



DefendX Software Control-Audit for EMC® Installation Guide Version 5.1

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



Table of Contents

Executive Summary.....	3
Preparing the EMC Isilon.....	4
Isilon OneFS Version	4
Configuring the Isilon	4
Preparing the EMC VNX	5
VNX DART Version.....	5
Configuring cepp.conf	5
Preparing the EMC Unity	7
Preparing DefendX Software Control-Audit Windows Machine	9
Assigning Permissions	11
Requirements	12
DefendX Software Control-Audit for NAS, EMC Edition Server Requirements...	12
EMC VNX Requirements.....	13
Before You Begin	13
Installation.....	14
Installing DefendX Software Smart Policy Manager	14
Installing DefendX Software Control-Audit for NAS, EMC Edition.....	23
Installing DefendX Software Control-Audit Reports, EMC Edition	32
Configuring Control-Audit Reports Website Security	41
Using the DefendX Software Control-Audit for NAS, EMC Edition Configuration Wizard.....	52
Adding VNXs to the DefendX Software Control-Audit Policy Hierarchy	56
About DefendX Software	60
DefendX Software Professional Services	60
Legal & Contact Information	61

Executive Summary

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

DefendX Software Control-Audit for NAS, EMC Edition now supports Virtual Data Movers (VDMs) in addition to the Physical Data Movers (PDMs) that were previously supported. VDMs are widely implemented currently due to their easy management; VDMs enable administrators to separate CIFS servers and their associated resources, such as file systems, into virtual containers. These virtual containers allow administrative separation between groups of CIFS servers.

Given the architecture of your EMC VNX®, DefendX Software Control-Audit for NAS, EMC Edition does its job remotely. DefendX Software Control-Audit for NAS, EMC Edition uses a connector service to create a bridge and include VNX as full participants in storage environments controlled by DefendX Software Control-Audit. In light of this fact, you will need to install the EMC 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 Defendx, version 5.6.36.2 or later of the DART® operating system is required on the VNX. DefendX Software Control-Audit for NAS, EMC Edition can be used to manage EMC 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 monitor file and directory operations on individual paths, directories, and/or shares.

To install DefendX Software Control-Audit on Windows, 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, and the EMC Connector service. The DefendX Software Smart Policy Manager service should be installed with a domain user account. The DefendX Software Control-Audit service requires a domain user account with local administrative rights on the EMC VNX. The EMC Connector service uses this account as well.

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

Preparing the EMC Isilon

Isilon OneFS Version

DefendX Software Control-Audit for NAS, EMC Edition requires the EMC Isilon to run OneFS version 8.0.0.0 or later. If your Isilon is not running version 8.0.0.0 or later, you must upgrade your operating system before you proceed. (Refer to your EMC documentation for instructions.)

To determine the version of OneFS installed on your Isilon, log on to the control station and type the command **version**.

Configuring the Isilon

1. From the Isilon console, run the following command:

Isi audit settings global modify --protocol-auditing-enabled true --audited-zones System

This will enable auditing over CIFS and will specify which zone (System by default) will be audited.

2. Verify the settings by running the following command: ***Isi audit settings global view***

3. Run the following command:

Isi audit settings modify --audit-success close,create,delete,rename,get_security,set_security --syslog-audit-events close,create,delete,rename,get_security,set_security --syslog-forwarding-enabled true

4. Verify the settings by running the following command: ***Isi audit settings view***

5. Make a backup copy of the file /etc/mcp/templates/syslong.conf

6. Edit the file /etc/mcp/templates/syslog.conf and search for the line !audit_protocol

7. Add the following line under !audit_protocol:

****.* @hostname-or-IP-address-of-DefendXControlServer***

8. Reload the syslog config with the following command: ***isi_for_array 'killall -HUP syslogd'***

Preparing the EMC VNX

VNX DART Version

DefendX Software Control-Audit for NAS, EMC Edition requires the EMC VNX to run DART version 5.6.36.2 or later. If your VNX is not running version 5.6.36.2 or later, you must upgrade your operating system before you proceed. (Refer to your EMC documentation for instructions.)

A separate copy of the DART operating system is installed on the VNX control station and on each Data Mover. The DART version installed on the Control Station must be version 5.6.36.2 or later.

To determine the version of DART installed on your Control Station, log on to the control station and type the command **nas_version**.

To determine the DART version installed on each Data Mover, log on to the control station and type the command **server_version ALL**.

Configuring cepp.conf

The **cepp.conf** configuration file contains the information needed by the DART operating system to notify the PC running Windows and DefendX Software Control-Audit of file operations performed by clients. These notifications are the primary information used by DefendX Software Control-Audit to monitor file and directory operations.

The **cepp.conf** file must be properly configured on every Data Mover that contains a CIFS server to be monitored by DefendX Software Control-Audit. Identify those Data Movers and follow these steps to edit the **cepp.conf** file for each Data Mover:

1. Log on to the VNX Control Station. Type the **su** command, enter the user's password, and press **Enter** to become the superuser.
2. Create a new directory (for example, **/mnt2**) at the file system root.

Mount the root of the Data Mover's file system to the new directory. For example, type **mount <DataMoverName>:/ /mnt2** and press **Enter**.

Type **cd /mnt2/.etc**, press **Enter**, and look for the file **cepp.conf**. Create the file if it does not exist.

Use vi to edit the **cepp.conf** file. Edit the servers field to use the IP address of the machine running DefendX Software Control-Audit. The result should look something like this:

```
pool name=cqm servers=<DFX IP Addr>
preevents=OpenFileNoAccess|OpenFileRead|OpenFileWrite|CreateFile|RenameFile|DeleteFile|CloseUnmodified|CloseModified|SetAclFile|CreateDir|RenameDir|DeleteDir|SetAclDir option=ignore reqtimeout=5000 retrytimeout=1000
```

NOTES:

- a. The DefendX Software Control-Audit machine's IP address is a critical piece of information. If the machine has more than one IP address, you need to be careful. The IP used by DefendX Software Control-Audit to contact the VNX must appear in the **cepp.conf** file. If the wrong IP address is used, DefendX Software Control-Audit will be denied access to the VNX and will not function properly.

- b. If Control-Audit is running on a Windows 2008 R2 server machine, you may have to enter the Fully Qualified Domain name of your machine instead of the IP address in Cepp.conf. This resolves an issue when the VNX is not able to resolve the machine name using its IP address.

Example:

```
pool name=cqm servers=DFXServer.Domain.com preevents=* option=ignore
reqtimeout=5000 retrytimeout=1000
```

- c. If DefendX Software Control-Audit is installed on an environment that has 'DefendX Software QFS with Proxy Service' installed on a different machine and it manages the same EMC VNX that you need Control-Audit to manage, you will need to add the IPs of both the QFS and the Control-Audit machines, separated by a vertical bar character "|". The result should look something like this example:

```
pool name=cqm servers=<DFX IP Addr>|<QFS IP Addr> preevents=* option=ignore
reqtimeout=5000                                retrytimeout=1000
```

Changes to the **cepp.conf** file will be registered when you restart the cepp service. Type **server_cepp <DataMoverName> -service -stop** and press **Enter**.

Type **server_cepp <DataMoverName> -service -start** and press **Enter**.

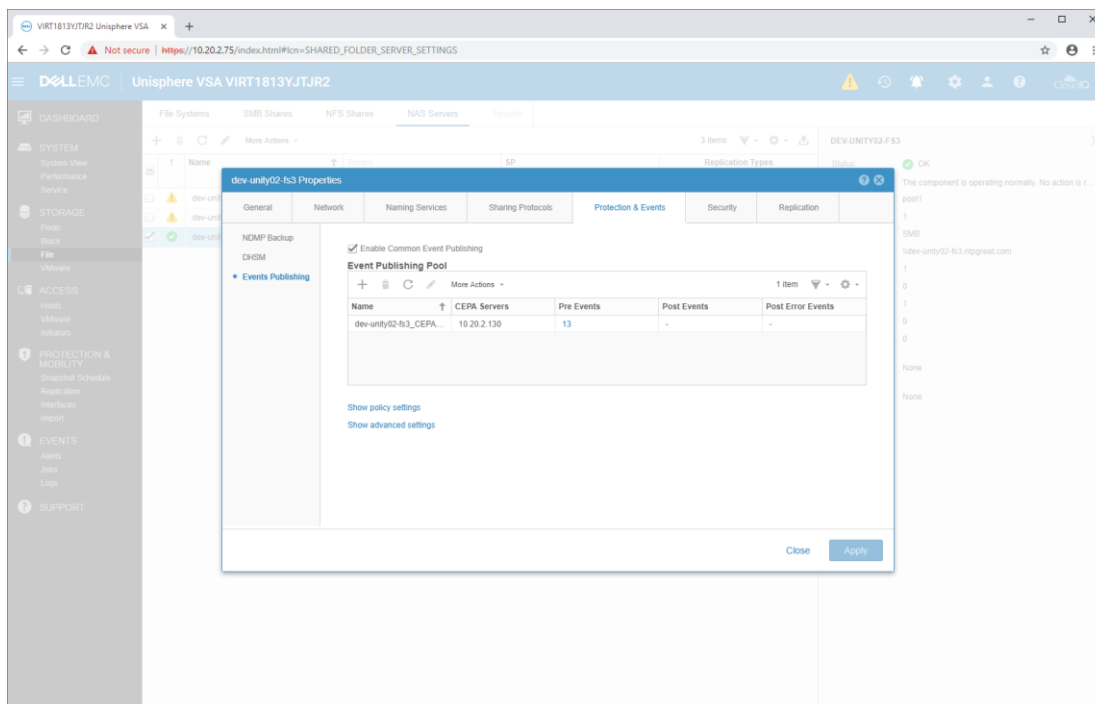
Repeat steps 2 through 6 for all Data Movers to be managed.

Preparing the EMC Unity

Since Unity uses CEE to send notifications to File Auditor just like the VNX does, the requirement for Unity are the same as VNX. The service account needs to have the EMC Virus Checking and EMC Event Notification Bypass rights and be a local admin on server being managed. CEE is required.

To enable Event Publishing on the NAS Server.

1. Log into the Unity Unisphere Console
2. Select File in the left menu
3. Select the NAS Servers tab across the top
4. Select the specific NAS Server
5. Click the Edit Icon (pencil)
6. On the Properties page that is displayed, select the Protection & Events tab.
7. Select the Events Publishing menu item on the left
8. Click the checkbox Enable Common Event Publishing



9. Click the + icon to add a new pool.
10. The name will be filled in by default. Click the Add button to add the name/ip address of the CEE server that File Auditor will use
11. Click the Configure link next to Pre Events.

Configure PreEvents for dev-unity02-fs3_CEPA_1

Select all
Select none

<input type="checkbox"/> CloseDir	<input type="checkbox"/> FileRead	<input type="checkbox"/> OpenFileWriteOffline
<input checked="" type="checkbox"/> CloseModified	<input type="checkbox"/> FileWrite	<input checked="" type="checkbox"/> RenameDir
<input checked="" type="checkbox"/> CloseUnmodified	<input type="checkbox"/> OpenDir	<input checked="" type="checkbox"/> RenameFile
<input checked="" type="checkbox"/> CreateDir	<input checked="" type="checkbox"/> OpenFileNoAccess	<input checked="" type="checkbox"/> SetAcDir
<input checked="" type="checkbox"/> CreateFile	<input checked="" type="checkbox"/> OpenFileRead	<input checked="" type="checkbox"/> SetAcFile
<input checked="" type="checkbox"/> DeleteDir	<input type="checkbox"/> OpenFileReadOffline	<input type="checkbox"/> SetSecDir
<input checked="" type="checkbox"/> DeleteFile	<input checked="" type="checkbox"/> OpenFileWrite	<input type="checkbox"/> SetSecFile

Close OK

12. Select the events shown above and click OK.
13. Click Configure. Then click Apply. The settings will be saved and you will be returned to the NAS Servers list.
14. Click on the File Systems link at the top.
15. In order to get events, each file system must have Events publishing enabled.
16. Select a file system on the nas server, and click the Edit icon.
17. On the properties dialog, select the Advanced tab. Check the option for Enable SMB Events publishing
18. Repeat for each file system that will be configured in File Auditor.

fs3_data Properties
?
X

General
Snapshots
FAST VP
Replication
Quota
Advanced

SMB Protocol Settings
☐ Sync Writes Enabled
☒ Oplocks Enabled
☐ Notify On Write Enabled
☐ Notify On Access Enabled

Events Notifications
☒ Enable SMB Events publishing

Close
Apply

Preparing DefendX Software Control-Audit Windows Machine

Follow these steps to prepare the Windows machine to host DefendX Software Control-Audit for NAS, EMC Edition:

1. Before installing DefendX Software Control-Audit for NAS, EMC Edition, you must make sure that Common Event Enabler (CEE) version 8.2 or later is appropriately installed and configured in your environment. Contact EMC for further information on this configuration.
2. After installing CEE on the DefendX Software Control-Audit machine, you need to specify the software with which the CEE will register. To do this, use the Windows Registry Editor to set **ntp** for the following REG_SZ registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\EMC\VN
X
Enabler\CEPP\CQM\Configuration\EndPoint

Event

3. Open the Service Control Manager and open the properties of the EMC CAVA service installed as part of CEE.
4. Stop the EMC CAVA service.
5. Change the service account to an account that can be assigned special permissions to access the CIFS Servers on the VN X Control Station. The following section describes these special permissions.
6. After changing the account, restart the CAVA service.

NOTE:

If DefendX Software Control-Audit is installed on an environment that has 'DefendX Software QFS with Proxy Service' installed and it manages the same EMC VN X that you need Control-Audit to manage, you should configure Control-Audit to use the EMC Proxy service installed on the QFS Server:

1. On the DefendX Software Control-Audit machine, perform the following steps:
 - a. Go to the following key in the registry editor HKEY_LOCAL_MACHINE\SOFTWARE\DefendXSoftware\Control-Audit\ECS
 - b. Create a string value called **ProxyServer** if it does not exist.
 - c. Set the **ProxyServer** value to the machine IP or name of the DefendX Software Quota and File Sentinel machine.
2. On the DefendX Software Control-Audit machine, make sure that the DefendX Software EMC Proxy Service is disabled:
 - a. Open the Windows Service Manager from **Control Panel\Administrative tools\Services**.
 - b. Look for the DefendX Software EMC Proxy Service entry; right-click this entry and select **Stop**.

Right-click **the** DefendX Software EMC Proxy Service entry and select **Properties**; then in the **General** tab, change **Startup type** to **Disabled**.

Assigning Permissions

For DefendX Software Control-Audit to work properly, the account used by the DefendX Software Control-Audit EMC Connector service and the EMC CAVA service should have the following permissions:

- EMC Virus Checking
- EMC Event Notification Bypass

Use the VNX CIFS Management Tools MMC snap-in provided by EMC to assign those permissions to the service account to be used by the DefendX Software Control-Audit EMC Connector.

NOTE: The EMC Virus Checking and the EMC Event Notification Bypass permissions should be added to at least one CIFS server defined on the Physical Data Mover to be managed; there is no need to create those permissions for each existing VDM.

Requirements

DefendX Software Control-Audit for NAS, EMC Edition 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:

- 4 GHz CPU
- Windows Server 2008 R2, 2012 RD, 2016 (Windows 2016 is recommended)
- 8 GB RAM
- 10 GB 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 2008, 2012, 2014, 2016
- SQL Server Reporting Services 2008 or later (2017 is recommended)
- Microsoft .NET Framework 2.0
- ASP.NET AJAX 1.0
- Microsoft Report Viewer 2005 SP1 (installed along with the Report Pack)

NOTES:

1. The Remote Connection to the SQL Server should be enabled.
2. The SQL Server user should have **db_datareader** and **execute** permissions on the Control-Audit database.
3. The Reporting Service on the database server must grant access to the currently logged Windows user while installing the application.

