Lepide

CONFIGURATION GUIDE

FILE SERVER ADVANCED GUIDE

Table of Contents

1 Introduction 3

2 Requirements and Prerequisites 3

3 Required User Rights 3

4 Install the Lepide Data Security Platform 3

5 Configure Service Credentials 3

6 Add Windows File Server with Advanced Configuration 4

6.1 Service Rights 4

7 Add NetApp Filer with Advanced Configuration 11

7.1 Add NetApp 7-Mode 11

7.1.1 Prerequisites to Audit NetApp 7-Mode 11

7.1.2 Auditing Flow of NetApp 7-Mode 13

7.1.3 Add NetApp Cluster Mode 19

7.2 Steps after Adding a File Server Component 28

8 Adding Multiple File Servers 31

8.1 Adding Multiple Windows File Servers 31

8.2 Adding Multiple NetApp 7 Mode File Servers 43

8.3 Adding Multiple NetApp Cluster File Servers 50

9 Audit Rule Management 56

9.1 Create Audit Rule 56

9.1.1 Common Issues with Reports 66

9.2 Change the Priority of Audit Rule 67

10 Create Audit Policy 68

11 Add User Group 90

12 Support 97

13 Trademarks 97

1 Introduction

This guide helps you to install, configure, and manage the Lepide Data Security Platform for File Server. The solution provides a comprehensive means of auditing Windows File Servers and NetApp Filers (both 7-Mode and Cluster Mode).

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

A list of supporting documentation is provided at the end of this guide.

2 Requirements and Prerequisites

Before you start installing the Lepide Data Security Platform for File Server, make sure that your computer meets the requirements and prerequisites. Please refer to the Windows File Server Quick Start Guide or the NetApp Quick Start Guide for information on what these requirements are.

3 Required User Rights

To install and work with Lepide, you need to have appropriate rights to the system where it will be installed. You will also need to have appropriate rights to access Active Directory, SQL Server, Windows File System, and NetApp Filer. For more information please refer to the Prerequisites and Installation Guide.

4 Install the Lepide Data Security Platform

To install the Lepide Data Security Platform, please refer to the Prerequisites and Installation Guide.

5 Configure Service Credentials

For information on how to configure service credentials, please refer to the Prerequisites and Installation Guide.

6 Add Windows File Server with Advanced Configuration

6.1 Service Rights

A Windows File Server can be audited with minimum permissions given to the Lepide Service Account. Please refer to our Principle of Least Privilege Guide to know the rights required for the service account.

After you have installed the software and configured Lepide service to run with the service account, you can add a File Server for auditing.

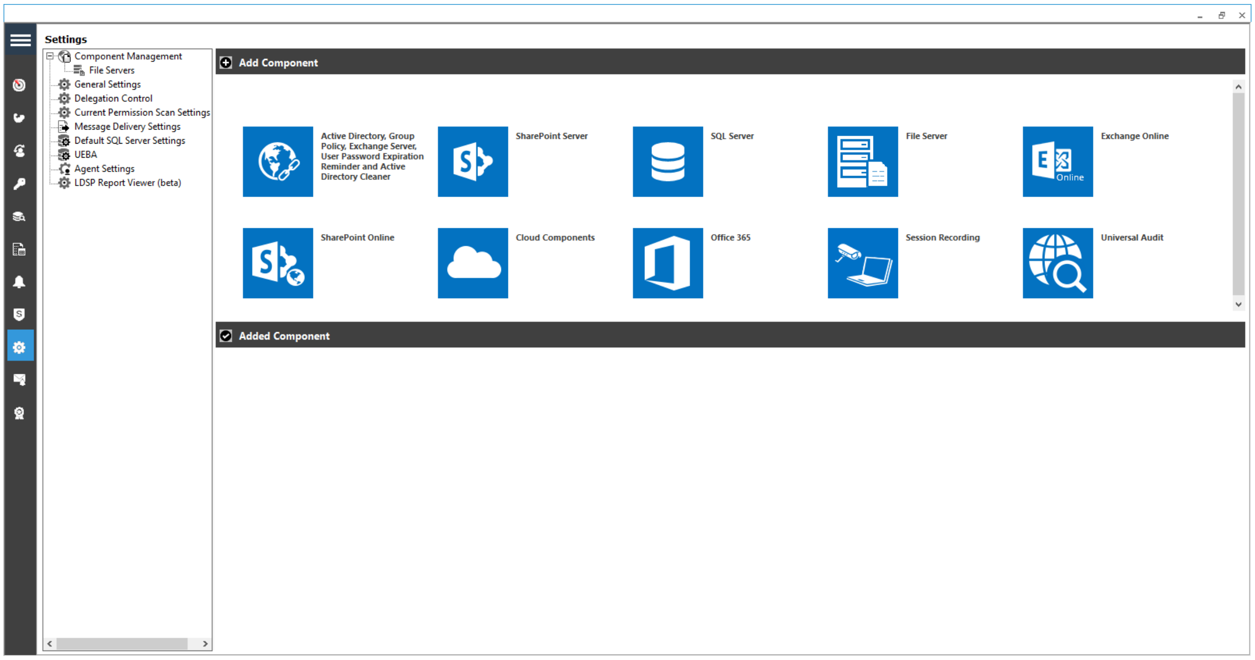
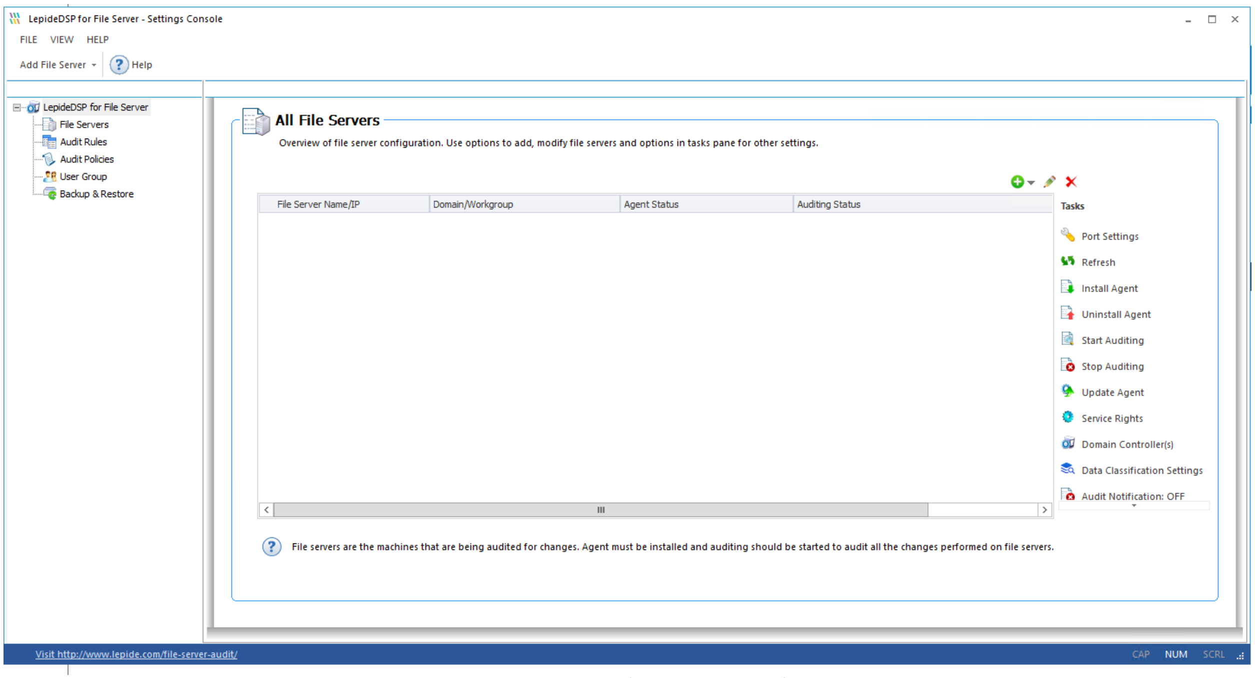


Figure 1: Component Management Window

From the Component Management window, under the Add Component section, click on the File Server icon to add this component to the solution.

The Settings Console dialog box is displayed:



Overview of file server configuration. Use options to add, modify file servers and options in tasks pane for other settings.

File Server Name/IP	Domain/Workgroup	Agent Status	Auditing Status

File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 2: File Server Console

Here, you can click **Add File Server** icon on the toolbar to add either of the following file servers:

- Windows File Server
- NetApp Filer

1. Click the **Add File Server** icon, select **Single** then select **Windows**.

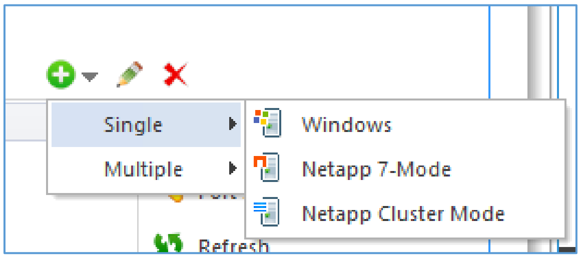
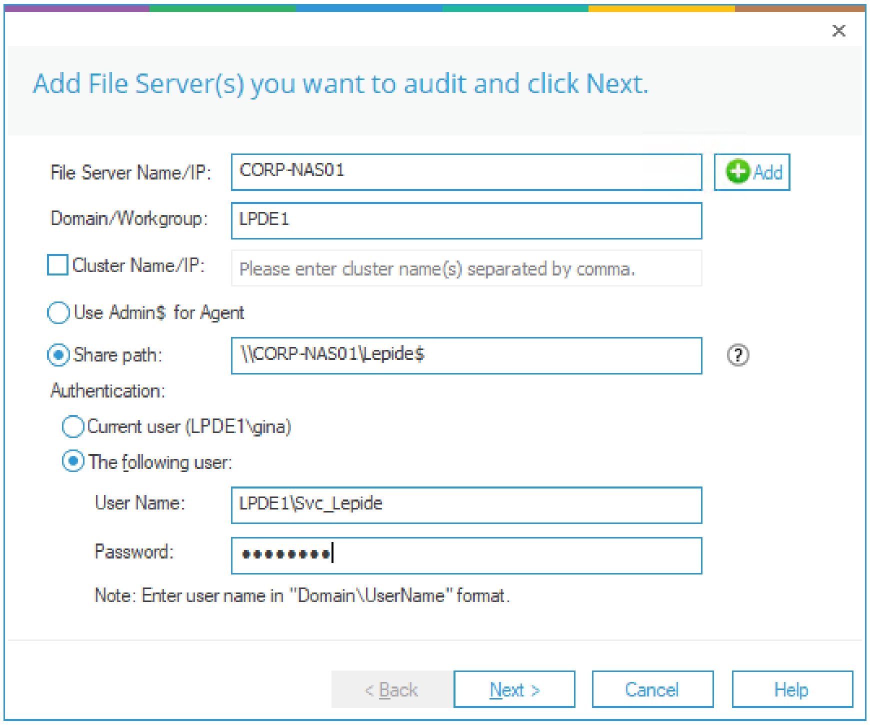


Figure 3: Option to add File Server

2. The **Add File Server** wizard starts:



Add File Server(s) you want to audit and click Next.

File Server Name/IP: CORP-NAS01

Domain/Workgroup: LPDE1

□ Cluster Name/IP: Please enter cluster name(s) separated by comma.

○ Use Admin$ for Agent

● Share path: \\CORP-NAS01\Lepide$

Authentication:

○ Current user (LPDE1\gina)

● The following user:

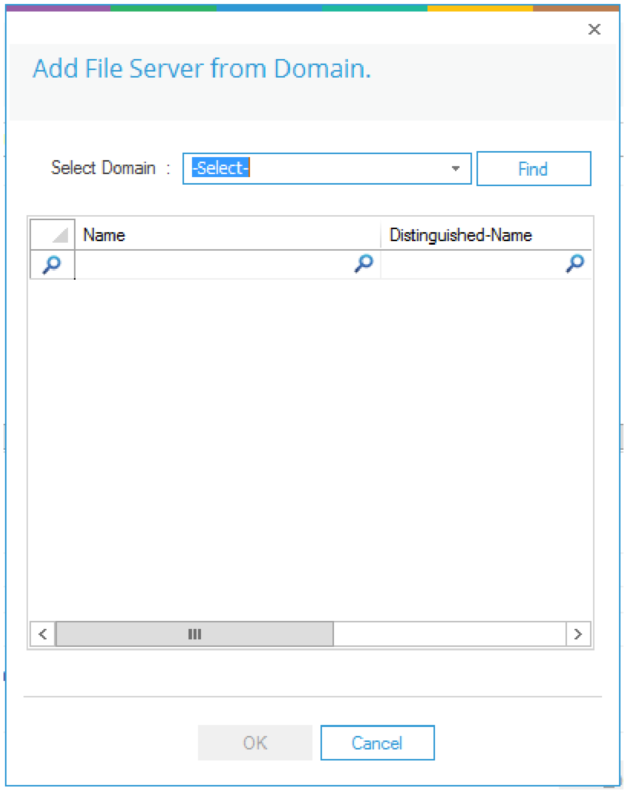
User Name: LPDE1\Svc_Lepide

Password: ●●●●●●●●●

Note: Enter user name in "Domain\UserName" format.

Figure 4: Add File Server Wizard

3. Enter the name or **IP Address** of the server along with its **Domain or Workgroup** name.
4. Instead of typing manually, you can click **Add** button to scan the domain network and select the required file server.



Add File Server from Domain.

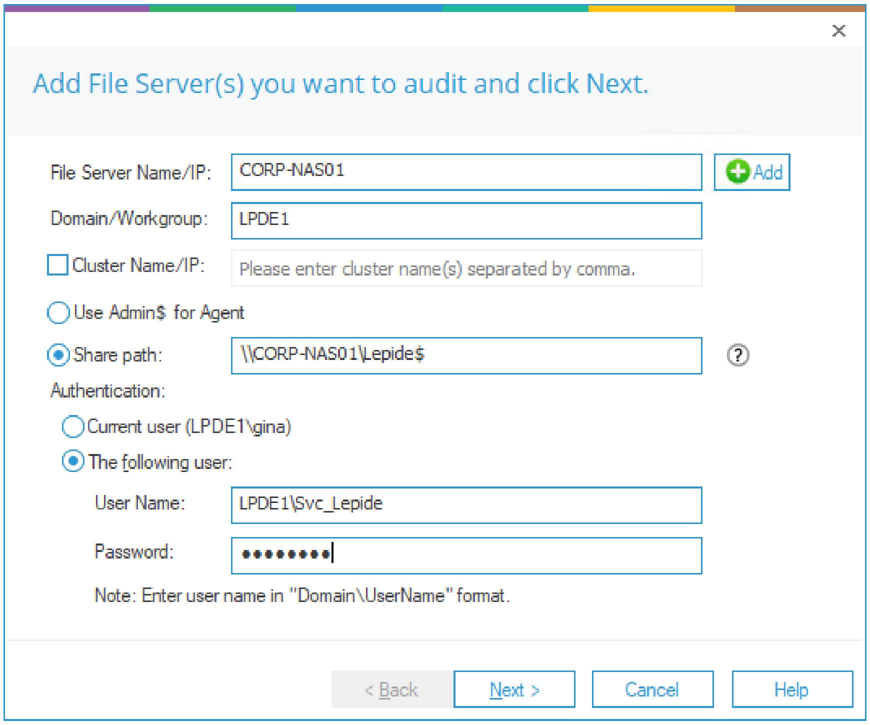
Select Domain : -Select-

Figure 5: Add File Server from Domain

5. You can select the **Domain name** in the drop-down menu or type its name.
6. Click the **Find** button to list its computers in the blank area.
7. Select the computer you want to audit and click **OK**.
   It takes you back to the previous wizard, which now displays the selected File Server.
8. **Cluster Name/IP:** If you are using Windows Failover Cluster Configuration, then you will need to add all the nodes of the cluster separately in the solution as individual file servers. The reports will be visible under the Section of the active node in the solution.

   Please add the cluster IP or Name here for scanning the permissions of the shares on a cluster.
9. You can use the default **Admin$** location for the agent if the Service Account has admin rights on the File Server. If not, you can create any shared folder on the File Server and specify its path in the **Share Path** Option. The Service account should have at least **Modify** permission on this folder.
10. Select the user with which you want to add the File Server.
11. If you are logged in as a user that has the above rights, then you can select **Current User**.

12. If the logged in user does not have the required rights, then you have to select **The following user** option and provide the login credentials of a user who has the required rights.



Add File Server(s) you want to audit and click Next.

File Server Name/IP: CORP-NAS01

Domain/Workgroup: LPDE1

□ Cluster Name/IP: Please enter cluster name(s) separated by comma.

○ Use Admin$ for Agent

● Share path: \\CORP-NAS01\Lepide$

Authentication:

○ Current user (LPDE1\gina)

● The following user:

User Name: LPDE1\Svc_Lepide

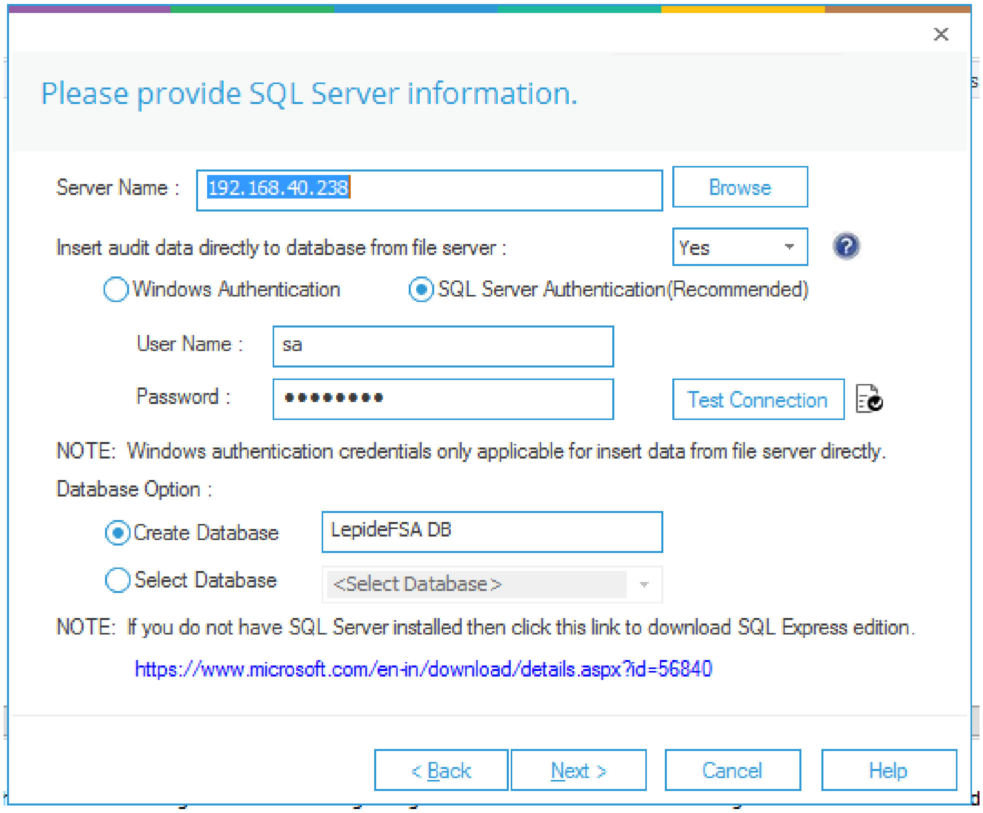
Password: ••••••••

Note: Enter user name in "Domain\UserName" format.

Figure 6: Enter File Server Details

13. After entering the details, click **Next**.

The next step is to provide the SQL Server details:



Please provide SQL Server information.

Server Name : 192.168.40.238

Insert audit data directly to database from file server : Yes

○ Windows Authentication ● SQL Server Authentication(Recommended)

User Name : sa

Password : ••••••••

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 7: SQL Server Details

14. Type the **Server Name** or click **Browse** to select the desired SQL Server.
15. There are two authentication options:

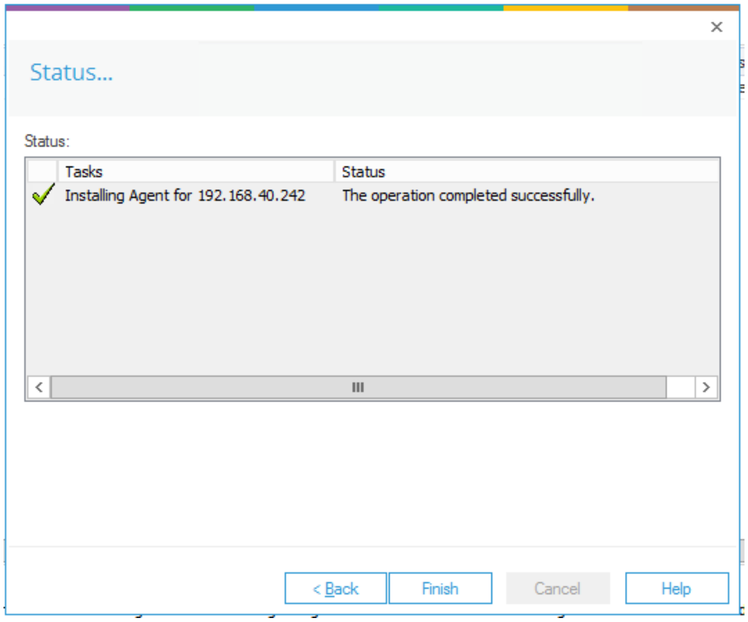
    a) **Windows Authentication:** In this method, you can use any domain user windows account which have at least **dbcreator** role on the SQL server.

    b) **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote machine or the local machine. We recommend that this option is selected.

    Provide the username and password of an SQL User, which has sufficient rights to create a new database.

16. Please select Insert Audit Data Directly to Database from File Server as **YES,** only if the SQL connection from the File Server to the SQL Server is open. Please select **NO** if the connection is not open and the insertion will happen from the Application Server then.
17. Enter a database name in the database name field to create a new database. You can also select an existing database created by Lepide or another application.
18. Click **Next** to start installing the auditing agent for Windows File Server.

    After the agent is installed, the following dialog box is displayed:



Status...

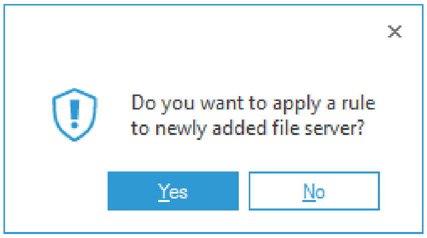
Status:

	Tasks	Status
✓	Installing Agent for 192.168.40.242	The operation completed successfully.

Figure 8: Auditing Agent is Installed

19. Click **Finish** to complete the process.

A dialog box is displayed asking whether you want to apply a rule to the newly added file server:



Do you want to apply a rule to newly added file server?

Figure 9: Option to Create a Rule

Audit Rule Management is explained in Section 9 of this document. Please refer to this for information on creating a rule.

7 Add NetApp Filer with Advanced Configuration

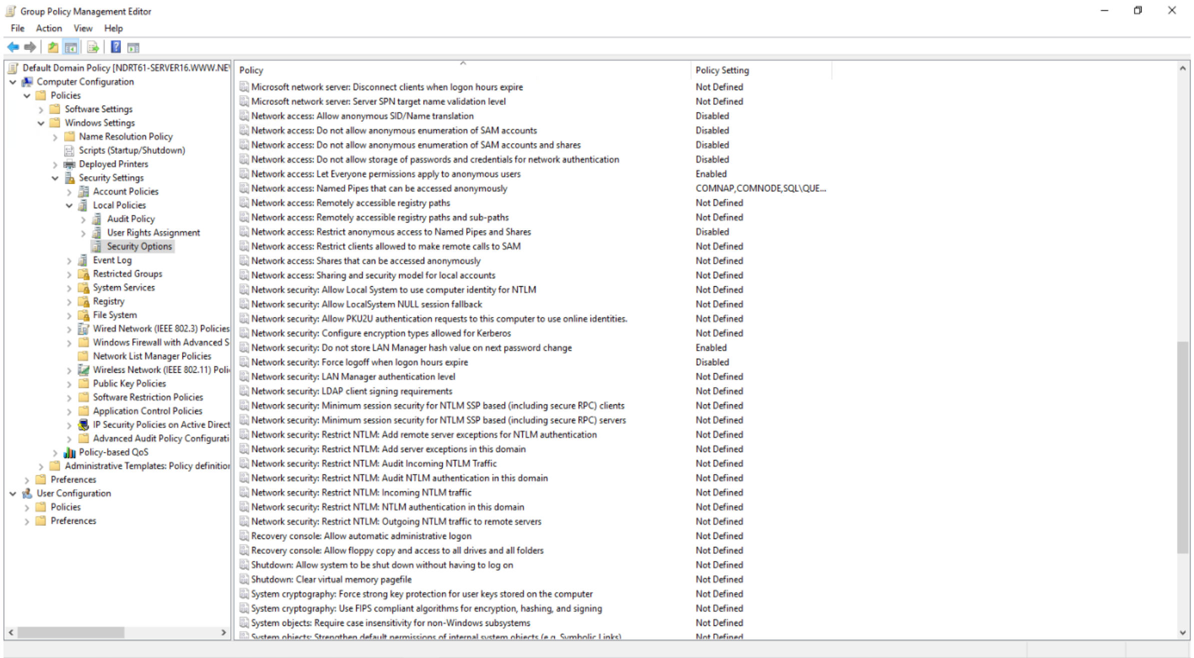
You can add NetApp 7-Mode and NetApp Cluster Mode for auditing.

7.1 Add NetApp 7-Mode

7.1.1 Prerequisites to Audit NetApp 7-Mode

Please refer to Section 3 of the NetApp Quick Start Guide. If you chose to setup the NetApp 7 mode manually, please make sure the following conditions are met:

- You need to verify the settings on the NetApp Filer before installing the agent. Ensure that the *httpd.admin.enable* option is on. It is **ON** by default, but we still recommend you check it first before installing the agent.
- Ensure that the NetApp Filer time is synced with the time on the agent system to get precise report timings.
- In the Agent system GPO Settings, change the required settings as shown:


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [NDRT61-SERVER16.WWW.NE
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced S
Network List Manager Policies
Wireless Network (IEEE 802.11) Poli
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Direct
Advanced Audit Policy Configurati
Policy-based QoS
Administrative Templates: Policy definitio
Preferences
User Configuration
Policies
Preferences

Policy	Policy Setting
Microsoft network server: Disconnect clients when logon hours expire	Not Defined
Microsoft network server: Server SPN target name validation level	Not Defined
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Enabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNODE,SQL\QUE...
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Disabled
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Not Defined
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Not Defined
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined
Shutdown: Allow system to be shut down without having to log on	Not Defined
Shutdown: Clear virtual memory pagefile	Not Defined
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
System objects: Require case insensitivity for non-Windows subsystems	Not Defined
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Not Defined

Figure 10: Highlighting Group Policies for NetApp Filer

Follow the steps below to perform these settings:

1. Type **gpmc.msc** in **Run** or search in the **Start Menu**. Press the **ENTER** key to open Group Policy Management.
2. Under the forest, navigate to **Domains, Local Domain, Default Policy**.
3. Right-click on it and select **Edit**. The **Group Policy Management Editor** window opens.

   Under the default domain policy, navigate to **Computer Configuration, Policies, Windows Settings, Security Settings, Local Policies.**
4. Click on Security Options. In this section, make the following policy settings:
   a) Network Access: Do not allow anonymous enumeration of **SAM accounts, Disabled**

   b) Network Access: Do not allow anonymous enumeration of **SAM accounts and shares, Disabled**

   c) Network Access: Do not allow storage of passwords and credentials for **network authentication, Disabled**

   d) Network Access: Let Everyone permissions apply to **anonymous users, Enabled**

e) Double-click Network Access: Named pipes that can be accessed anonymously and select the checkbox to define policy settings. Type **NTAPVSRQ** and click **Apply**.

f) Network Access: Restrict anonymous access to **Named Pipes and Shares, Disabled**

7.1.2 Auditing Flow of NetApp 7-Mode

Please refer to Section 3 of the [NetApp Quick Start Guide]()

Follow the steps below to add NetApp 7-Mode for auditing.

1. Click the **Add File Server** icon, ⊕▾ select **Single** then select **NetApp 7-Mode**.

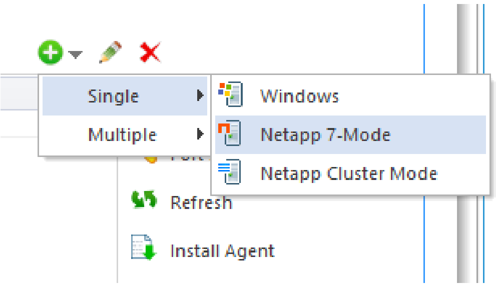
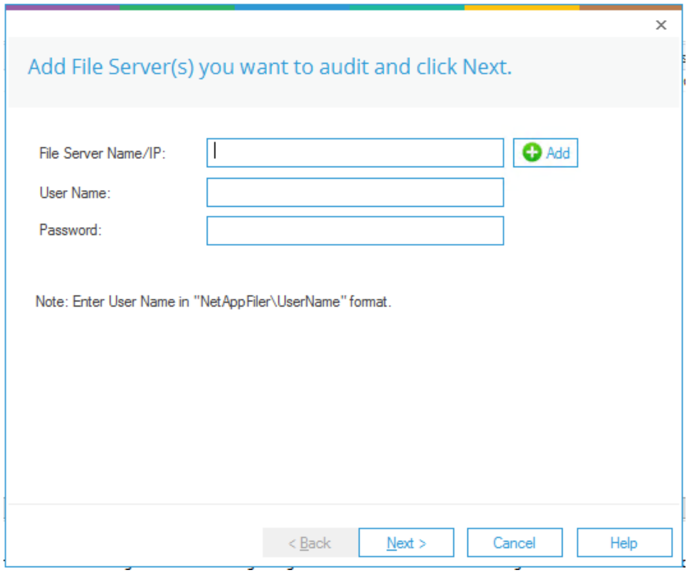


Figure 11: Option to Add NetApp 7-Mode File Server

2. The **Add File Server** wizard starts:



Add File Server(s) you want to audit and click Next.

File Server Name/IP:

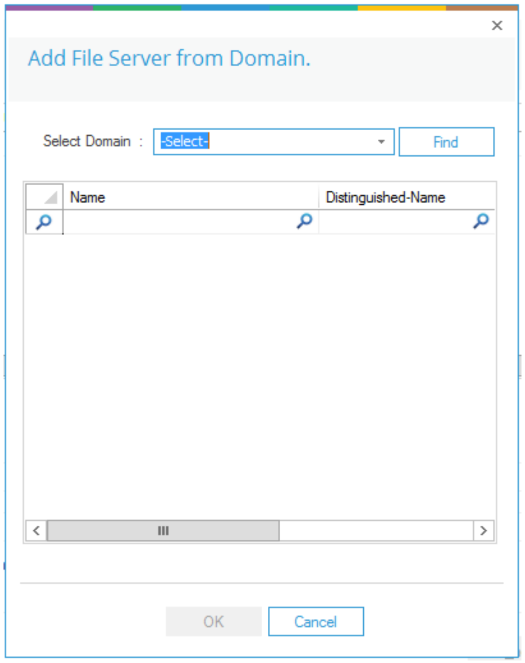
User Name:

Password:

Note: Enter User Name in "NetAppFiler\UserName" format.

Figure 12: Select File Server Type

3. Either enter the name or IP Address of NetApp Filer Name manually or click **Add** to select a NetApp Filer from the network.



