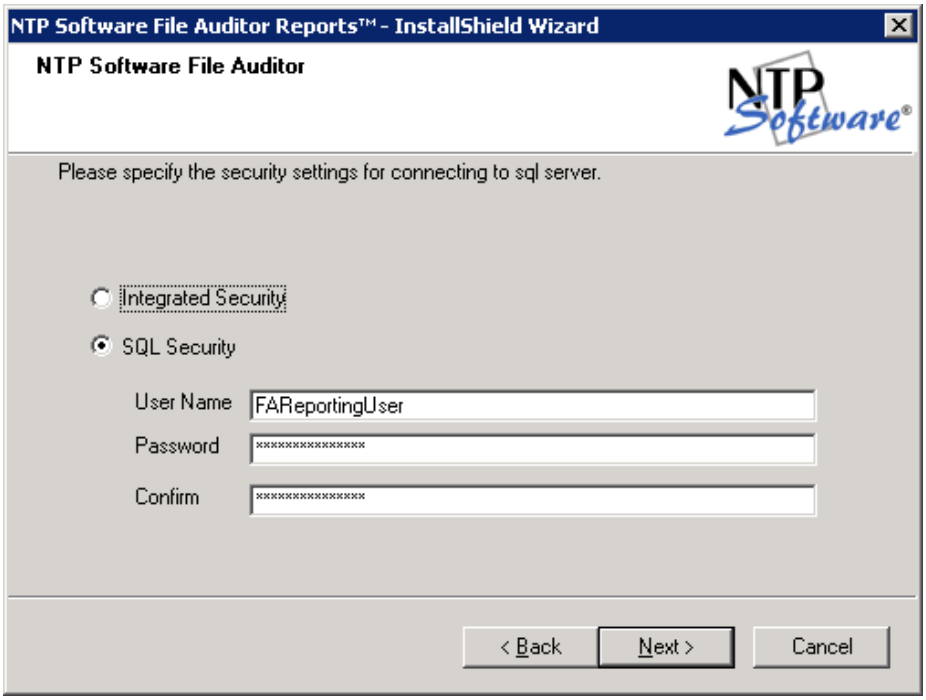
6. In the **DefendX Software Control-Audit** dialog box, specify the web application virtual directory. Click **Next**.



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**.



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



NOTES:

- Control-Audit has a default user "DFXReportingUser" and default password “DFXReportingUser” 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, “DFXReportingUser” 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 logged-in Windows user account to access the Database. The Windows user account must be given read access to the Control-Audit Database, or that user account must be added to a group that has read access to the Control-Audit Database.
- 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.
- 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. Specify the needed data source.

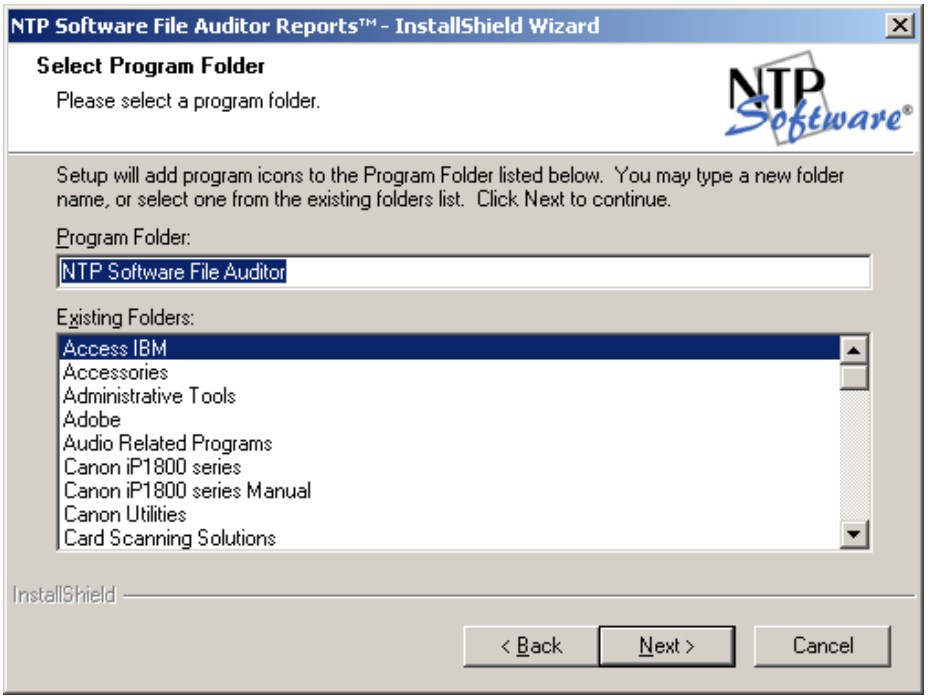
- The network users who should run to the reports must assigned to the browser role on reporting Service reports. To give a user or group access to the reports, you need to do the following:

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.