EMC VNX Requirements

The EMC VNX® to which DefendX Software Control-Audit for NAS, EMC Edition will be connected requires the following:

- DART version 5.6.36.2 or later
- Network interface card

NOTE: It is strongly recommended that two network adapters be installed on both the VNX and Windows Server. The connection between the server and VNX 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 the DefendX Software Control-Audit for NAS, EMC Edition installer, make sure you have the following ready for a smooth installation:

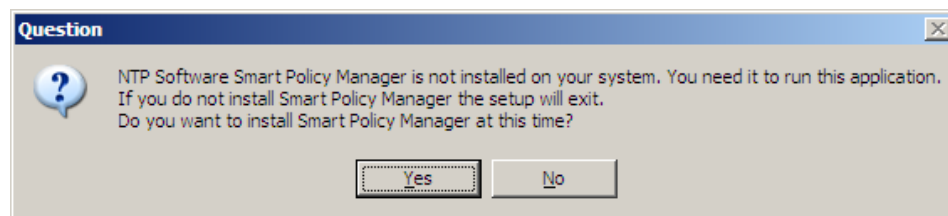
1. The Microsoft SQL Server user name and password for authentication.
2. Access to server/File.
3. The license key you were given when you purchased the Control-Audit product.

Installation

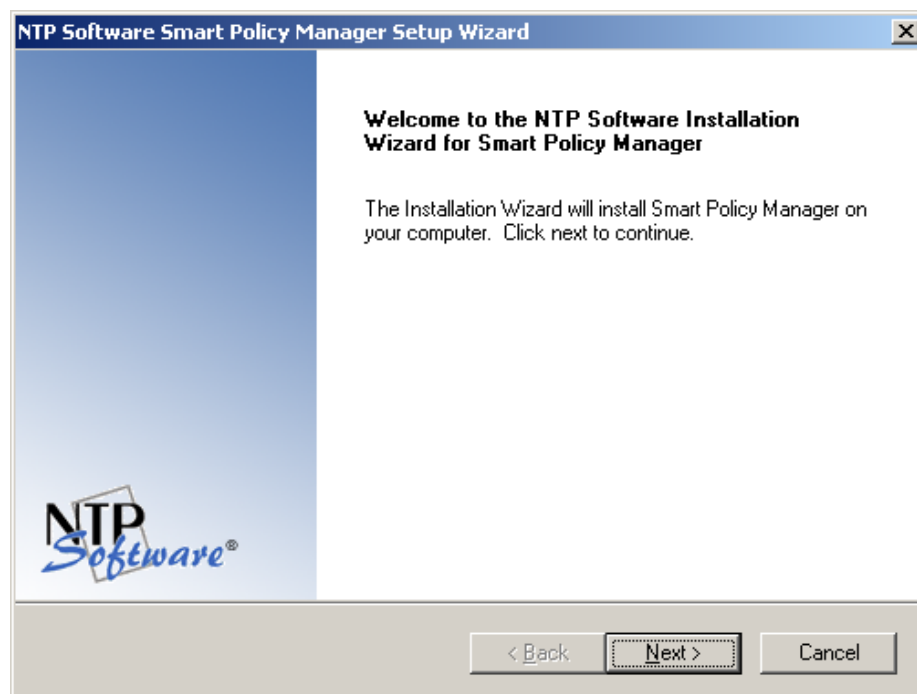
Prior to installing DefendX Software Control-Audit for NAS, EMC Edition, DefendX Software recommends verifying that the installation server meets the requirements listed in the *Requirements* section of this document.

Installing DefendX Software Smart Policy Manager

1. Log on to your server 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, EMC Edition*.



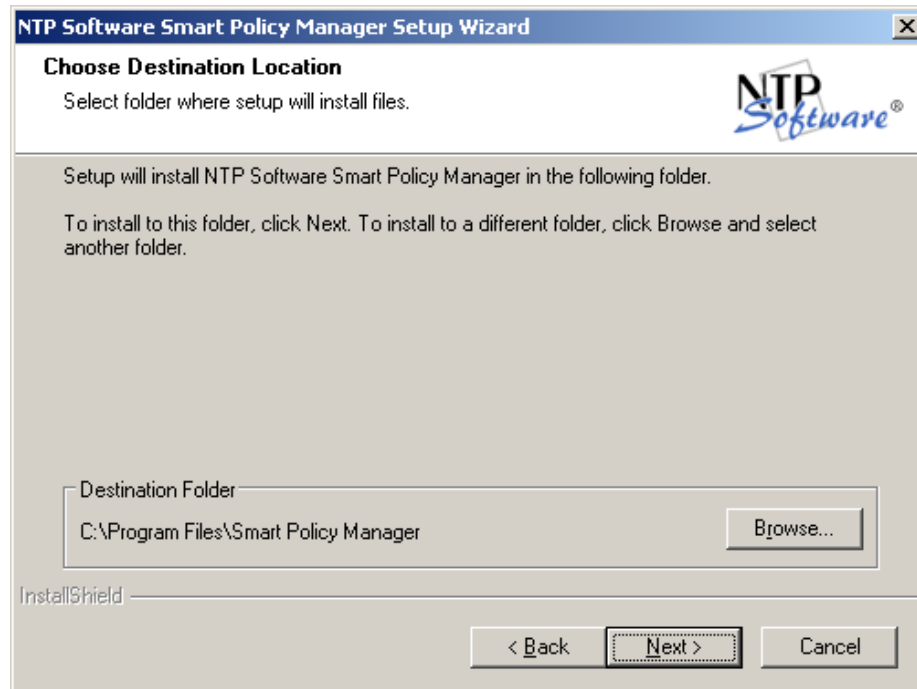
3. The DefendX Software Smart Policy Manager Installation Wizard opens. Click **Next** to begin the installation.



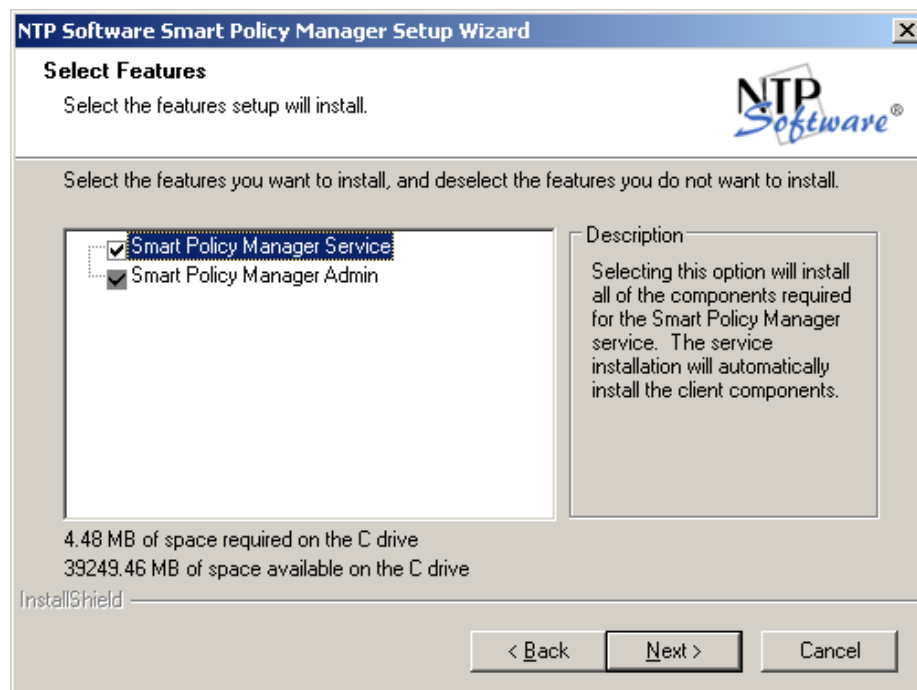
4. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



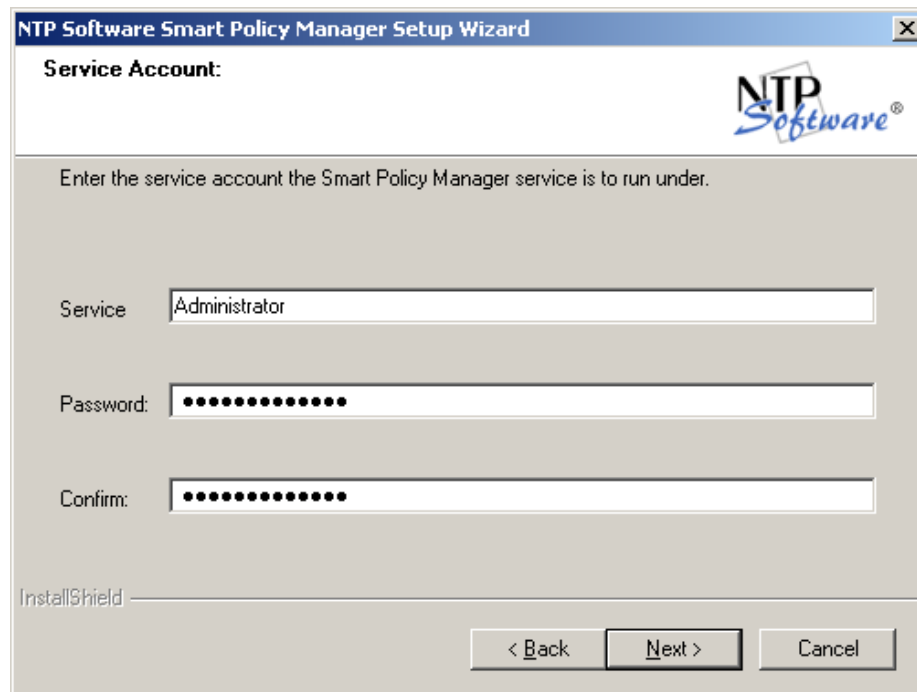
5. In the **Choose Destination Location** dialog box, click **Browse** to choose the location where you want to install DefendX Software Smart Policy Manager and then click **Next**.



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

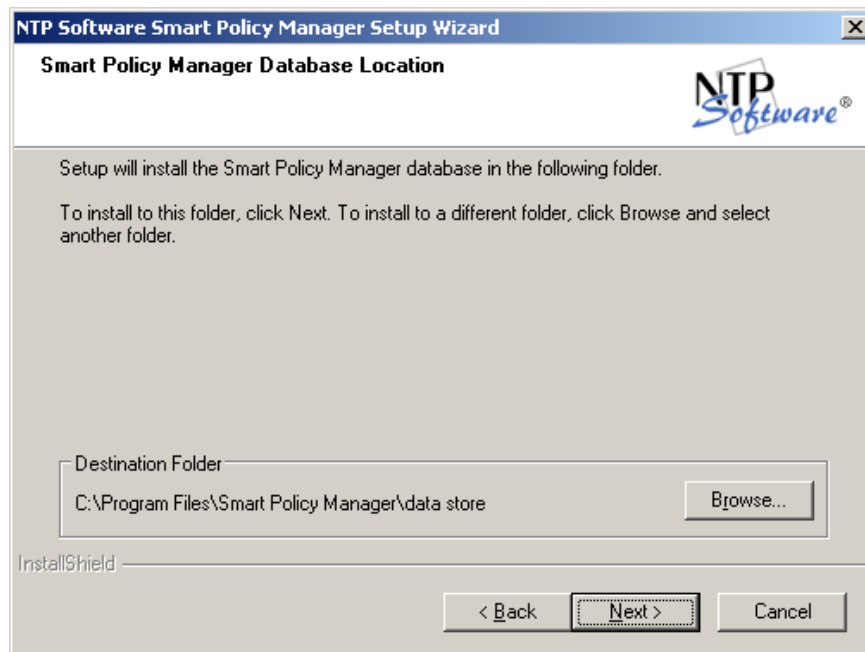


7. In the **Service Account** dialog box, when prompted for a Windows domain user account to run the DefendX Software Smart Policy Manager service, enter the username and password for a domain user account with administrative rights on the local machine. Click **Next**.

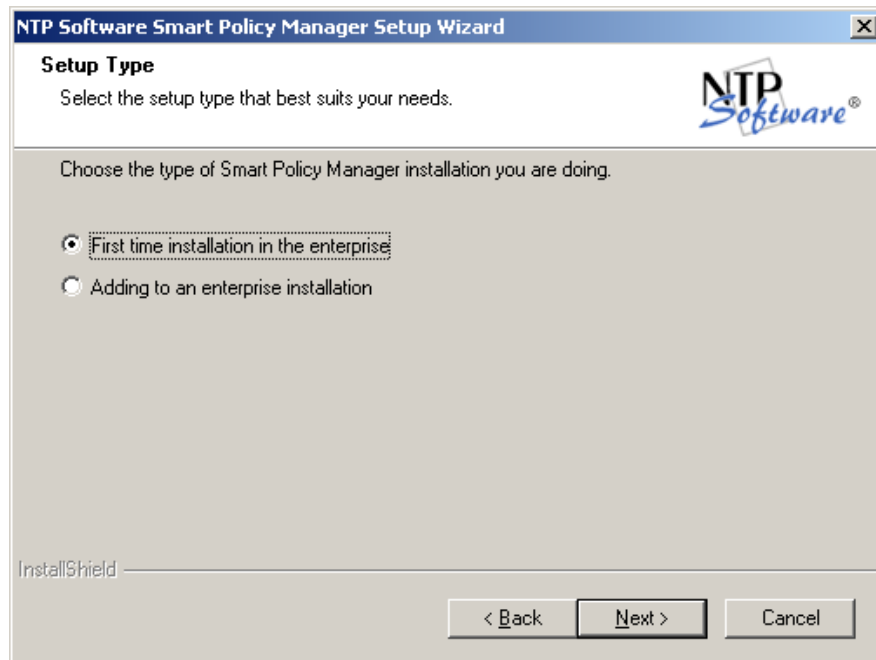


The image shows a Windows-style dialog box titled "NTP Software Smart Policy Manager Setup Wizard". The main heading is "Service Account:". Below this, there is a sub-heading "Enter the service account the Smart Policy Manager service is to run under." followed by the NTP Software logo. The dialog contains three input fields: "Service" with the text "Administrator", "Password:" with masked characters (dots), and "Confirm:" with masked characters (dots). 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".

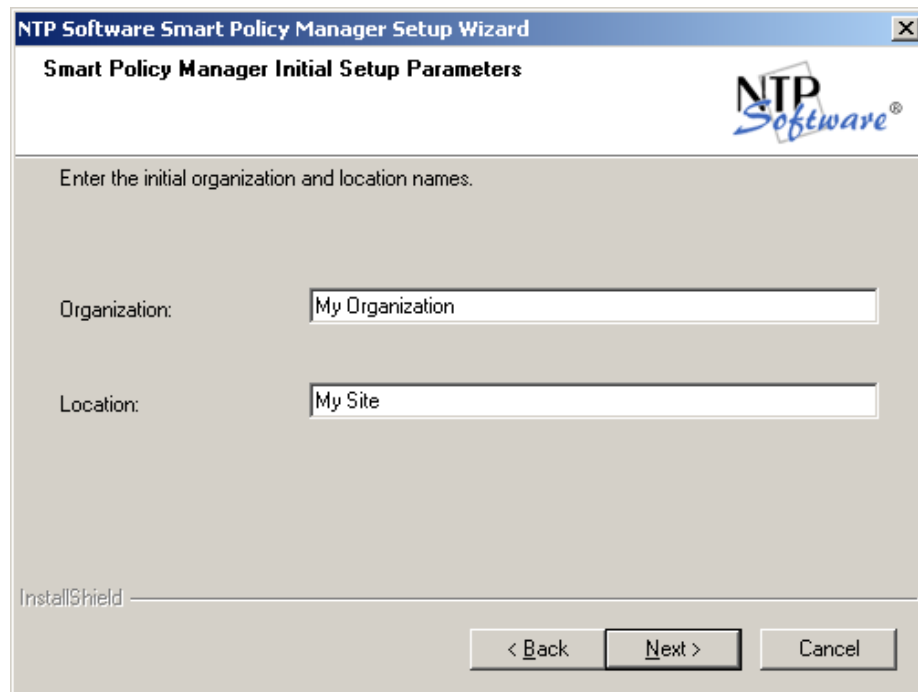
8. In the **Smart Policy Manager Database Location** dialog box, enter the directory name where you want to install the DefendX Software Smart Policy Manager database or just accept the default location. Click **Next**.