Add File Server from Domain.

Select Domain : -Select-

Name	Distinguished-Name

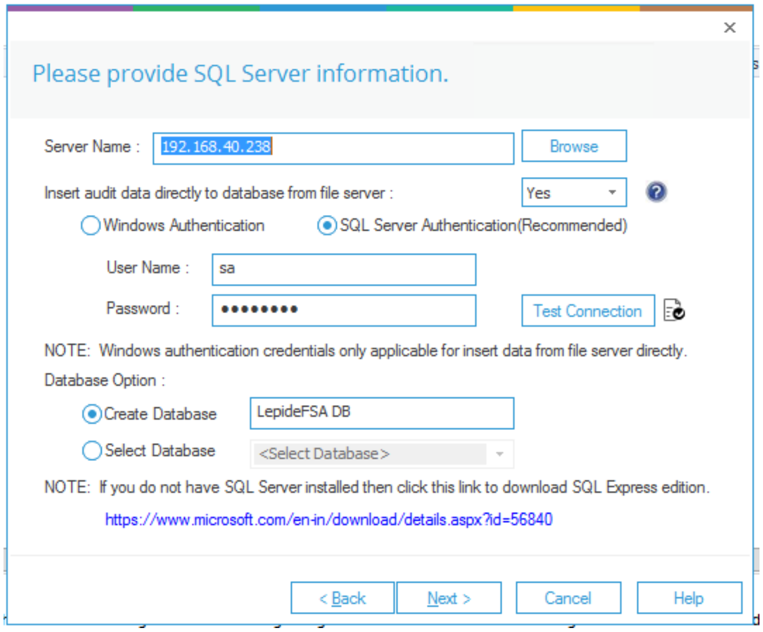
Figure 13: Select a NetApp Filer

4. Here, you can select a domain name and click **Find** to list the available Filers in it.

5. Select a NetApp Filer and click **OK**.

6. After the required NetApp Filer is selected, enter the login credentials of a NetApp Administrator to add it.

7. Click **Next** to go to the next step, to provide the details of SQL Server to create a database for storing auditing logs.



Please provide SQL Server information.

Server Name : 192.168.40.238

Insert audit data directly to database from file server : Yes

○ Windows Authentication ● SQL Server Authentication(Recommended)

User Name : sa

Password : •••••••••

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 14: SQL Server Details to add NetApp Filer

18. Click the **Server Name** dropdown to select the desired SQL Server.

19. There are two authentication options under it.

    a) **Windows Authentication:** This mode can be selected if SQL Server is installed on the same computer where the solution is installed.

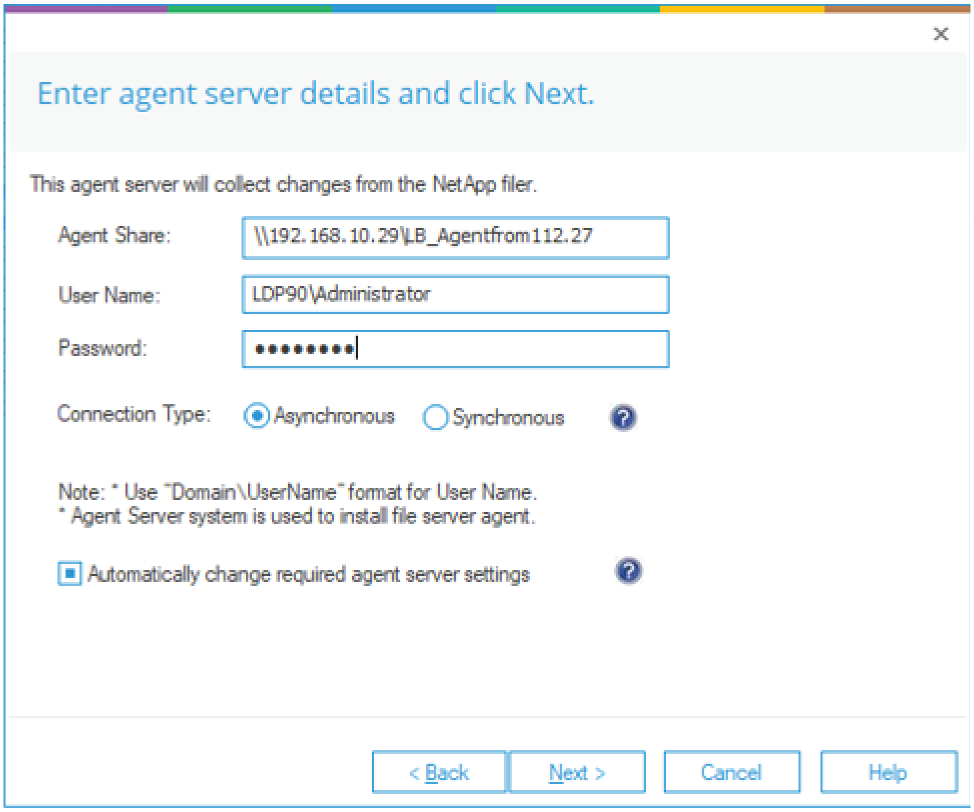
    b) **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote or local computer. We recommend that this option is selected.

    Provide the username and password of a SQL user, who has sufficient rights to create the database.

20. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.

21. Click **Next**

The NetApp Agent Information dialog box is displayed:



Enter agent server details and click Next.

This agent server will collect changes from the NetApp filer.

Agent Share: \\192.168.10.29\LB_Agentfrom112.27

User Name: LDP90\Administrator

Password: ●●●●●●●●●

Connection Type: ● Asynchronous ○ Synchronous

Note: * Use "Domain\UserName" format for User Name.
* Agent Server system is used to install file server agent.

☑ Automatically change required agent server settings

Figure 15: NetApp Agent Information

22. Enter the details of the system where you wish to install the agent to collect the changes from NetApp Filer.

NOTE: You can install the agent on another system apart from NetApp Filer. However, it is important to note that the agent can only be installed on any client system or the domain controller. We recommend that you do not to install it on workgroup computers and the agent is installed only on the connected Windows Computer and not on NetApp

23. Enter the name or IP Address of the agent system.

24. Provide the Username and Password of an administrator of the agent system to allow access to the software to install the agent.

NOTE: The provided user should be a member of any one group out of Administrators, Domain Admins, Enterprise Admins, and Schema Admins groups, at the agent system, to enable the auditing of NetApp Filer. If the above rights are not assigned to the user, then follow the steps below.

a. Go to Administrative Tools.

b. Open Active Directory Users and Computers.

c. Select User Properties.

d. Go to Member Of, Add Group.

e. Select any of the following groups as per the above requirements.
   i. Administrators
   ii. Domain Admins
   iii. Enterprise Admins
   iv. Schema Admins

f. Click Apply and OK

25. Now you need to choose the Connection Type. Lepide provides the following two types of connections with the NetApp Filer from the agent:

    a. **Asynchronous**: This option is quick, but it cannot capture security details. It captures the security events but does not show details.

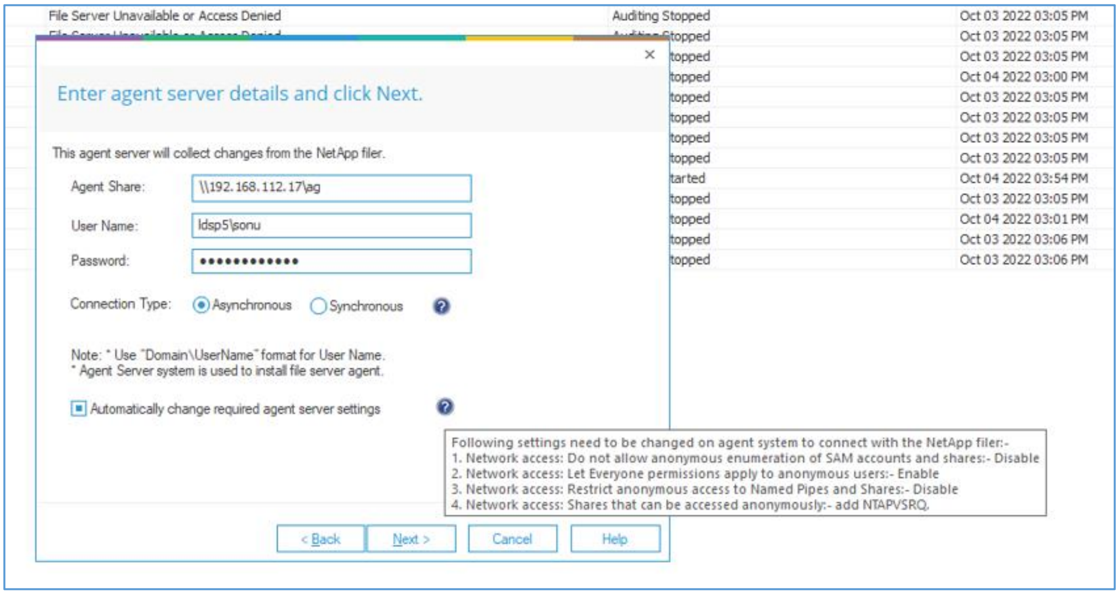
    b. **Synchronous**: This option captures security details, but the process slightly slows down the performance of the Filer.

NOTE: If you need the Permission Analysis of NetApp Filer, we recommend using synchronous mode to connect to NetApp Filer.

26. Certain changes are required in the Local Security Policies to allow the software to audit Filers. The software provides a checkbox to make such changes automatically from its end.

27. If you do not want to go for automatic changes or face an error in applying these changes automatically, then uncheck this option and make these manually. To know more, refer to Section 7.1.1 Prerequisites to Audit NetApp 7-Mode.

28. Click the checkbox to make the changes automatically. The software displays the list of required changes in the next screen and reconfirms it.



Enter agent server details and click Next.

This agent server will collect changes from the NetApp filer.

Agent Share: \\192.168.112.17\ag

User Name: ldsp5\sonu

Password: •••••••••••••

Connection Type: ● Asynchronous ○ Synchronous

Note: * Use "Domain\UserName" format for User Name.
* Agent Server system is used to install file server agent.

☑ Automatically change required agent server settings

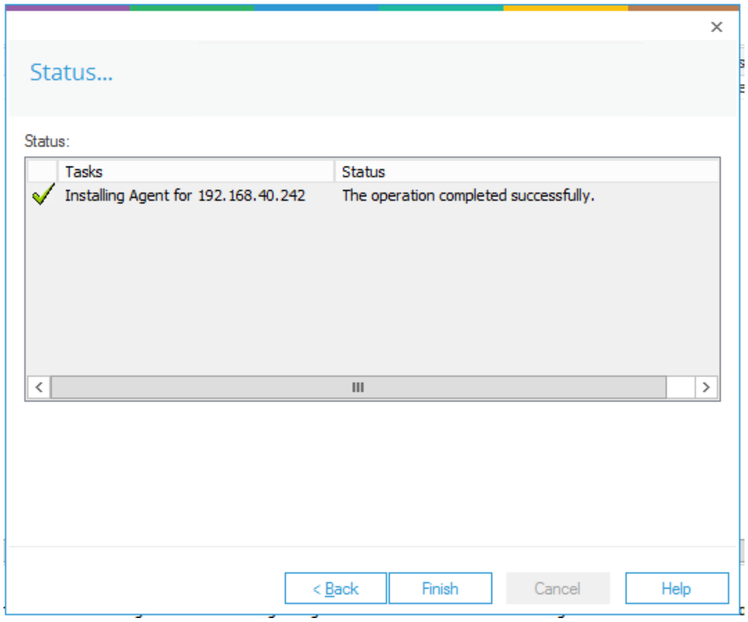
Following settings need to be changed on agent system to connect with the NetApp filer:-
1. Network access: Do not allow anonymous enumeration of SAM accounts and shares:- Disable
2. Network access: Let Everyone permissions apply to anonymous users:- Enable
3. Network access: Restrict anonymous access to Named Pipes and Shares:- Disable
4. Network access: Shares that can be accessed anonymously:- add NTAPVSRQ.

Figure 16: List of Changes to be made for Auditing NetApp Filer

29. Click **Yes** to make these changes and to install the agent.

If you click **No**, then the changes will not be made, but still, the agent will be installed. Because of no agent installation, the audit reports will not be generated in this case.

To generate the audit reports after clicking **No**, you have to make these changes manually. For further information, refer to Section 7.1.1 Prerequisites to Audit NetApp 7-Mode.



	Tasks	Status
✓	Installing Agent for 192.168.40.242	The operation completed successfully.

Figure 17: Installing the Agent for NetApp Filer

30. Click **Finish** to complete the process.

7.1.3 Add NetApp Cluster Mode

Follow the steps below to add NetApp Cluster Mode for auditing.

1. Click the **Add File Server** button on the toolbar and click **NetApp Filer**.

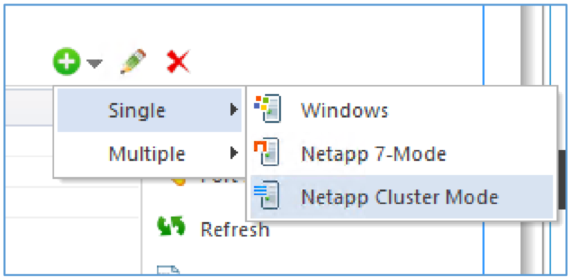
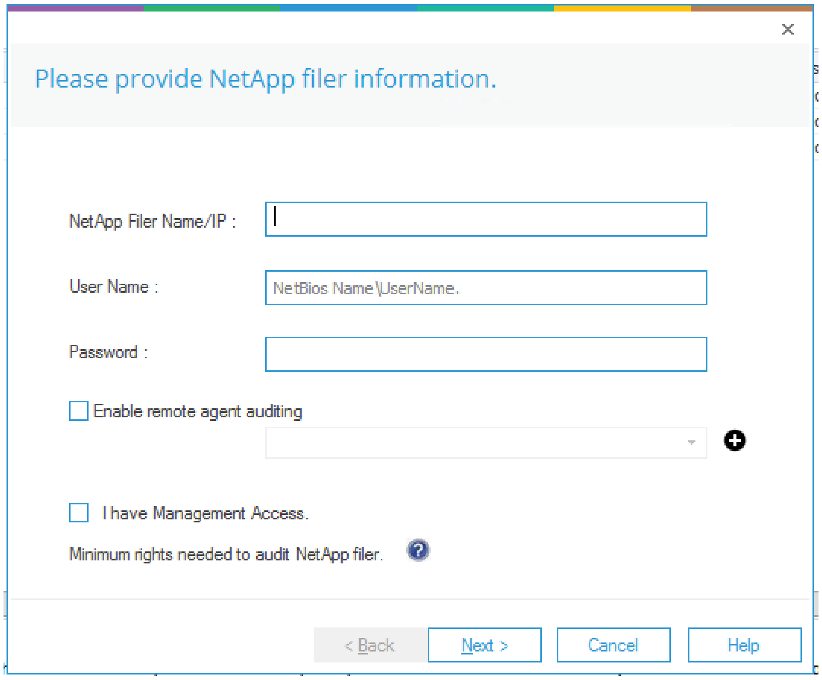


Figure 18: Option to Add File Server

You can also click the ⊕ ▾ icon in the Right Panel, go to **NetApp Filer** sub-menu and click the **NetApp Cluster-Mode**.

The Wizard to add **NetApp Cluster Mode** is displayed:



Please provide NetApp filer information.

NetApp Filer Name/IP :

User Name : NetBios Name\UserName.

Password :

□ Enable remote agent auditing

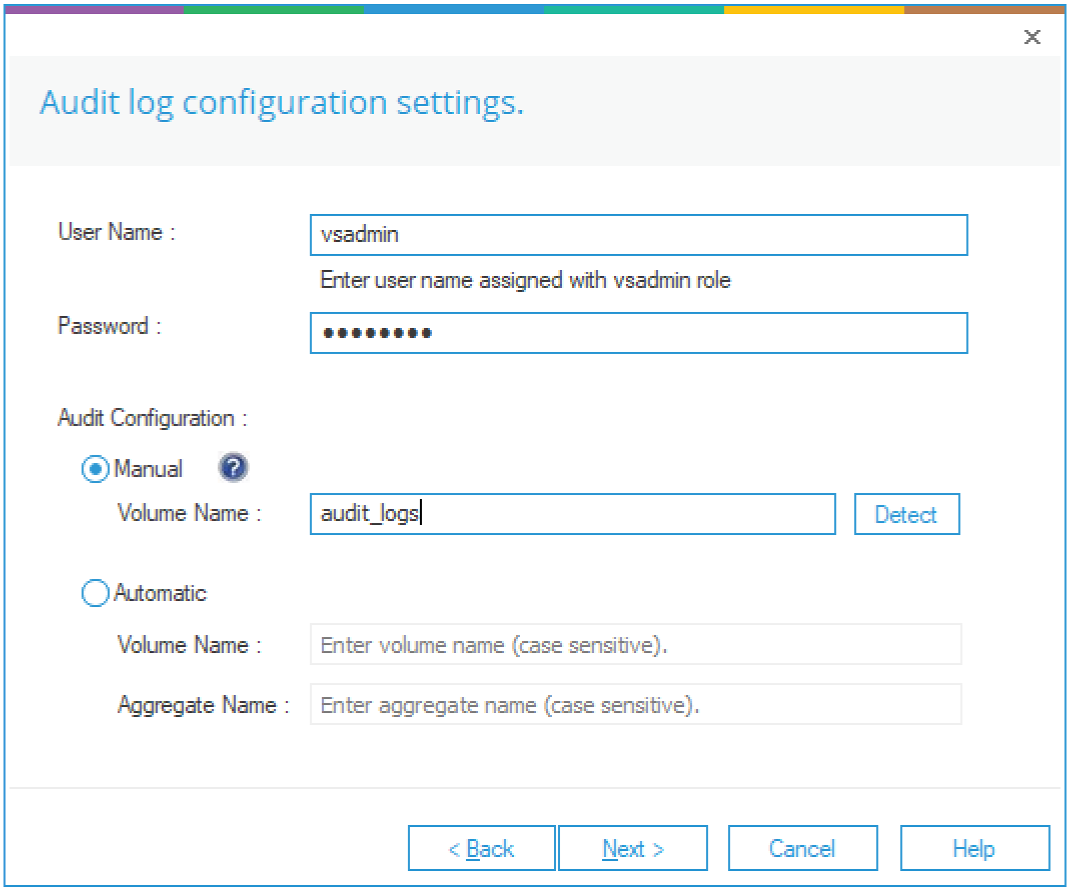
□ I have Management Access.

Minimum rights needed to audit NetApp filer.

Figure 19: Wizard to Add NetApp Cluster Mode

2. Add the following details:
   a. **Domain Name:** Enter the name or IP Address of the domain, where the NetApp Cluster Mode is located, in the **Domain** text field.
   b. **User Name:** Enter the name of a user, who is a member of **Domain Admins** group or a normal domain user account with at least **Change** Permissions to the **C$** of the SVM which is to be audited.
   c. **Password**: Enter the password of the selected user.
3. Click **Next**

The **Add File Server** dialog box is displayed:



Audit log configuration settings.

User Name : vsadmin

Enter user name assigned with vsadmin role

Password : ●●●●●●●●●

Audit Configuration :

● Manual

Volume Name : audit_logs

○ Automatic

Volume Name : Enter volume name (case sensitive).

Aggregate Name : Enter aggregate name (case sensitive).

Figure 20: Audit Log Configuration Settings

4. Add the following details:

    a. **File Server Name/IP**: Enter the name or IP Address of NetApp Filer.

    b. **User Name**: Enter the name of a user, who has vsadmin role.

    c. **Password**: Enter the password of the selected user.

    d. **Audit Configuration**: Select either **Manual Auditing** or **Automatic Auditing**. Please refer to the following points to understand these two options further to make your selection:

7.1.3.1 Which Audit Configuration should be selected?

You can select the Automatic Auditing option to enable the auditing settings automatically without giving any user input. However, you should select Manual Auditing when you are doing any of the following:

- receiving errors in enabling Automatic Auditing

- wanting to allocate 2 GB to 3 GB (not less than 2 GB and not more than 3 GB) space to a volume for auditing
- wanting to allocate more than 3 GB space to a volume for auditing

7.1.3.2 Prerequisites of Manual Auditing

Make sure that any existing manual auditing meets the following prerequisites:

a. Auditing should be enabled.

b. The minimum Log File Size (rotate-size) should be 1 MB.

c. The format of auditing should be XML.

d. The size of the selected volume should be at least 3 GB.

e. The rotate limit should be set to 2000.

7.1.3.3 Steps to Create Manual Auditing on NetApp Cluster Mode

If manual auditing does not exist already or does not meet the above prerequisites, you need to add and enable an Audit Setting manually on the selected Storage Virtual Machine (SVM).

To do this, perform the following steps:

1. Execute the following commands to configure auditing manually at NetApp Cluster Mode.

   vserver audit create -vserver <Name_SVM> -destination "/<Name_Volume>"

   -format XML -rotate-size <XX><XB>

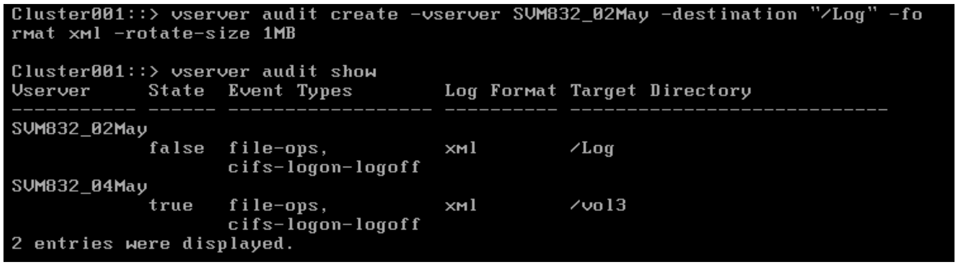
2. Change the following values.

   - <Name_SVM> : Name of SVM
   - <Name_Volume> : Name of Volume
   - **WARNING**: The minimum size of the selected volume should be 3 GB.
   - <XX> : Value in numbers. It is the size of Log File.
   - <XB> : Measurement of the file size. It can be in KB, MB, GB, TB, or PB.

   NOTE: The minimum Log File Size (rotate-size) must be 1MB.

3. After creating the auditing setting, you can execute the following command to view the auditing setting created for an SVM.

vserver audit show



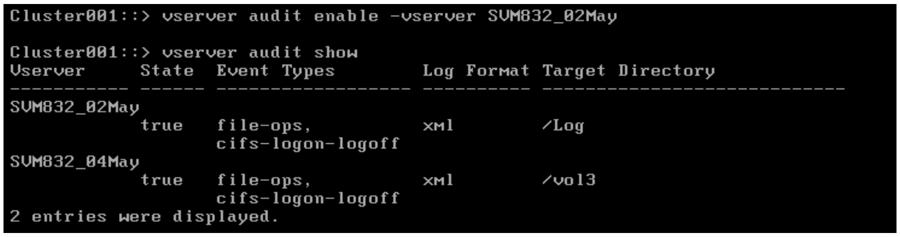
```
Cluster001::> vserver audit create -vserver SVM832_02May -destination "/Log" -fo
rmat xml -rotate-size 1MB

Cluster001::> vserver audit show
Vserver      State  Event Types        Log Format Target Directory
------------ ------ ------------------ ---------- ----------------------------
SVM832_02May
             false  file-ops,          xml        /Log
                    cifs-logon-logoff
SVM832_04May
             true   file-ops,          xml        /vol3
                    cifs-logon-logoff
2 entries were displayed.
```

Figure 21: Commands to Set Auditing and Show its Status

a. Execute the following command to enable the auditing:
setting. vserver audit enable -vserver <Name_SVM>
Replace <Name_SVM> with the name of SVM.

4. After enabling the auditing setting, execute the following command to view the status of added auditing.

vserver audit show



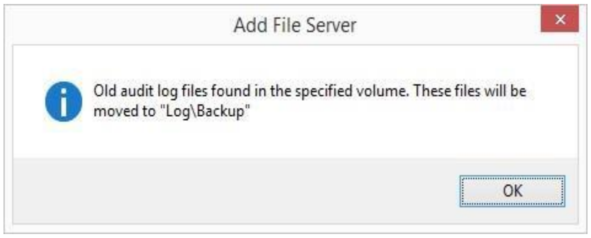
```
Cluster001::> vserver audit enable -vserver SVM832_02May

Cluster001::> vserver audit show
Vserver      State  Event Types        Log Format Target Directory
------------ ------ ------------------ ---------- ----------------------------
SVM832_02May
             true   file-ops,          xml        /Log
                    cifs-logon-logoff
SVM832_04May
             true   file-ops,          xml        /vol3
                    cifs-logon-logoff
2 entries were displayed.
```

Figure 22: Commands to Set Auditing and Show its Status

– **Manual Auditing:** In the Audit Configuration Section, click the Manual option to enable its options. If the manual auditing is already configured on the selected Storage Virtual Machine (SVM) and if it meets the above-listed prerequisites, you can click the Detect button to find and add it here.

NOTE: Old log files existing in the log volume generated before adding the file server in the solution will be moved to the Back Up folder in the log volume.

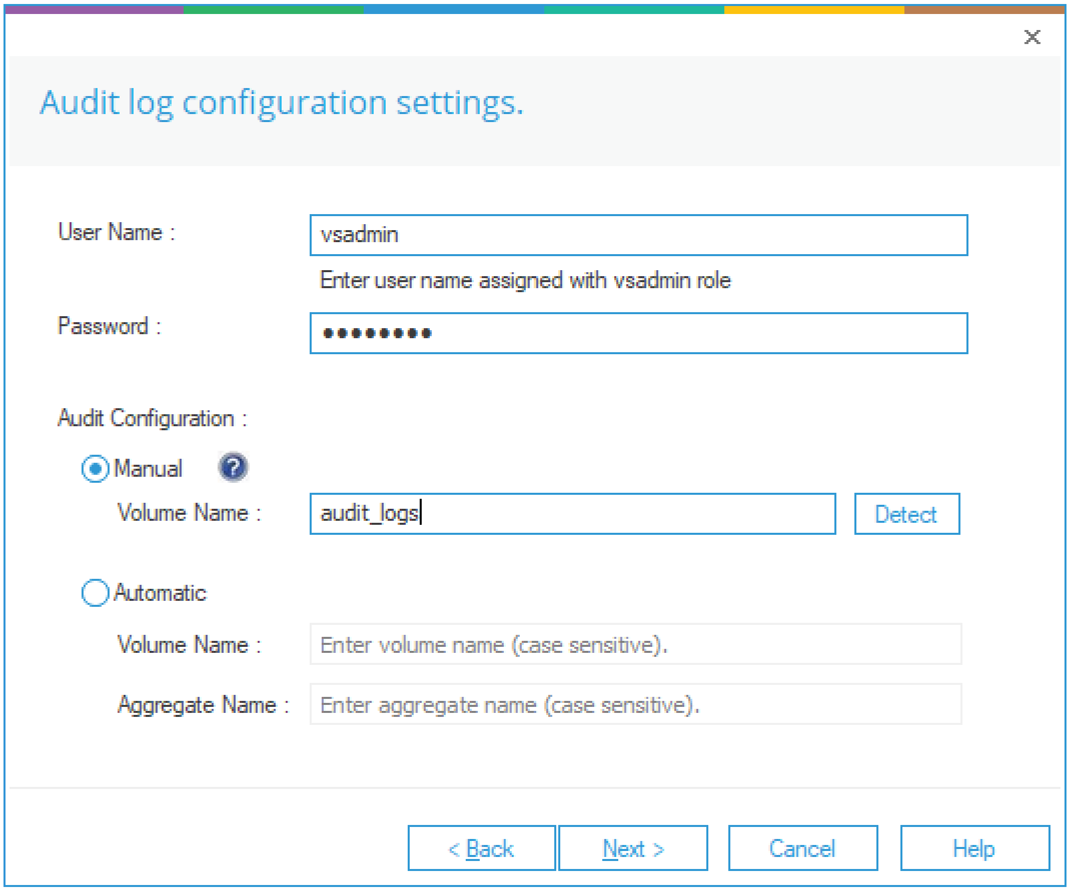
The following message box appears on the screen in this case:



Add File Server

Old audit log files found in the specified volume. These files will be moved to "Log\Backup"

Figure 24: Audit Log Message



Audit log configuration settings.

User Name : vsadmin

Enter user name assigned with vsadmin role

Password : ●●●●●●●●●

Audit Configuration :

● Manual

Volume Name : audit_logs

○ Automatic

Volume Name : Enter volume name (case sensitive).

Aggregate Name : Enter aggregate name (case sensitive).

Figure 23: Manual Auditing Selected

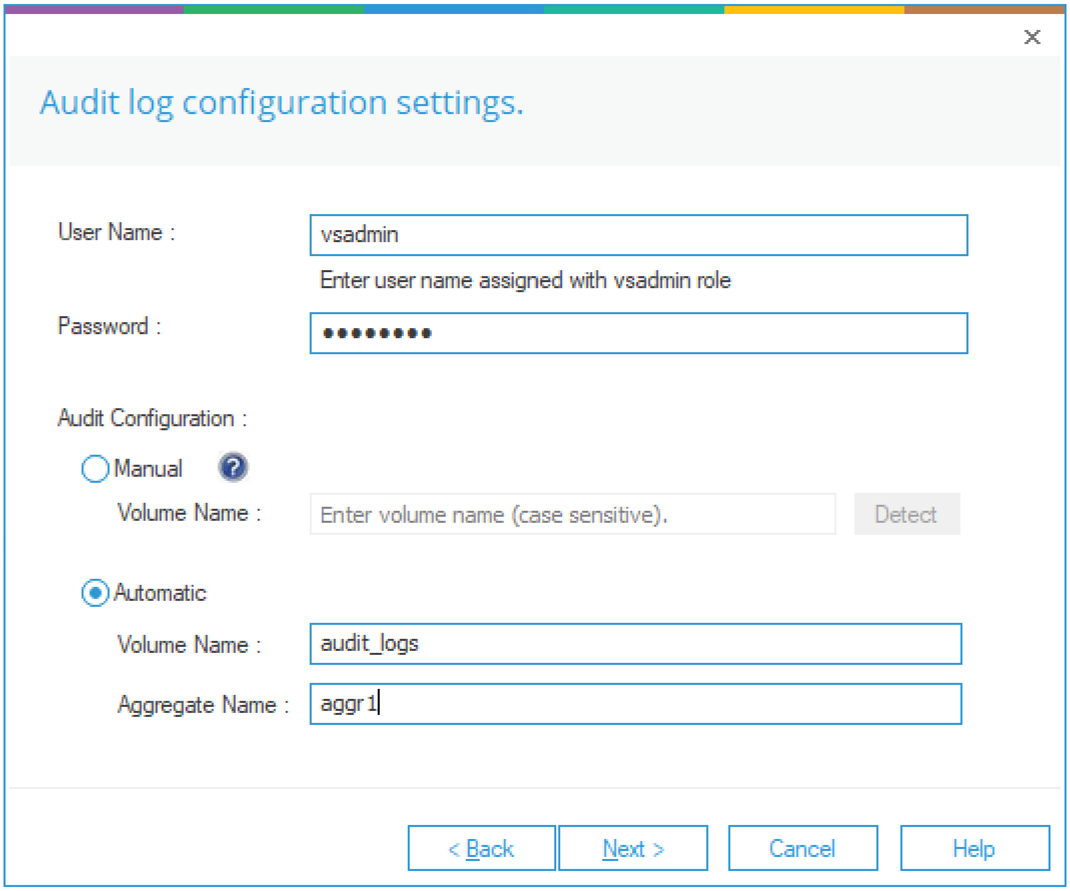
b. **Automatic Auditing:** Select this option if you have not already configured auditing. You need to provide the following inputs:

- Volume Name
- Aggregate Name

5. Click **Next** to proceed. The Solution enables auditing with the following settings:

- Log Volume Size :3 GB
- Log format: XML
- Log File Size: 1 MB

NOTE: The Lepide Data Security Platform needs at least 3 GB of free space at the selected aggregate to enable the auditing automatically.