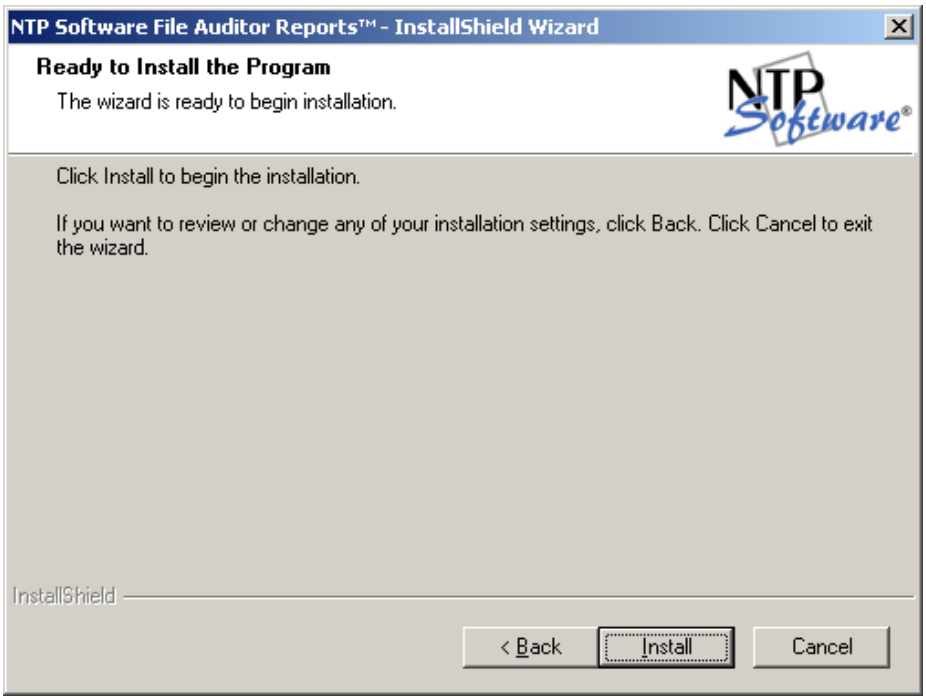
3. Open the **Properties** top tab, then select the **Security** left tab.
4. Click on **New Role Assignment**.
5. Write the user or group name, select the **Browser** role, then click **OK**.

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

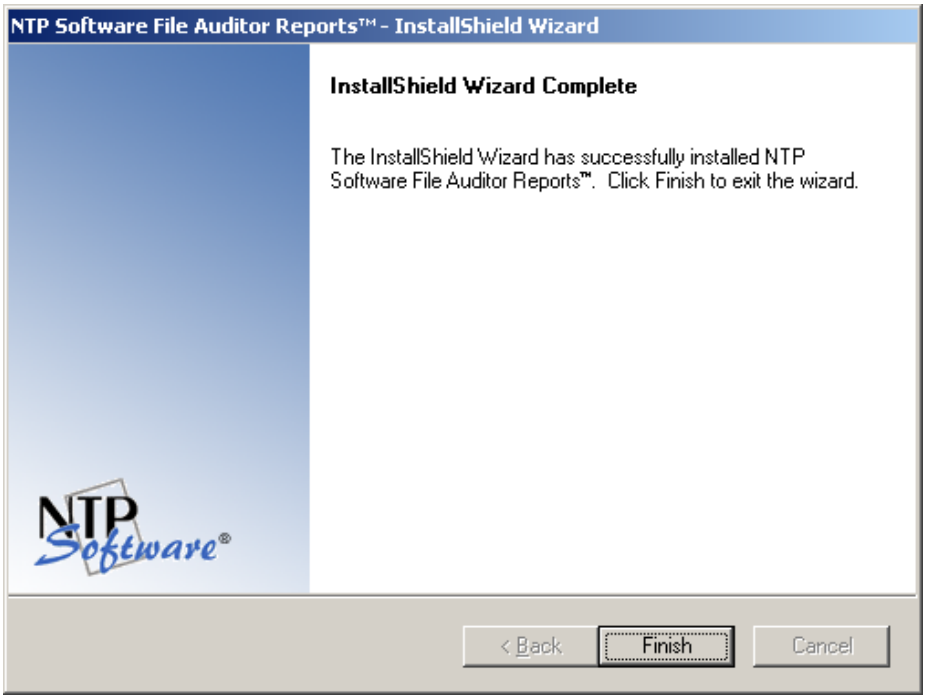
10. In the **Select Program Folder** dialog box, select the program folder to host the DefendX Software Control-Audit for NAS startup group. Click **Next**.



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

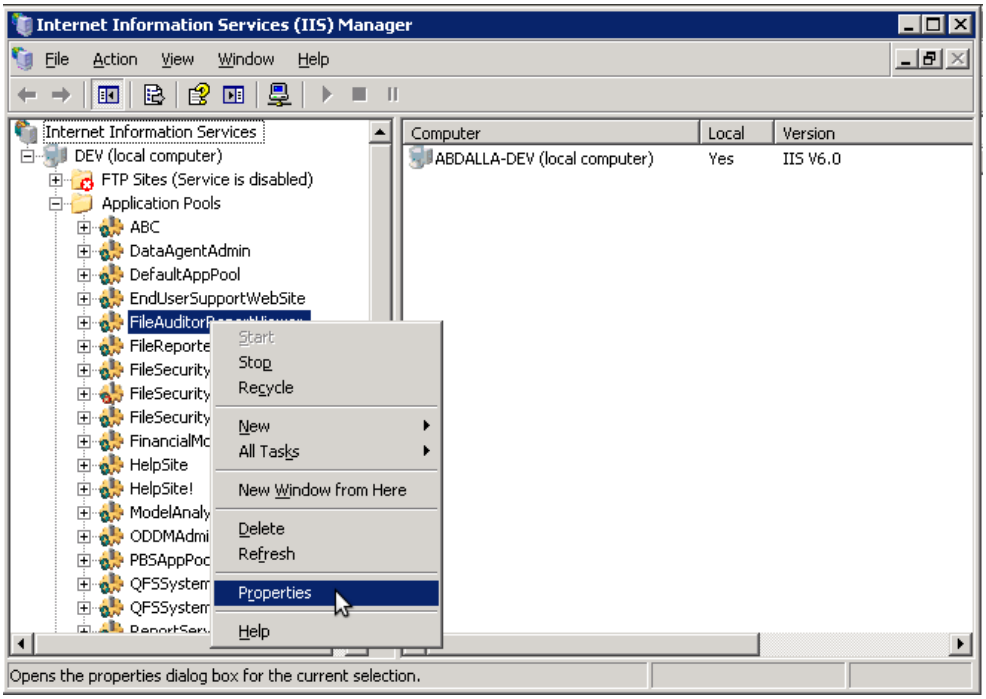
For the Historical Data feature to function properly under the **Integrated Security** setting, the Windows user account who will recall the historical data should have ADMINISTER BULK OPERATIONS permission to the database, along with ALTER and INSERT permissions to the HistoricalOperations and HistoricalDACLs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