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**.

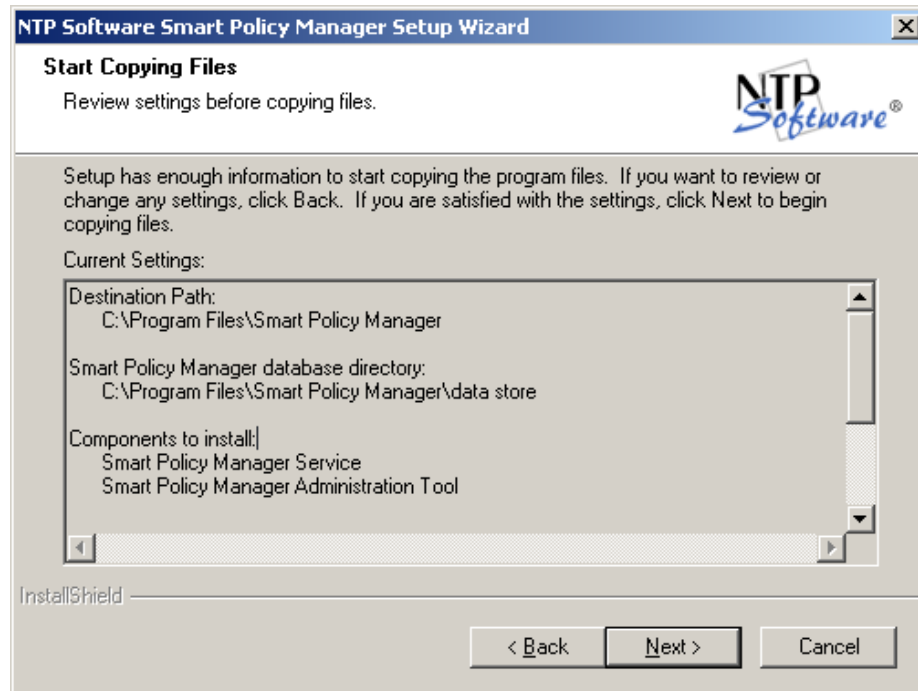


10. In the **Smart Policy Manager Initial Setup Parameters** dialog box, provide DefendX Software Smart Policy Manager with a name for your organization and a location name for this DefendX Software Smart Policy Manager instance, or accept the default settings. Click **Next**.

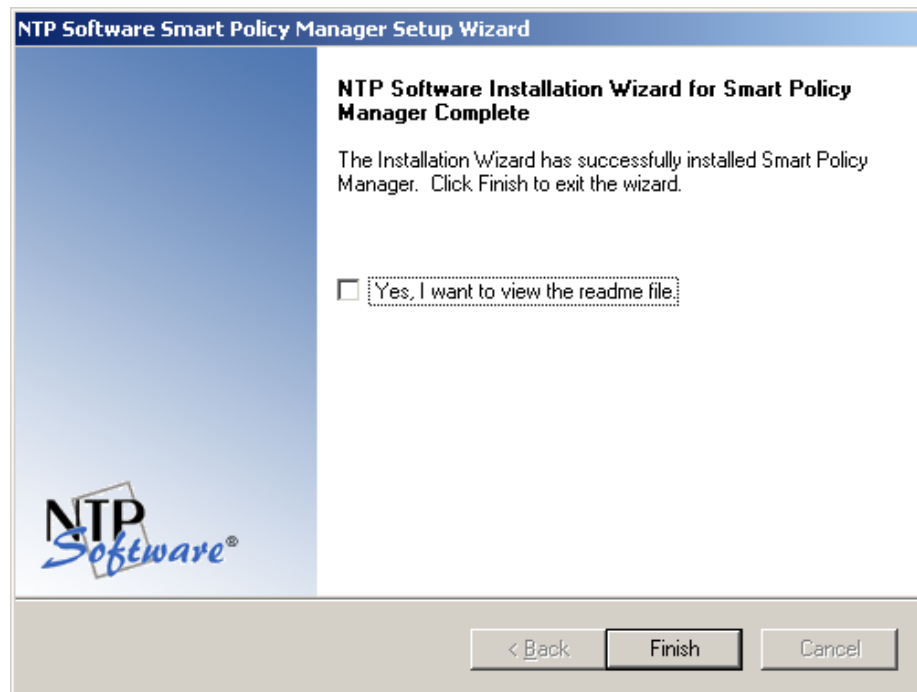


The screenshot shows a Windows-style dialog box titled "NTP Software Smart Policy Manager Setup Wizard". The main heading inside is "Smart Policy Manager Initial Setup Parameters". In the top right corner, there is a logo for "NTP Software®". Below the heading, a text prompt says "Enter the initial organization and location names." There are two input fields: "Organization:" with the text "My Organization" and "Location:" with 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.

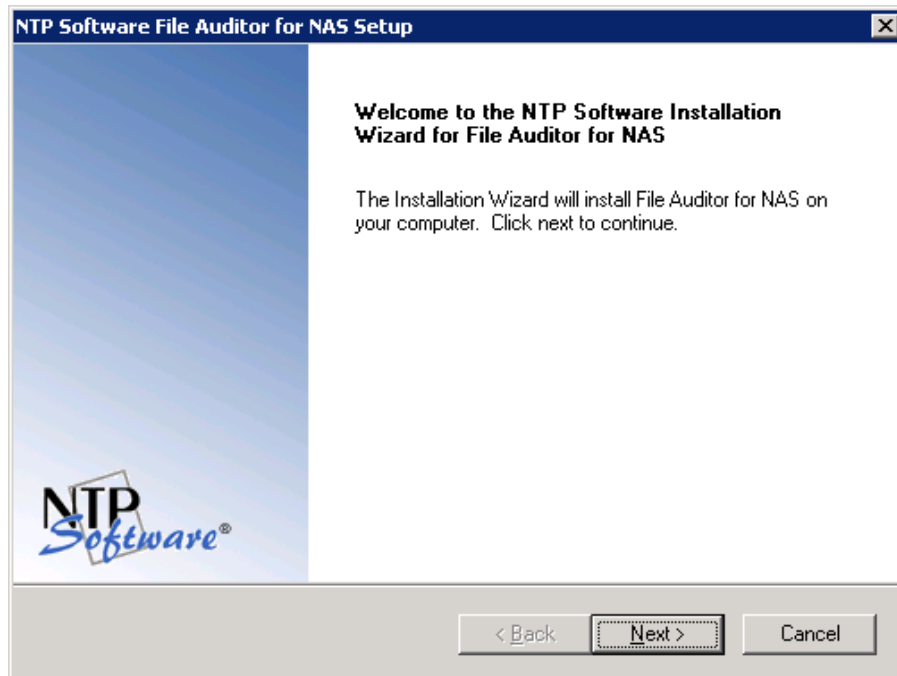


12. If you do not want to view the DefendX Software Smart Policy Manager readme file, clear the **Yes, I want to view the readme file** checkbox. When you click **Finish**, the DefendX Software Control-Audit for NAS Installer opens.

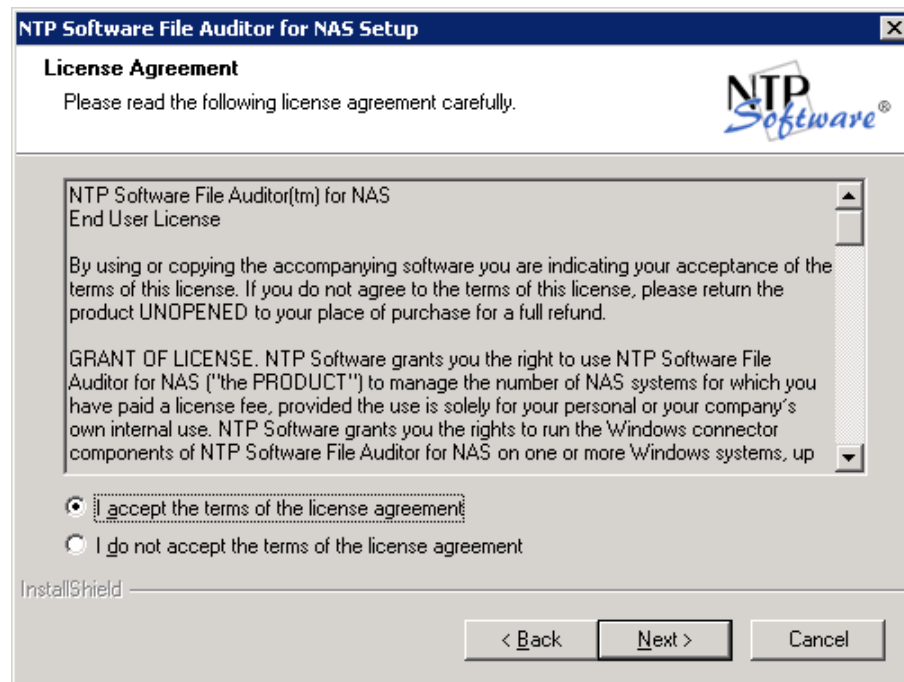


Installing DefendX Software Control-Audit for NAS, EMC Edition

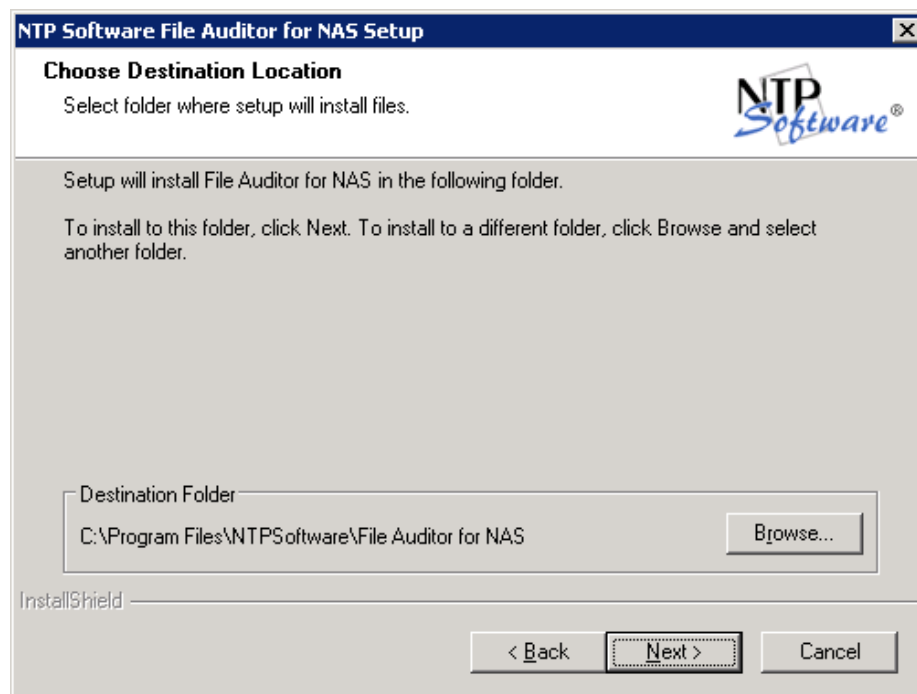
1. When the DefendX Software Control-Audit for NAS Installation Wizard opens, click **Next** to begin the installation.



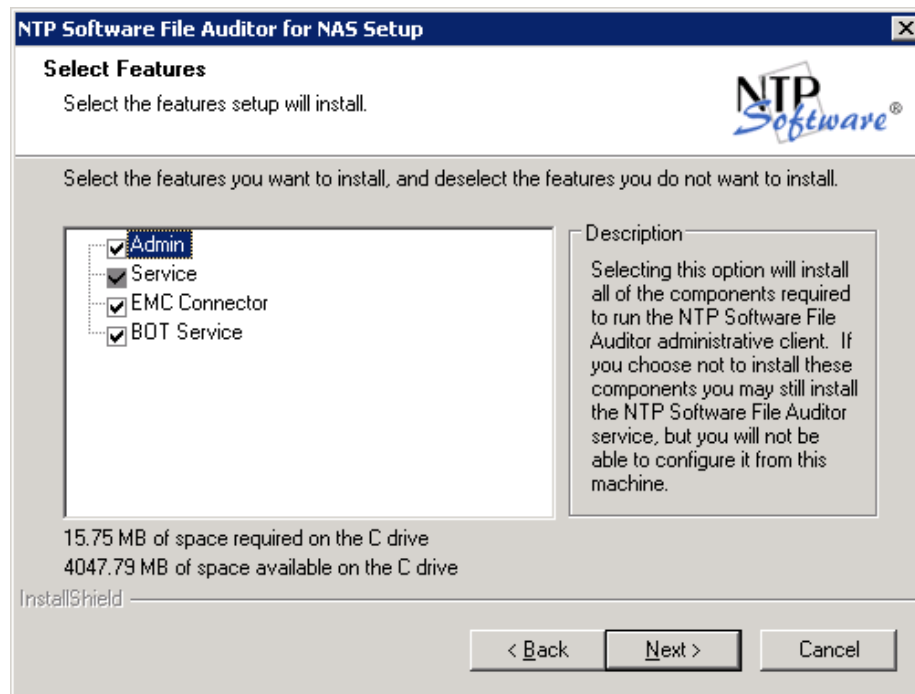
2. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



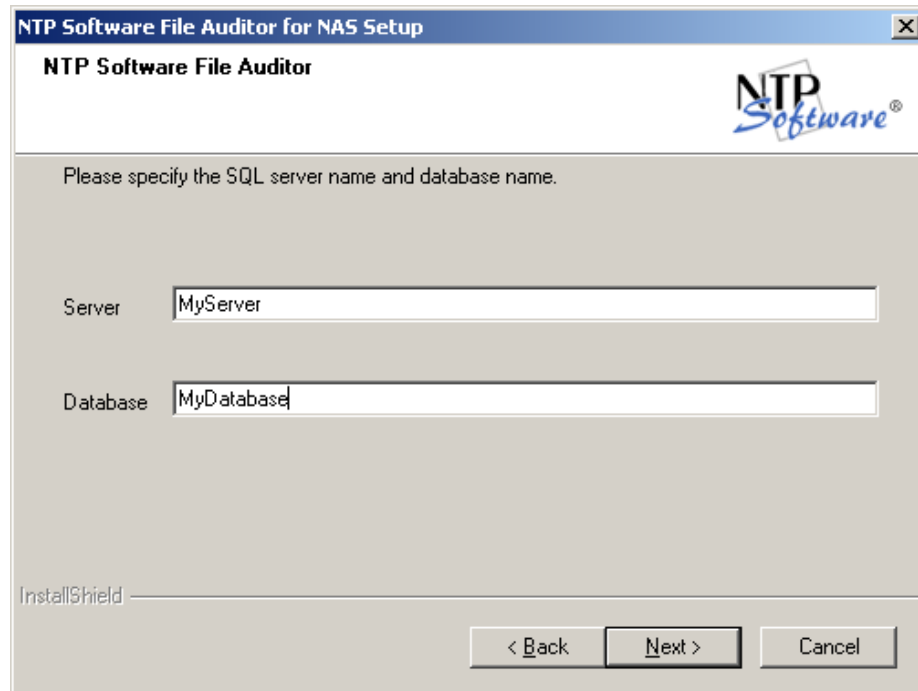
3. In the **Choose Destination Location** dialog box, choose the location where you want to install DefendX Software Control-Audit and then click **Next**.



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 **EMC Connector** component is required if this machine will need to communicate with a VNX for file and directory operations monitoring purposes. The BOT Service component is required if you wish to have the Business Overwatch Tasks Service and its configuration interface.