Audit log configuration settings.

User Name : vsadmin

Enter user name assigned with vsadmin role

Password : ●●●●●●●●

Audit Configuration :

○ Manual

Volume Name : Enter volume name (case sensitive).

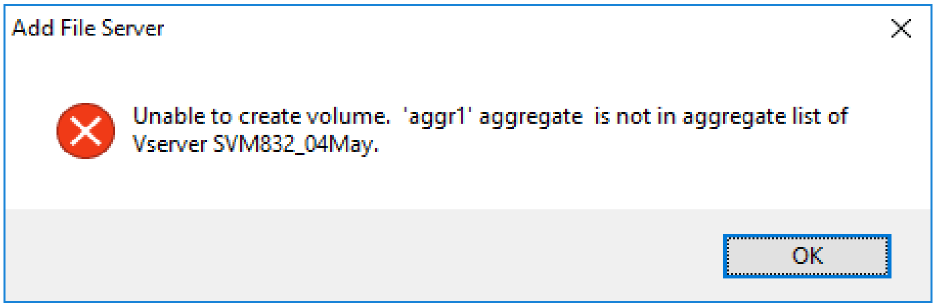
● Automatic

Volume Name : audit_logs

Aggregate Name : aggr1

Figure 25: Selected Automatic Auditing for NetApp

NOTE: The following error message may appear when you try to apply the Automatic Auditing option.



Add File Server

Unable to create volume. 'aggr1' aggregate is not in aggregate list of Vserver SVM832_04May.

Figure 26: Error Message while Enabling Automatic Auditing

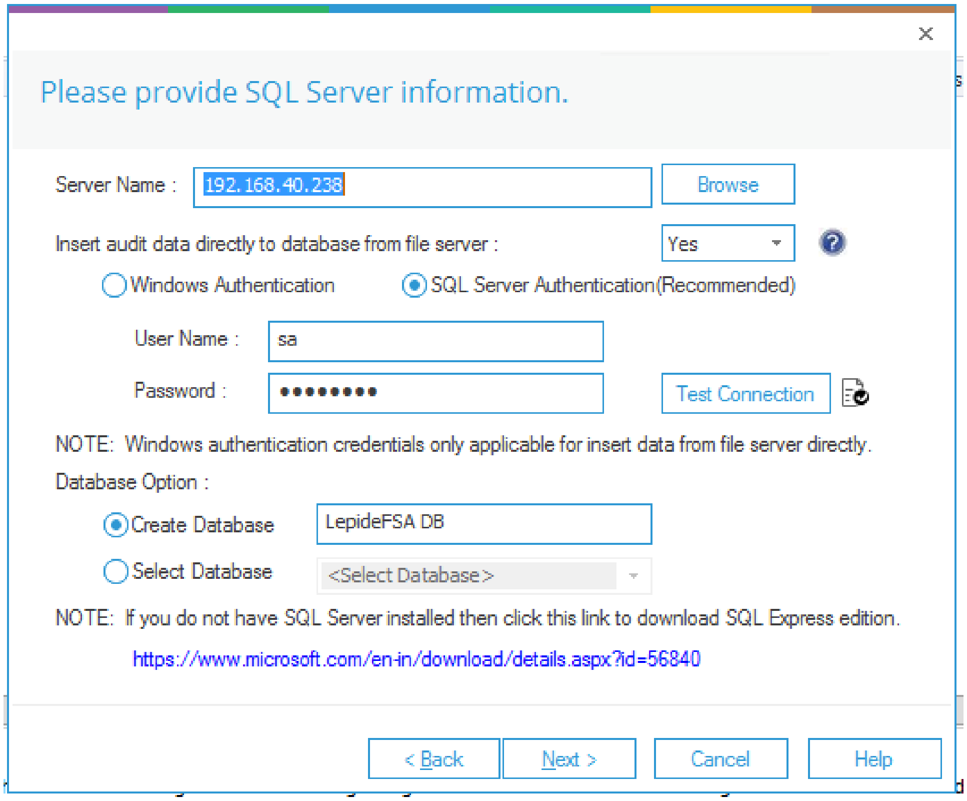
To solve this issue, add the aggregate in the Vserver's list by the following command:

```
vserver modify -vserver <server_name> -aggr-list <aggregate_value>
```

To see whether the aggregate has been added to the list, use the following command:

```
vserver show -fields aggr-list
```

6. Click **Next**
7. The **SQL Server Information** dialog box is displayed. Here, you need to provide the details of SQL Server to create a database for storing auditing logs.



Please provide SQL Server information.

Server Name : 192.168.40.238

Insert audit data directly to database from file server : Yes

○ Windows Authentication ● SQL Server Authentication(Recommended)

User Name : sa

Password : ●●●●●●●●●

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 27: SQL Server Details to Add NetApp Cluster Mode

8. Click the Server Name dropdown to select the desired SQL Server.

   There are two authentication options under it:

   a. **Windows Authentication**: This mode can be selected if SQL Server is installed on the same computer where the solution is installed.

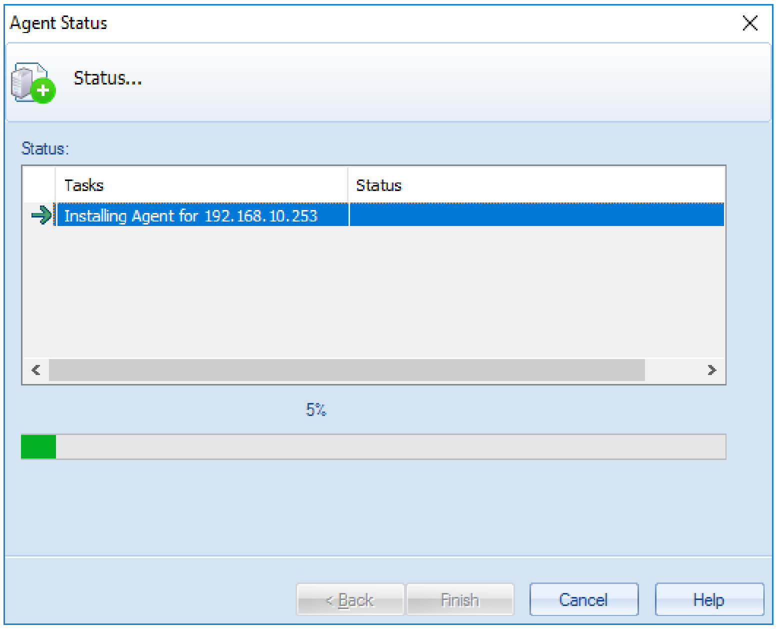
   b. **SQL Server Authentication**: Select this mode if SQL Server is installed on a remote or local computer. We recommend that this option is selected.

9. Provide the username and password of a SQL user, who has sufficient rights to create the database.

10. Enter a database name in the database name field to create a new database. You can also select an existing database created earlier by Lepide or another application.

11. Click **Next**

The installation of the agent starts:



Agent Status

Status...

Status:

	Tasks	Status
→	Installing Agent for 192.168.10.253	

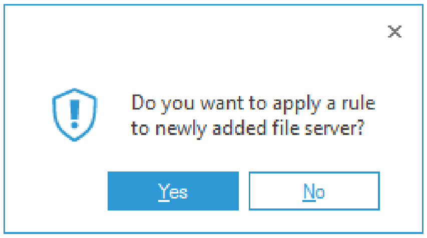
5%

Figure 28: Install Agent on NetApp Cluster Mode

12. Click **Finish** to complete the process.

7.2Steps after Adding a File Server Component

After you have added a Windows File System or NetApp Filer component, the application asks you if you want to create a new rule for File Server.



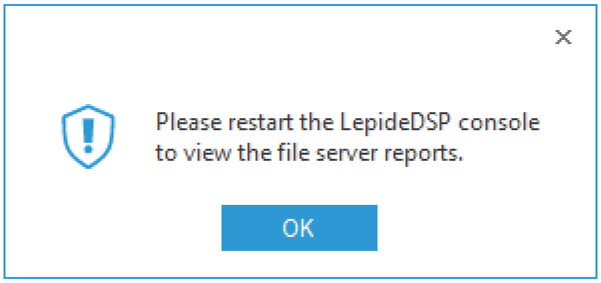
Do you want to apply a rule to newly added file server?

Figure 29: Starting Add Rule to the File Server Wizard

- Click **Yes** to add a new rule.

NOTE: You need an Audit Rule to start monitoring of the newly added File Server. If you want to skip the step of creating a rule, then click No. However, the audit reports will not be generated until you create an Audit Rule and update the agent. It is necessary to Update Agent if you are creating or modifying an Audit Rule.

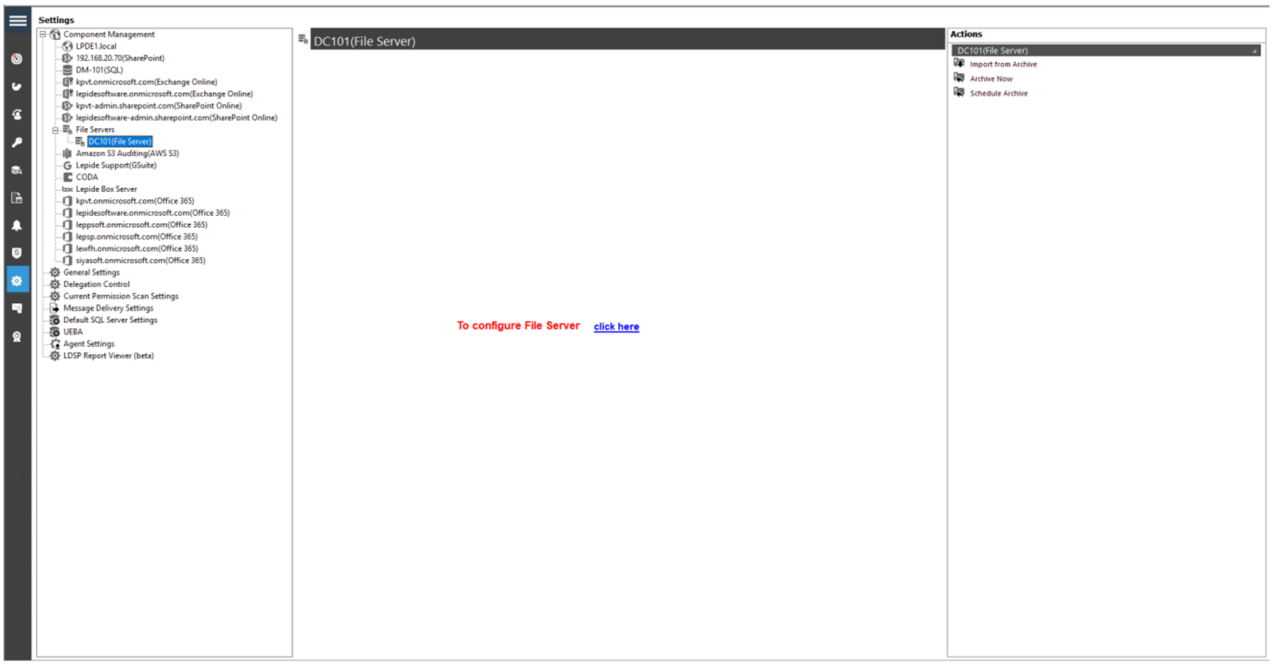
- After the Audit Rule has been created, or you clicked **No** in above step, a dialog box appears on the screen:



Please restart the LepideDSP console to view the file server reports.

Figure 30: Message to Restart the Software

- Click **OK**. then close the File Server Auditor console and restart the software.
- After the restart, the software displays the **File Server** in the Radar Tab and a node under **Component Management** in the Settings Tab.
- You can click **File Server** node under **Component Management** to manage the added File Server.

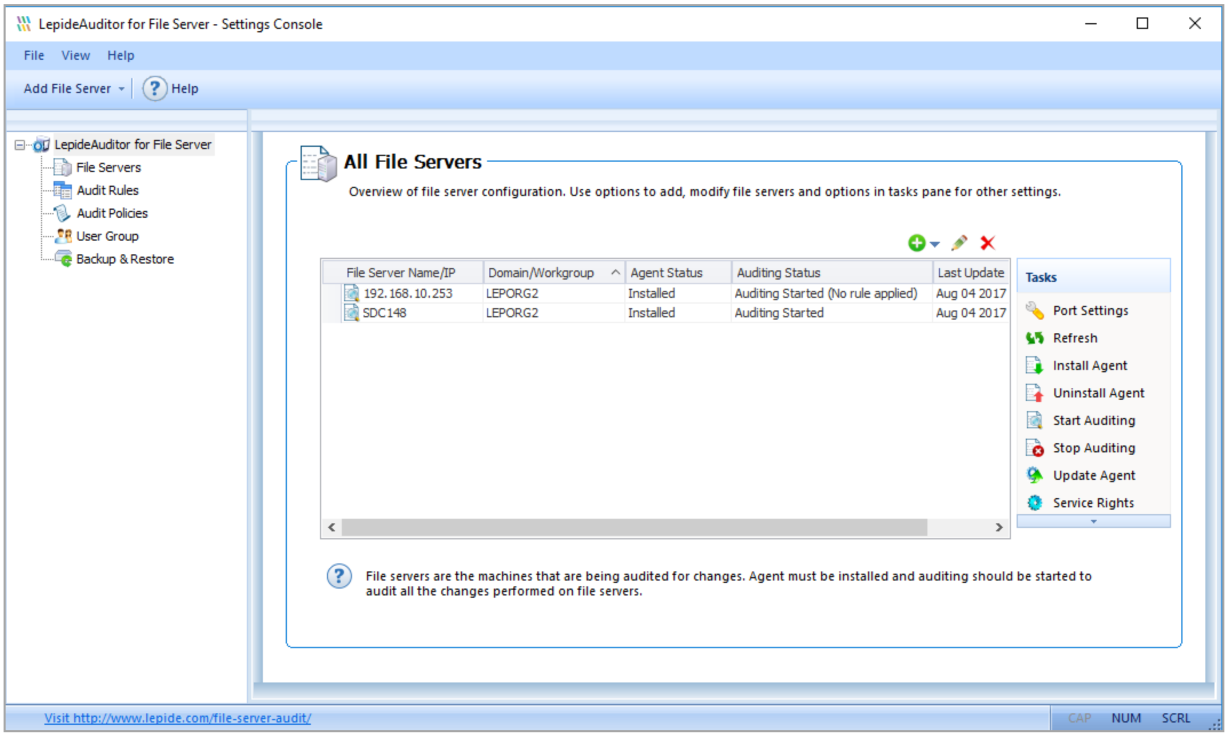


Settings
Component Management
LPDE1.local
192.168.20.70(SharePoint)
DM-101(SQL)
kpvt.onmicrosoft.com(Exchange Online)
lepidesoftware.onmicrosoft.com(Exchange Online)
kpvt-admin.sharepoint.com(SharePoint Online)
lepidesoftware-admin.sharepoint.com(SharePoint Online)
File Servers
DC101(File Server)
Amazon S3 Auditing(AWS S3)
Lepide Support(GSuite)
CODA
Lepide Box Server
kpvt.onmicrosoft.com(Office 365)
lepidesoftware.onmicrosoft.com(Office 365)
leppsoft.onmicrosoft.com(Office 365)
lepsp.onmicrosoft.com(Office 365)
lewfh.onmicrosoft.com(Office 365)
siyasoft.onmicrosoft.com(Office 365)
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Report Viewer (beta)
DC101(File Server)
Actions
DC101(File Server)
Import from Archive
Archive Now
Schedule Archive

To configure File Server click here

Figure 31: File Server Management

- Click the **Click Here** link to access the File Server Auditor console



All File Servers

Overview of file server configuration. Use options to add, modify file servers and options in tasks pane for other settings.

File Server Name/IP	Domain/Workgroup	Agent Status	Auditing Status	Last Update
192.168.10.253	LEPORG2	Installed	Auditing Started (No rule applied)	Aug 04 2017
SDC148	LEPORG2	Installed	Auditing Started	Aug 04 2017

File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 32: Displaying the Added File Servers

8 Adding Multiple File Servers

You can now add multiple file servers to the solution in one step. Please follow the instructions below:

8.1 Adding Multiple Windows File Servers

After you have installed the software and configured Lepide service to run with administrative credentials, you can add multiple File Servers for auditing in one step.

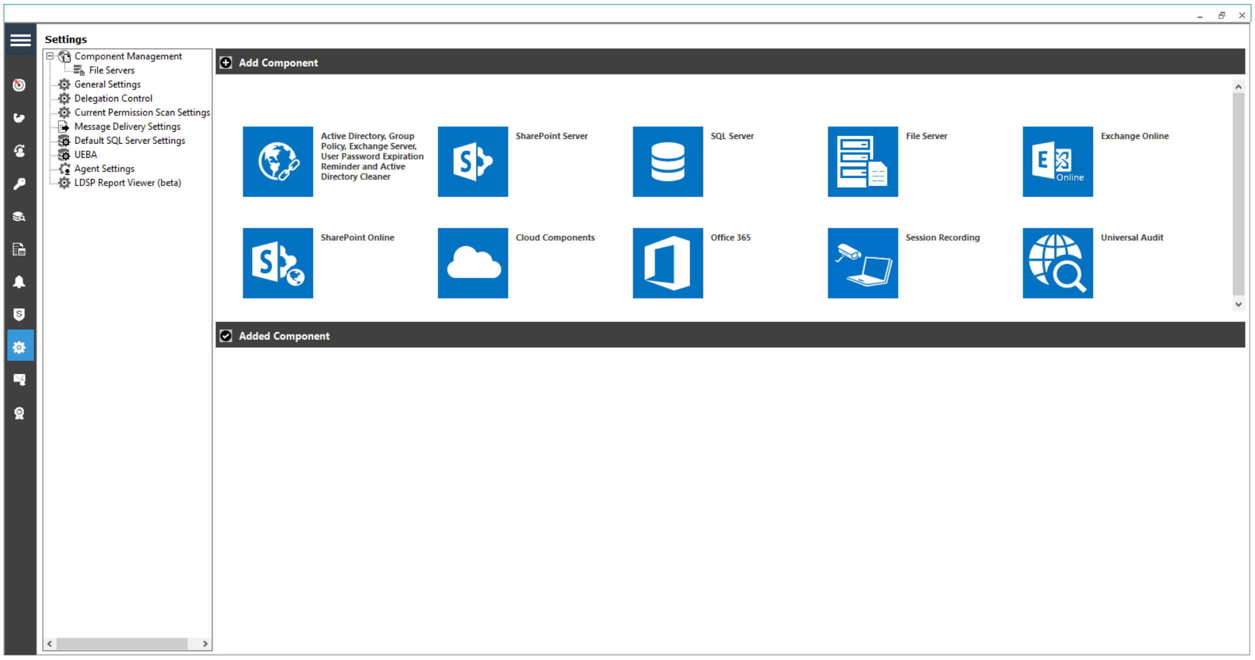
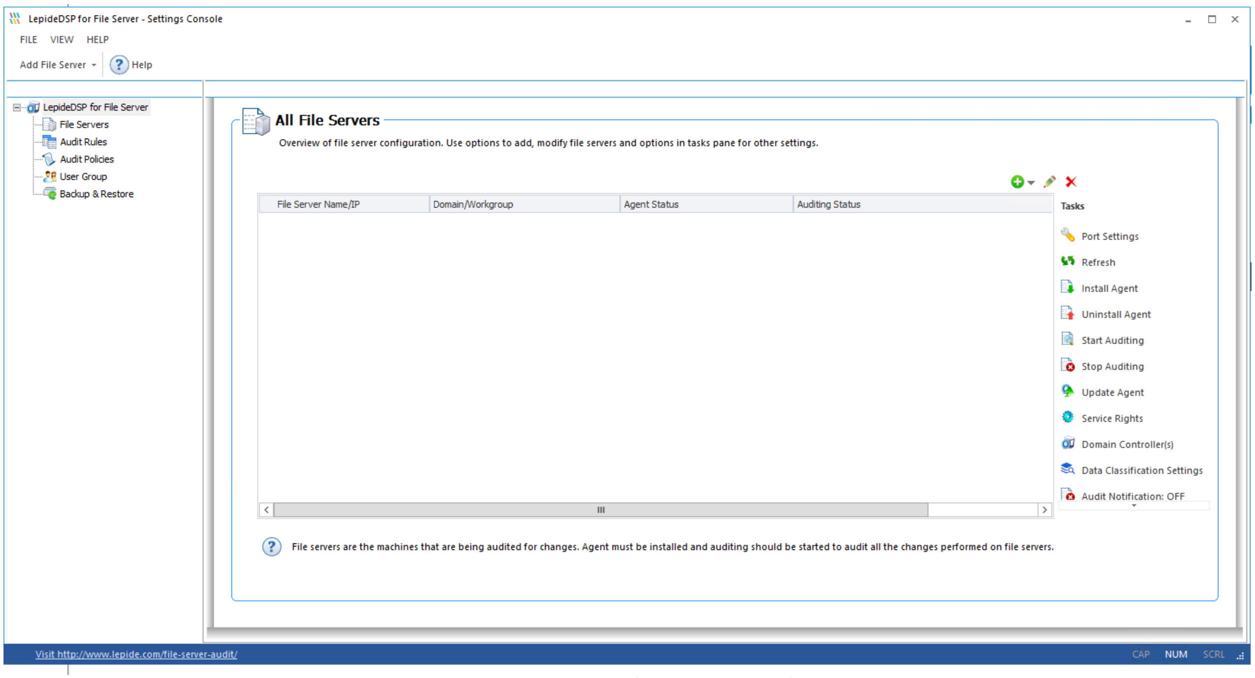


Figure 33: Component Management Window

From the Component Management window, under the Add Component section, click on the File Server icon to add this component to the solution.

The Settings Console dialog box is displayed:



Overview of file server configuration. Use options to add, modify file servers and options in tasks pane for other settings.

File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 34: File Server Console

Here, you can click **Add File Server** icon on the toolbar to add either of the following file servers:

- Windows File Server
- NetApp Filer

20. Click the **Add File Server** icon, select **Multiple** then select **Windows**.

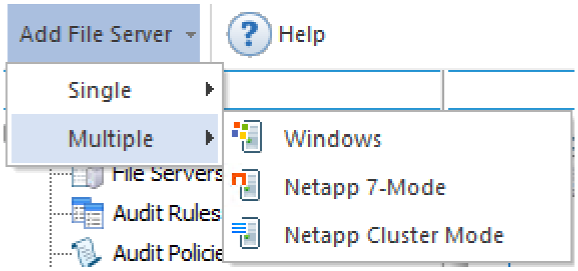
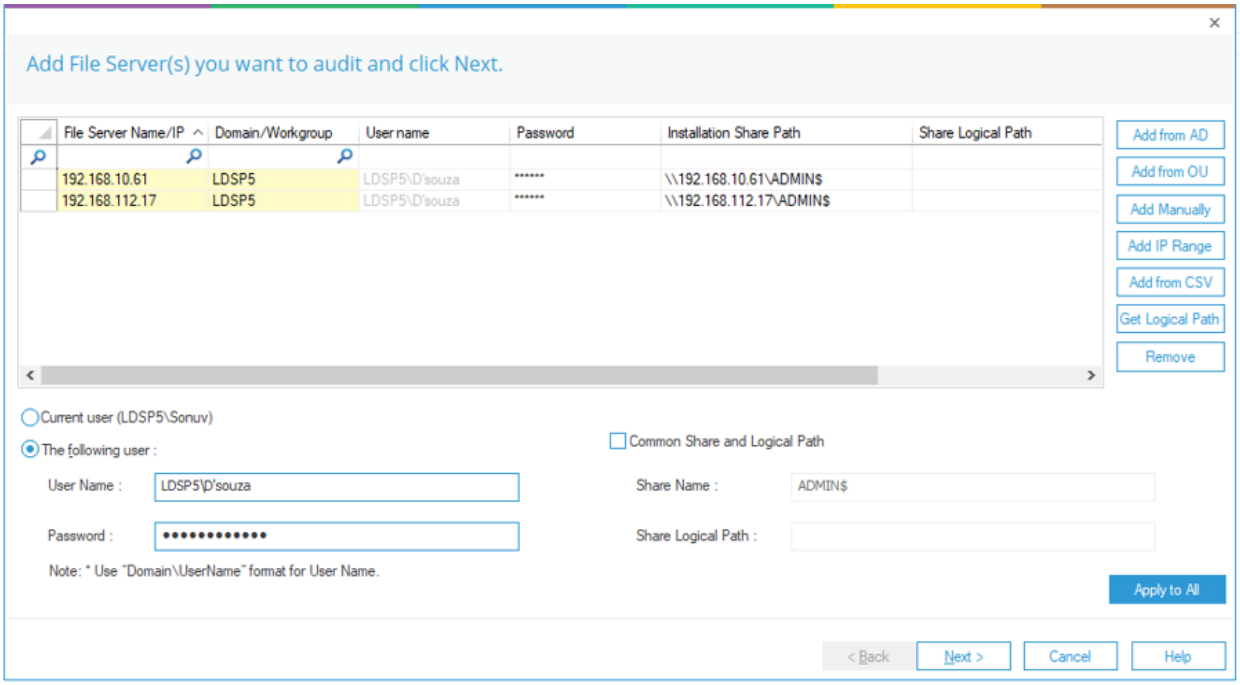


Figure 35: Option to add Multiple File Servers

21. The **Add File Servers** wizard starts:



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
192.168.10.61	LDSP5	LDSP5\D'souza	******	\\192.168.10.61\ADMIN$	
192.168.112.17	LDSP5	LDSP5\D'souza	******	\\192.168.112.17\ADMIN$	

○ Current user (LDSP5\Sonuv)

● The following user :

User Name : LDSP5\D'souza

Password : •••••••••••••

Note: * Use "Domain\UserName" format for User Name.

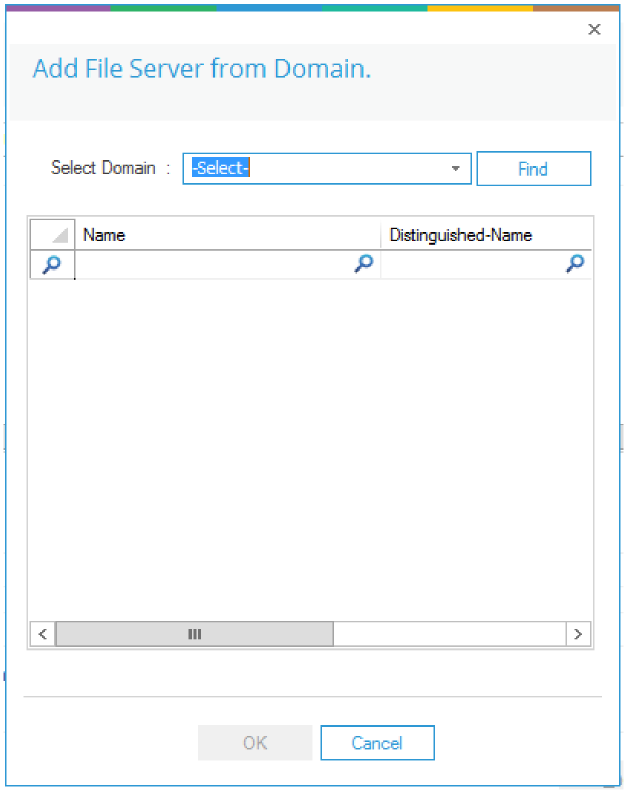
□ Common Share and Logical Path

Share Name : ADMIN$

Share Logical Path :

Figure 36: Add File Server Wizard

22. **Add From AD:** Click on **Add from AD** button to scan the domain network and select the required file servers.


Add File Server from Domain.

Select Domain : -Select-

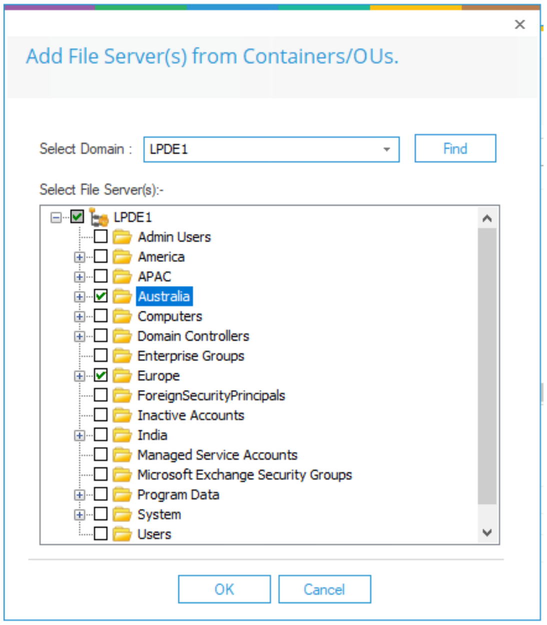
Figure 37: Add File Server from Domain

a) You can select the **Domain name** in the drop-down menu or type it in the box provided.

b) Click the **Find** button to list its computers in the blank area.

c) Select the computers you want to audit and click **OK**.
It takes you back to the previous wizard, which now displays the selected File Servers.

23. **Add from OU:** Click on the **Add from OU** button if you want to select the file servers from specific OUs.



Add File Server(s) from Containers/OUs.