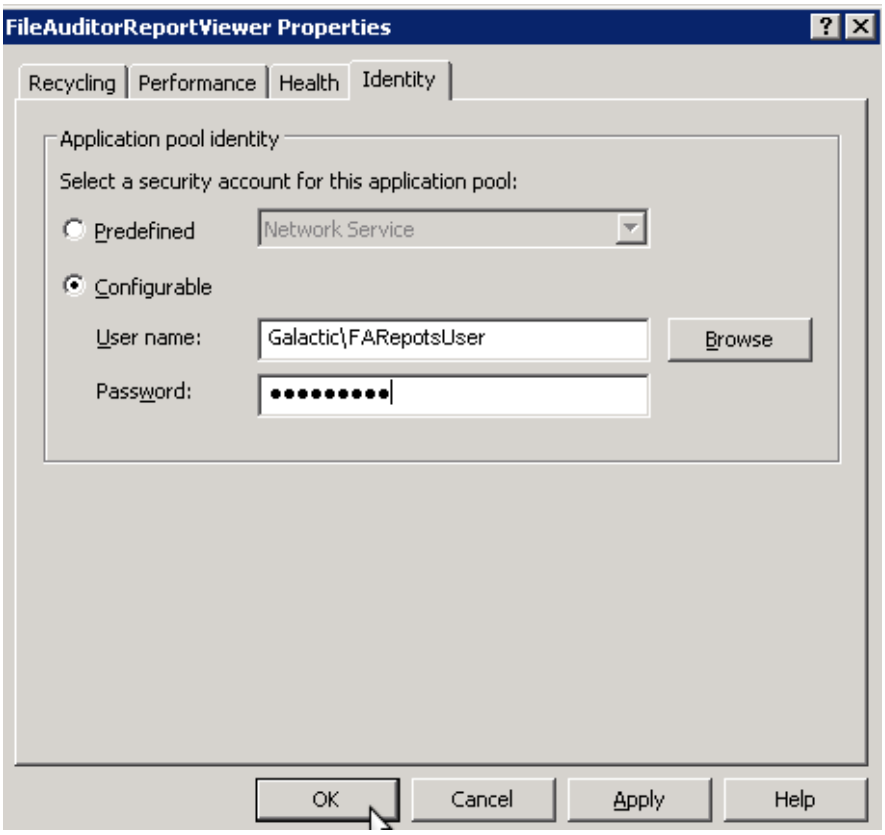
To assign a User Account to an Application Pool in IIS 6, please perform the following steps:

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

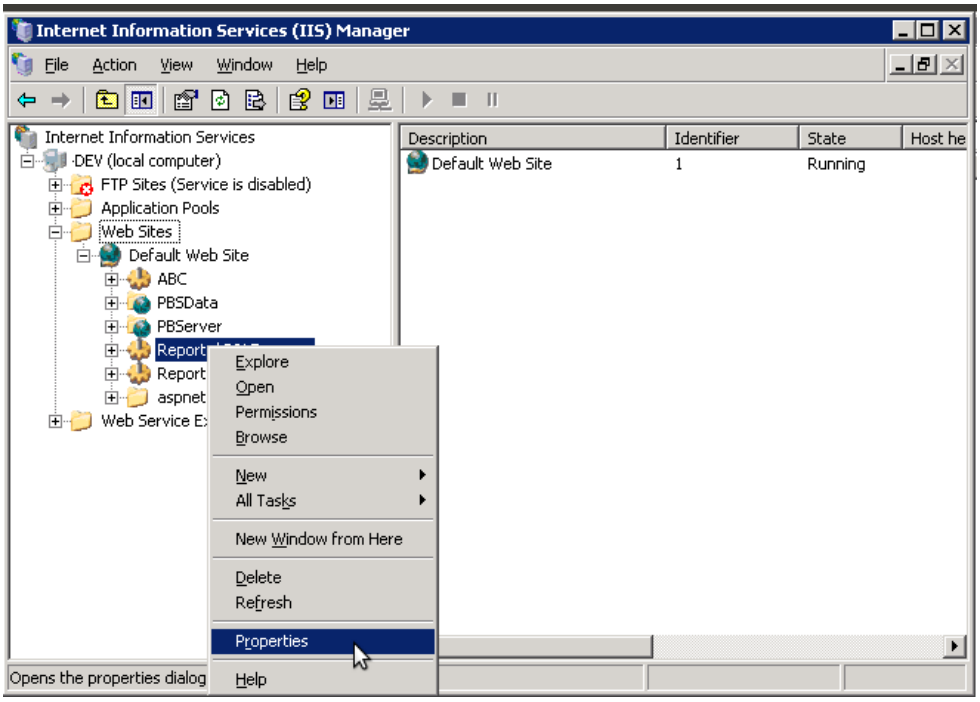


3. In the **Identity** tab select **Configurable**.

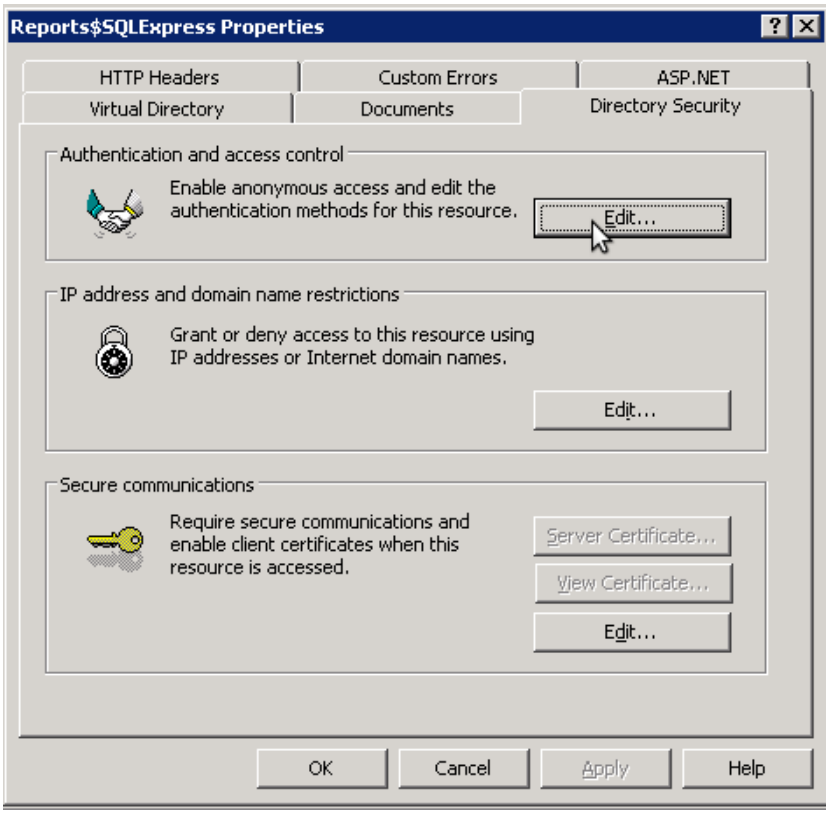
4. Enter the account details, then click **OK**.



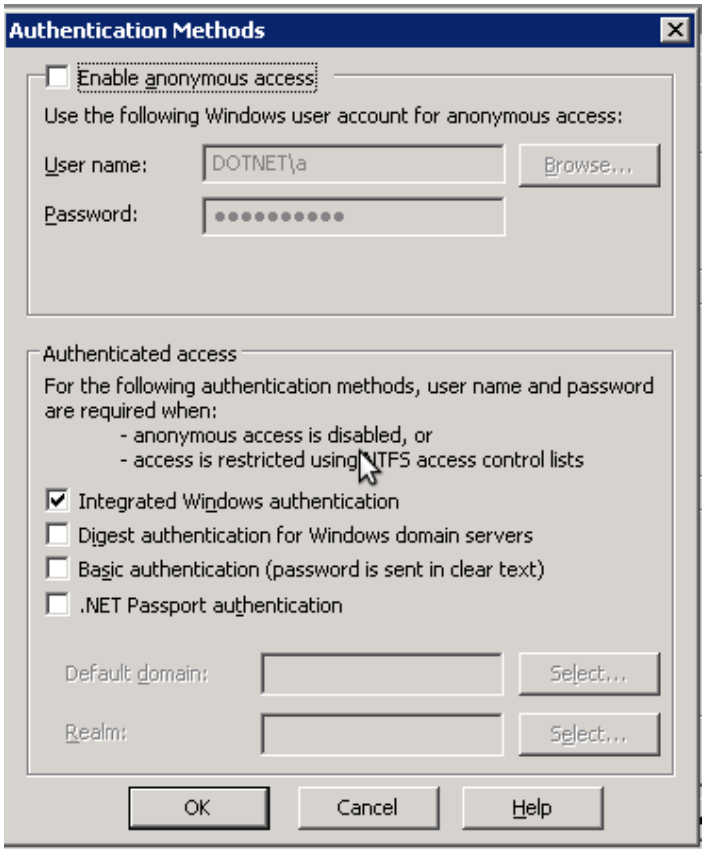
5. Open the DFXReportViewer website properties.