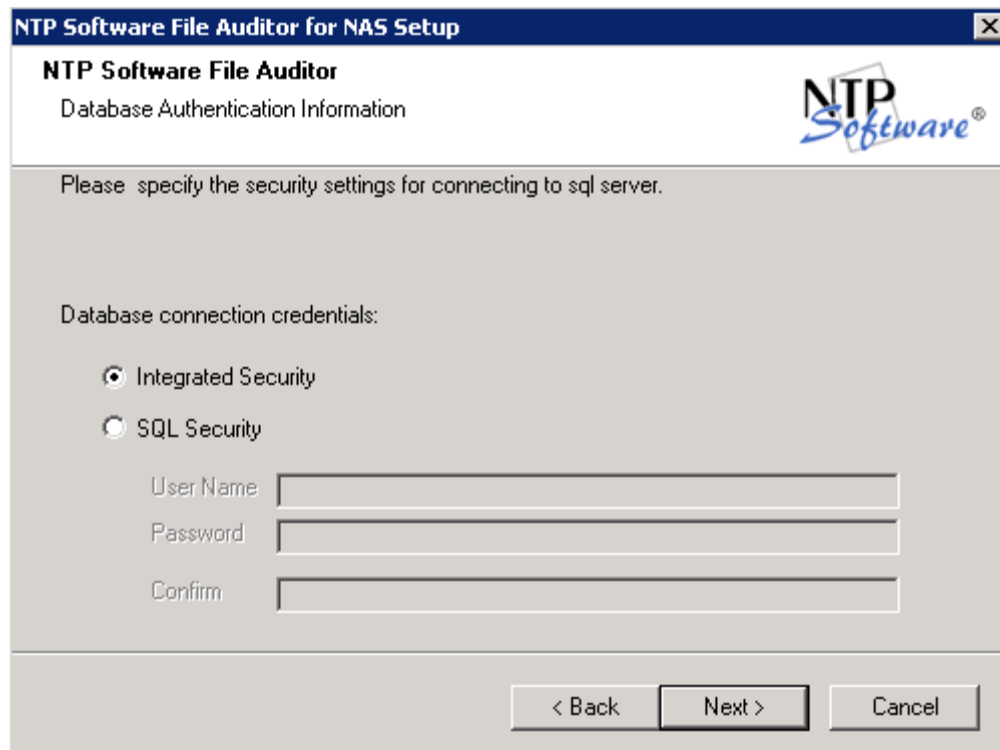


5. In the **DefendX Software Control-Audit** dialog box, provide your SQL Server name and your database name.



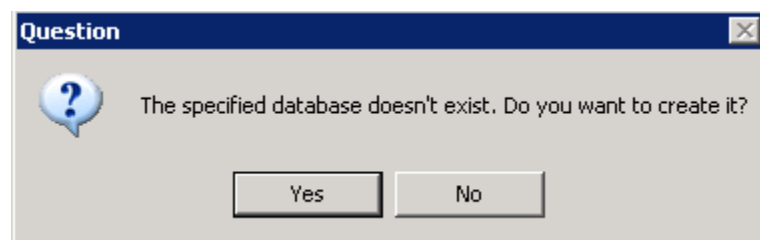
The screenshot shows a Windows-style dialog box titled "NTP Software File Auditor for NAS Setup". The title bar is blue with a close button (X) on the right. Below the title bar, the text "NTP Software File Auditor" is displayed on the left, and the "NTP Software" logo is on the right. The main area of the dialog box has a light gray background and contains the instruction "Please specify the SQL server name and database name." Below this instruction are 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 box, 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.



The image shows a Windows-style dialog box titled "NTP Software File Auditor for NAS Setup". The main title bar is blue with white text. Below the title bar, the text "NTP Software File Auditor" is displayed in bold, followed by "Database Authentication Information" in a smaller font. The NTP Software logo is in the top right corner. The main area of the dialog box has a light gray background and contains the text "Please specify the security settings for connecting to sql server." Below this, the text "Database connection credentials:" is followed by two radio button options: "Integrated Security" (which is selected) and "SQL Security". Below these options are three text input fields labeled "User Name", "Password", and "Confirm". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

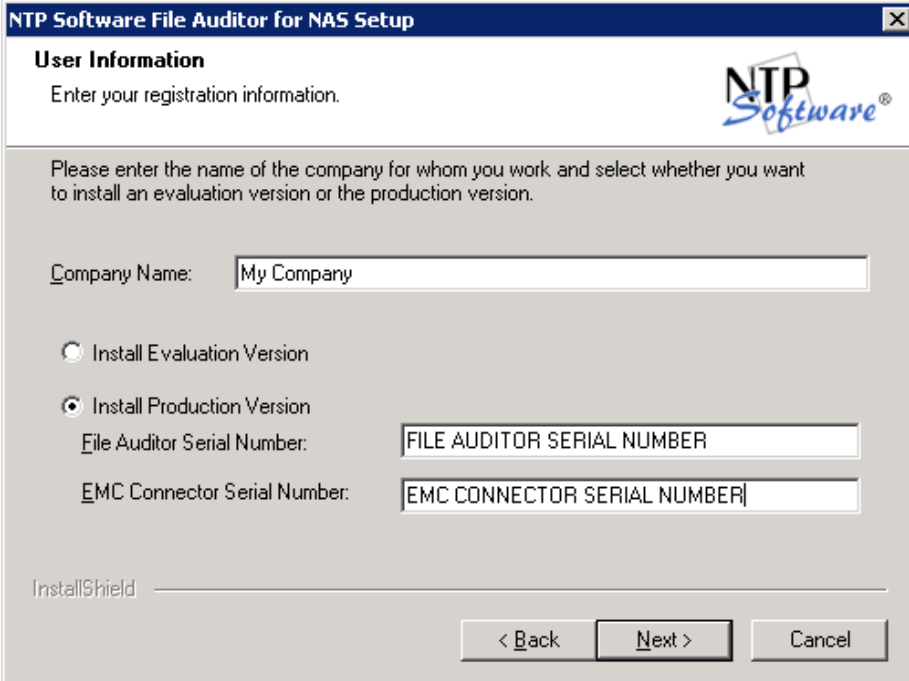
If the database doesnot exist, the below question dialog will be displayed. Click the **Yes** button. If you wish to create the database yourself, run the SQL Scripts in the Control-Audit for NAS installation folder after the setup is complete. The script file is "Control-Audit DB Schema and User Script.sql".



The image shows a small Windows-style dialog box titled "Question". It has a light gray background and a blue question mark icon on the left. The text inside the dialog box reads "The specified database doesn't exist. Do you want to create it?". At the bottom of the dialog box, there are two buttons: "Yes" and "No".

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 EMC Connector serial numbers. Click **Next**.



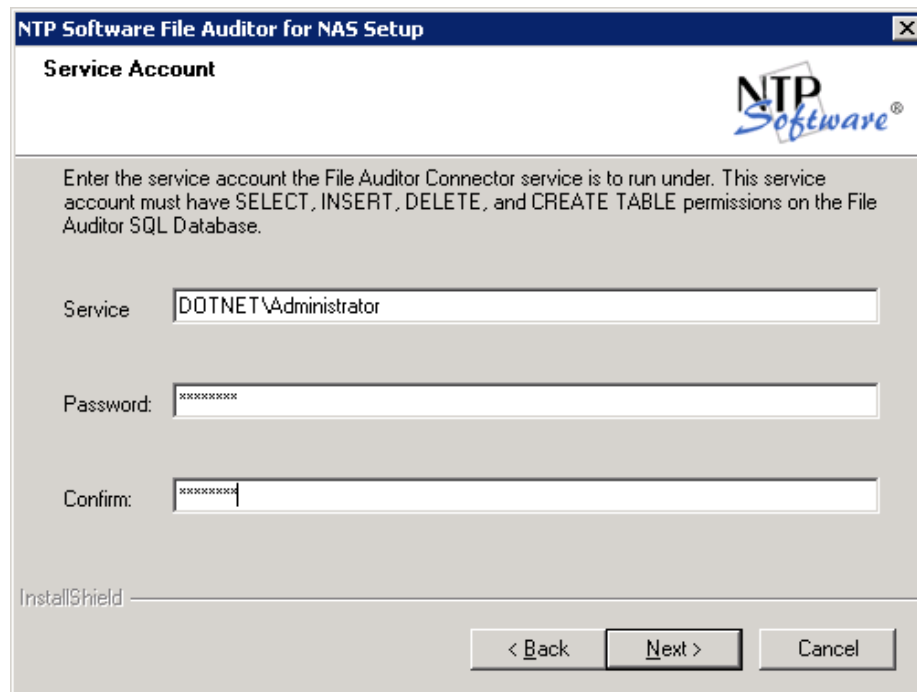
The dialog box is titled "NTP Software File Auditor for NAS Setup". It has a "User Information" section with the instruction "Enter your registration information." and the NTP Software logo. Below this, it says "Please enter the name of the company for whom you work, and select whether you want to install 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 "EMC Connector Serial Number" containing "EMC 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**.



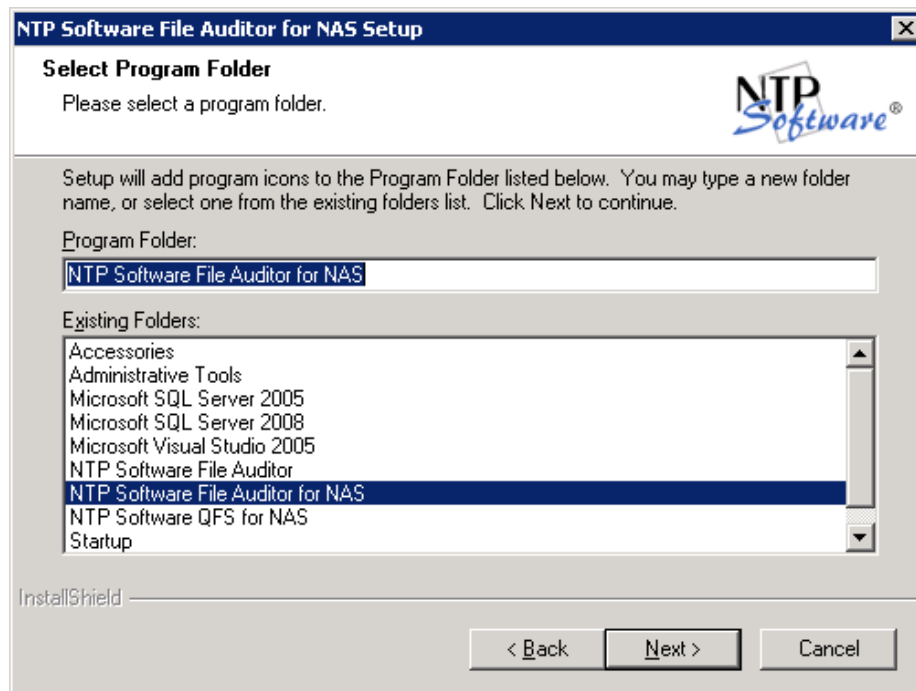
The dialog box is titled "NTP Software File Auditor for NAS Setup". It has an "Account Type" section with the instruction "Please specify the type of account to use." and the NTP Software logo. Below this, it says "The File Auditor service can run as a specified account or the built-in system account." 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 and directory operations. Click **Next**.

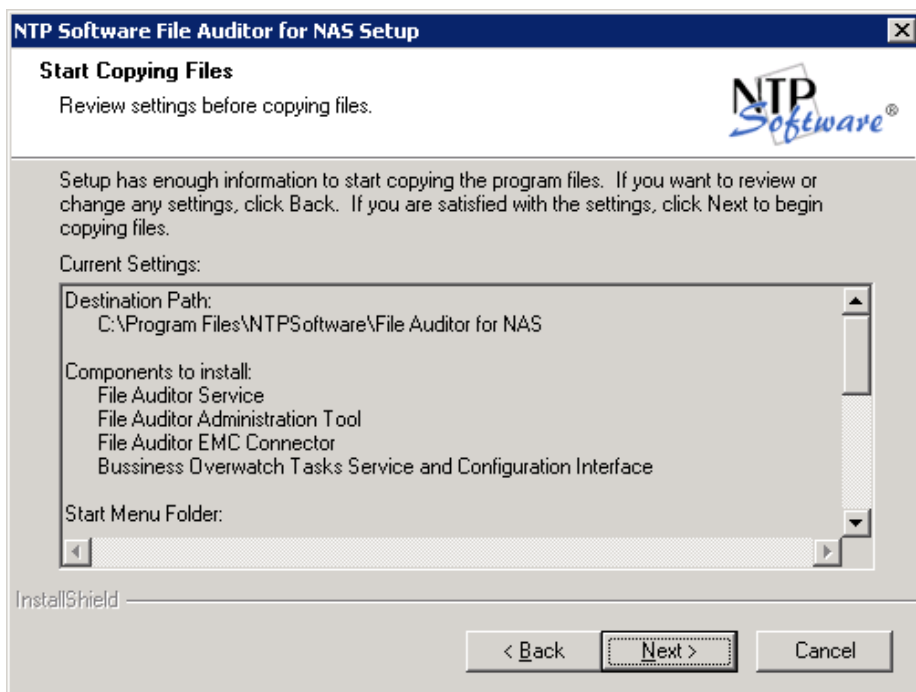


The screenshot shows a Windows-style dialog box titled "NTP Software File Auditor for NAS Setup". The main heading is "Service Account". In the top right corner is the "NTP Software" logo. Below the heading, a text block states: "Enter the service account the File Auditor Connector service is to run 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" containing "DOTNET\Administrator", "Password:" with masked characters "xxxxxxx", and "Confirm:" with masked characters "xxxxxxx". At the bottom left is the "InstallShield" logo. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

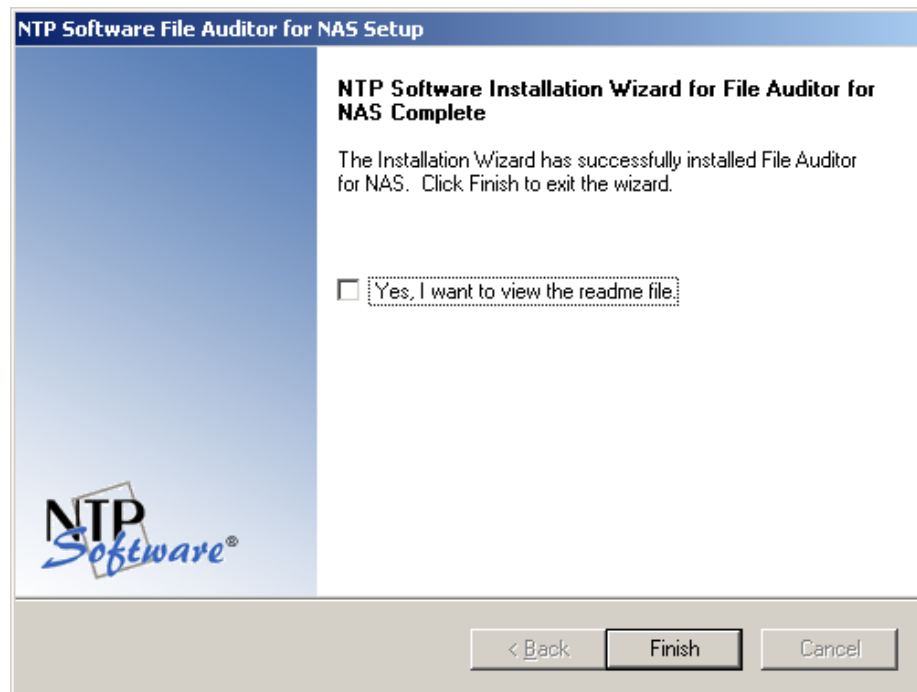
10. In the **Select Program Folder** dialog box, select the program folder to host the DefendX Software Control-Audit for NAS startup group. Click **Next**.