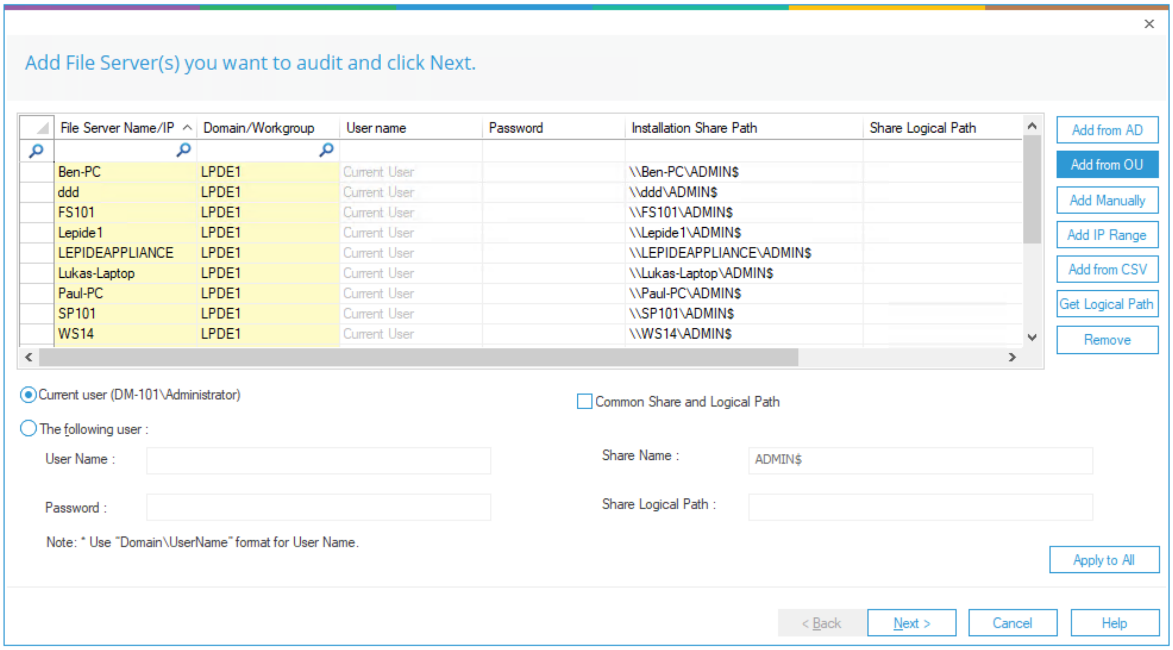
Select Domain : LPDE1

Select File Server(s):-

- ☑ LPDE1
  - □ Admin Users
  - □ America
  - □ APAC
  - ☑ Australia
  - □ Computers
  - □ Domain Controllers
  - □ Enterprise Groups
  - ☑ Europe
  - □ ForeignSecurityPrincipals
  - □ Inactive Accounts
  - □ India
  - □ Managed Service Accounts
  - □ Microsoft Exchange Security Groups
  - □ Program Data
  - □ System
  - □ Users

Figure 38: Add File Server from OU

a) Select the File Servers to be added and click **OK**. The following dialog box is displayed:



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
Ben-PC	LPDE1	Current User		\\Ben-PC\ADMIN$	
ddd	LPDE1	Current User		\\ddd\ADMIN$	
FS101	LPDE1	Current User		\\FS101\ADMIN$	
Lepide1	LPDE1	Current User		\\Lepide1\ADMIN$	
LEPIDEAPPLIANCE	LPDE1	Current User		\\LEPIDEAPPLIANCE\ADMIN$	
Lukas-Laptop	LPDE1	Current User		\\Lukas-Laptop\ADMIN$	
Paul-PC	LPDE1	Current User		\\Paul-PC\ADMIN$	
SP101	LPDE1	Current User		\\SP101\ADMIN$	
WS14	LPDE1	Current User		\\WS14\ADMIN$	

● Current user (DM-101\Administrator)

○ The following user :

User Name :

Password :

Note: * Use "Domain\UserName" format for User Name.

□ Common Share and Logical Path

Share Name : ADMIN$

Share Logical Path :

Figure 39: Selected File Servers

b) Here you can specify the following:

Current user or **The following user**

If you select **The following user**, you will need to specify the User Name in the format Domain\UserName and the Password

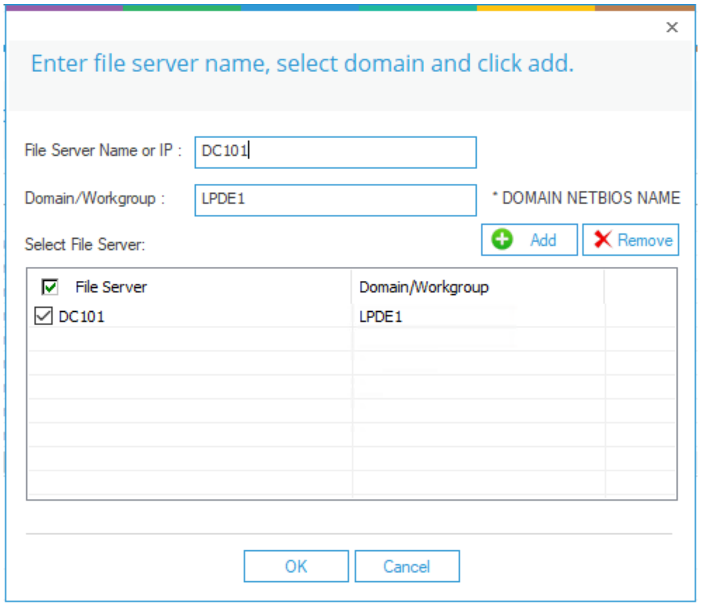
Check the Common Share and Logical Path box if you want to use this

Specify the share name – for example Admin$ and the Share Logical Path which will be C:\Windows for admin$

c) Click **Next** to continue

It takes you back to the previous wizard, which now displays the selected File Servers.

24. **Add Manually:** Click on the **Add Manually** button to add the file server manually into the solution by specifying its name and domain name.



Enter file server name, select domain and click add.

File Server Name or IP : DC101

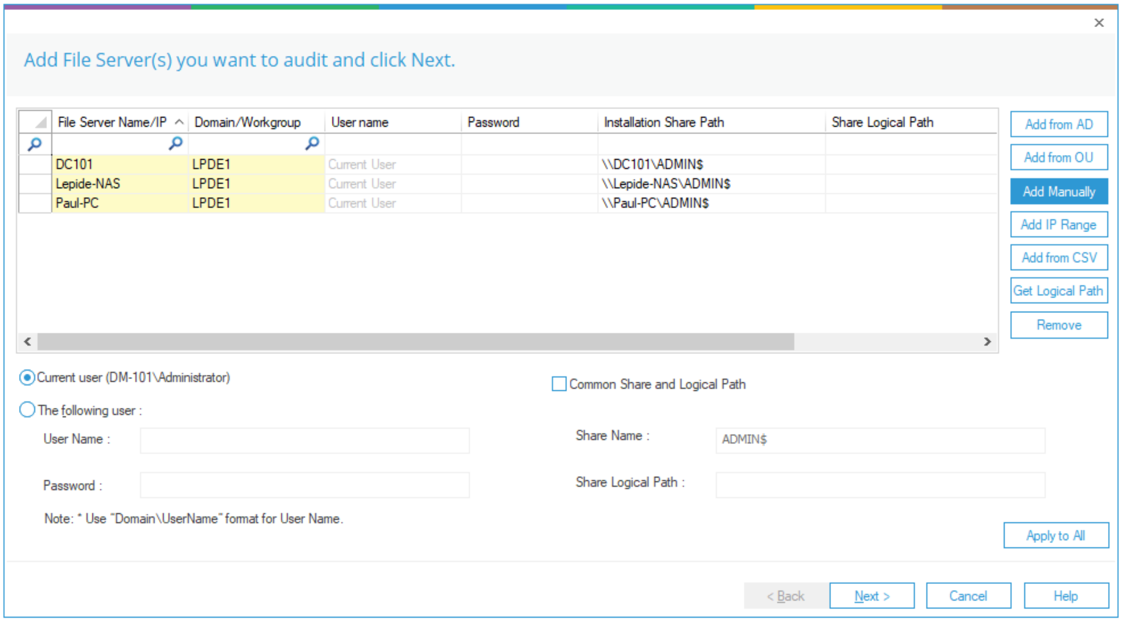
Domain/Workgroup : LPDE1 * DOMAIN NETBIOS NAME

Select File Server:

☑ File Server	Domain/Workgroup
☑ DC101	LPDE1

Figure 41: Add File Server Manually

a) Select the File Servers to be added and click **OK**. The following dialog box is displayed:



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
DC101	LPDE1	Current User		\\DC101\ADMIN$	
Lepide-NAS	LPDE1	Current User		\\Lepide-NAS\ADMIN$	
Paul-PC	LPDE1	Current User		\\Paul-PC\ADMIN$	

● Current user (DM-101\Administrator)

○ The following user :

User Name :

Password :

Note: * Use "Domain\UserName" format for User Name.

□ Common Share and Logical Path

Share Name : ADMIN$

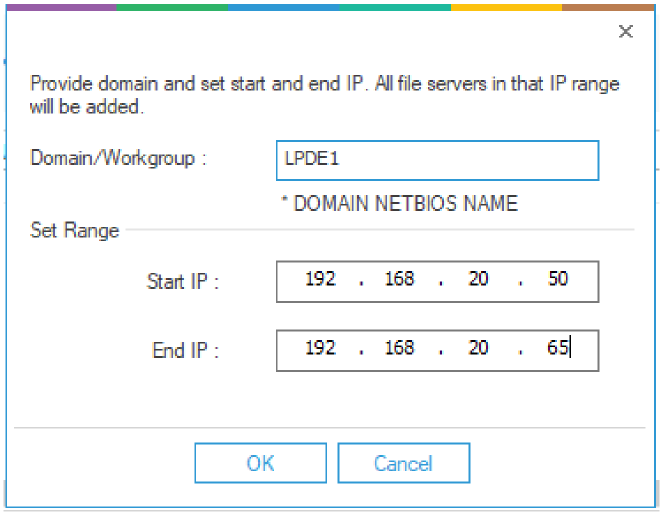
Share Logical Path :

Figure 40: File Servers added Manually

b) Specify the options you require.

c) Click **Next** to continue
It takes you back to the previous wizard, which now displays the selected File Servers.

25. **Add IP Range:** Click on **Add IP Range** button to scan the domain network and select the required file servers.



Provide domain and set start and end IP. All file servers in that IP range will be added.

Domain/Workgroup : LPDE1

* DOMAIN NETBIOS NAME

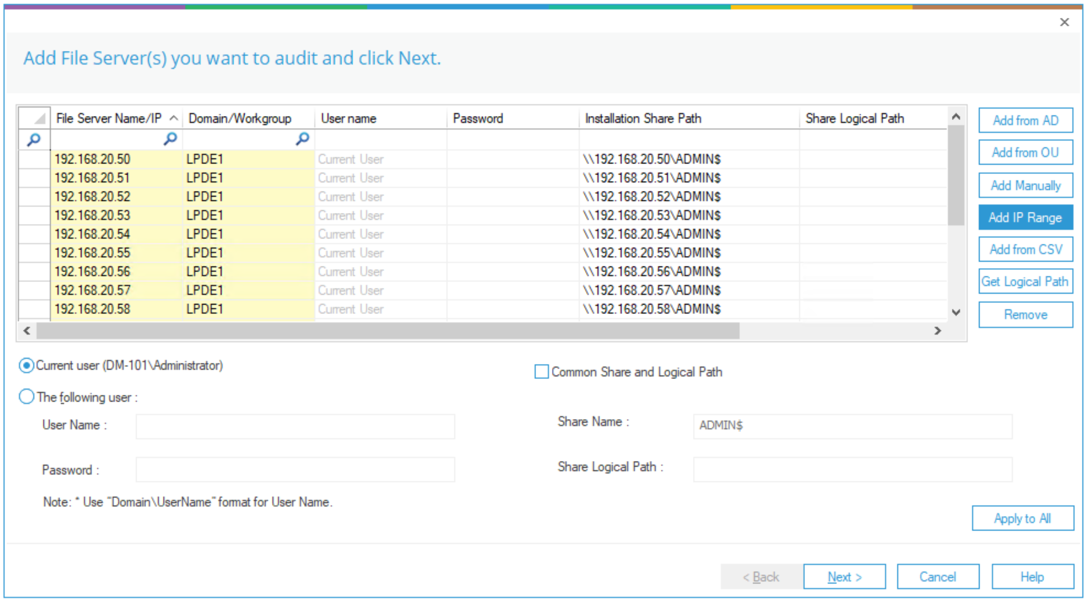
Set Range

Start IP : 192 . 168 . 20 . 50

End IP : 192 . 168 . 20 . 65

Figure 42: Add File Server using IP Range

a) Type the **Domain/Workgroup** name and the **IP Start and Stop Addresses**. Click **OK.** The following dialog box is displayed:



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
192.168.20.50	LPDE1	Current User		\\192.168.20.50\ADMIN$	
192.168.20.51	LPDE1	Current User		\\192.168.20.51\ADMIN$	
192.168.20.52	LPDE1	Current User		\\192.168.20.52\ADMIN$	
192.168.20.53	LPDE1	Current User		\\192.168.20.53\ADMIN$	
192.168.20.54	LPDE1	Current User		\\192.168.20.54\ADMIN$	
192.168.20.55	LPDE1	Current User		\\192.168.20.55\ADMIN$	
192.168.20.56	LPDE1	Current User		\\192.168.20.56\ADMIN$	
192.168.20.57	LPDE1	Current User		\\192.168.20.57\ADMIN$	
192.168.20.58	LPDE1	Current User		\\192.168.20.58\ADMIN$	

● Current user (DM-101\Administrator)

○ The following user :

User Name :

Password :

Note: * Use "Domain\UserName" format for User Name.

□ Common Share and Logical Path

Share Name : ADMIN$

Share Logical Path :

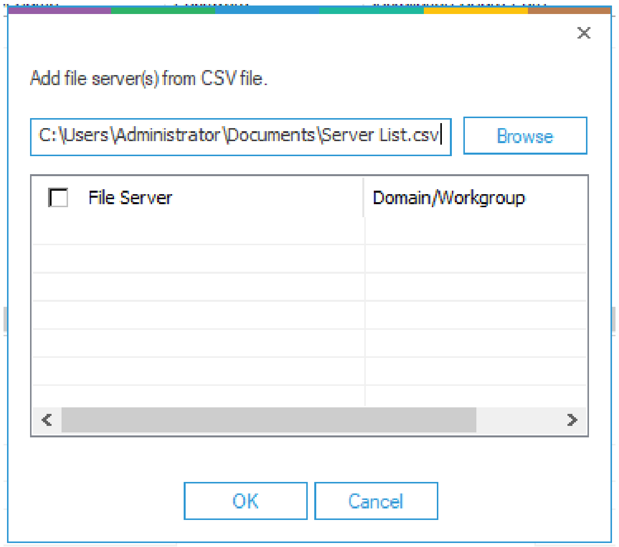
Figure 43: File Servers added using IP Range

b) Specify the options you require.

c) Click **Next** to continue

It takes you back to the previous wizard, which now displays the selected File Servers.

26. **Add From CSV:** Click on **Add from CSV** button to scan the domain network and select the required file servers.

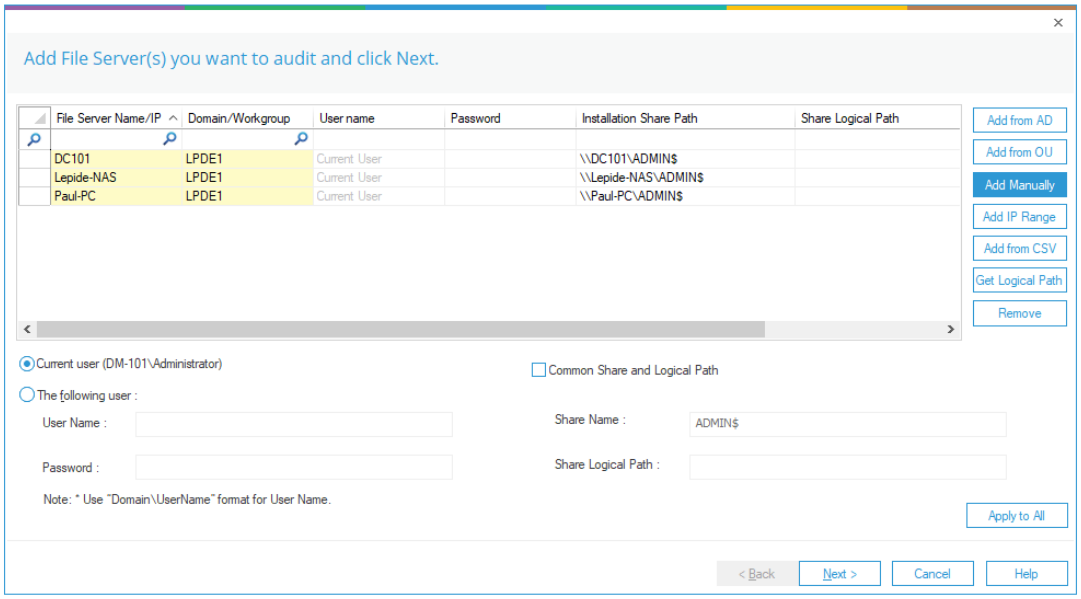


Add file server(s) from CSV file.

C:\Users\Administrator\Documents\Server List.csv

Figure 44: Add File Server using CSV File

a) Click Browse to select the CSV file required
Click **OK.** The following dialog box is displayed:



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
DC101	LPDE1	Current User		\\DC101\ADMIN$	
Lepide-NAS	LPDE1	Current User		\\Lepide-NAS\ADMIN$	
Paul-PC	LPDE1	Current User		\\Paul-PC\ADMIN$	

● Current user (DM-101\Administrator)

○ The following user :

User Name :

Password :

Note: * Use "Domain\UserName" format for User Name.

□ Common Share and Logical Path

Share Name : ADMIN$

Share Logical Path :

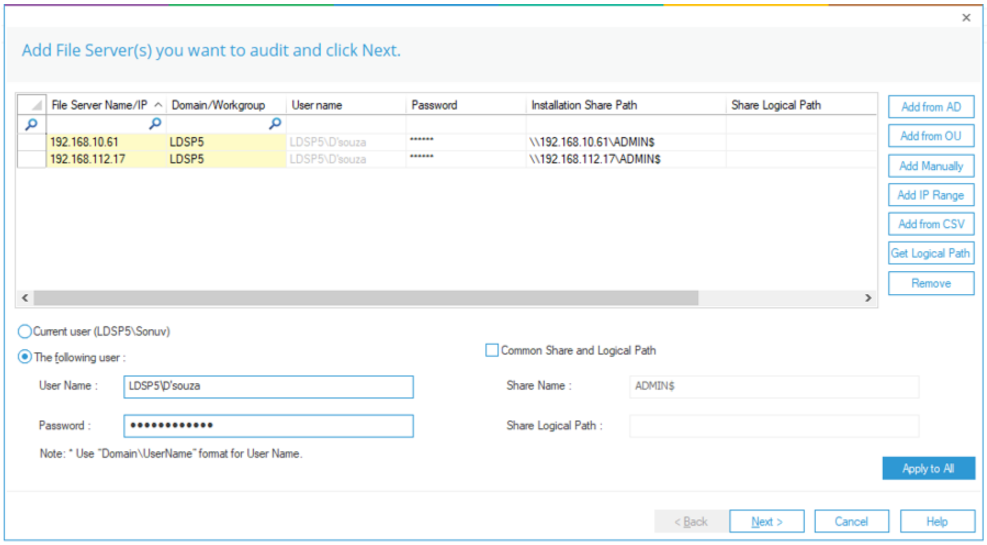
Figure 45: Add File Server using CSV File

b) Specify the options you require.

c) Click **Next** to continue

It takes you back to the previous wizard, which now displays the selected File Servers.

27. Select the user with which you want to add the File Server If you are logged in as a user that has the above rights, then you can select **Current User**.
28. If the logged in user does not have the required rights, then you have to select **The following user** option and provide the login credentials of a user who has the required rights
29. You can use the default Admin$ location for the agent if the Service Account has admin rights on the File Server. If not, you can create any shared folder on the File Server and specify its path in the **Share Path** Option.
30. Click **Apply to All** to apply these settings to all selected file servers.



Add File Server(s) you want to audit and click Next.

File Server Name/IP	Domain/Workgroup	User name	Password	Installation Share Path	Share Logical Path
192.168.10.61	LDSP5	LDSP5\D'souza	******	\\192.168.10.61\ADMIN$	
192.168.112.17	LDSP5	LDSP5\D'souza	******	\\192.168.112.17\ADMIN$	

○ Current user (LDSP5\Sonuv)

● The following user :

User Name : LDSP5\D'souza

Password : ••••••••••••

Note: * Use "Domain\UserName" format for User Name.

□ Common Share and Logical Path

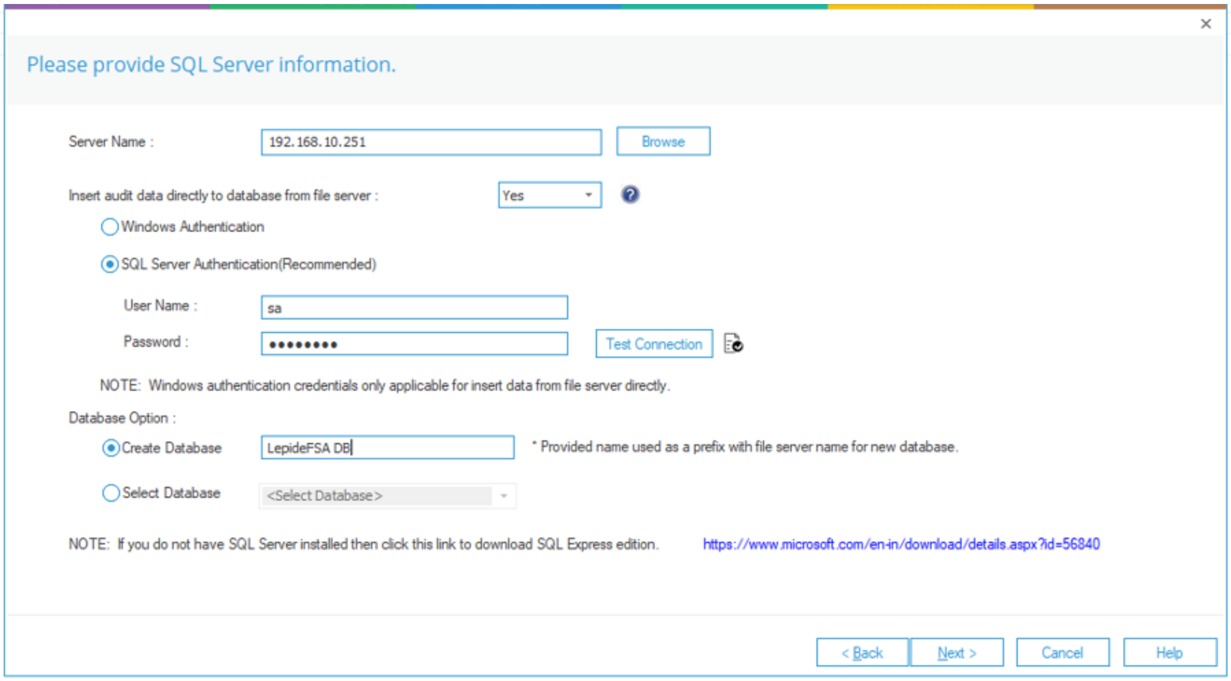
Share Name : ADMIN$

Share Logical Path :

Figure 46: Enter User Name Details

31. After entering the details, click **Next**.

The next step is to provide the SQL Server details:



Please provide SQL Server information.

Server Name : 192.168.10.251

Insert audit data directly to database from file server : Yes

○ Windows Authentication

● SQL Server Authentication(Recommended)

User Name : sa

Password : •••••••••

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB * Provided name used as a prefix with file server name for new database.

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition. https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 47: SQL Server Details

32. Type the **Server Name** or click **Browse** to select the desired SQL Server.

33. There are two authentication options:

    a) **Windows Authentication:** In this method, you can use any domain user windows account which have at least **dbcreator** role on the SQL server.

    b) **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote machine or the local machine. We recommend that this option is selected.

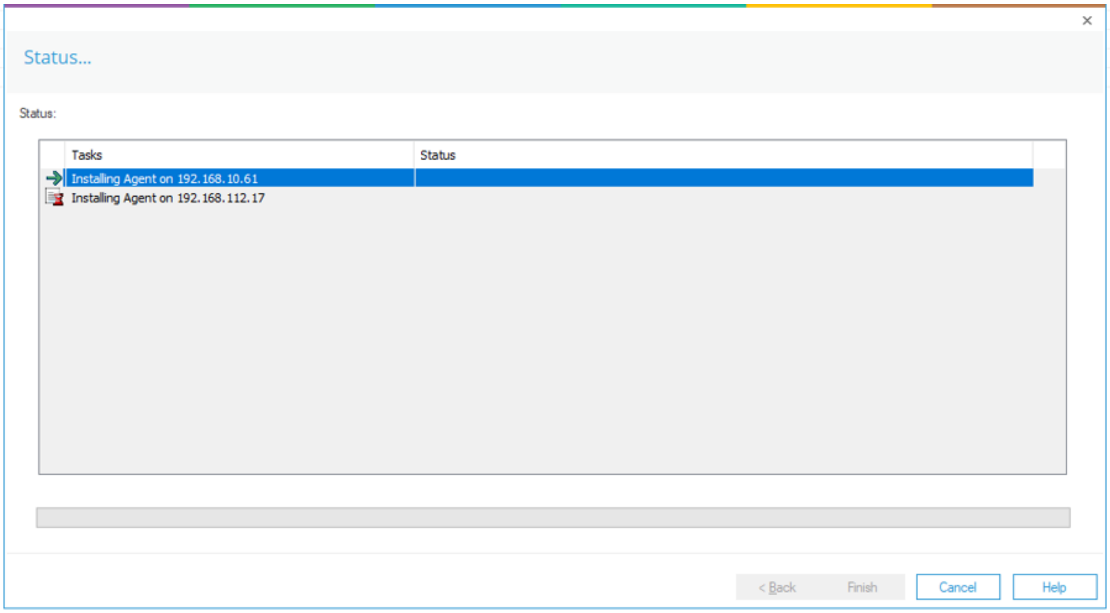
    Provide the username and password of an SQL User, which has sufficient rights to create a new database.

34. Please select Insert Audit Data Directly to Database from File Server as **YES,** only if the SQL connection from the File Server to the SQL Server is open. Please select **NO** if the connection is not open and the insertion will happen from the Application Server then.

35. Enter a database name in the database name field to create a new database. You can also select an existing database created by Lepide or another application.

36. Click **Next** to start installing the auditing agent for Windows File Servers.

    The following dialog box is displayed showing the progress of agent installation.



Status...

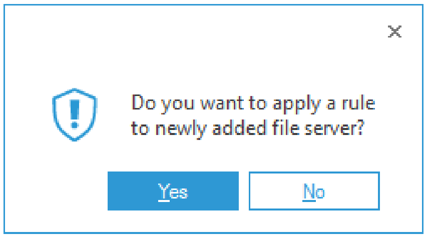
Status:

Tasks	Status
Installing Agent on 192.168.10.61	
Installing Agent on 192.168.112.17	

Figure 49: Auditing Agent is Installed

37. Click **Finish** once the agents are installed to complete the process.

A dialog box is displayed asking whether you want to apply a rule to the newly added file server:



Do you want to apply a rule to newly added file server?

Figure 50: Option to Create a Rule

Audit Rule Management is explained in Section 9 of this document. Please refer to this for information on creating a rule.

8.2 Adding Multiple NetApp 7 Mode File Servers

After you have installed the software and configured Lepide service to run with administrative credentials, you can add multiple File Servers for auditing in one step.

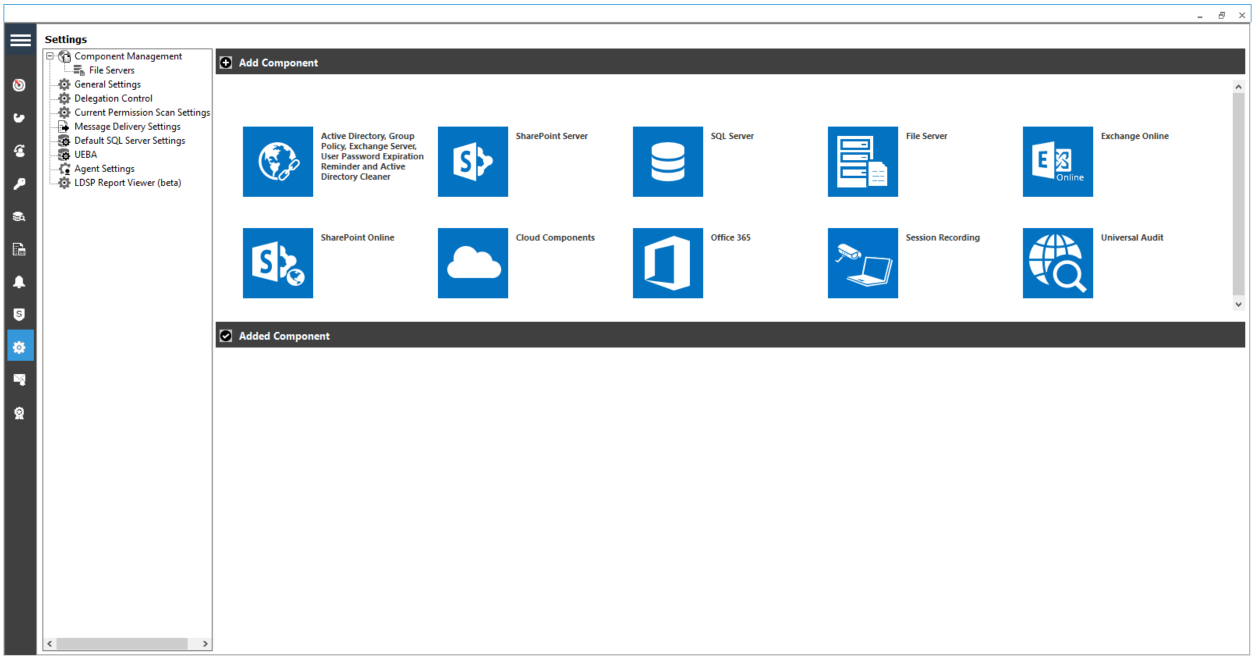
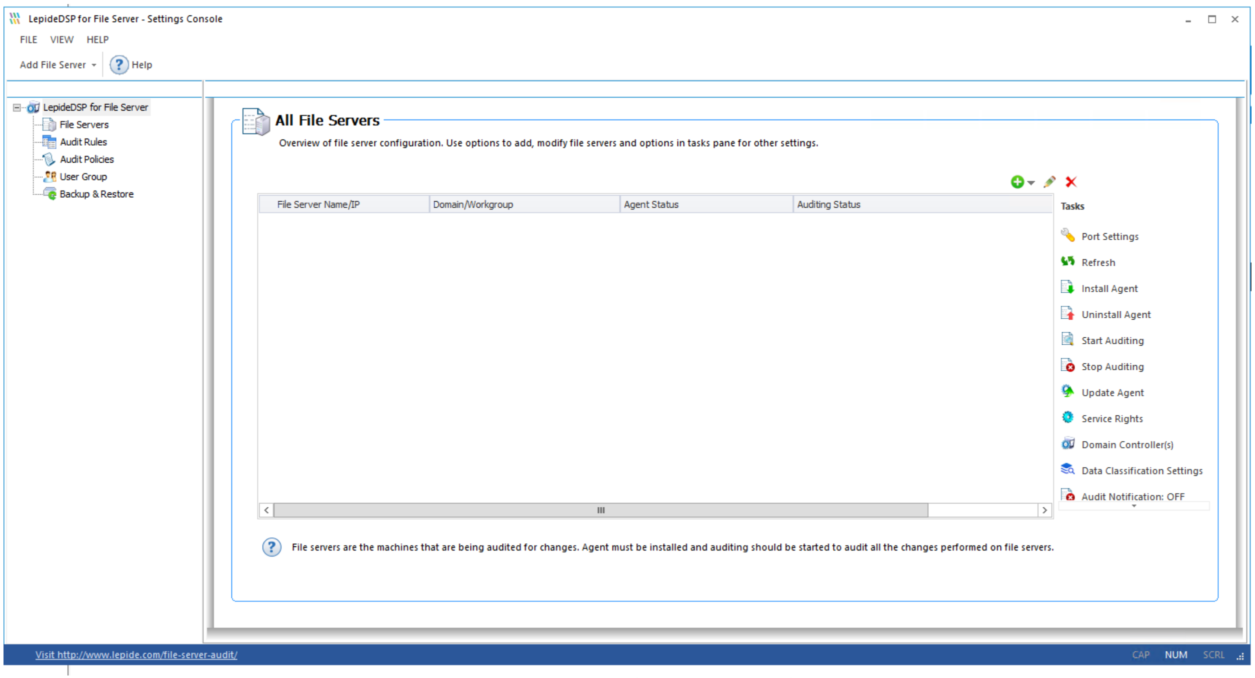


Figure 51: Component Management Window

From the Component Management window, under the Add Component section, click on the File Server icon to add this component to the solution.