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

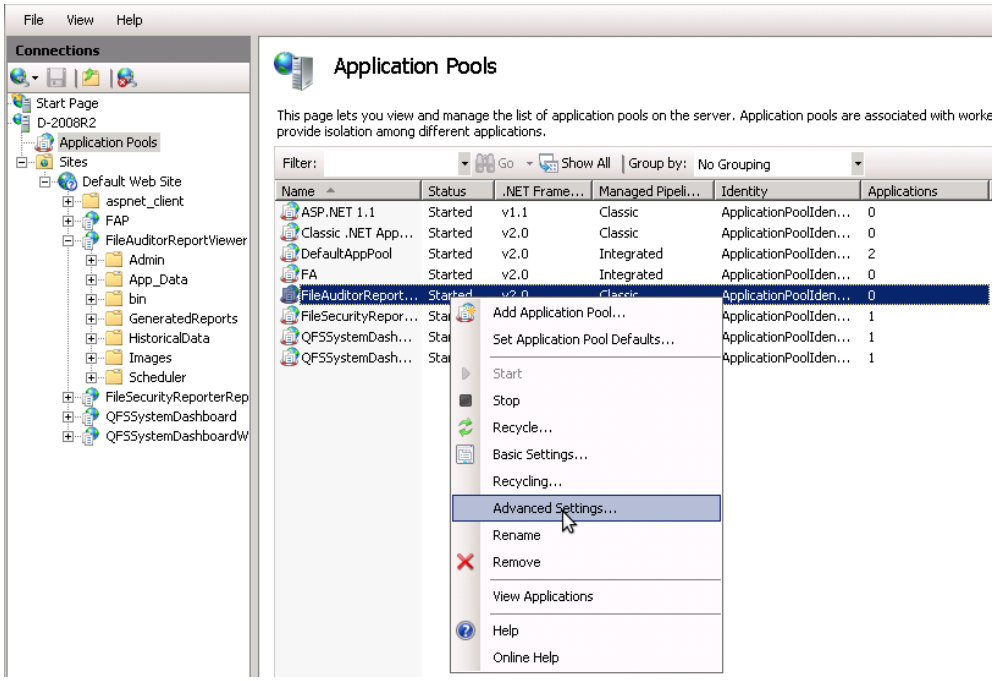


7. Disable all authentication methods except **Integrated Windows Authentication**.

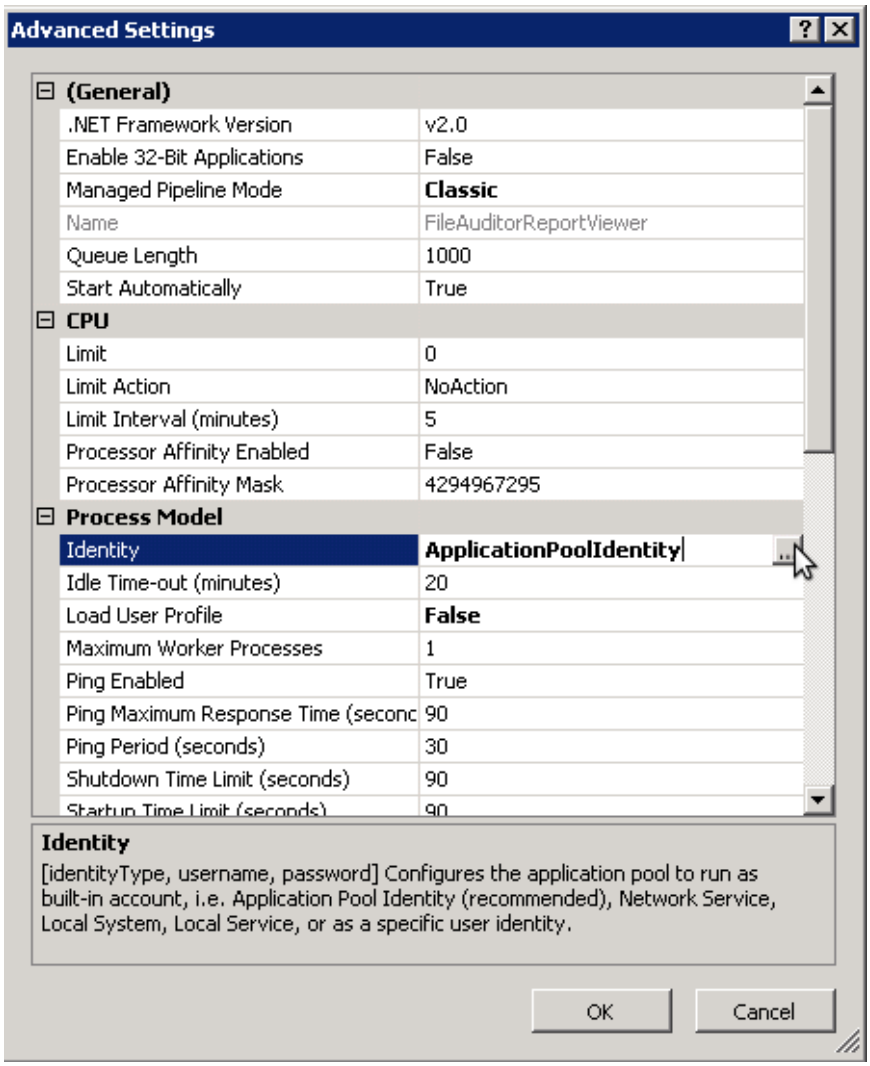


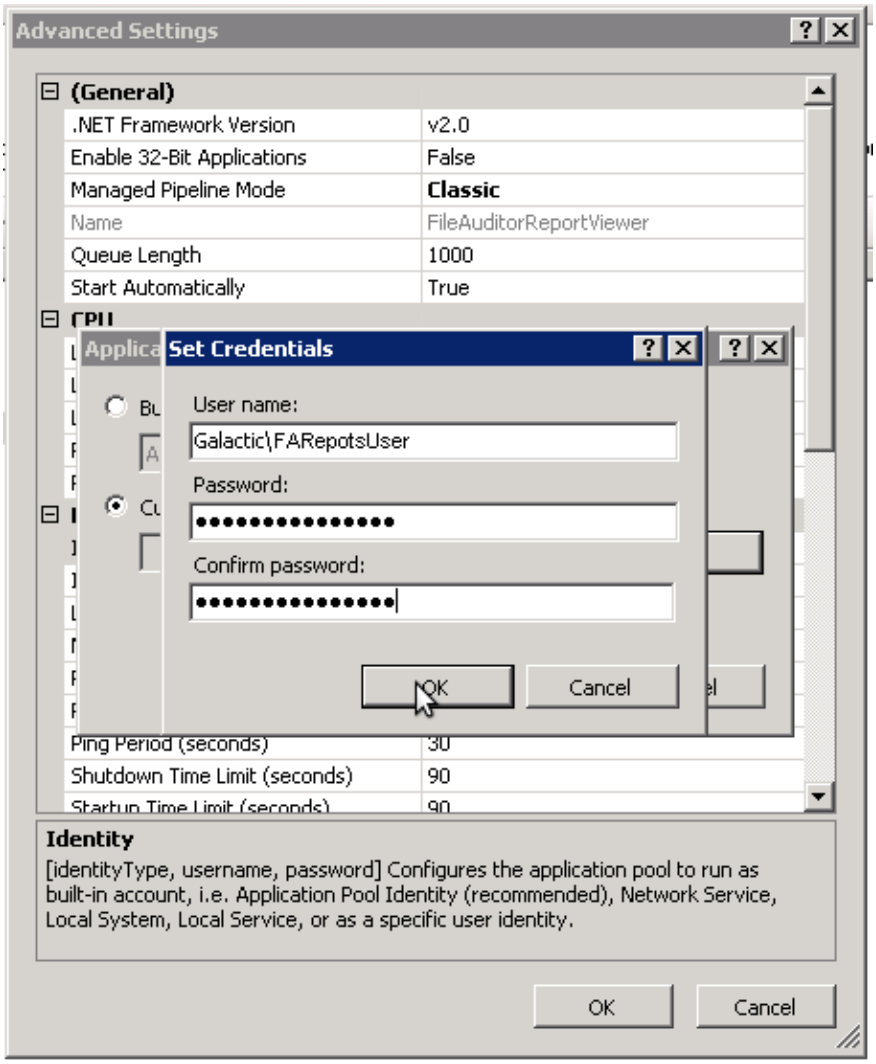
To assign a User Account to an Application Pool in IIS 7, please perform the following steps:

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

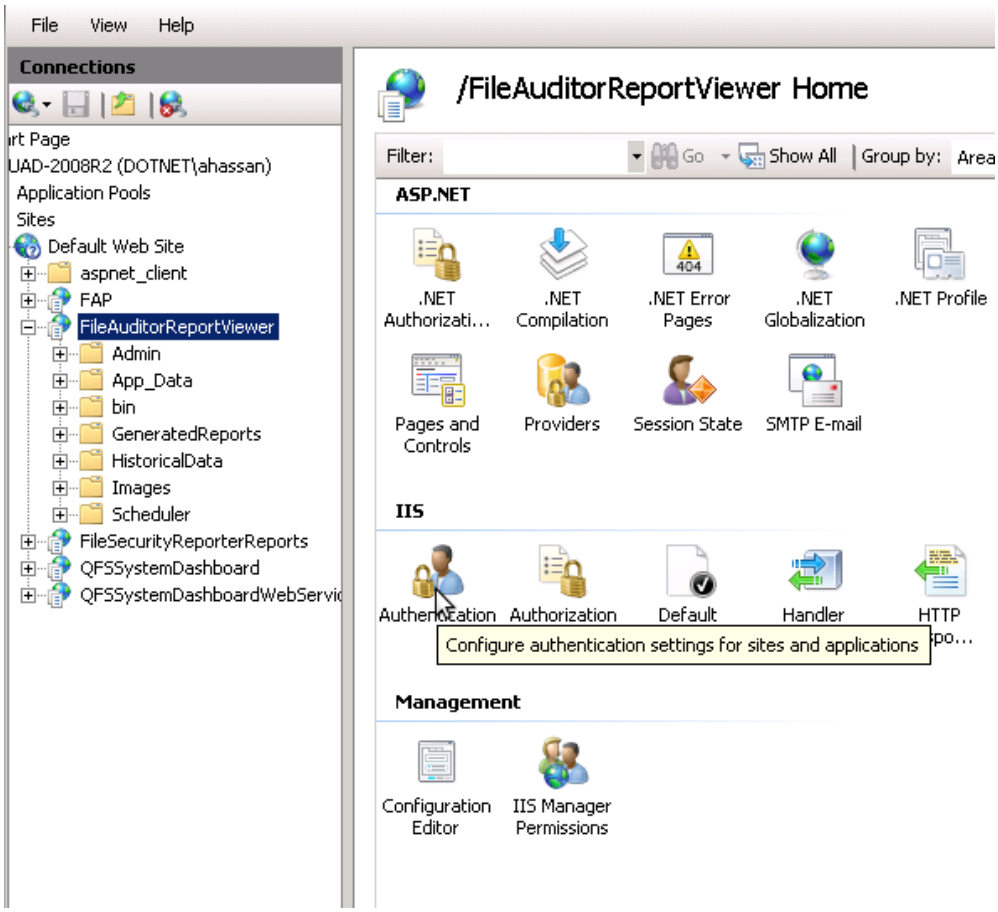


3. Change the default app pool created to the user you need.

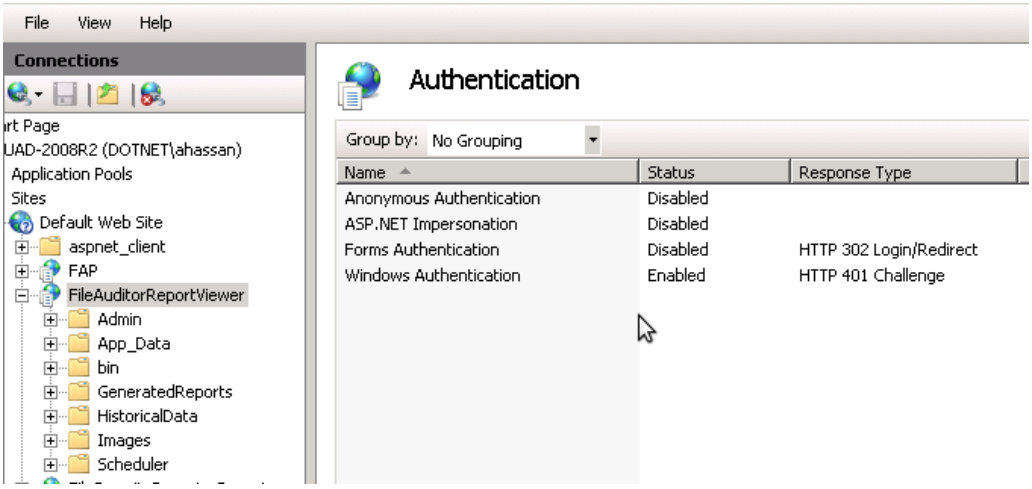




4. In IIS, choose the DFXReportViewer website and open the Authentication view.



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