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



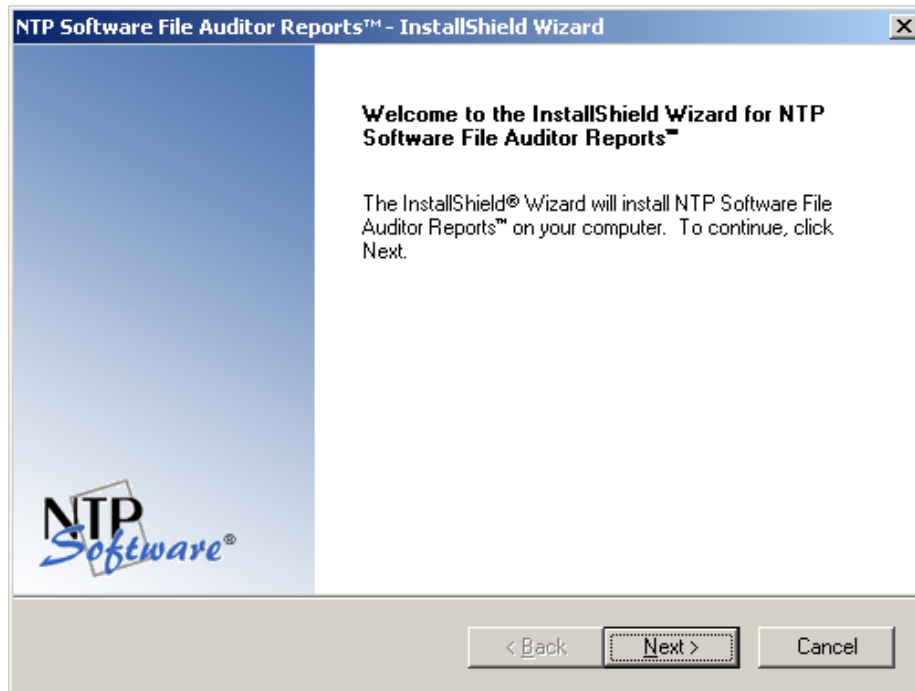
12. If you do not want to view the DefendX Software Control-Audit for NAS readme file, clear the **Yes, I want to view the readme file** checkbox. When you click **Finish**, the DefendX Software Control-Audit for NAS, EMC Edition Configuration Wizard will open.



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

Installing DefendX Software Control-Audit Reports, EMC Edition

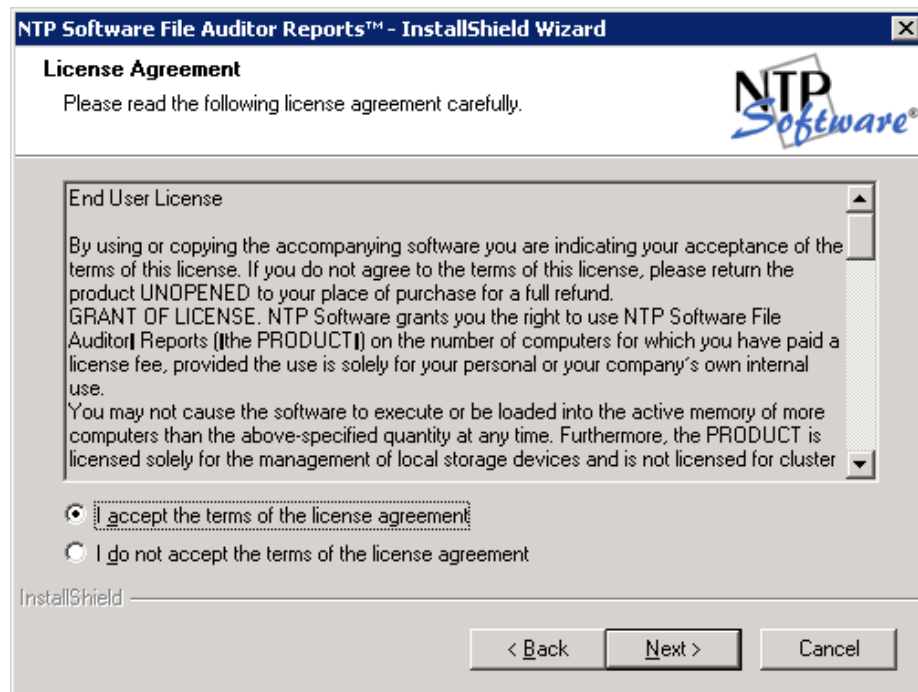
1. When the DefendX Software Control-Audit Reports™ Wizard opens, click **Next** to begin the installation.



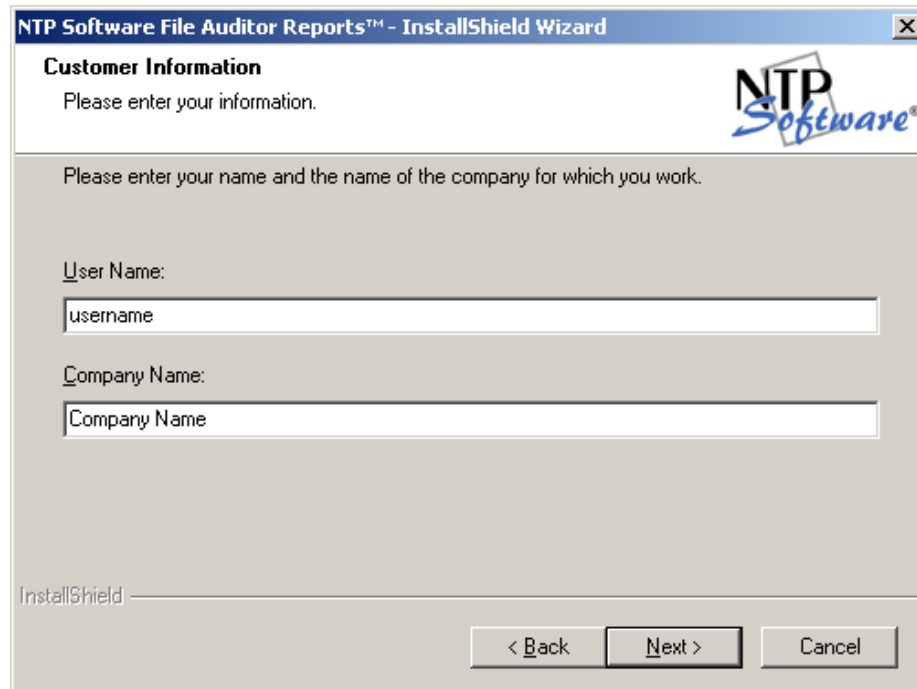
NOTE: The user installing the Control-Audit Reports must be assigned the Content Management role. To assign a user the Content Management role, perform the following steps:

- 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.

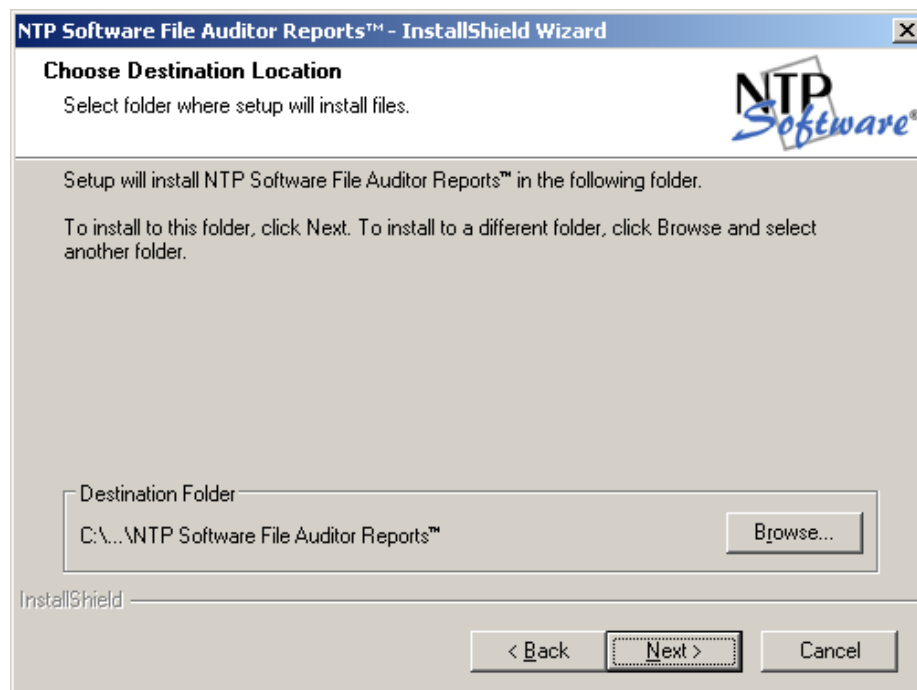
2. In the **License Agreement** dialog box, read the end-user license agreement. If you agree to the terms, click **I accept the terms of the license agreement** and then click **Next**. If you do not accept the terms, click **Cancel** to exit the installation.



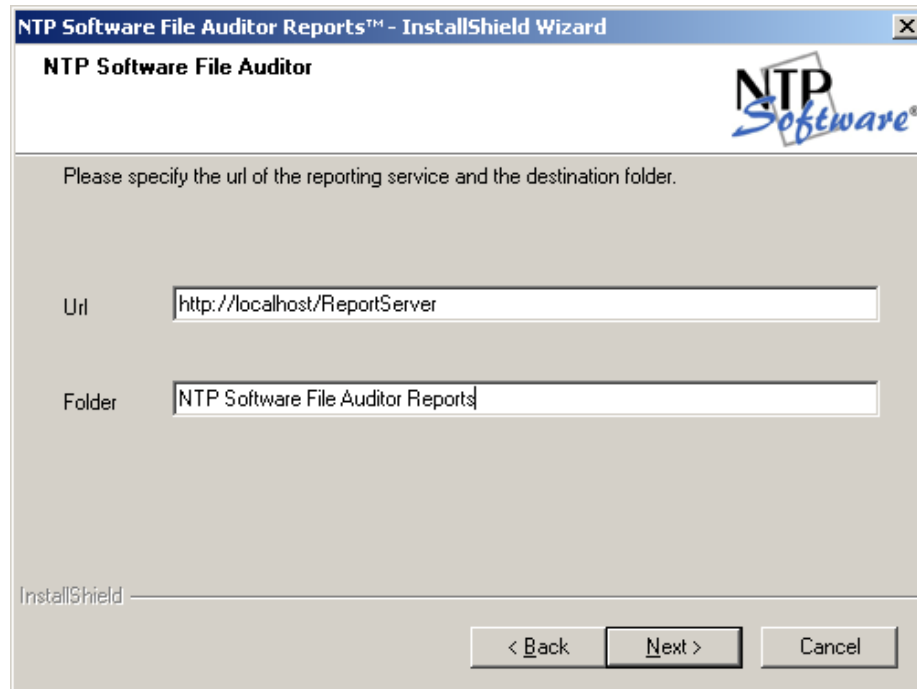
3. In the **Customer Information** dialog box, provide your user name and the company name. Click **Next**.



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**.

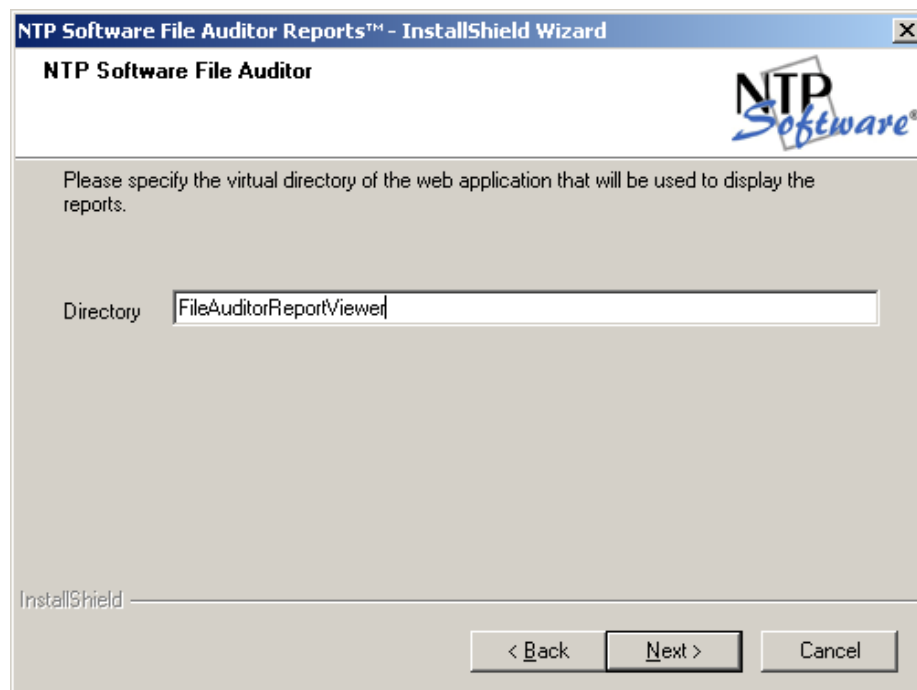


5. In the **DefendX Software Control-Audit** dialog box, specify the URL of the reporting service and the destination folder. Click **Next**.



The dialog box is titled "NTP Software File Auditor Reports™ - InstallShield Wizard". It features the NTP Software logo in the top right corner. The main text reads: "Please specify the url of the reporting service and the destination folder." Below this, there are two input fields: "Url" with the value "http://localhost/ReportServer" and "Folder" with the value "NTP Software File Auditor Reports". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted.

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



The dialog box is titled "NTP Software File Auditor Reports™ - InstallShield Wizard". It features the NTP Software logo in the top right corner. The main text reads: "Please specify the virtual directory of the web application that will be used to display the reports." Below this, there is one input field: "Directory" with the value "FileAuditorReportViewer". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted.

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.

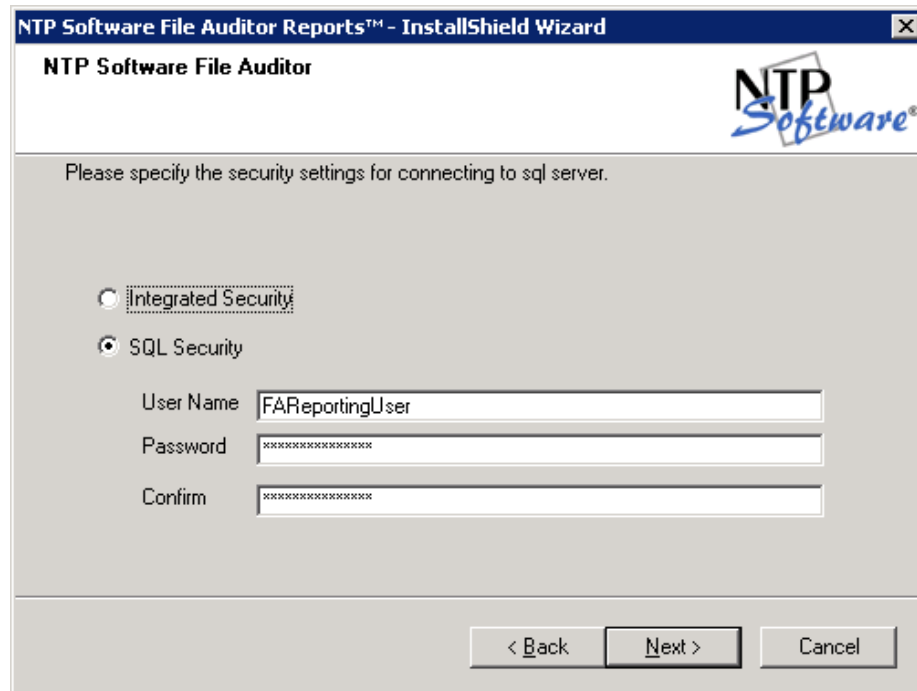
Server: localhost

Database: FileAuditor

InstallShield

< 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**.