The Settings Console dialog box is displayed:



Overview of file server configuration. Use options to add, modify file servers and options in tasks pane for other settings.

File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 52: File Server Console

1. Click the **Add File Server** icon, ⊕ ▾ select **Multiple** then select **NetApp 7-Mode**.

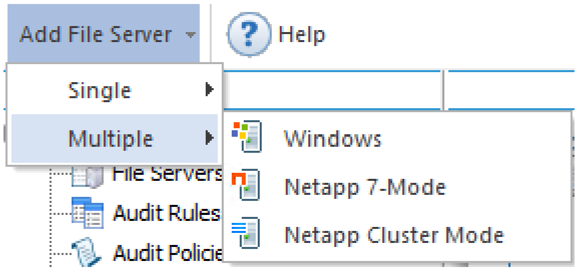
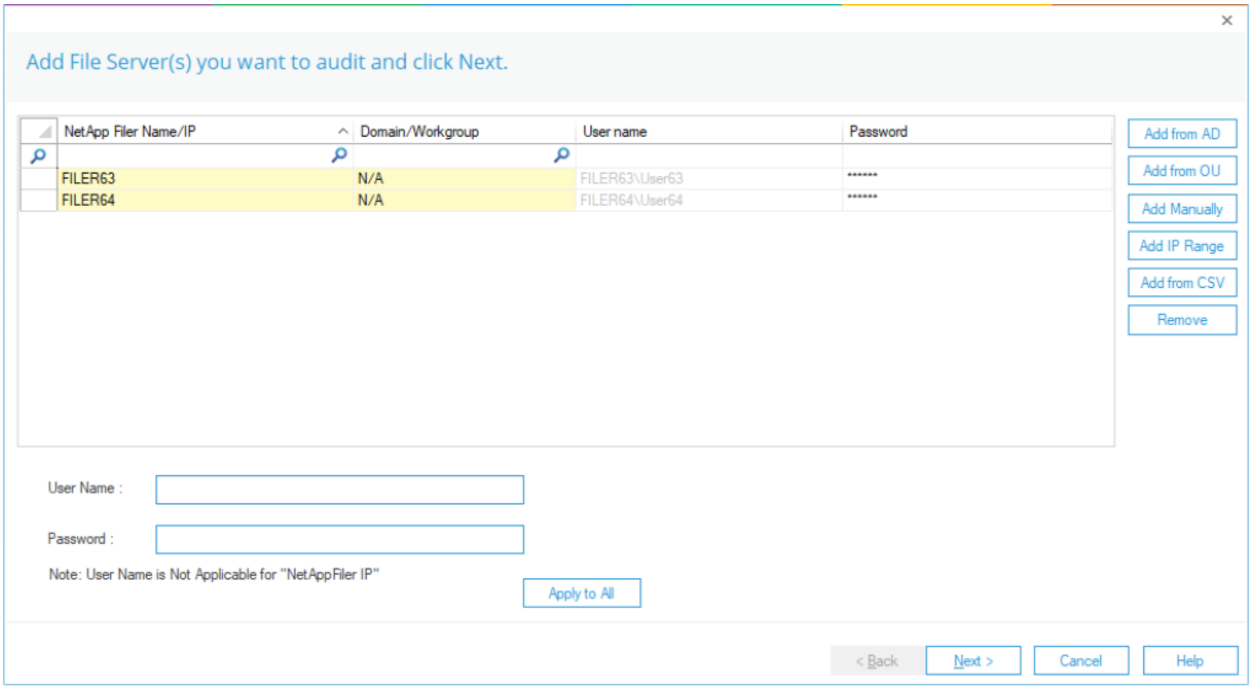


Figure 53: Option to add Multiple File Servers

2. The **Add File Servers** wizard starts:



Add File Server(s) you want to audit and click Next.

NetApp Filer Name/IP	Domain/Workgroup	User name	Password
FILER63	N/A	FILER63\User63	******
FILER64	N/A	FILER64\User64	******

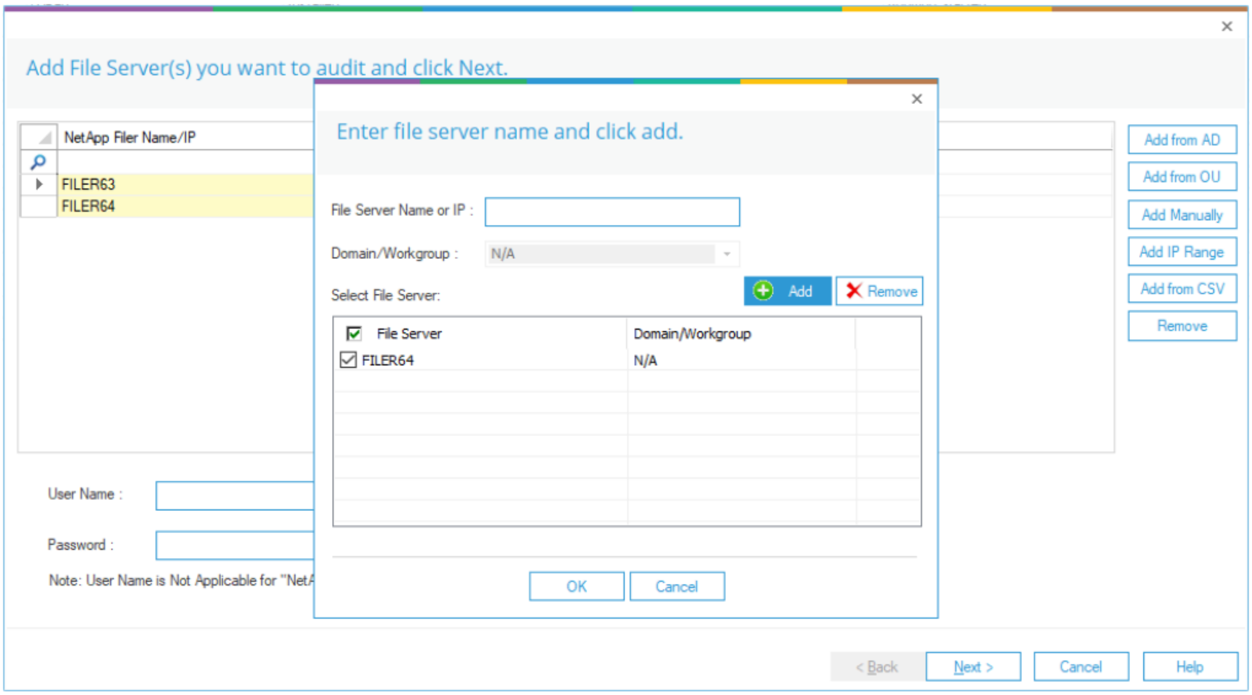
User Name :

Password :

Note: User Name is Not Applicable for "NetAppFiler IP"

Figure 54: Add File Server Wizard

3. From this screen, you can add the file servers. Click the button to select where the file server should be added from. The options are: Add from AD, Add from OU, Add Manually, Add IP Range, Add from CSV..



Add File Server(s) you want to audit and click Next.

NetApp Filer Name/IP
FILER63
FILER64

User Name :

Password :

Note: User Name is Not Applicable for "NetA

Enter file server name and click add.

File Server Name or IP :

Domain/Workgroup : N/A

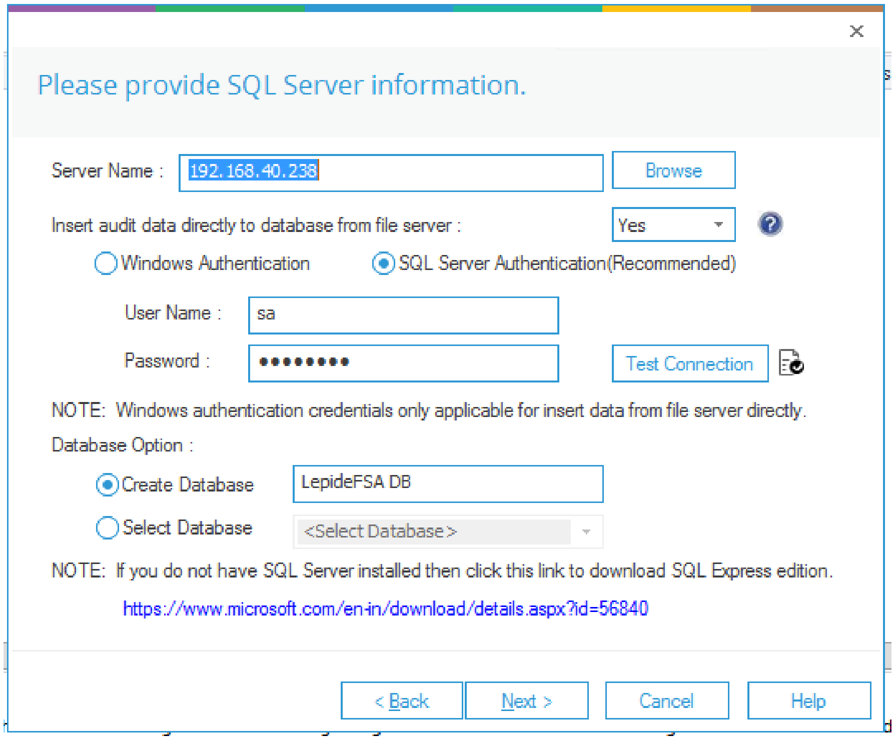
Select File Server:

☑ File Server	Domain/Workgroup
☑ FILER64	N/A

Figure 55: Enter File Server Name

4. Enter the **File Server Name** or **IP**
5. Click **Add**
6. Repeat the two steps for all File Servers you want to add
7. Click **OK** when finished adding file servers
8. Click **Next**

The next step is to provide the SQL Server details:



Please provide SQL Server information.

Server Name : 192.168.40.238

Insert audit data directly to database from file server : Yes

○ Windows Authentication ● SQL Server Authentication(Recommended)

User Name : sa

Password : ••••••••

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

https://www.microsoft.com/en-in/download/details.aspx?id=56840

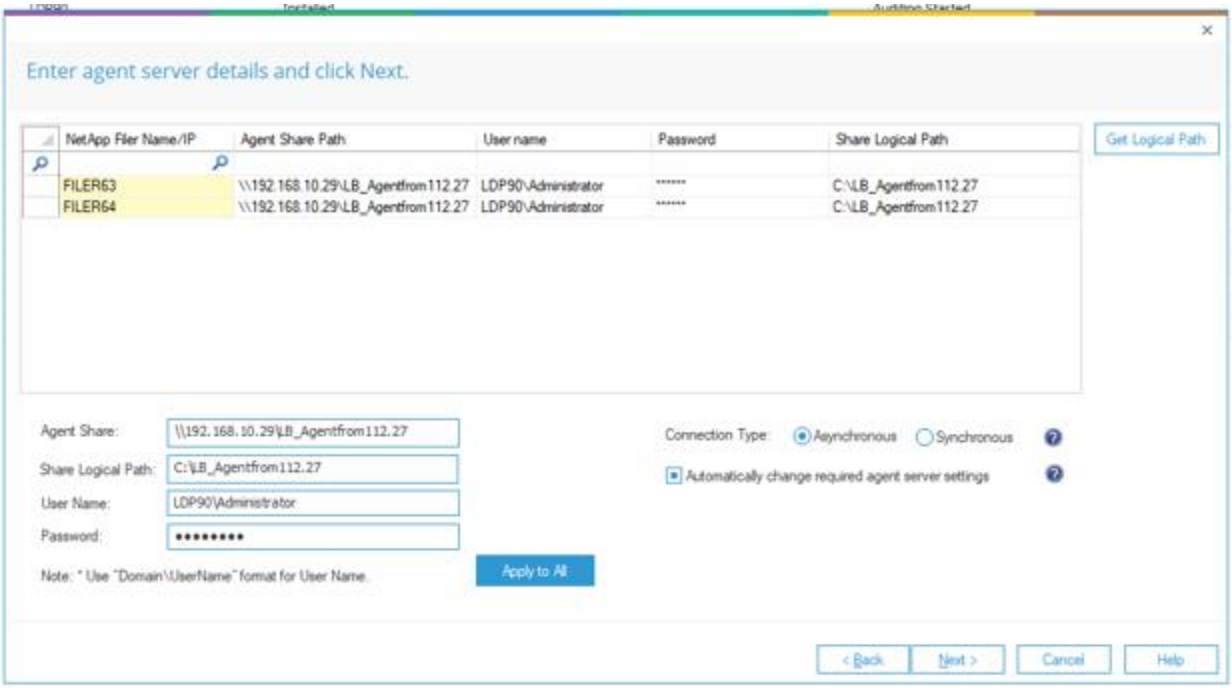
Figure 56: SQL Server Details

9. Type the **Server Name** or click **Browse** to select the desired SQL Server.
10. There are two authentication options:
    a) **Windows Authentication:** In this method, you can use any domain user windows account which have at least **dbcreator** role on the SQL server.

    b) **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote machine or the local machine. We recommend that this option is selected.

    Provide the username and password of an SQL User, which has sufficient rights to create a new database.

11. Please select Insert Audit Data Directly to Database from File Server as **YES,** only if the SQL connection from the File Server to the SQL Server is open. Please select **NO** if the connection is not open and the insertion will happen from the Application Server then.
12. Enter a database name in the database name field to create a new database. You can also select an existing database created by Lepide or another application.
13. Click **Next**



Enter agent server details and click Next.

NetApp Filer Name/IP	Agent Share Path	User name	Password	Share Logical Path
FILER63	\\192.168.10.29\LB_Agentfrom112.27	LDP90\Administrator	******	C:\LB_Agentfrom112.27
FILER64	\\192.168.10.29\LB_Agentfrom112.27	LDP90\Administrator	******	C:\LB_Agentfrom112.27

Agent Share: \\192.168.10.29\LB_Agentfrom112.27

Share Logical Path: C:\LB_Agentfrom112.27

User Name: LDP90\Administrator

Password: ••••••••

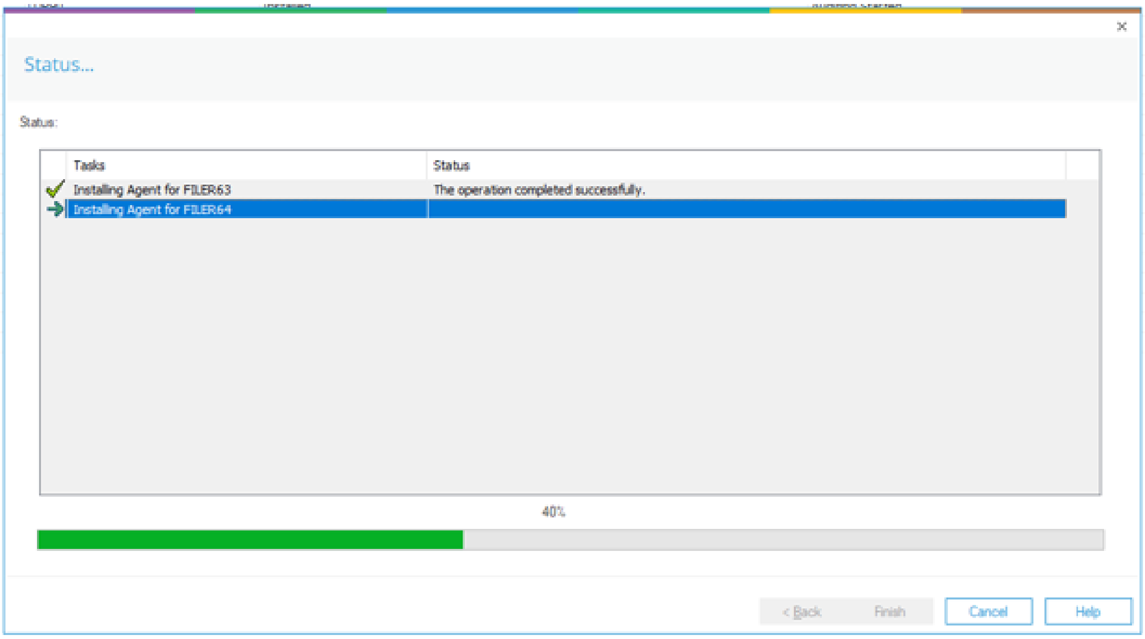
Note: * Use "Domain\UserName" format for User Name.

Connection Type: ● Asynchronous ○ Synchronous

☑ Automatically change required agent server settings

Figure 58: Enter Agent Server Details

14. Enter the Agent Server Details and click **Next**
15. The status dialog box will be displayed showing the status of the installation of each agent:


Status...

Status:

Tasks	Status
Installing Agent for FILER63	The operation completed successfully.
Installing Agent for FILER64	

40%

Figure 59: Status of Agent Installation

16. Click **Finish** to complete the process.

A dialog box is displayed asking whether you want to apply a rule to the newly added file server:

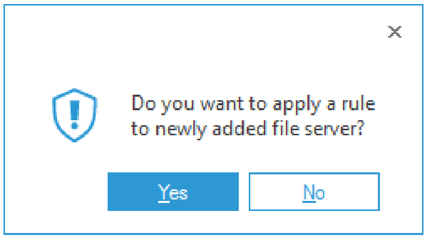

Do you want to apply a rule to newly added file server?

Figure 60: Option to Create a Rule

Audit Rule Management is explained in Section 9 of this document. Please refer to this for information on creating a rule.

8.3 Adding Multiple NetApp Cluster File Servers

After you have installed the software and configured Lepide service to run with administrative credentials, you can add multiple File Servers for auditing in one step.

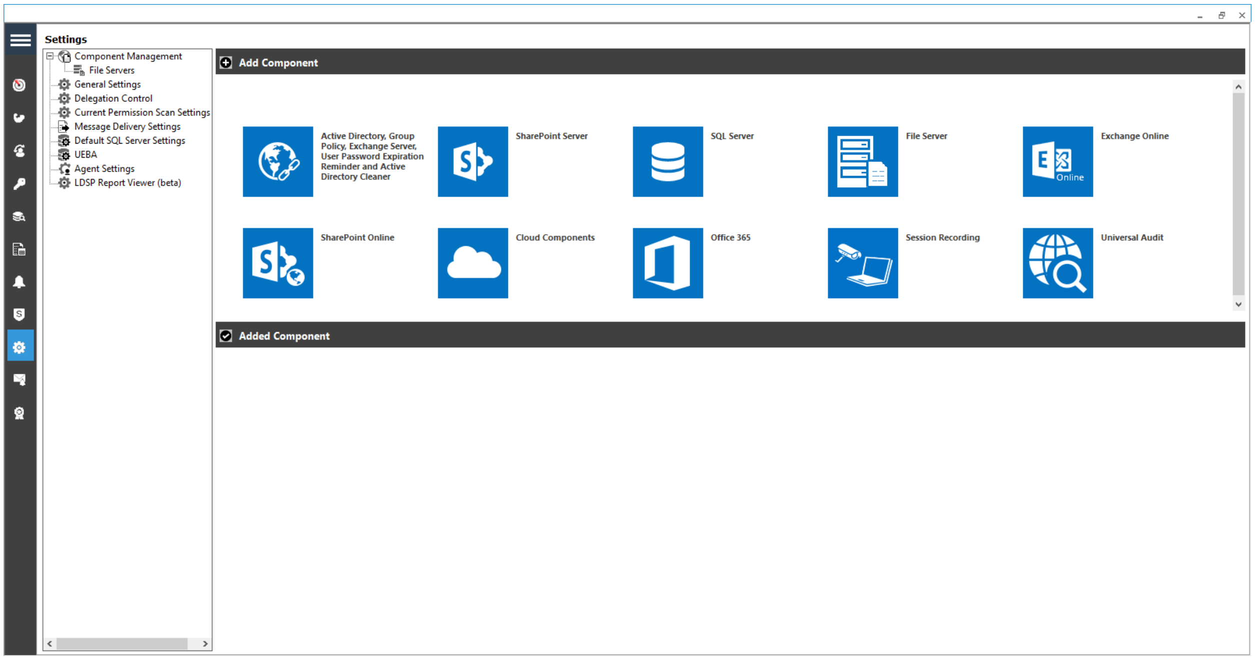
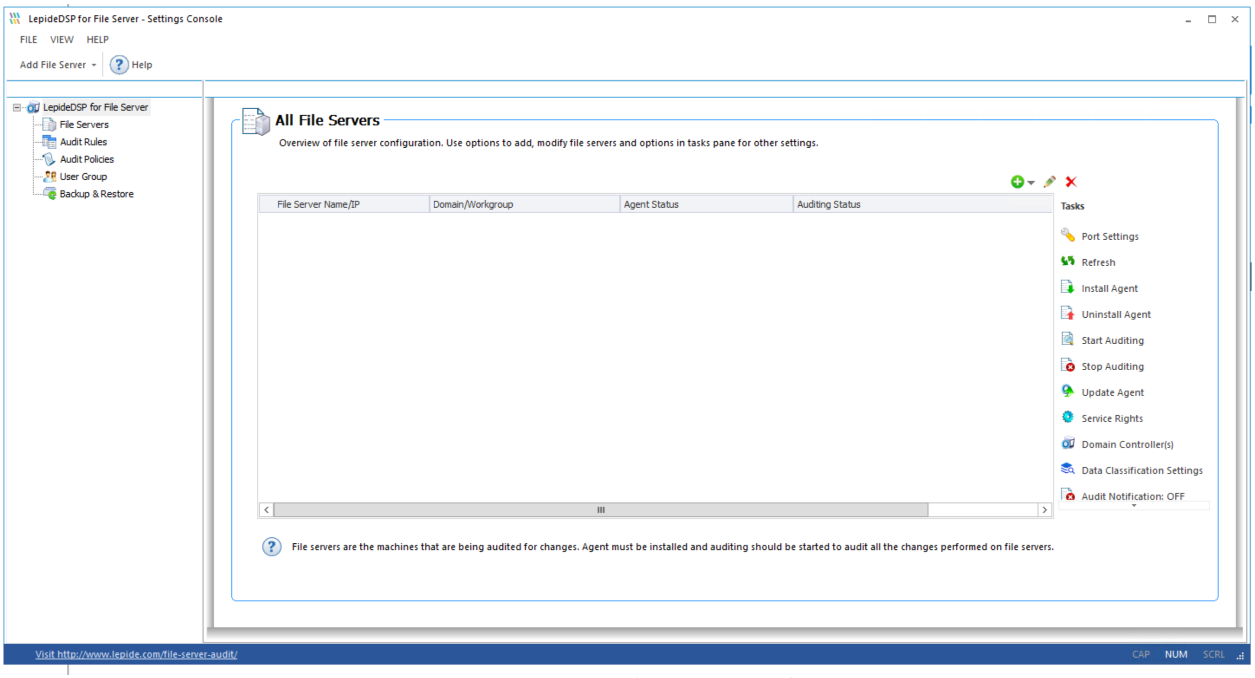


Figure 61: Component Management Window

From the Component Management window, under the Add Component section, click on the File Server icon to add this component to the solution.

The Settings Console dialog box is displayed:



Overview of file server configuration. Use options to add, modify file servers and options in tasks pane for other settings.

File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 62: File Server Console

Here, you can click **Add File Server** icon on the toolbar to add either of the following file servers:

- Windows File Server
- NetApp Filer

1. Click the **Add File Server** icon, select **Multiple** then select **NetApp Cluster Mode**.

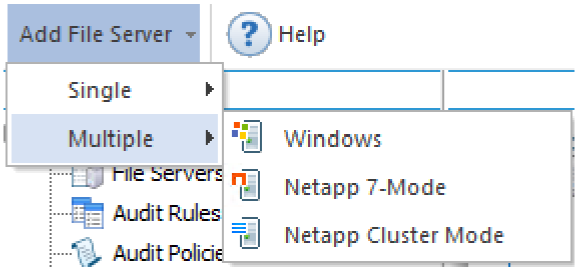
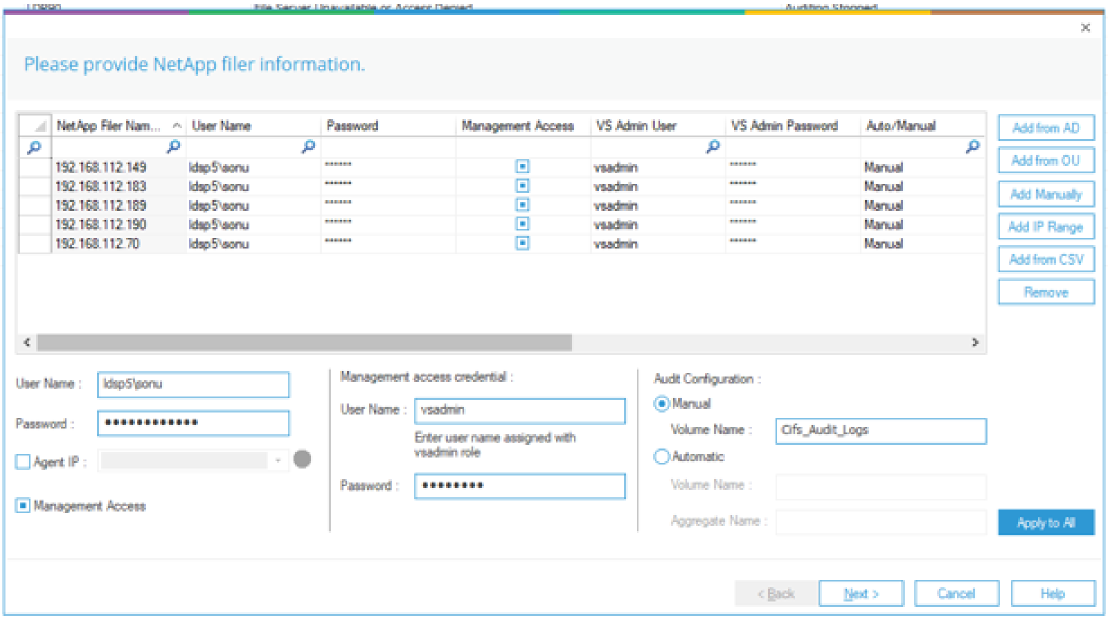


Figure 63: Option to add Multiple File Servers

2. The **Add File Servers** wizard starts:



Please provide NetApp filer information.

NetApp Filer Nam...	User Name	Password	Management Access	VS Admin User	VS Admin Password	Auto/Manual
192.168.112.149	ldsp5\sonu	******	▣	vsadmin	******	Manual
192.168.112.183	ldsp5\sonu	******	▣	vsadmin	******	Manual
192.168.112.189	ldsp5\sonu	******	▣	vsadmin	******	Manual
192.168.112.190	ldsp5\sonu	******	▣	vsadmin	******	Manual
192.168.112.70	ldsp5\sonu	******	▣	vsadmin	******	Manual

User Name : ldsp5\sonu

Password : ●●●●●●●●●●●●●

□ Agent IP :

▣ Management Access

Management access credential :

User Name : vsadmin

Enter user name assigned with vsadmin role

Password : ●●●●●●●●

Audit Configuration :

● Manual

Volume Name : Cifs_Audit_Logs

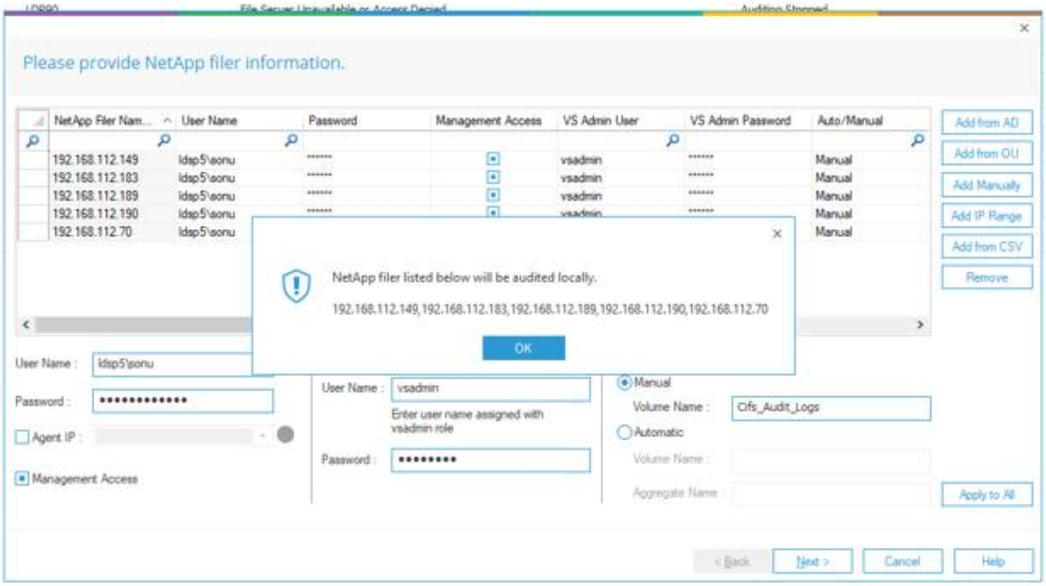
○ Automatic

Volume Name :

Aggregate Name :

Figure 64: Add NetApp File Server Wizard

3. From this screen, you can add the file servers. Click the button to select where the file server should be added from. The options are: Add from AD, Add from OU, Add Manually, Add IP Range, Add from CSV.



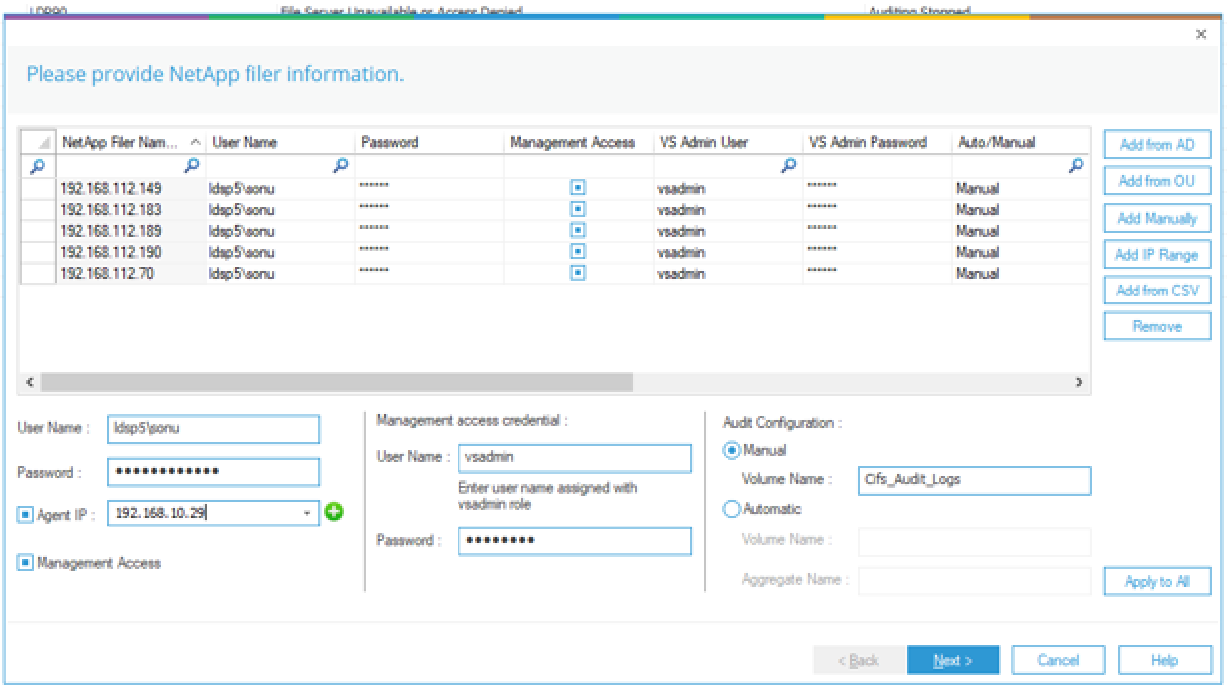
NetApp filer listed below will be audited locally.