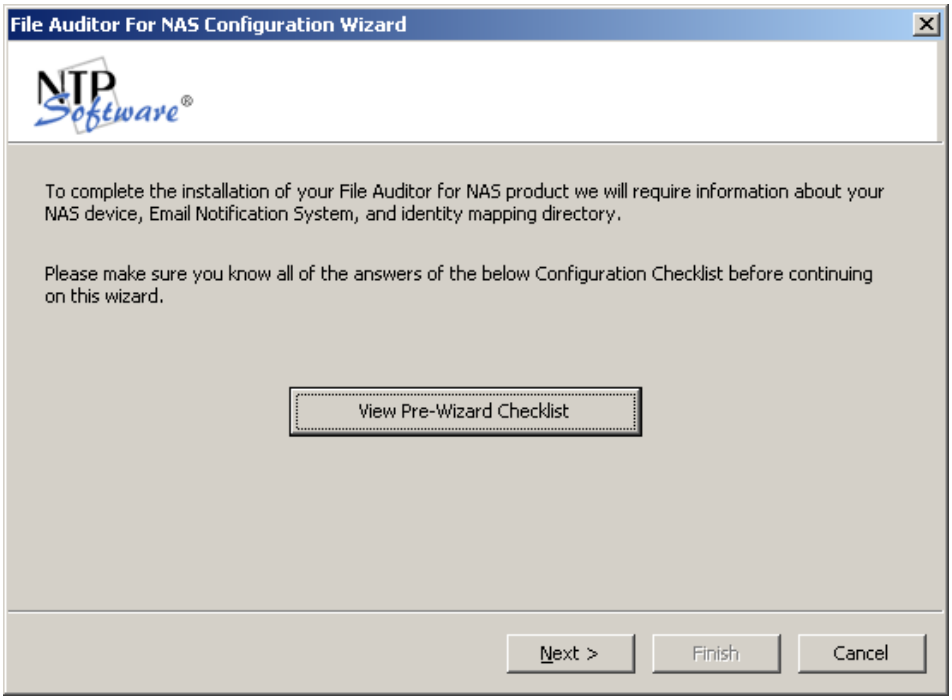


Adding Your First EVS

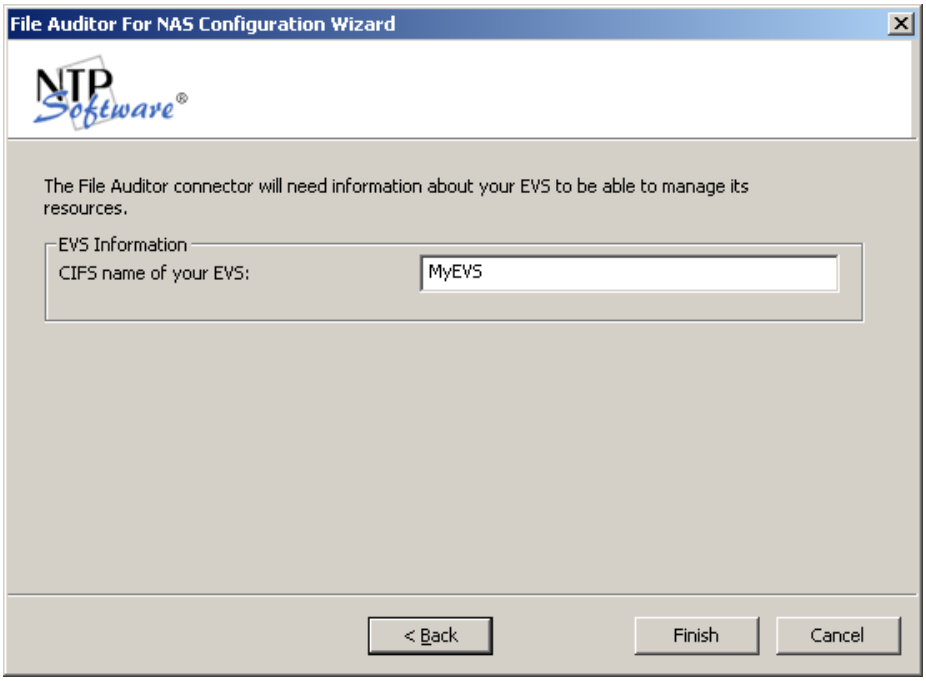
There are two ways to add an EVS to the DefendX Software Control-Audit hierarchy. You can either add it through the DefendX Software Control-Audit Configuration Wizard or add the EVS manually. Both methods are explained in detail here.