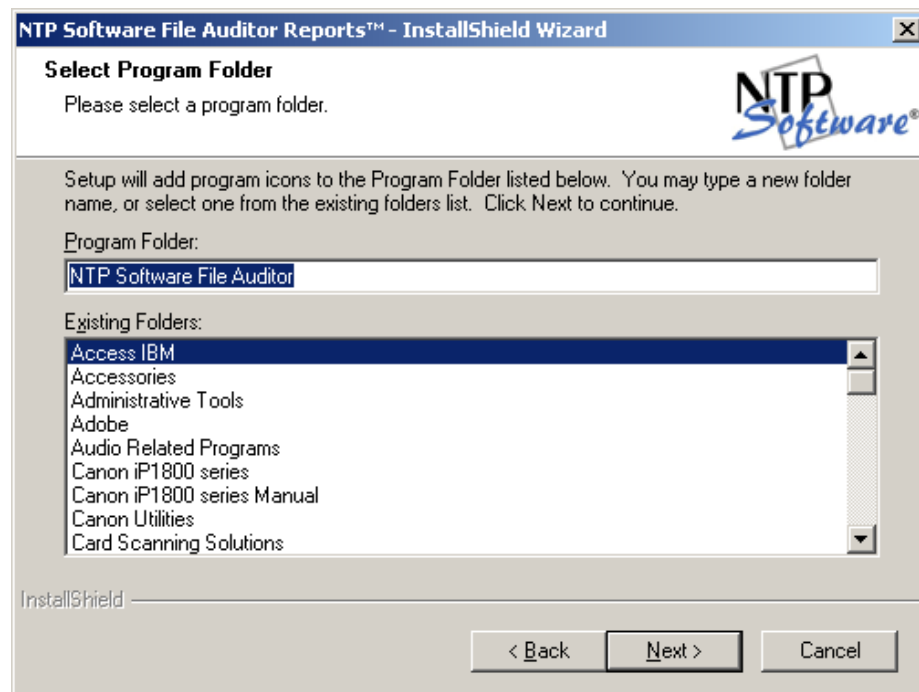


The image shows a Windows-style dialog box titled "NTP Software File Auditor Reports™ - InstallShield Wizard". The main heading is "NTP Software File Auditor" with the NTP Software logo on the right. The instruction text reads: "Please specify the security settings for connecting to sql server." There are two radio button options: "Integrated Security" (unselected) and "SQL Security" (selected). Below these are three text input fields: "User Name" containing "FAReportingUser", "Password" with masked characters, and "Confirm" with masked characters. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

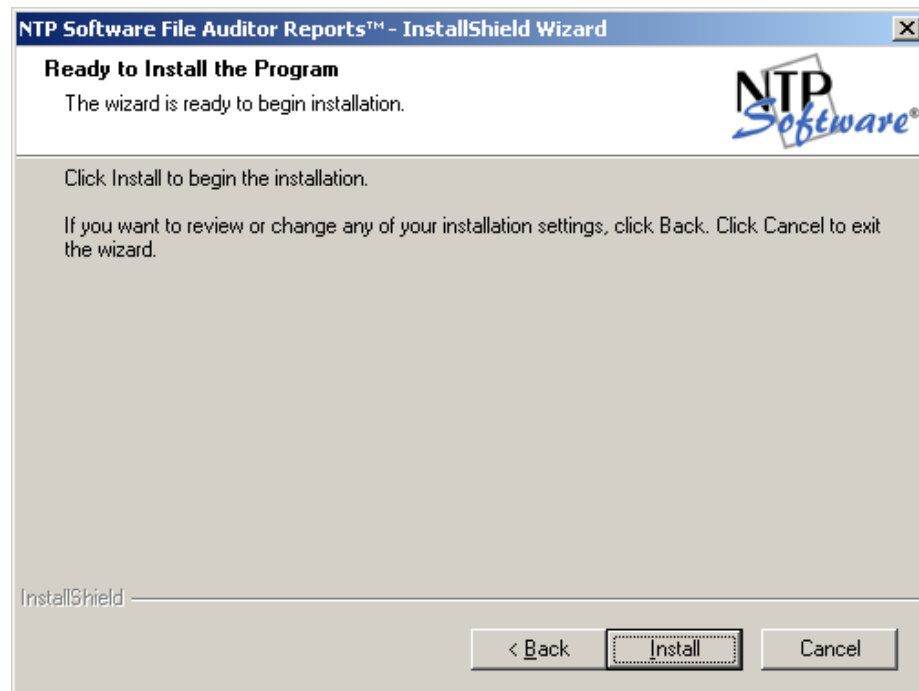
NOTES:

- 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](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 reports 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](http://[SQLReportingHostMachine]/Reports)].
 2. Open the **DefendX Software Control-Audit Reports** folder or the reports folder specified in the installation.

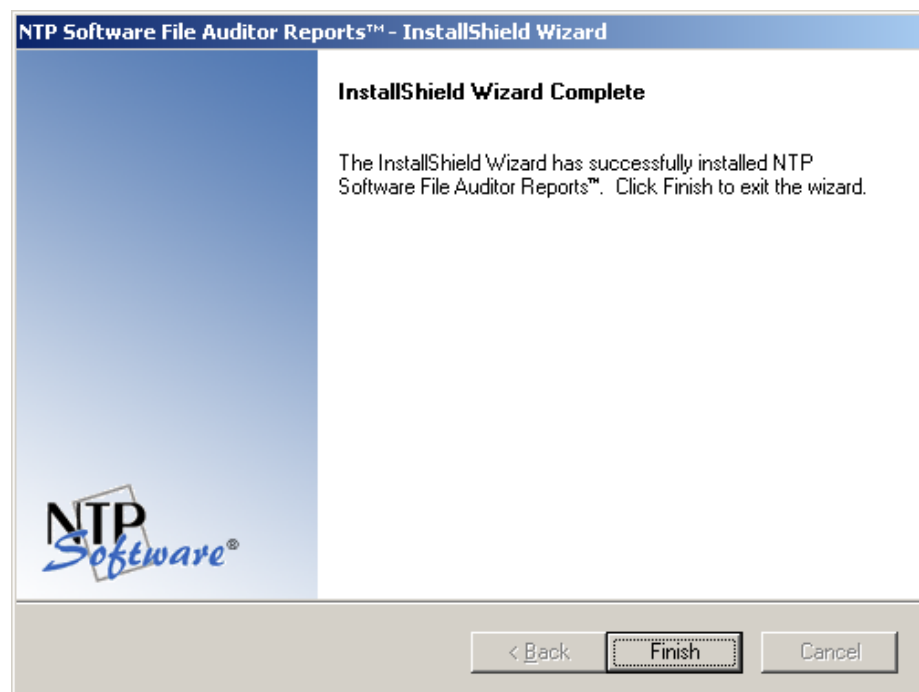
3. Open the **Properties** top tab, then select the **Security** left tab.
 4. Click on **New Role Assignment**".
 5. Write the user or group name, select the **Browser** role, then click **OK**.
9. If the **Please upgrade to SP3** dialog box was displayed, click **OK**.
 10. In the **Select Program 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

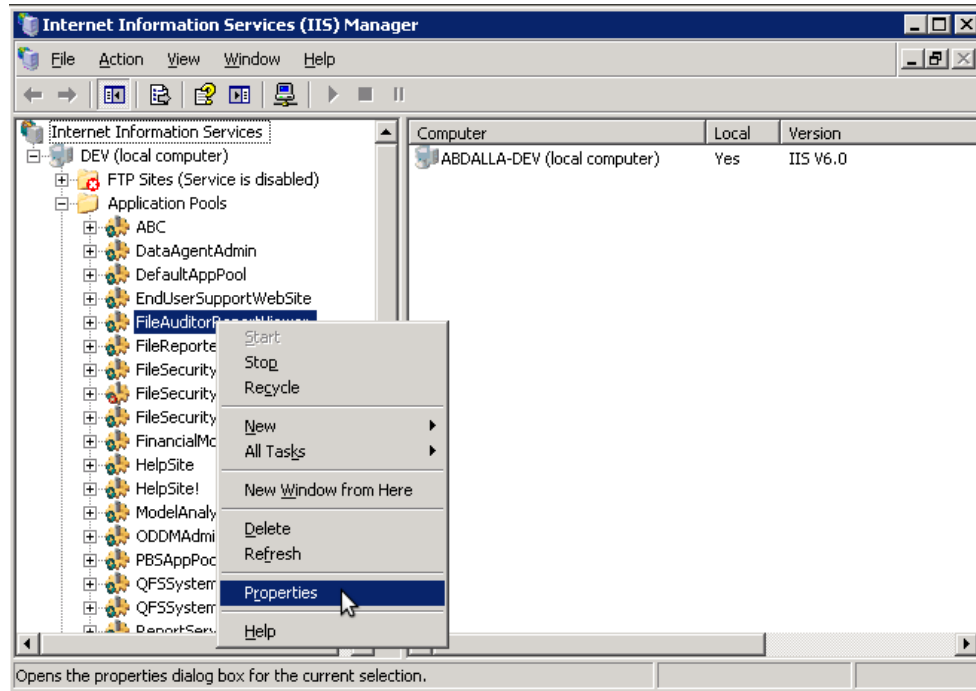
For the Historical Data feature to function properly under the Integrated Security setting, the Windows user account who will recall the historical data should have ADMINISTER BULK OPERATIONS permission to the database, along with ALTER and INSERT permissions to the HistoricalOperations and HistoricalDAcls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

This section will help you configure Control-Audit Reports website to use 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:
 - d. ADMINISTER BULK OPERATIONS permission to Control-Audit database.
 - e. ALTER and INSERT permissions to the HistoricalOperations and HistoricalDAcls tables.
 - f. Read and Change permissions to a share on an DefendX Software ODDM Primary server.
4. Configure the 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**.

The screenshot shows the 'FileAuditorReportViewer Properties' dialog box with the 'Identity' tab selected. The 'Application pool identity' section is active, showing options for 'Predefined' (Network Service) and 'Configurable' (selected). The 'Configurable' section includes fields for 'User name' (Galactic\FARepotsUser) and 'Password' (masked with dots), along with a 'Browse' button. The 'OK' button is highlighted with a mouse cursor.

FileAuditorReportViewer Properties

Recycling Performance Health Identity

Application pool identity

Select a security account for this application pool:

☐ Predefined Network Service

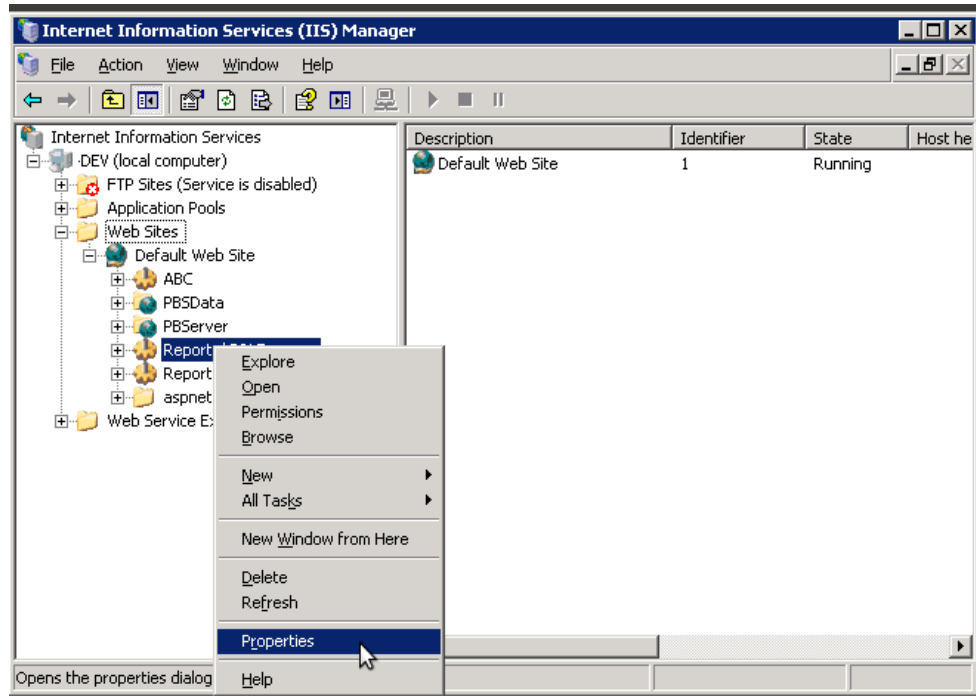
☒ Configurable

User name: Galactic\FARepotsUser Browse

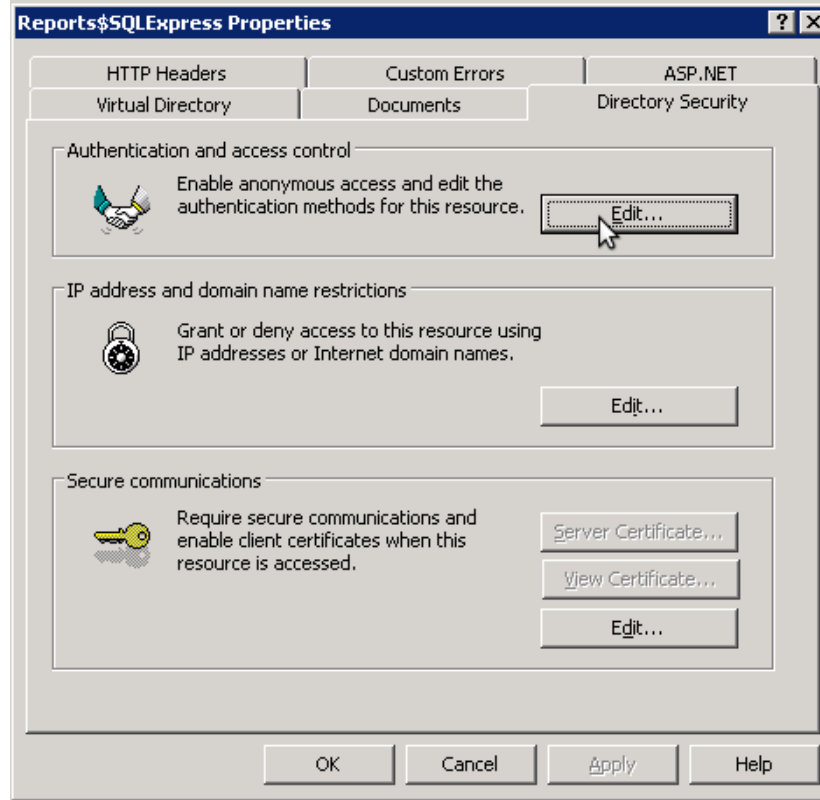
Password:

OK Cancel Apply Help

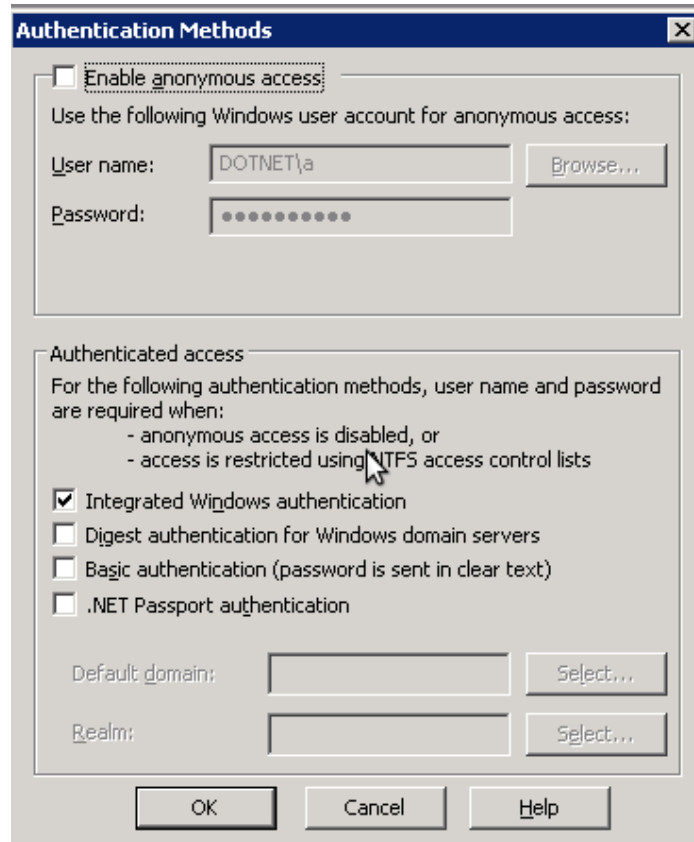
5. Open the DFXReportViewer website properties.