192.168.112.149, 192.168.112.183, 192.168.112.189, 192.168.112.190, 192.168.112.70

Figure 65: NetApp Filer to be Added

4. Enter the **File Server Name** or **IP**
5. Click **Add**
6. Repeat the two steps for all File Servers you want to add
7. Click **OK** when finished adding file servers
8. The dialog box above will be displayed listing the file servers to be added
9. Click **OK**
10. Click **Next**

Alternatively, you can check the **Agent IP** box and you will need to then add the Agent IP address:



Please provide NetApp filer information.

NetApp Filer Nam...	User Name	Password	Management Access	VS Admin User	VS Admin Password	Auto/Manual
192.168.112.149	ldsp5\sonu	******	☑	vsadmin	******	Manual
192.168.112.183	ldsp5\sonu	******	☑	vsadmin	******	Manual
192.168.112.189	ldsp5\sonu	******	☑	vsadmin	******	Manual
192.168.112.190	ldsp5\sonu	******	☑	vsadmin	******	Manual
192.168.112.70	ldsp5\sonu	******	☑	vsadmin	******	Manual

User Name : ldsp5\sonu
Password : ************
☑ Agent IP : 192.168.10.29
☑ Management Access

Management access credential :
User Name : vsadmin
Enter user name assigned with vsadmin role
Password : ********

Audit Configuration :
● Manual
Volume Name : Cifs_Audit_Logs
○ Automatic
Volume Name :
Aggregate Name :

Figure 66: Add NetApp Filer with Agent IP Selected

Add the NetApp file information as follows:

Username: This should be a domain user account with at least CHANGE permission on the C$ of the SVM.

Agent IP: This is the IP address where the auditing agent will be installed. By default, it is installed on the local application server. Select this option only if you want to install the agent on a different machine.

Management Access: Check this box if the Management Access to the Network Interface is allowed. In this mode, the solution will do the configuration on the NetApp automatically. Keep the box unchecked if you are using the Least Privilege Model.

Management Access Credentials: Add the username and password with vsadmin role on the Netapp.

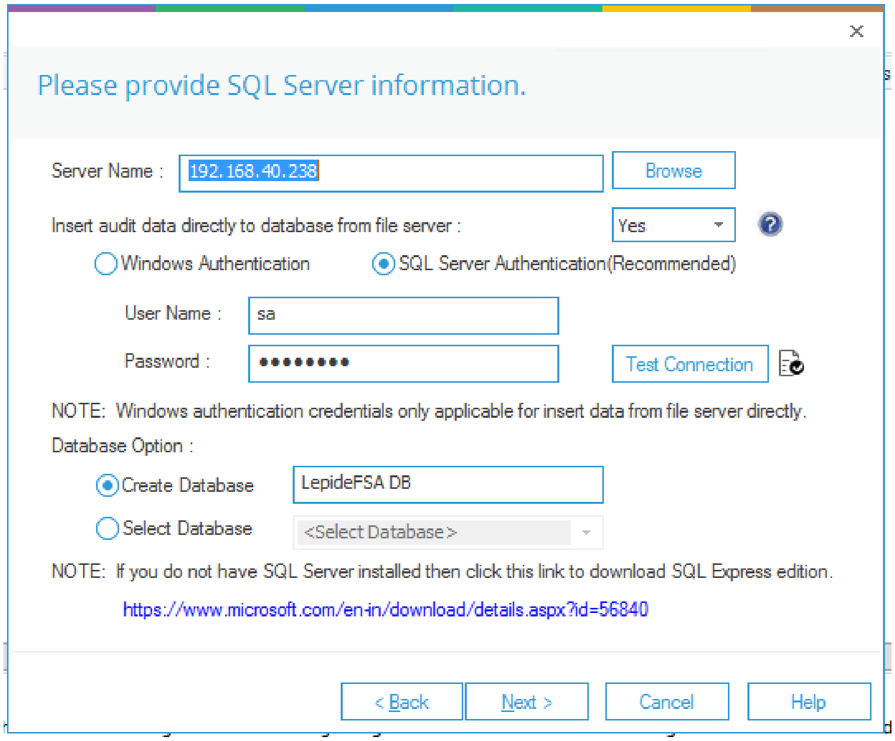
Audit Configuration:

Manual: Enter the name of the Audit Log Volume which has been created manually if the Least Privilege Model is used.

Automatic: Select this option if the Full Privilege Model is being used and Management Access is enabled. Enter the **Volume Name** and the **Aggregate Name** in the boxes.

Apply to All: Click this option to apply the same settings to all the NetApp Cluster Mode filers.

The next step is to provide the SQL Server details:



Please provide SQL Server information.

Server Name : 192.168.40.238

Insert audit data directly to database from file server : Yes

○ Windows Authentication ● SQL Server Authentication(Recommended)

User Name : sa

Password : ●●●●●●●●●

NOTE: Windows authentication credentials only applicable for insert data from file server directly.

Database Option :

● Create Database LepideFSA DB

○ Select Database <Select Database>

NOTE: If you do not have SQL Server installed then click this link to download SQL Express edition.

https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 67: SQL Server Details

11. Type the **Server Name** or click **Browse** to select the desired SQL Server.
12. There are two authentication options:

    a) **Windows Authentication:** In this method, you can use any domain user windows account which have at least **dbcreator** role on the SQL server.

b) **SQL Server Authentication:** Select this mode if SQL Server is installed on a remote machine or the local machine. We recommend that this option is selected.

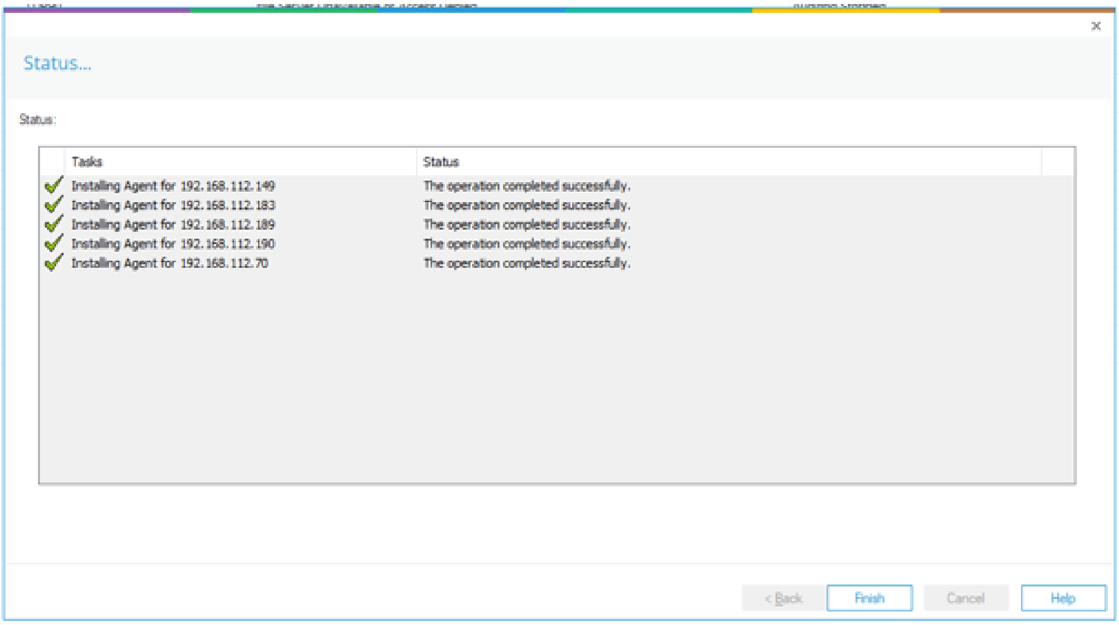
Provide the username and password of an SQL User, which has sufficient rights to create a new database.

13. Please select Insert Audit Data Directly to Database from File Server as **YES,** only if the SQL connection from the File Server to the SQL Server is open. Please select **NO** if the connection is not open and the insertion will happen from the Application Server then.

14. Enter a database name in the database name field to create a new database. You can also select an existing database created by Lepide or another application.

15. Click **Next**

16. The status dialog box will be displayed showing the status of the installation of each agent:

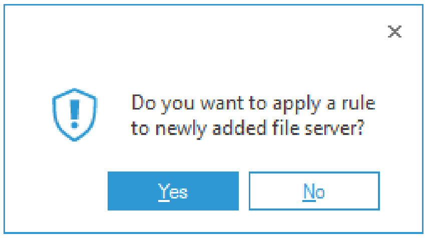


	Tasks	Status
✓	Installing Agent for 192.168.112.149	The operation completed successfully.
✓	Installing Agent for 192.168.112.183	The operation completed successfully.
✓	Installing Agent for 192.168.112.189	The operation completed successfully.
✓	Installing Agent for 192.168.112.190	The operation completed successfully.
✓	Installing Agent for 192.168.112.70	The operation completed successfully.

Figure 69: Status of Agent Installation

17. Click **Finish** to complete the process.

A dialog box is displayed asking whether you want to apply a rule to the newly added file server:



Do you want to apply a rule to newly added file server?

Figure 70: Option to Create a Rule

Audit Rule Management is explained in Section 9 of this document. Please refer to this for information on creating a rule.

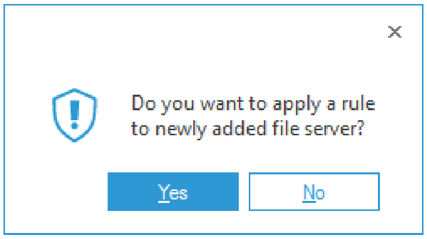
9 Audit Rule Management

After you have added the File Server to the application, you must create an audit rule for that File Server. In the audit rule, you can base your auditing on:

- Objects such as Directories, Drives, Events, Files, Monitoring Time, and Processes that you want to audit.
- Users/ User Groups actions which you want to audit.

9.1 Create Audit Rule

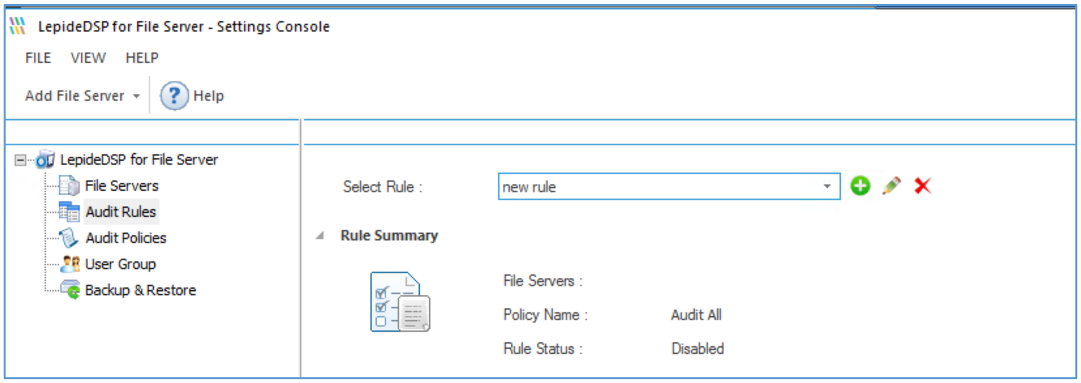
Follow the steps below to create a new Audit Rule. If you had selected **Yes** in the last step of the Add File Server Wizard, the **Add Rule to the File Server** wizard starts automatically.



Do you want to apply a rule to newly added file server?

Figure 71: Option to Add Rule

Alternatively, you can navigate to the **Audit Rules** section in the left pane and click ⊕ icon in the **Select Rule** section of the right pane to start this wizard:



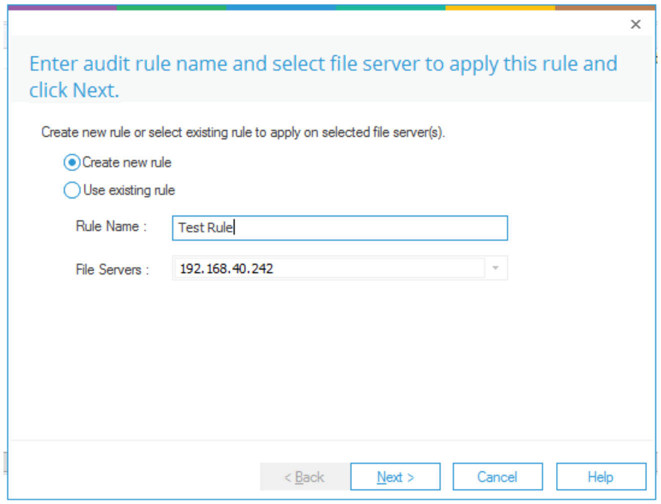
Select Rule : new rule

File Servers :

Policy Name : Audit All

Rule Status : Disabled

Figure 72: Settings Console


Enter audit rule name and select file server to apply this rule and click Next.

Create new rule or select existing rule to apply on selected file server(s).

● Create new rule

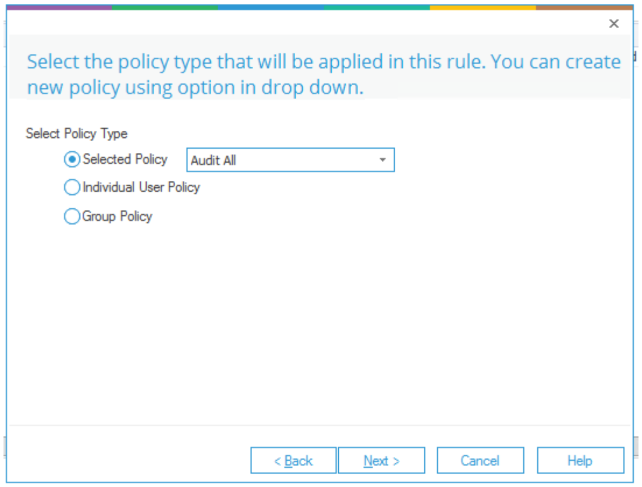
○ Use existing rule

Rule Name : Test Rule

File Servers : 192.168.40.242

Figure 73: Create New Rule

- Enter a rule name and select the File Server for which you want to create the rule if it is not already selected in the **File Servers** drop-down menu.
  You can select multiple file servers to apply the audit rule.
- Click **Next**. The audit policies dialog box is displayed:



Select the policy type that will be applied in this rule. You can create new policy using option in drop down.

Select Policy Type

● Selected Policy Audit All

○ Individual User Policy

○ Group Policy

Figure 74: Audit Policies

- Select the policy type from the following options:

  Lepide allows you to link an Audit policy to both a User and a User Group.

  a. **Individual User Policy:** Data will be collected as per the specified users only. Data will not be collected if the changes are made by other users, who are not listed.

  b. **Group Policy:** Data will be collected as per the Group's policy no matter which User of the Group has logged in. This means that the policy associated with the user will be overridden by the group's policy.

A few possible scenarios are listed below:

i. Four users have been added. Each of them belongs to the **same** group and they have the same or different audit policy. In this example, if you select **Individual User Policy**, the audit data will be collected as per each user's policy.

ii. Four users have been added. Each of them belongs to **different** groups, and they have the same or different audit policy. In this example, if you select **Individual User Policy**, the audit data will be collected as per each user's policy.

iii. Four users have been added. Each of them belongs to **same** group, and they have the same or different audit policy. In this example, if you select **Group Policy**, the audit data will be collected as per that group's policy.

iv. Four users have been added. Each of them belongs to **different** groups, and they have same or different audit policy. In this example if you select **Group Policy**, the audit data will be collected as per the policy applied on the group of each user.

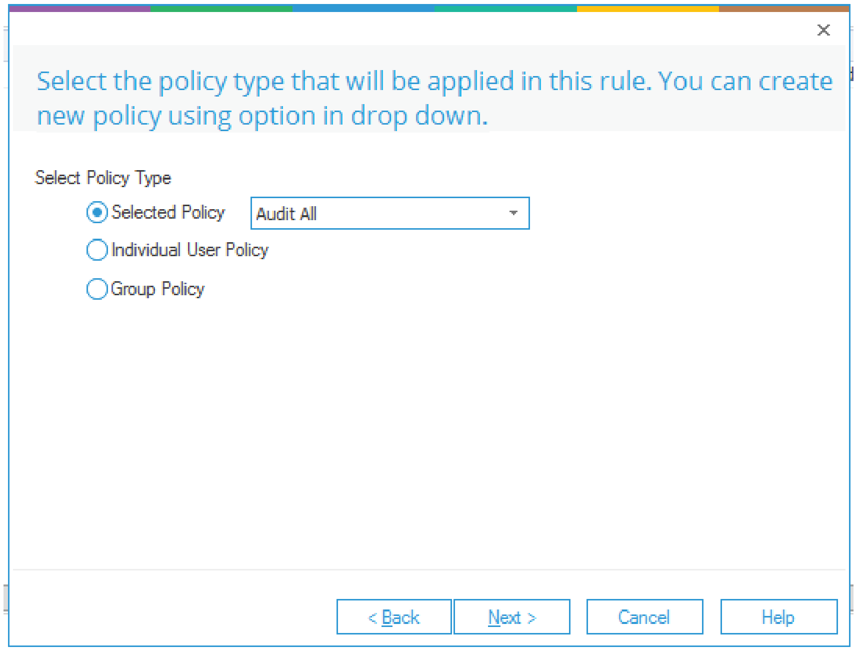
Selecting Individual User policy and Group Policy will not generate a report here as we have not yet created any User Group in the application. These policies can be selected only if you have pre-defined groups in the application.

c. Selected Policy: This has four options available. The first three are pre-defined policies while the fourth one can be configured:

- **Audit All:** Audit all File and Folder accesses to the File Server
- **Audit Shares Only:** Audit only shared files and folders.
- **Audit all but Shares**: Audit all File and Folder accesses except shared files and folders.
- **Create New Policy**: Create new policy where you can define what Objects you want to audit.

NOTE: In this example, we are creating an audit rule with predefined policy. To create an auditing rule with a user-configured policy refer to Section 10 Create Audit Policy.

For this example, we will select the Audit All policy:



Select the policy type that will be applied in this rule. You can create new policy using option in drop down.

Select Policy Type

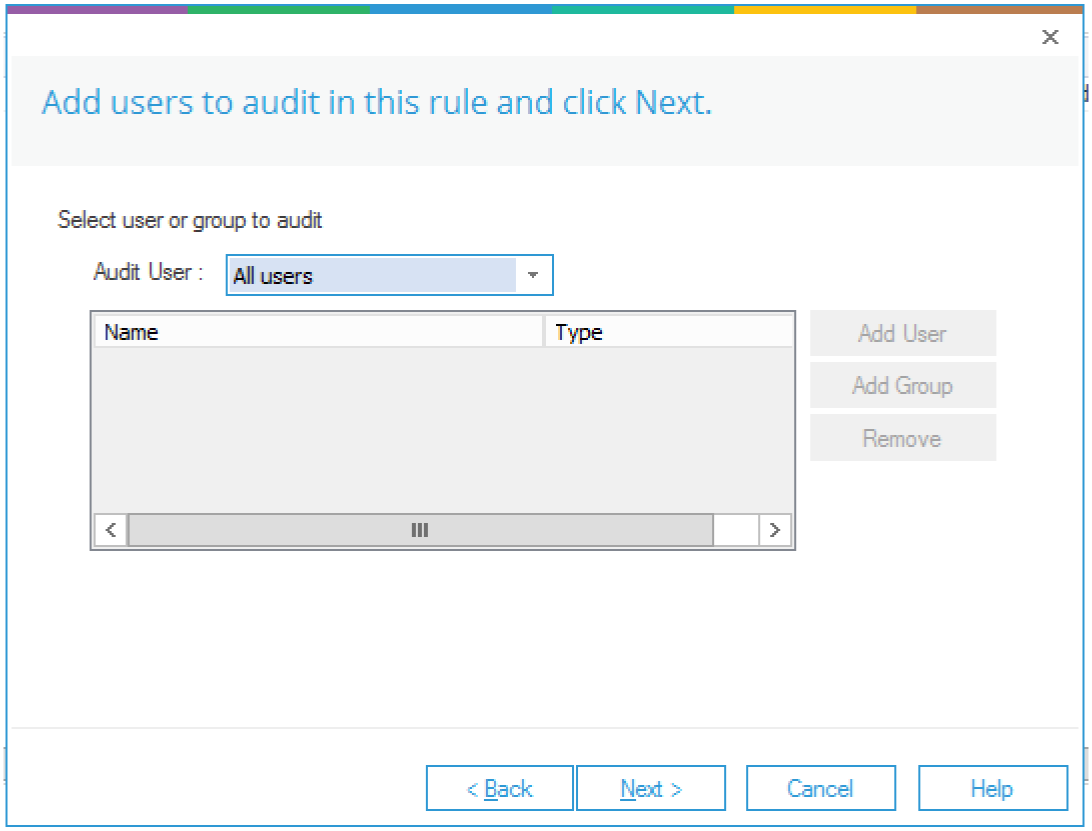
● Selected Policy Audit All

○ Individual User Policy

○ Group Policy

Figure 75: Select Policy Type

- Click **Next**



Add users to audit in this rule and click Next.

Select user or group to audit

Audit User : All users

Figure 76: Add Users to Audit

- Select any of the following options to define the users:

  a. **All users:** The selected rule will be applicable to all users.

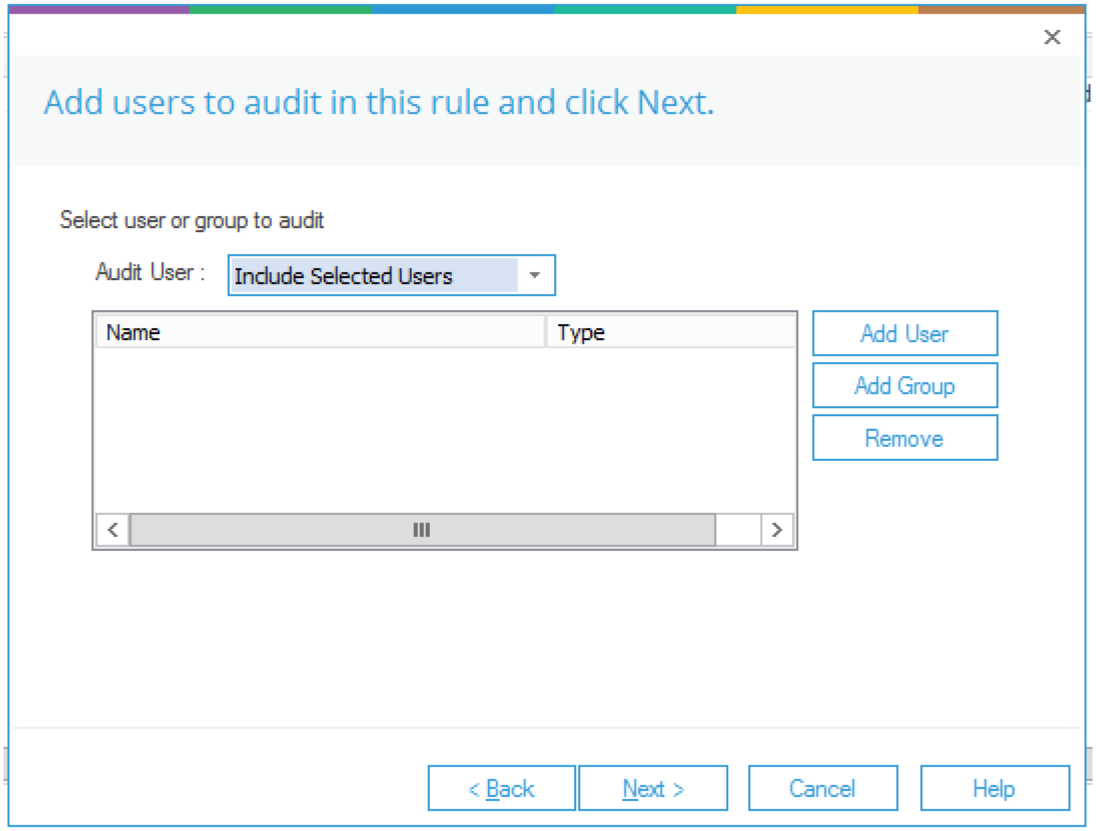
  b. **Include Selected Users:** The rule will be applicable to the selected users only. Other users will be excluded from the rule.

  c. **Exclude Selected Users:** The rule will **not** be applicable to the selected users, but it **will** be applied to all other users.

  Selecting **Include Selected Users** or **Exclude Selected Users** enables the next section. Follow the steps below to add the selected users.

  a. To add the **selected** or **all** users.

     i. Click the **Add User** button.



Add users to audit in this rule and click Next.

Select user or group to audit

Audit User : Include Selected Users

Name	Type

Figure 77: Add Users to Rule

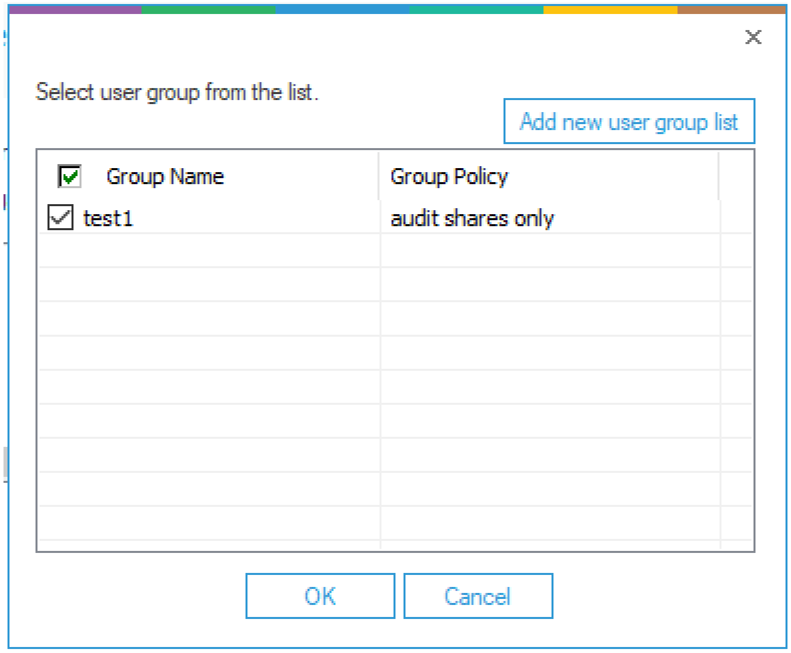
ii. If no user is listed here, then it means that no user group has been created in the Solution. Refer to Section 11 Add User Group to follow the steps to create a user group.

iii. You can also click the **Add User** button here to create a new user group and add the user to it.

iv. After adding and listing the users you can check the boxes of the users to include them and uncheck others to exclude them.

v. Click **OK** to go back to the previous wizard which now shows the list of selected users.

b. Click the Add Group button to add the group.



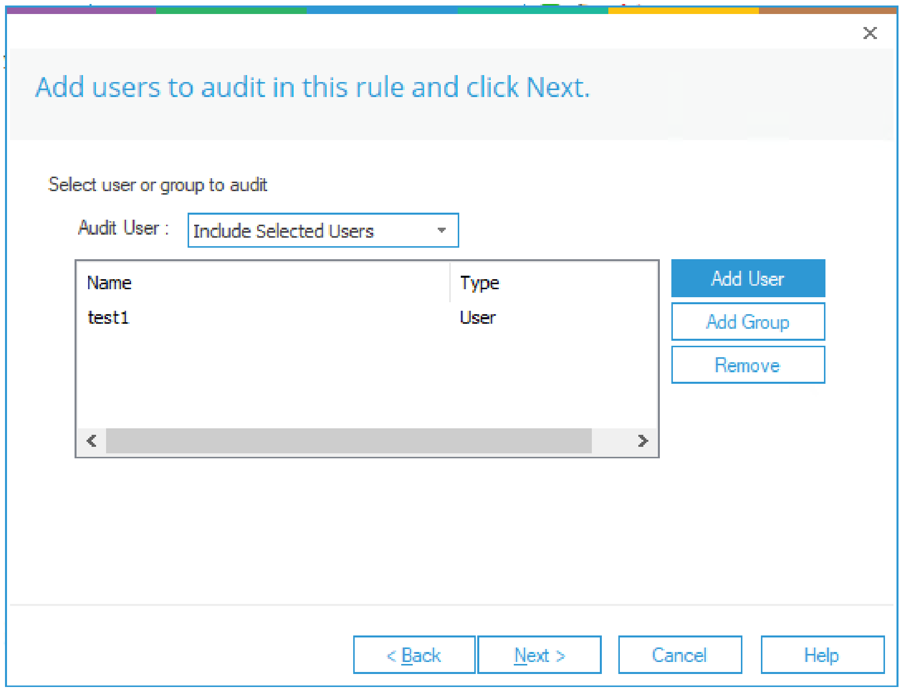
Select user group from the list.

☑ Group Name	Group Policy
☑ test1	audit shares only

Figure 78: Select User Group from the List

If no group is listed here, then it means that you have not added a group. Refer to Section 11 Add User Group to know more. You can also click **Add new user group list** button to add a new group.

c. Select the group and click **OK**. It takes you to the Add Rule wizard, which now shows the list of users added from the selected group.



Add users to audit in this rule and click Next.

Select user or group to audit

Audit User : Include Selected Users

Name	Type
test1	User

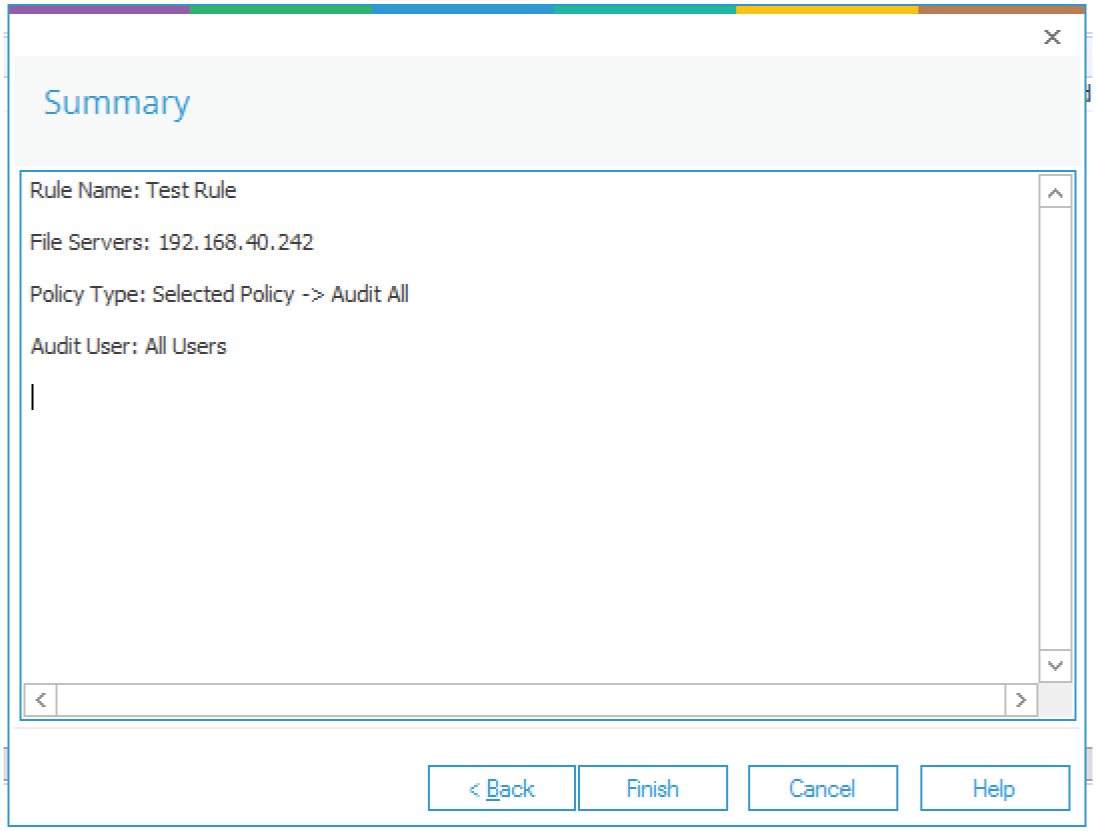
Figure 79: Added Users

d. You can select any user here and click the Remove button to remove a user from the list.