To add your first EVS to the DefendX Software Control-Audit hierarchy through the DefendX Software Control-Audit Configuration Wizard, complete the following steps:

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



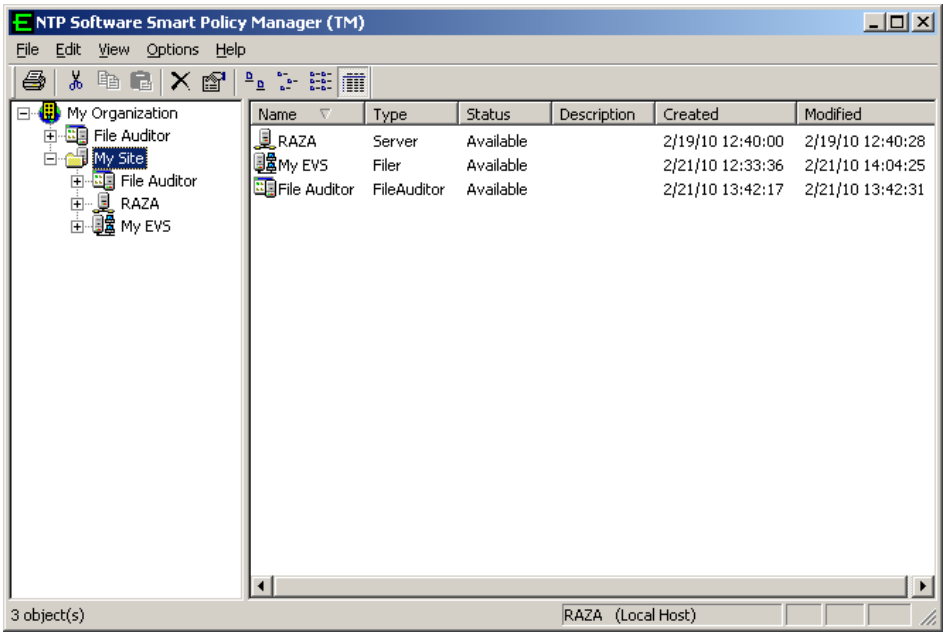
2. Enter the CIFS name of the Virtual Server.



To add an EVS to the DefendX Software Control-Audit policy hierarchy manually, follow these steps:

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 EVS Server is listed in the right pane, below the server on which DefendX Software Control-Audit is installed.



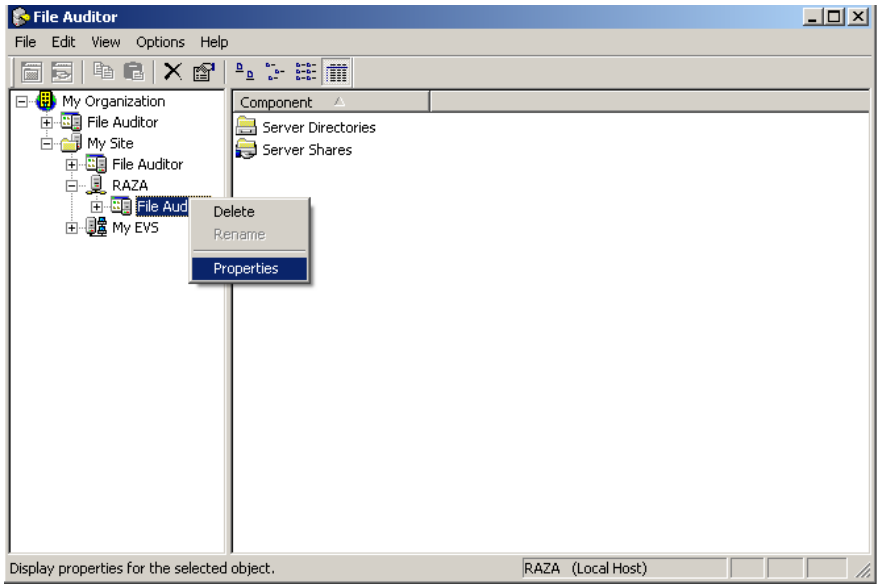
Right-click on the container node, then select **New > EVS** to add the EVS to the tree.

You need to add the EVS to the Hitachi Connector tab and restart the service.

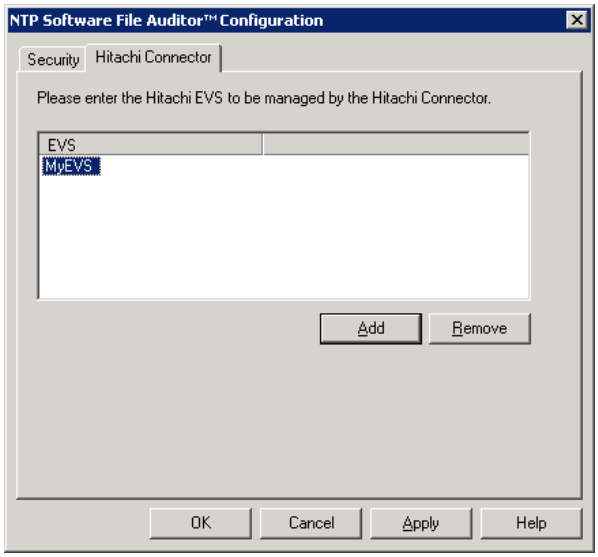
The EVS server will be listed in the Control-Audit Admin left panel tree view.

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

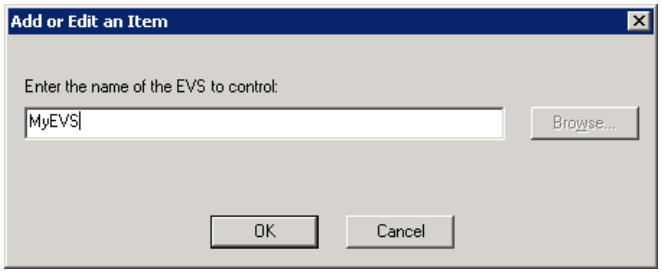
3. In the left pane, expand the server on which DefendX Software Control-Audit is installed and right-click **Control-Audit**. From the pop-up menu, select **Properties**.



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



5. Enter the name of your EVS. Click **OK**.



Verifying Registration with the EVS

The following event log message is logged when DefendX Software Control-Audit successfully registers with an EVS:

Event Source: Control-Audit Hitachi Connector

Event ID: 81

Date: 5/15/2009

Time: PM 12:24:42

Computer: INSTANCE-DEV

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

 Doc#DFX1282EF