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



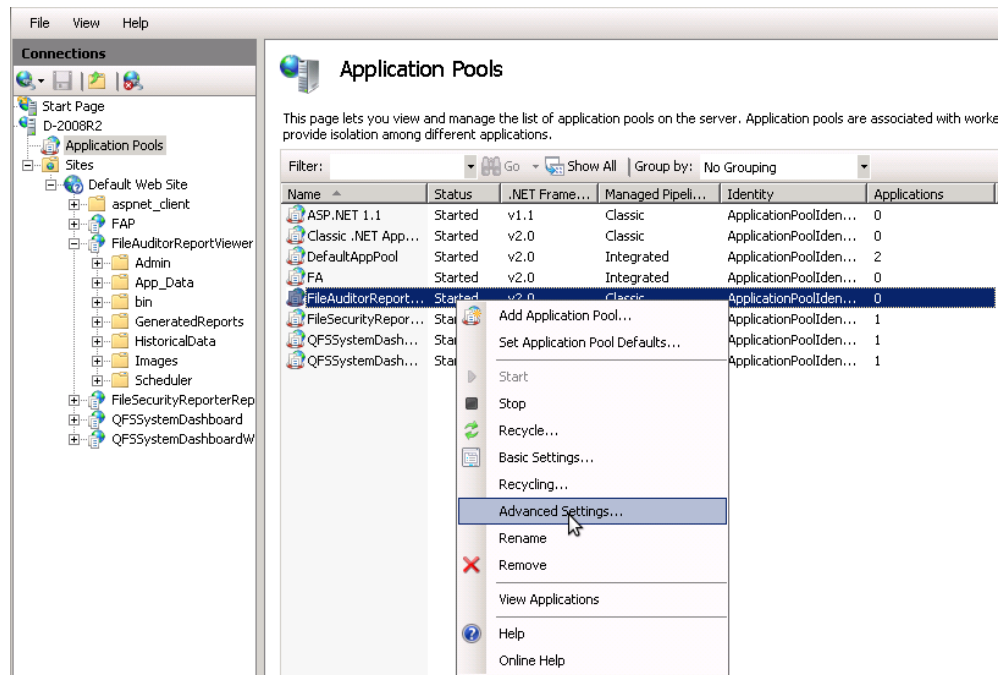
7. Disable all authentication methods except **Integrated Windows Authentication**.



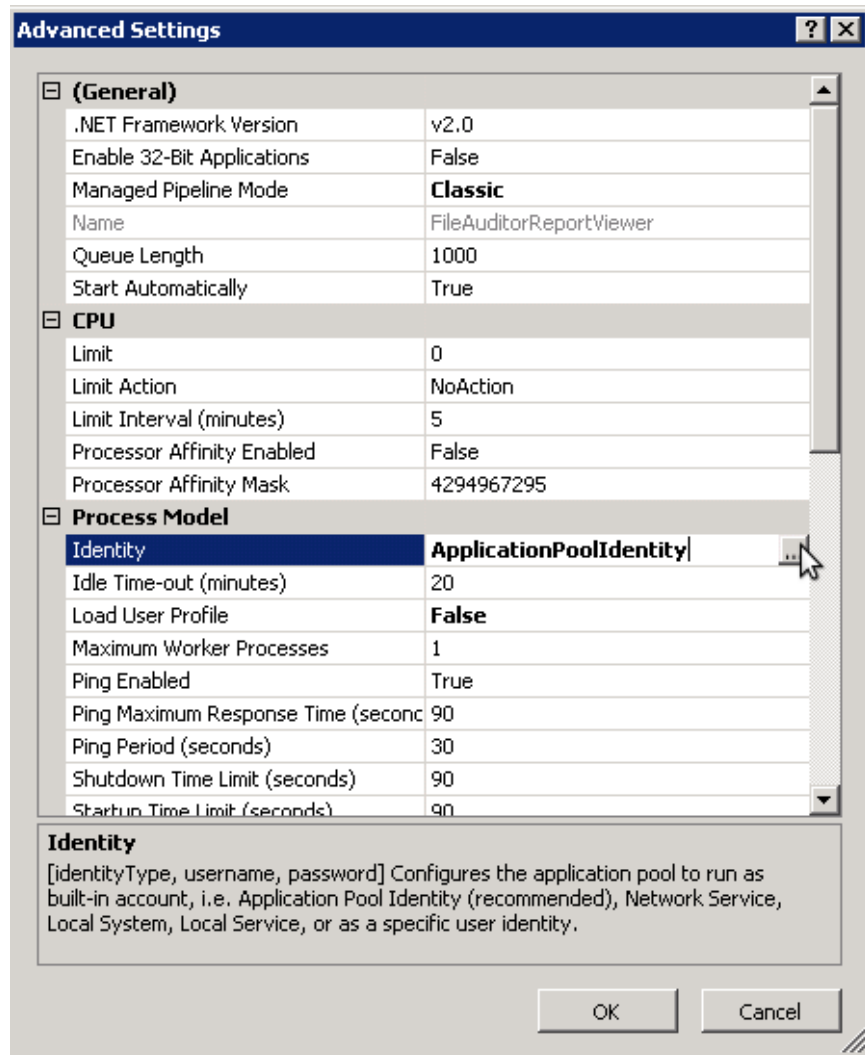
The image shows a Windows-style dialog box titled "Authentication Methods". It has a standard title bar with a close button (X). The dialog is divided into two main sections. The top section is for "Anonymous access" and contains a checkbox labeled "Enable anonymous access:" which is currently unchecked. 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:" containing the text "DOTNET\administrator" and "Password:" containing a series of dots. To the right of the "User name:" field is a "Browse..." button. 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". Below the bullet points are four checkboxes: "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".

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 **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

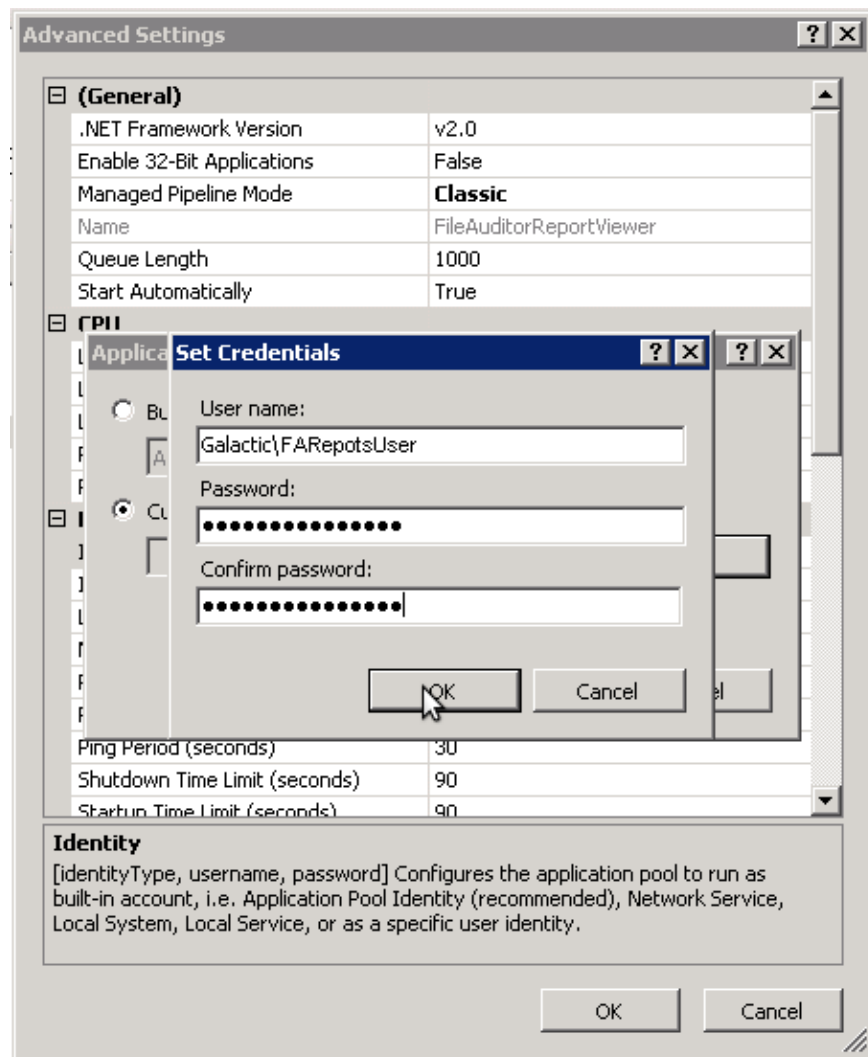
Limit	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295

Process Model

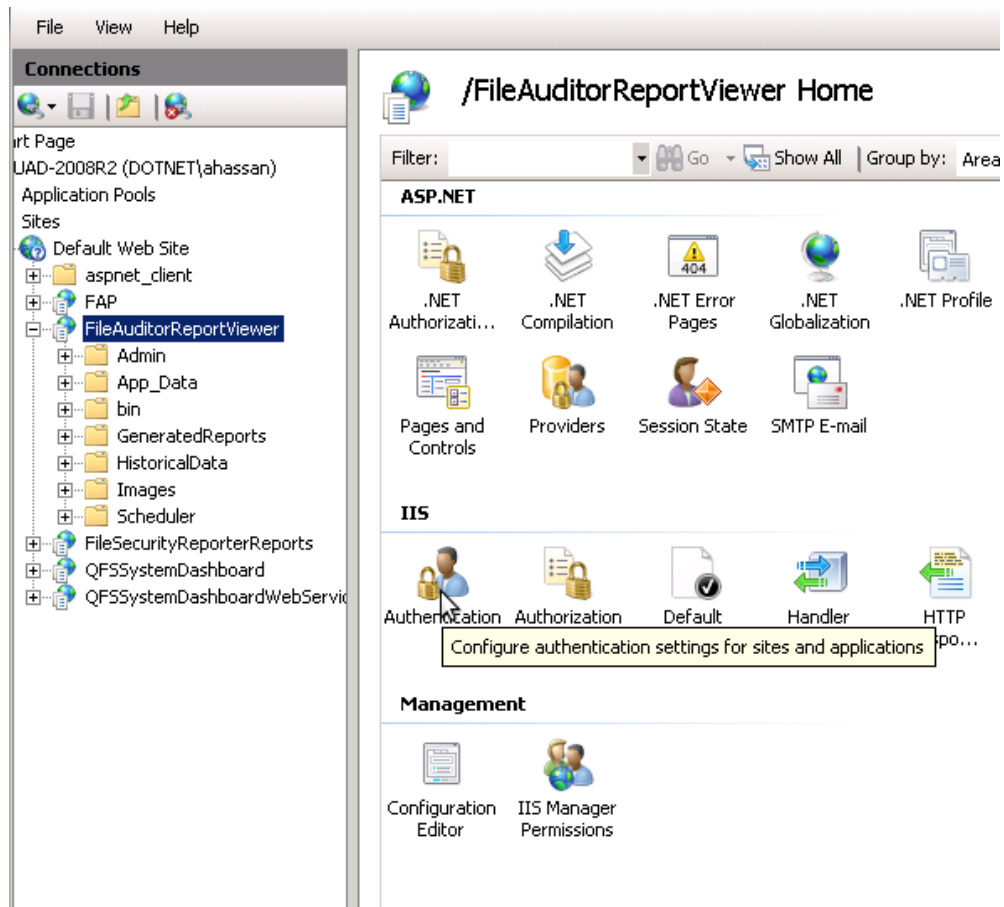
Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	20
Load User Profile	False
Maximum Worker Processes	1
Ping Enabled	True
Ping Maximum Response Time (seconds)	90
Ping Period (seconds)	30
Shutdown Time Limit (seconds)	90
Startup Time Limit (seconds)	90

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.

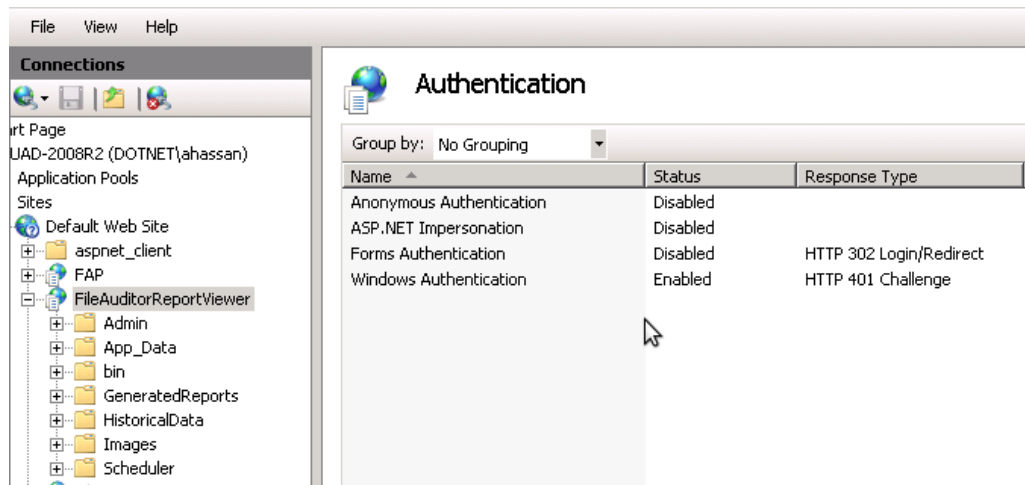
OK Cancel



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

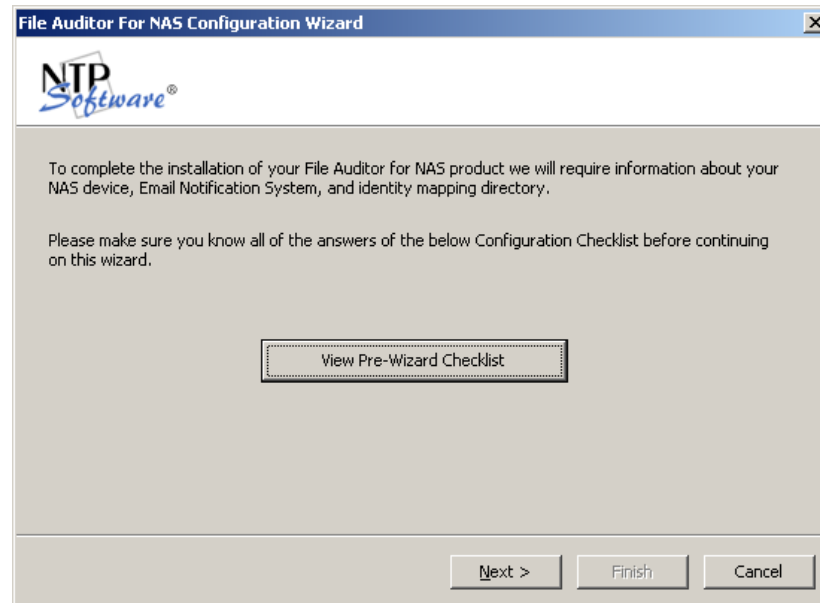


5. Disable all authentication methods except **Windows Authentication**.

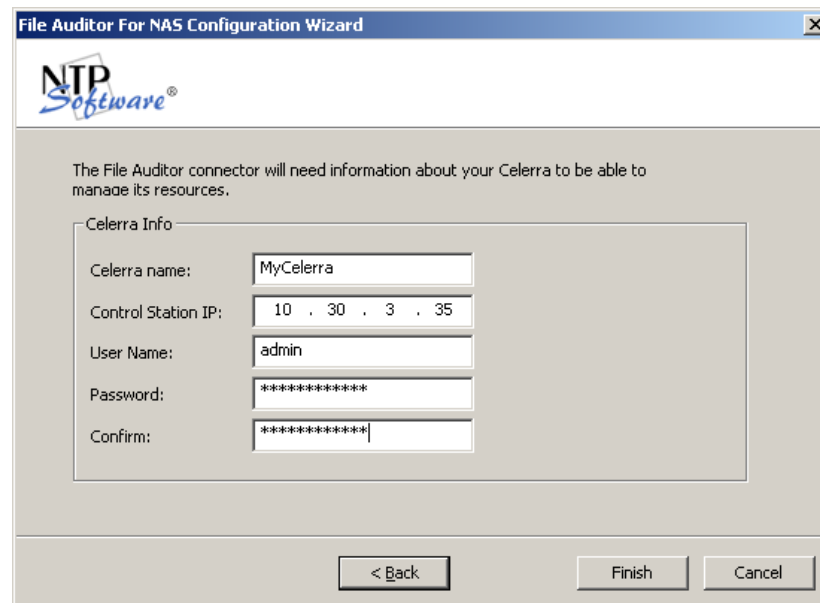


Using the DefendX Software Control-Audit for NAS, EMC Edition Configuration Wizard