The rule is applied to all users in this test case.

- Click **Next**

The Summary box is displayed:



Rule Name: Test Rule

File Servers: 192.168.40.242

Policy Type: Selected Policy -> Audit All

Audit User: All Users

Figure 80: Summary

- Click **Finish** to complete the process. The newly added audit rule is displayed in the list.
- Click **Update Agent on all File Servers to apply new Settings** notification and follow the on-screen instructions to update the agent.

NOTE: It is necessary to update the agent each time you change the applied Audit Rule. If this is not done, the auditing will not be updated, and the reports will not include the new modifications when generated.

After you have created the auditing rules, go to the **Audit Reports** tab in the main panel to view the reports.

9.1.1 Common Issues with Reports

If you cannot view the reports after doing the configuration, try the following:

1. Navigate the root node of File Server Console, which displays the list of all added File Servers. Here, you must check if the agent on File Server is properly installed and working. For the selected File Server, **Agent Status** should be **Installed** and **Auditing Status** should be started.

2. If the agent status is not installed, then install the agent and start the auditing. If the auditing status is stopped, but agent status is installed, then you should start the auditing.

3. If the agent is properly installed, check whether the Rule and Policy have been properly applied. Check the Rule Name (box should be filled), Rule Status (it should be enabled) and Assigned Policies (policy name should be displayed) under File Server in the left pane.

4. It is advised to use SQL authentication even if SQL Server is installed on the local system. If you cannot use SQL authentication for any reason and you are using Windows authentication, try the following:

    i. Type services.msc in **RUN** and press **Enter** to access the Windows Services, on the system where the software is installed.

    ii. Double click Lepide FSA Service, go to **Logon** tab and select **This Account**.

    iii. Browse the username by which you have logged into the system.

    iv. Provide the password in the given field.

    v. In case the username is already selected re-enter the password in the given field.

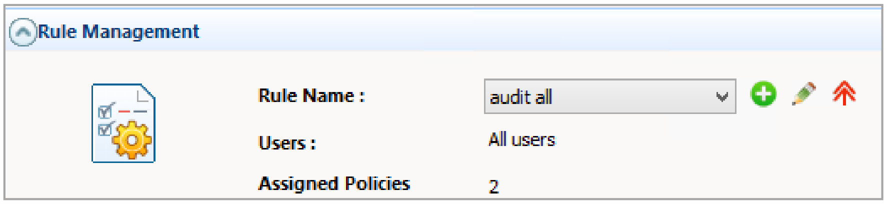
    vi. Click **Apply** and **OK**.

    vii. Again right-click on Lepide FSA Service and select **Restart** in the pop-up menu.

9.2Change the Priority of Audit Rule

Follow the steps below to change the priority of Audit Rule:

1. Navigate to **File Servers** section from the left panel and go to **Rules Management**.



Rule Management

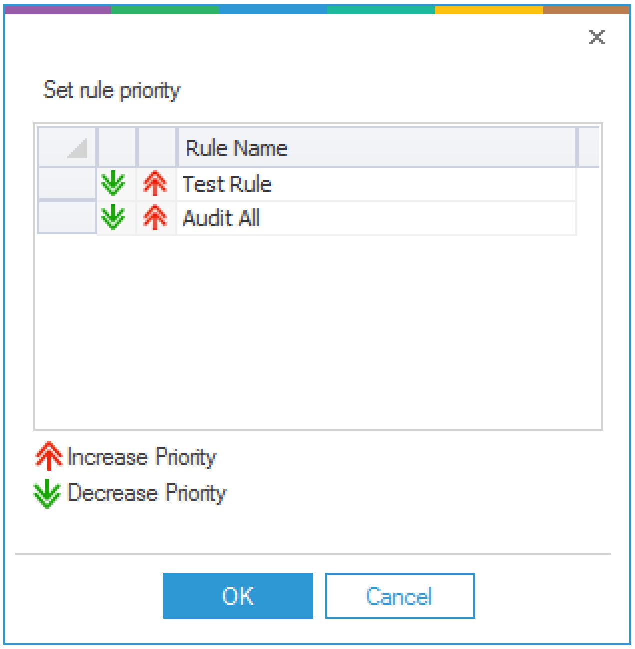
Rule Name : audit all

Users : All users

Assigned Policies 2

Figure 82: Rules Management

2. In Rules Management, click ⇑ icon. It displays the following dialog box.



Set rule priority

		Rule Name
⇓	⇑	Test Rule
⇓	⇑	Audit All

⇑ Increase Priority
⇓ Decrease Priority

Figure 83: Set Priority

3. Select an audit rule and click ⇓ icon to decrease its priority.

4. Select an audit rule and click ⇑ icon to increase its priority.

5. Click **OK**.

NOTE: After you have created an audit rule, you can click the Modify icon ✎ to modify it.

10 Create Audit Policy

By creating a new audit policy, you can ensure that you audit only the objects you require such as specified Files, Folders, Directories, Events, and Processes.

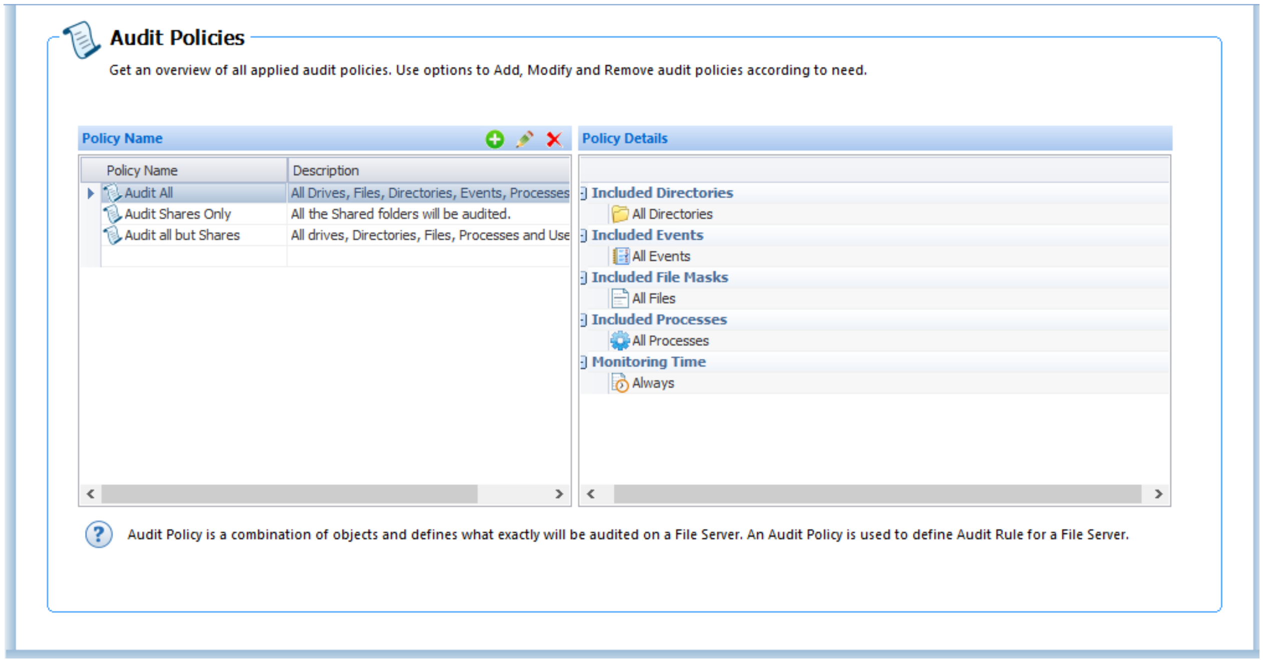
There are three default policies:

- **Audit All:** Select this policy to audit all objects on the File Server.
- **Audit Shares Only:** Select this policy to audit the shared folders only.
- **Audit All but Shares:** Select this policy to audit all except shared folders.

For customized auditing, you need to create an audit policy with the desired object monitoring list. While creating a policy, an administrator can set the priority of policy rules to streamline the audit report further.

The following steps explain how to create new audit policy. Once this is done, you can associate it with an audit rule to audit only selected objects.

1. Navigate to the Audit Policies in the left pane.



Audit Policies

Get an overview of all applied audit policies. Use options to Add, Modify and Remove audit policies according to need.

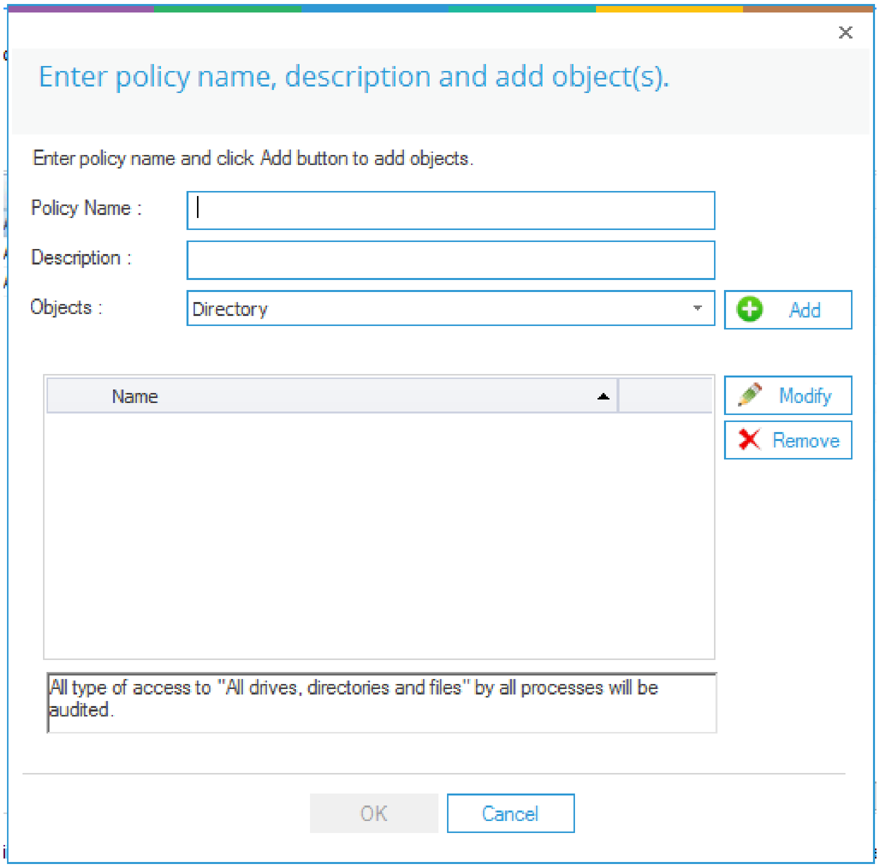
Policy Name	Description
Audit All	All Drives, Files, Directories, Events, Processes
Audit Shares Only	All the Shared folders will be audited.
Audit all but Shares	All drives, Directories, Files, Processes and Use

- Included Directories
  - All Directories
- Included Events
  - All Events
- Included File Masks
  - All Files
- Included Processes
  - All Processes
- Monitoring Time
  - Always

Audit Policy is a combination of objects and defines what exactly will be audited on a File Server. An Audit Policy is used to define Audit Rule for a File Server.

Figure 84: Audit Policies section

2. At the top of the Policy Name section click the ⊕ icon to add a new Policy



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name :

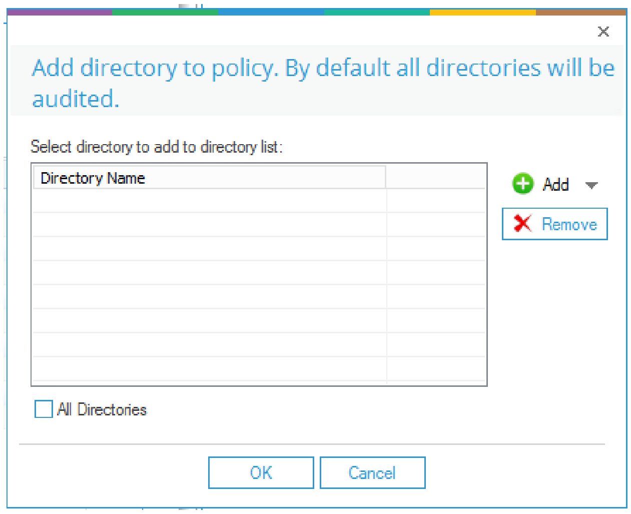
Description :

Objects : Directory

All type of access to "All drives, directories and files" by all processes will be audited.

Figure 85: Add New Policy Wizard

3. Enter the Policy Name and description.
4. Now, select the type of object list from the drop-down menu.
    a. Directory
    b. File Mask
    c. Process
    d. Event
    e. Monitoring Time
5. There are different ways to add each object list which are explained as follows:
    a. **Add Directory:** Follow the steps below to add a directory.
        i. Select Directory and click **Add** to open the following dialog box:



Add directory to policy. By default all directories will be audited.

Select directory to add to directory list:

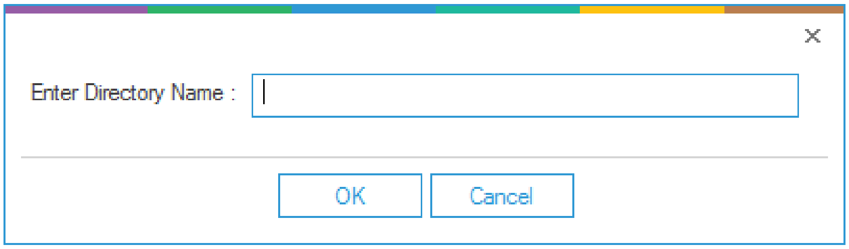
Directory Name	

Figure 86: Add Directory

If you wish to add all directories, check the **All Directories** box. Uncheck this option to add a customized list of directories.

ii. Click the **Add** button to access the following options to add the directories:

- **Manually:** Select this option to add a directory manually with its name. It displays the following dialog box.

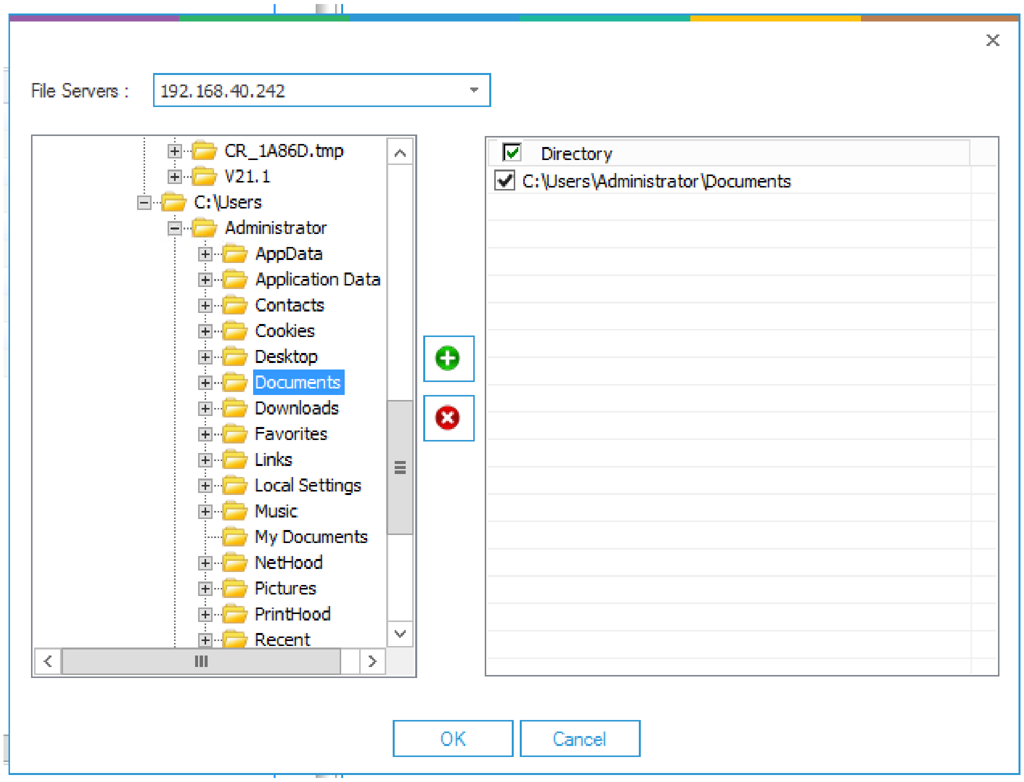


Enter Directory Name :

Figure 87: Add Directory Manually

Enter the name of the directory and click **OK**. It takes you back to **Add Directory** dialog box, which now displays the name of the added directory.

- **Scan:** Select this option to scan the File Server and select the directories from the list.



File Servers : 192.168.40.242

```
CR_1A86D.tmp
V21.1
C:\Users
  Administrator
    AppData
    Application Data
    Contacts
    Cookies
    Desktop
    Documents
    Downloads
    Favorites
    Links
    Local Settings
    Music
    My Documents
    NetHood
    Pictures
    PrintHood
    Recent
```

☑ Directory
☑ C:\Users\Administrator\Documents

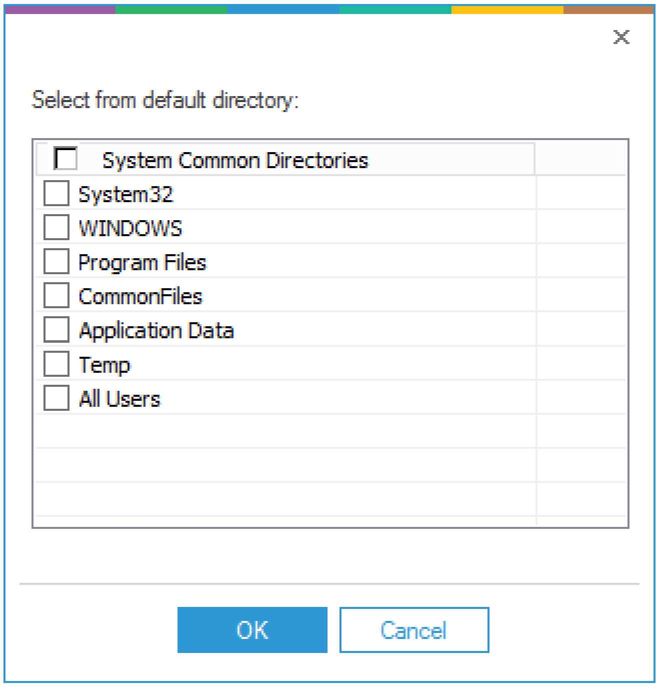
Figure 88: Scan and Add Directory

In the **Scan and Add** dialog box, select the name of File Server from the drop-down menu. It lists all directories in a tree structure on the File Server in the Left Panel. Expand the nodes to access the directories. Select a directory and click the ⊕ icon to add it.

In the Right Panel, you can uncheck the directories which you do not want to add. To remove a directory from the added list, select it and click the ⊗ icon to remove it.

After you have selected the directories, click **OK**. It takes you back to **Add Directory** wizard.

- **Default:** You can select this option to add the selected default directories on the File Server. It displays the following dialog box.



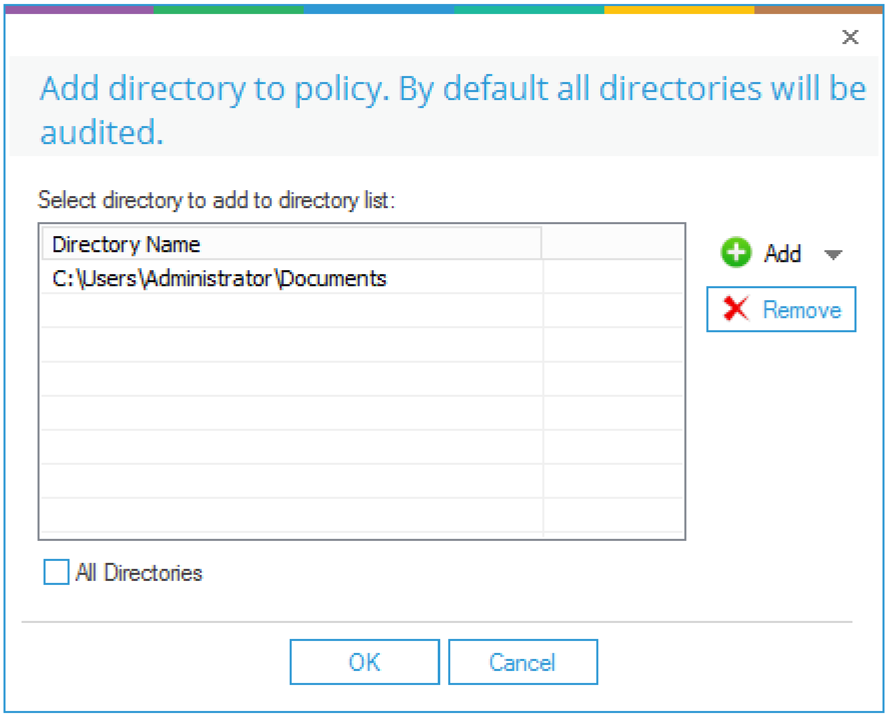
Select from default directory:

- ☐ System Common Directories
- ☐ System32
- ☐ WINDOWS
- ☐ Program Files
- ☐ CommonFiles
- ☐ Application Data
- ☐ Temp
- ☐ All Users

Figure 89: Add the Default User Directories

Select the desired default directories and click **OK.** It takes you back to **Add Directory** wizard.

iii. You can add the directories using any of the above methods. The added directories are listed in the dialog box.



Add directory to policy. By default all directories will be audited.

Select directory to add to directory list:

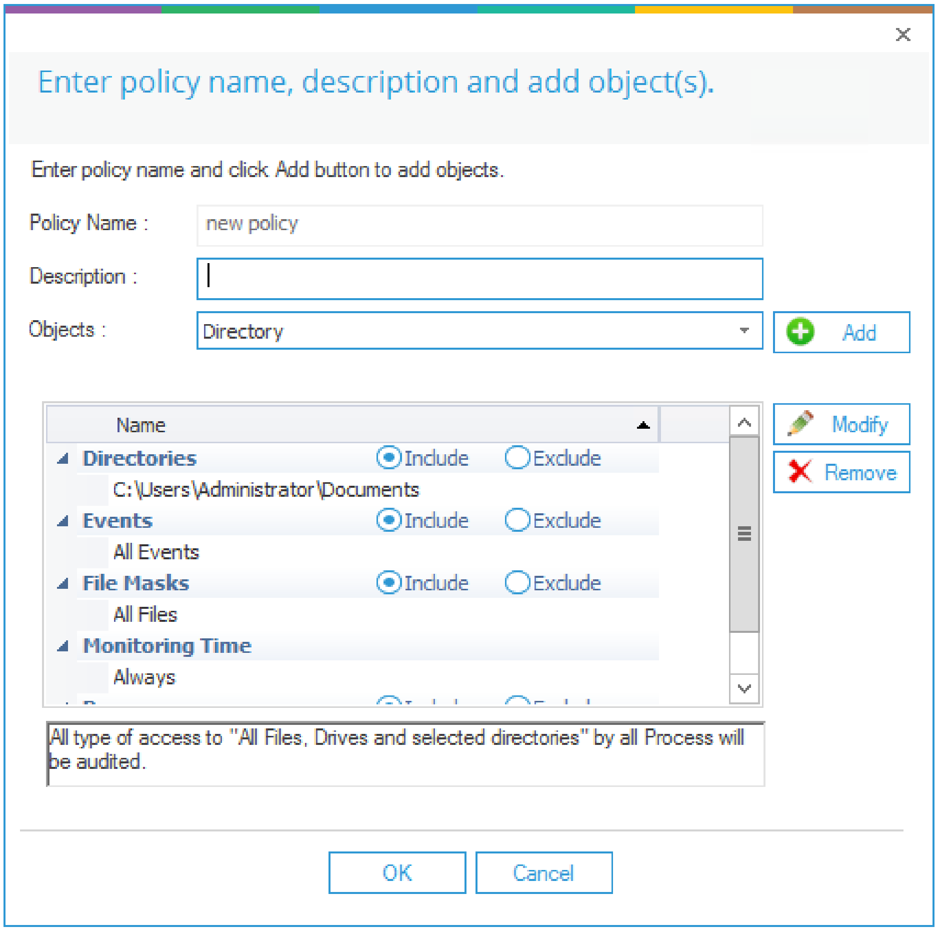
Directory Name	
C:\Users\Administrator\Documents	

□ All Directories

Figure 90: Displaying the Added Directories

iv. To delete a directory, you can select it and click the **Remove** button.

v. Click **OK** after you have added the required directories. It takes you back to the **Add New Policy** wizard, where all added directories are listed in the section as a separate category named **Directories**.



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name : new policy

Description :

Objects : Directory

Directories ● Include ○ Exclude
C:\Users\Administrator\Documents
Events ● Include ○ Exclude
All Events
File Masks ● Include ○ Exclude
All Files
Monitoring Time
Always

All type of access to "All Files, Drives and selected directories" by all Process will be audited.

Figure 91: List of Added Directories

You can expand or collapse the **Directories** categories.

vi. You can click the **Include** radio button to include the list of added directories in the auditing, which means that only the listed directories will be audited.

vii. Click the **Exclude** radio button to exclude the list of added directories from auditing.

After adding the directories, if you click **Add** button again for adding further directories, then the **Modify Directory** dialog box appears on the screen. Follow the same steps as listed above to add or remove the directories.

b. **Add File Mask:** You can specify the name or extension of the files to be monitored in File Masks. Follow the steps below to add the File Masks:

i. Select **File Mask** in the **Objects** drop-down menu and click **OK**. It displays the **Add File Mask** dialog box:

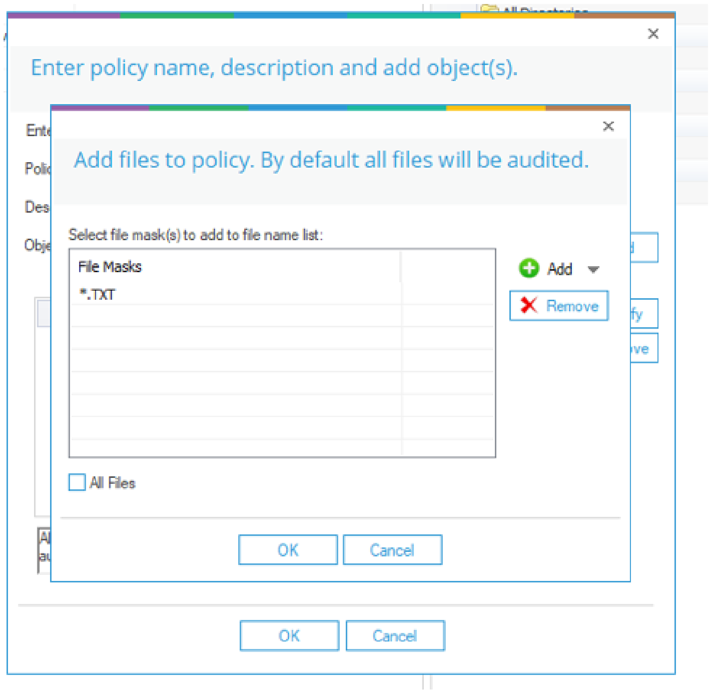

Enter policy name, description and add object(s).
Add files to policy. By default all files will be audited.
Select file mask(s) to add to file name list:
File Masks
*.TXT
Add
Remove
All Files
OK
Cancel
OK
Cancel

Figure 92: Add Files to Policy

If you have checked the **All Files** option, then all files on the File Server will be added. Uncheck this option to add a customized list of files.

ii. The process to add File Mask is same as when adding directories except for the **Default** option.

Click the **Add** button to access the following options:

- **Manually:** Click this option to add a file mask manually by providing its name.

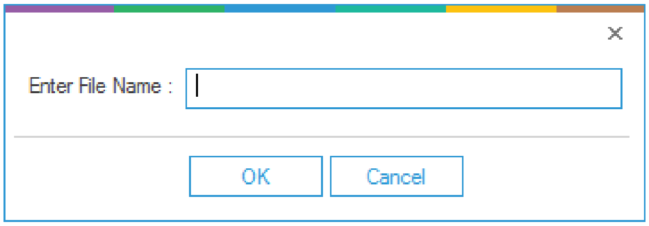
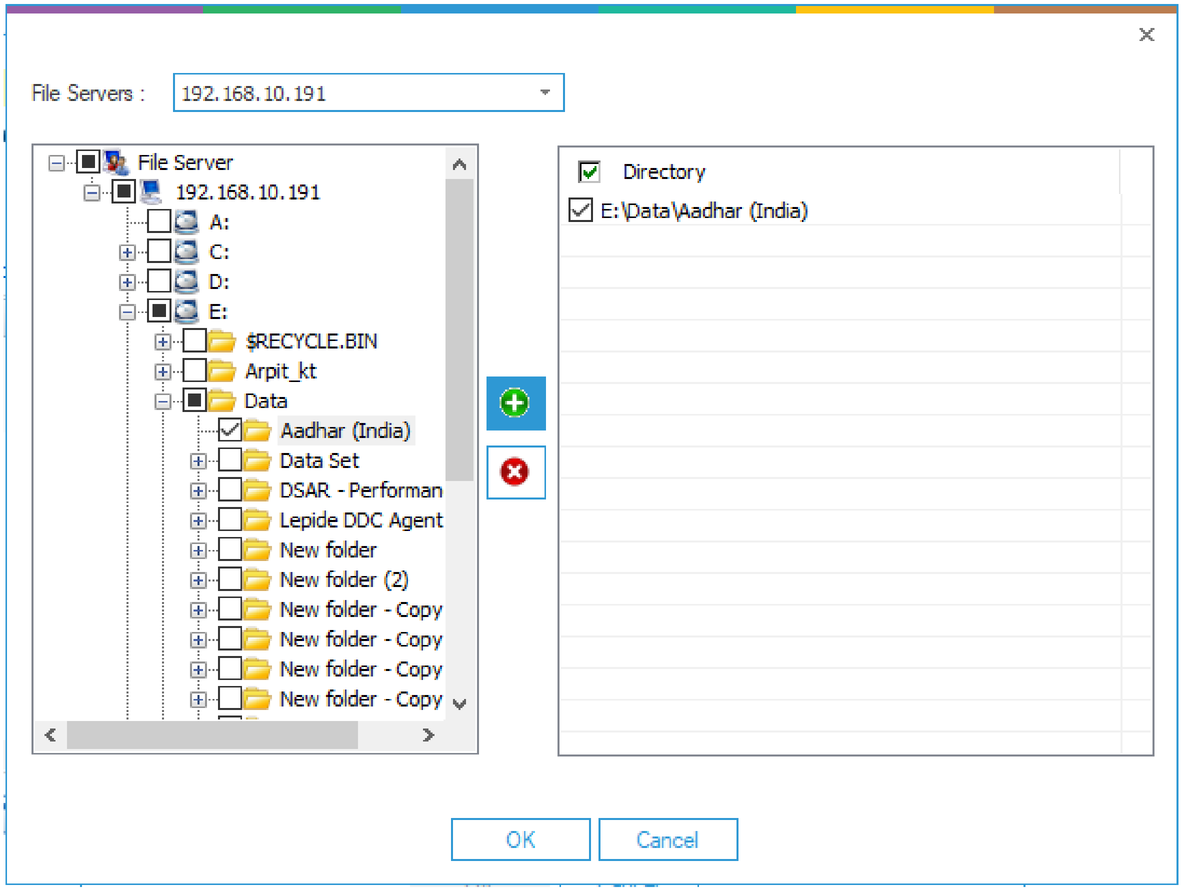


Figure 93: Add File Mask Manually

Provide the name or extension of the file and click **OK**. It adds the file mask and takes you back to **Add File Mask** dialog box.