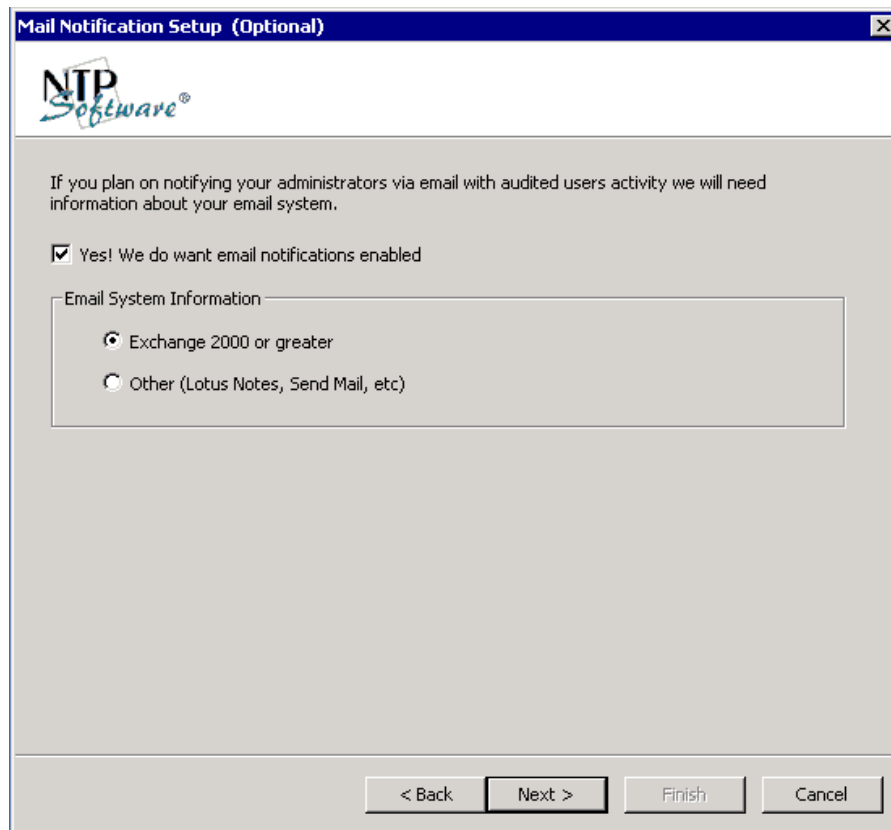
1. Click the **View Pre-Wizard Checklist** button and gather the required information before continuing. Click **Next**.



2. Enter the name of your VNX, the IP address of the station controlling the VNX, and the username and password on the Control Station. Click **Next**.



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 >" (which is highlighted with a black border), "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.

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

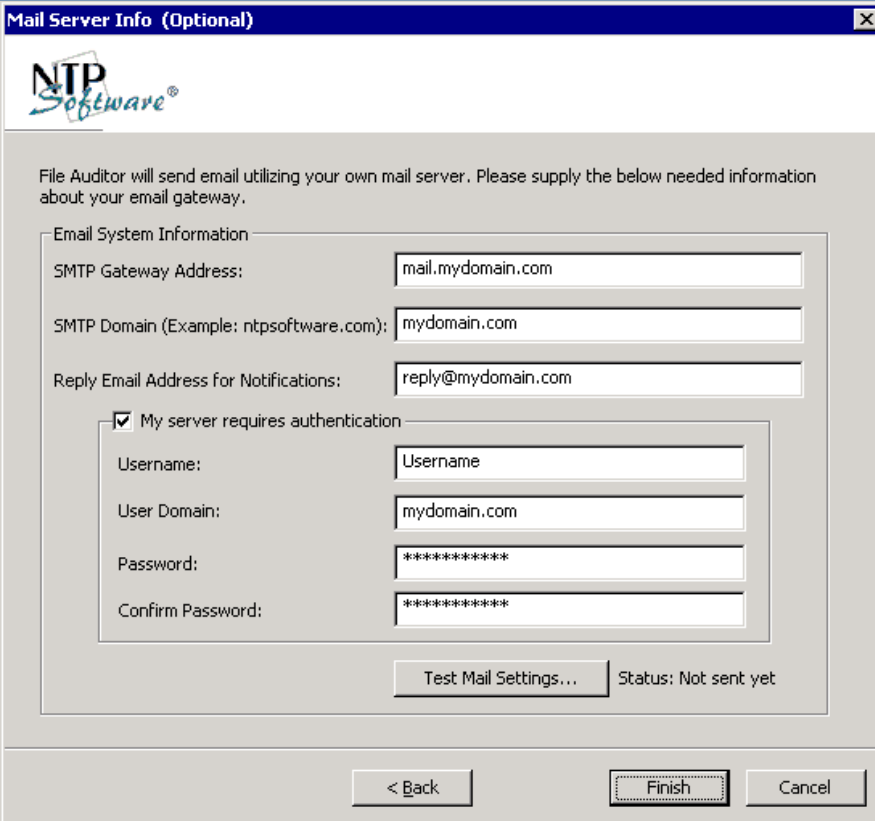
Primary Active Directory Server: PrimaryServer Port: 389

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**.

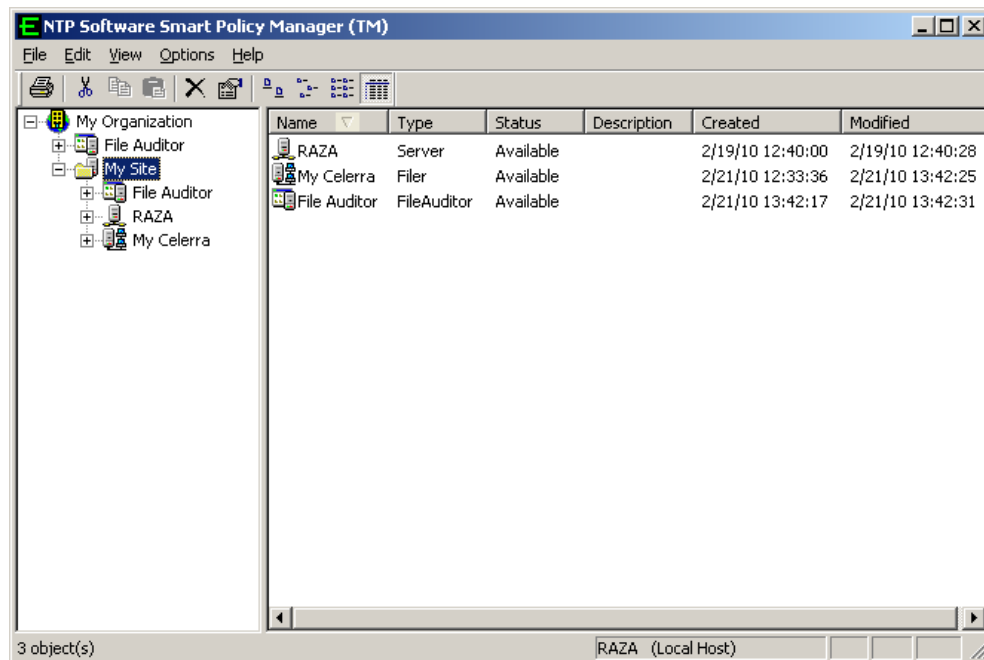


The image shows a Windows-style dialog box titled "Mail Server Info (Optional)". At the top left is the NTP Software logo. Below the title bar, a message states: "File Auditor will send email utilizing your own mail server. Please supply the below needed information about your email gateway." The main 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 checkbox labeled "My server requires authentication" which is checked. This checkbox is followed by a sub-section with four fields: "Username:" (value: "Username"), "User Domain:" (value: "mydomain.com"), "Password:" (value: "*****"), and "Confirm Password:" (value: "*****"). At the bottom of this sub-section is a button labeled "Test Mail Settings..." and a status indicator that says "Status: Not sent yet". The bottom of the dialog box has three buttons: "< Back", "Finish" (which is highlighted with a dashed border), and "Cancel".

Adding VNXs to the DefendX Software Control-Audit Policy Hierarchy

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

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



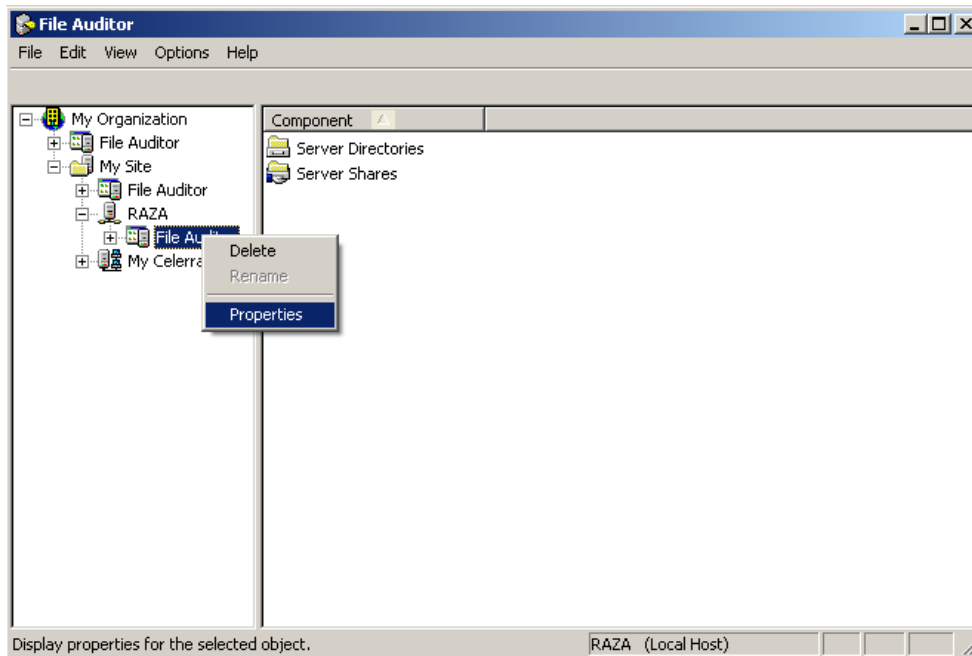
Right-click on a container node, then select **New > VNX**.

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

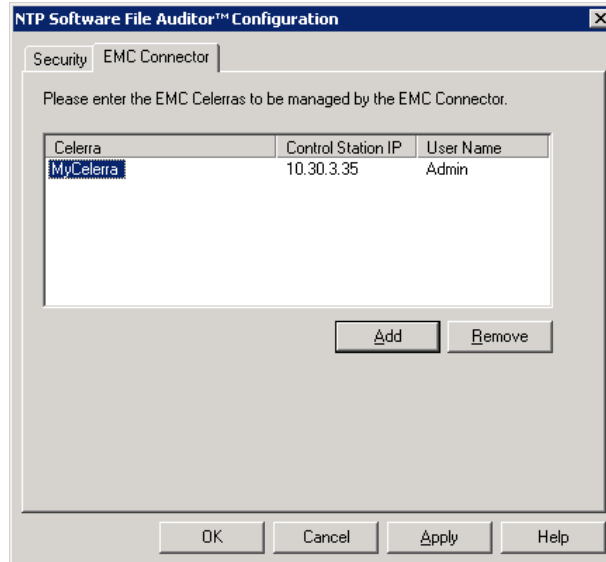
The EMC VNX server will be listed in the Control-Audit Admin left panel tree view.

This allows a company with multiple VNXs and multiple Control-Audit Servers to control which Control-Audit Server will manage which EMC VNX.

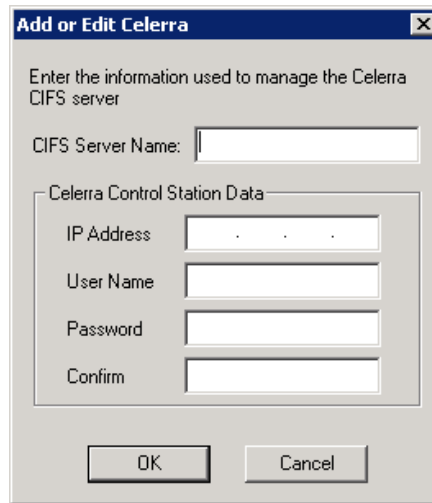
In the left pane, expand the server on which DefendX Software Control-Audit is installed and right-click **Control-Audit**. From the pop-up menu, choose **Properties**.



3. Click the **EMC Connector** tab. Your VNX should be listed; if it is not, click **Add**.



4. Enter the name of your VNX, the Control Station IP, the username, and the password. Click **OK**.



The image shows a Windows-style dialog box titled "Add or Edit Celerra". Inside the dialog, there is a text label "Enter the information used to manage the Celerra CIFS server". Below this, there is a text input field labeled "CIFS Server Name:". Underneath that is a section titled "Celerra Control Station Data" which contains four text input fields: "IP Address", "User Name", "Password", and "Confirm". At the bottom of the dialog are two buttons: "OK" and "Cancel".

To make sure that DefendX Software Control-Audit for NAS, EMC Edition will work properly, you must make sure that the VNX is generating events properly. Once events are generated, DefendX Software Control-Audit for NAS, EMC Edition is responsible for controlling those events.

The registration and details of each event DefendX Software Control-Audit receives are logged by DefendX Software Control-Audit as needed. Logging is turned off by default to avoid negative impact on DefendX Software Control-Audit performance. Only part of the logging file will be enabled.

To test that events are generated from the VNX, follow these steps on the DefendX Software Control-Audit machine:

1. Create two new DWORDs in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\DefendXSoftware\ECS

2. Name the DWORDs **Trace VNX RPC** and **Trace CAVA Detail**.
3. Set their values to **1**.

The Registration event may already have been sent, so it will not be logged unless the NTP Connector service is restarted. However, if events were detected in the log file, this is an indication that the registration was successful.

The registration message, if logged, should look like this:

```
CEPA Register Response: <RegisterResponse><EndPoint version="1.0" desc="DefendX  
Software Control-Audit EMC Connector" /><Filter><EventTypeFilter value="0x000700FF"  
/></Filter></RegisterResponse>
```

Any detected event, if logged, should have an entry that starts with the following:

```
CEPA event received: <CheckEventRequest>
```

The rest of the logged event is the event details: type, path, user, and so on.

NOTE: Remember to disable the logging you just enabled, as it has a negative effect on DefendX Software Control-Audit performance.

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#DFX1281EF