- **Scan:** Select this option to scan the File Server and add the selected files.



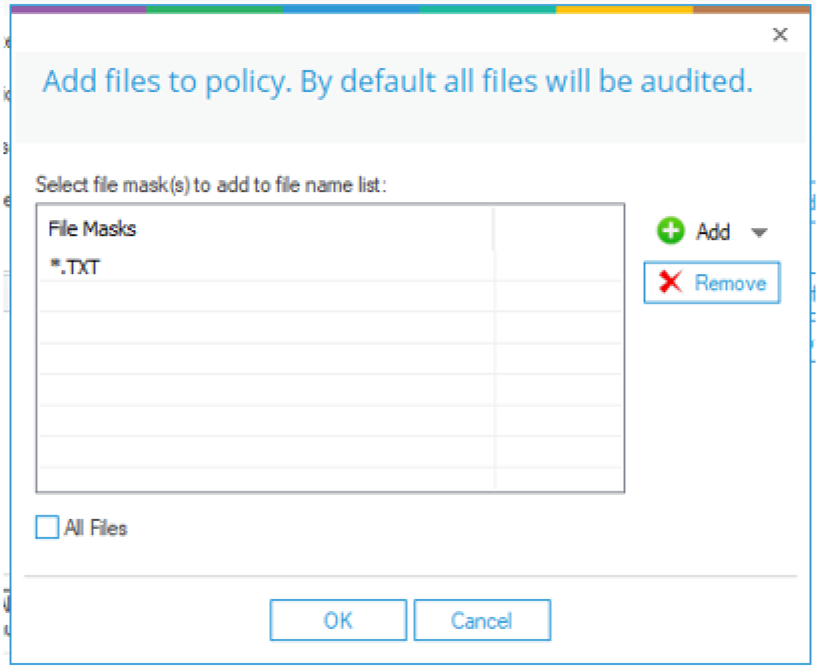
File Servers : 192.168.10.191

☑ Directory

☑ E:\Data\Aadhar (India)

Figure 94: Scan and Add

- Select the files in the left panel and click the ⊕ icon to add the file mask.
- In the Right Panel, you can uncheck the files which you do not want to add.
- To remove a file from the added list, select it and click the ⊗ icon to remove it.
- After you have selected the file masks, click **OK**. It takes you back to **Add File Mask** dialog box, which displays the list of all added File Masks.



Add files to policy. By default all files will be audited.

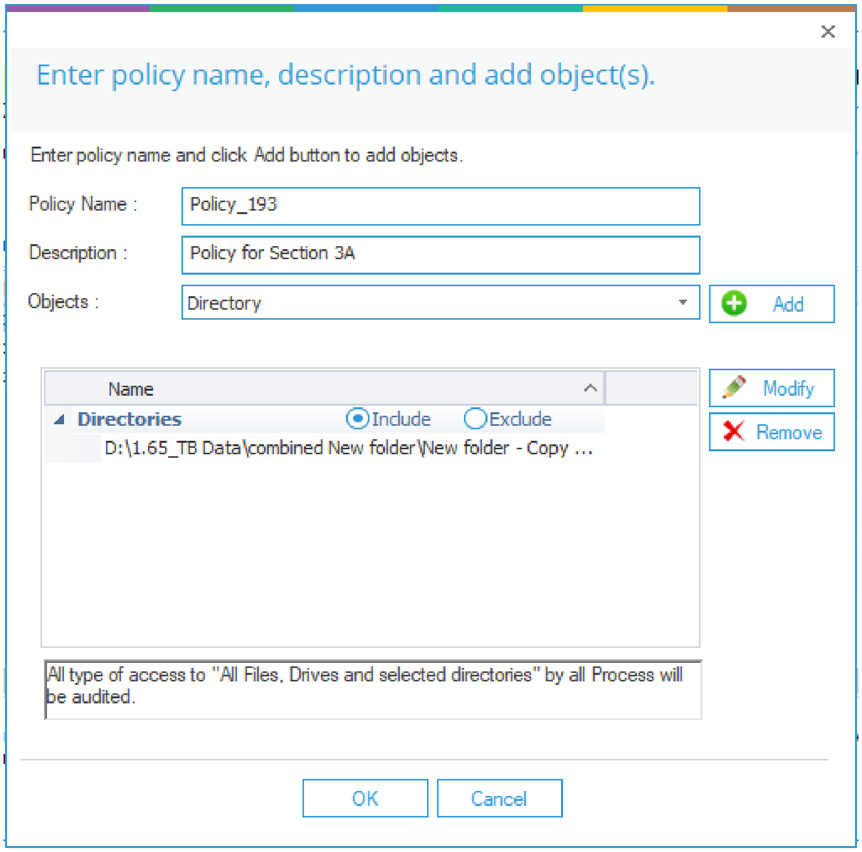
Select file mask(s) to add to file name list:

File Masks
*.TXT

Figure 95: Add File Masks

iii. To delete a File Mask, you can select it and click the **Remove** button.

iv. Click **OK** after you have added the required file masks. It takes you back to **Add New Policy** wizard, where all added File Masks are listed in the section as a separate category named **File Masks**.



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name : Policy_193

Description : Policy for Section 3A

Objects : Directory

Name	
Directories	● Include ○ Exclude
D:\1.65_TB Data\combined New folder\New folder - Copy ...	

All type of access to "All Files, Drives and selected directories" by all Process will be audited.

Figure 96: Enter Policy Name

You can expand or collapse **File Masks** categories.

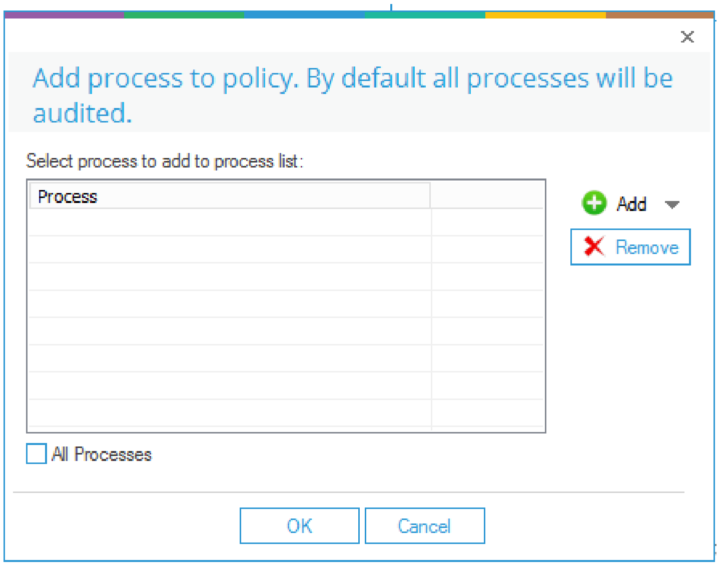
v. You can click **Include** radio button to include the list of added file masks in the auditing, which means that only the listed file masks will be audited.

vi. Click **Exclude** radio button to exclude the list of added file masks from auditing.

After adding the file masks, if you click **Add** button again for adding further file masks then **Modify File Mask** dialog box appears onscreen. Follow the same steps as listed above to add or remove the file masks.

c. **Add Process:** Follow the steps below to add the processes.

i. Select **Process** in the drop-down menu of **Objects** and click **OK**. It displays the **Add Process** dialog box:


Add process to policy. By default all processes will be audited.

Select process to add to process list:

Figure 97: Add Processes

If you have checked the **All Processes** option, then all processes running on the File Server will be added. Uncheck this option to add a customized list of processes.

ii. Click the **Add** button to access the following options to add the processes:

- **Manually**: Click this option to add a process manually by providing its name:

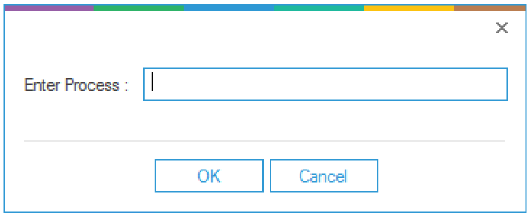
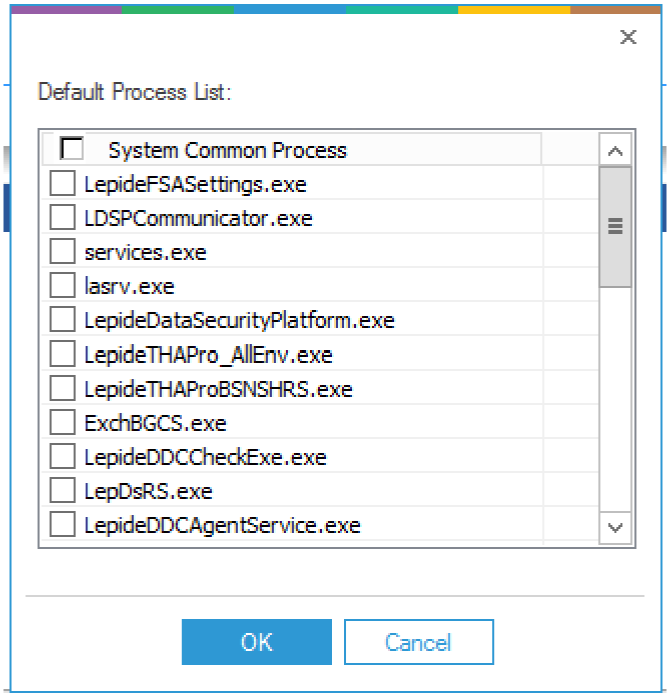


Figure 98: Add Process Manually

Provide the name of the process and click **OK**.
It adds the process and takes you back to **Add Process** dialog box.

- **Default**: Select this option to choose the processes from a predefined list.

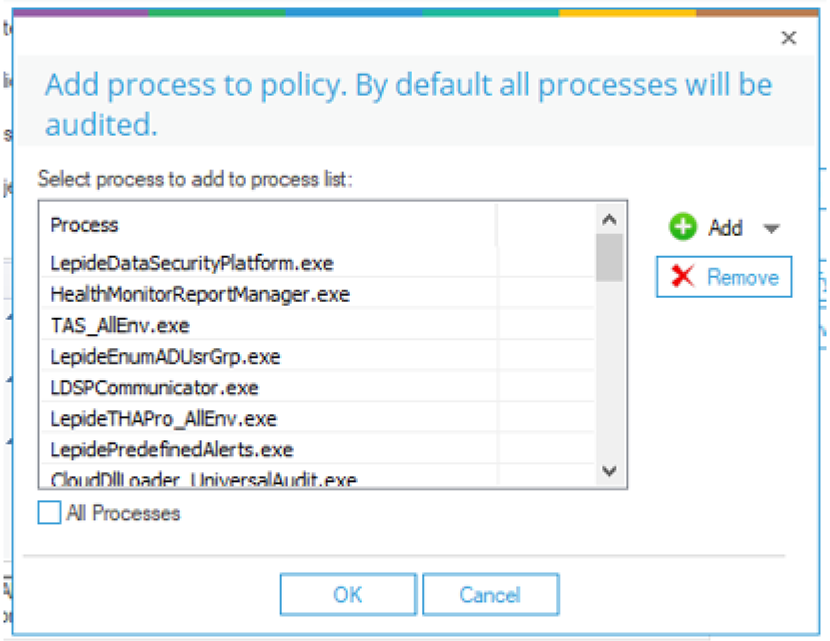


Default Process List:

- □ System Common Process
- □ LepideFSASettings.exe
- □ LDSPCommunicator.exe
- □ services.exe
- □ lasrv.exe
- □ LepideDataSecurityPlatform.exe
- □ LepideTHAPro_AllEnv.exe
- □ LepideTHAProBSNSHRS.exe
- □ ExchBGCS.exe
- □ LepideDDCCheckExe.exe
- □ LepDsRS.exe
- □ LepideDDCAgentService.exe

Figure 99: Add Processes

Check the boxes of those processes, which want to add. Click **OK** after you have made your selection. It takes you back to **Add Process** dialog box that now shows the list of added processes.



Add process to policy. By default all processes will be audited.

Select process to add to process list:

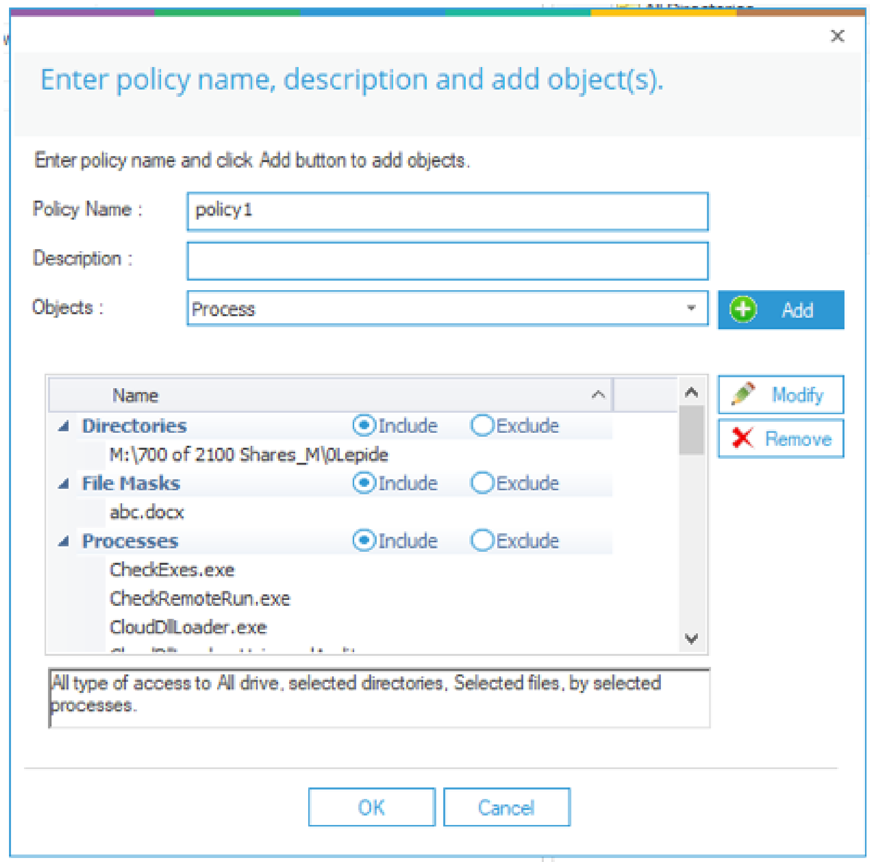
Process
LepideDataSecurityPlatform.exe
HealthMonitorReportManager.exe
TAS_AllEnv.exe
LepideEnumADUsrGrp.exe
LDSPCommunicator.exe
LepideTHAPro_AllEnv.exe
LepidePredefinedAlerts.exe
CloudDllLoader_UniversalAudit.exe

□ All Processes

Figure 100: Add Process to Policy

iii. To delete a process, you can select it and click the **Remove** button.

iv. Click **OK** after you have added the required processes. It takes you back to **Add New Policy** wizard, where all added Processes are listed in the section as a separate category named **Processes**.



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name : policy1

Description :

Objects : Process

Add
Modify
Remove
Name
Directories ● Include ○ Exclude
M:\700 of 2100 Shares_M\0Lepide
File Masks ● Include ○ Exclude
abc.docx
Processes ● Include ○ Exclude
CheckExes.exe
CheckRemoteRun.exe
CloudDllLoader.exe
OK
Cancel

All type of access to All drive, selected directories, Selected files, by selected processes.

Figure 101: List of added processes

v. You can expand or **collapse** the **Processes** categories.

vi. You can click the **Include** radio button to include the list of added processes in the auditing, which means that only the listed processes will be audited.

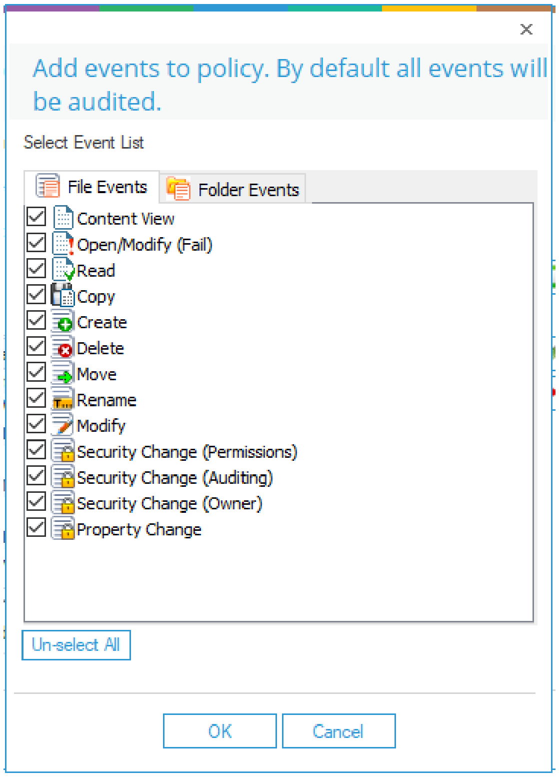
vii. Click the **Exclude** radio button to exclude the list of added processes from auditing.

viii. Click the **Modify** button to modify a process. Follow the same steps as listed above to Modify the processes.

ix. Click the **Remove** button to remove a process

d. **Add Event**: Follow the steps below to add events.

i. Click the **Add** button to access the following dialog box, which has two tabs, File Events and Folder Events:



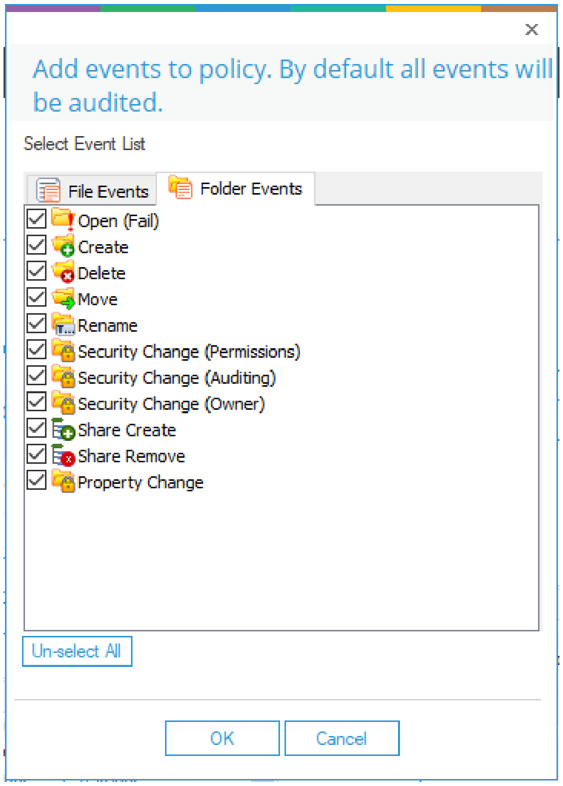
Add events to policy. By default all events will be audited.

Select Event List

File Events | Folder Events

☑ Content View
☑ Open/Modify (Fail)
☑ Read
☑ Copy
☑ Create
☑ Delete
☑ Move
☑ Rename
☑ Modify
☑ Security Change (Permissions)
☑ Security Change (Auditing)
☑ Security Change (Owner)
☑ Property Change

Figure 103: Add File Event



Add events to policy. By default all events will be audited.

Select Event List

File Events | Folder Events

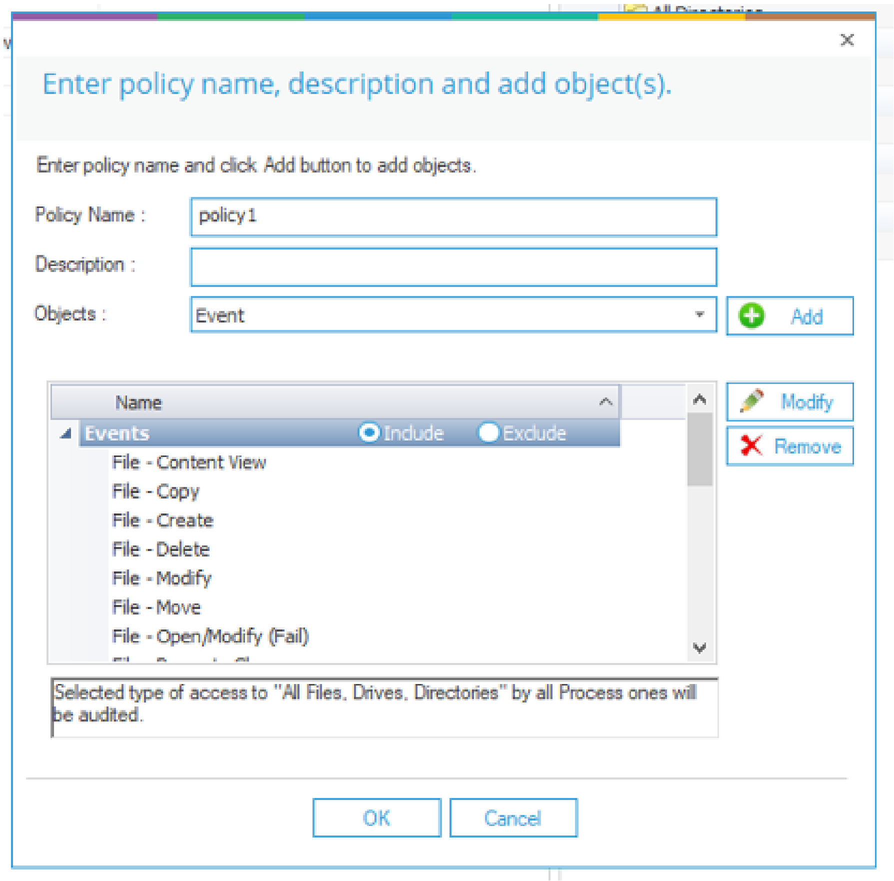
☑ Open (Fail)
☑ Create
☑ Delete
☑ Move
☑ Rename
☑ Security Change (Permissions)
☑ Security Change (Auditing)
☑ Security Change (Owner)
☑ Share Create
☑ Share Remove
☑ Property Change

Figure 102: Add Folder Event

ii. In both tabs, you can check the boxes of the events to be added.

iii. You can uncheck the events, which you do not want to add.

iv. Click **OK** after you have selected the required events. It takes you back to **Add New Policy** wizard, where all added events are listed in the section as a separate category named **Events**.



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name : policy1

Description :

Objects : Event

Name
Events ● Include ○ Exclude
File - Content View
File - Copy
File - Create
File - Delete
File - Modify
File - Move
File - Open/Modify (Fail)

Selected type of access to "All Files, Drives, Directories" by all Process ones will be audited.

Figure 104: List of Added Events

v. You can expand or collapse **Events** categories.

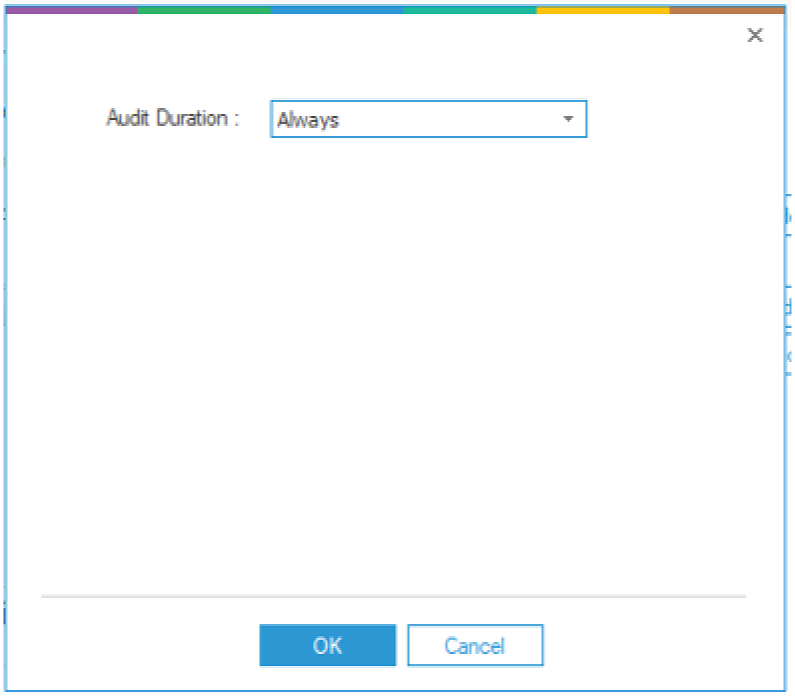
vi. You can click **Include** radio button to include the list of added events in the auditing, which means that only the listed events will be audited.

vii. Click Exclude radio button to exclude the list of added events from auditing.

After adding the events, if you click **Add** button again for events, then **Modify Event** dialog box appears onscreen. Follow the same steps as listed above to add or remove the events.

e. **Add Monitoring Time**: Follow the steps below to add monitoring time.

i. Select **Monitoring Time** in the **Objects** drop-down menu and click **Add** button to access the following dialog box:

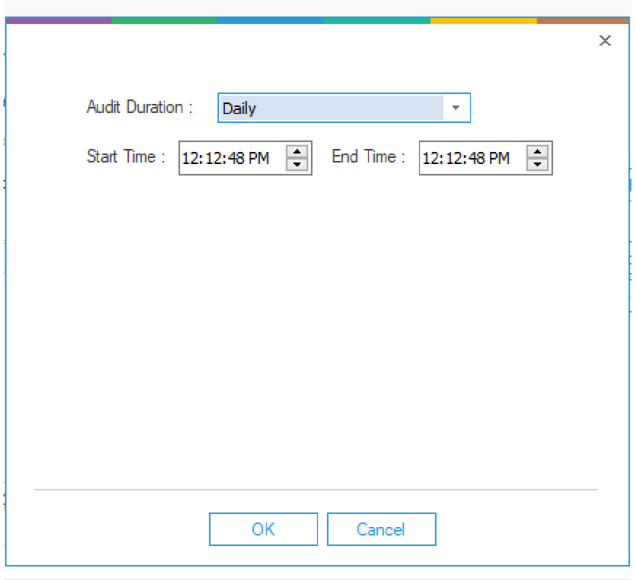


Audit Duration : Always

Figure 105: Add Monitoring Time

ii. Select any of the following options in the drop-down menu.

- **Always**: Select this option to audit always.
- **Daily**: Select this option to audit daily. You need to provide the start and end time for the auditing.

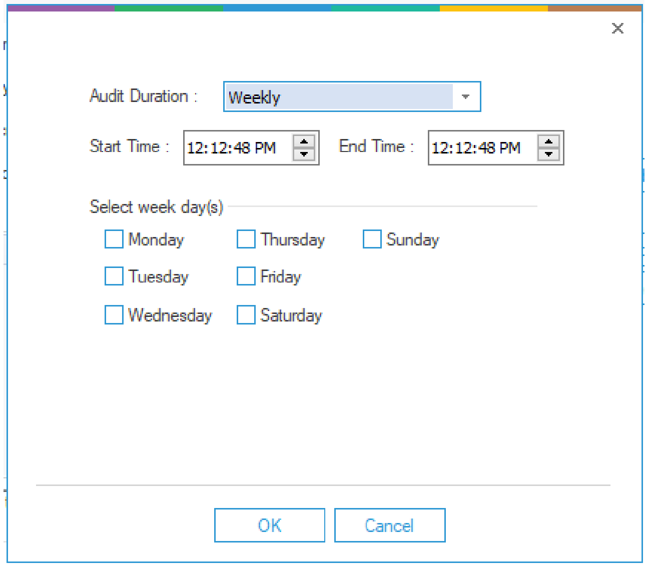


Audit Duration : Daily

Start Time : 12:12:48 PM End Time : 12:12:48 PM

Figure 106: Add Daily Monitoring Time

- **Weekly**: Select this option to audit on a weekly basis.



Audit Duration : Weekly

Start Time : 12:12:48 PM End Time : 12:12:48 PM

Select week day(s)

☐ Monday ☐ Thursday ☐ Sunday

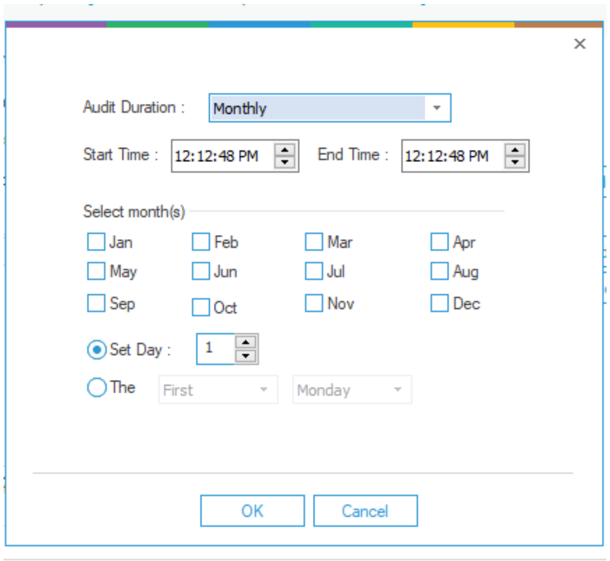
☐ Tuesday ☐ Friday

☐ Wednesday ☐ Saturday

Figure 107: Add Weekly Monitoring Time

Define the start and date time. Select the days on which the auditing will be performed.

- **Monthly**: Select this option to audit monthly.



Audit Duration : Monthly

Start Time : 12:12:48 PM End Time : 12:12:48 PM

Select month(s)

□ Jan □ Feb □ Mar □ Apr
□ May □ Jun □ Jul □ Aug
□ Sep □ Oct □ Nov □ Dec

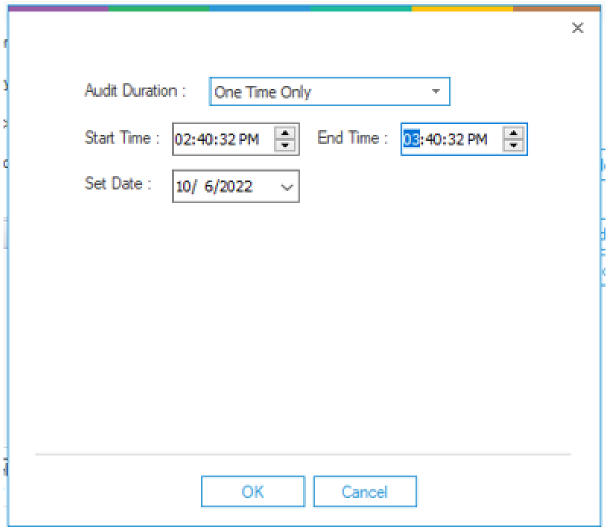
● Set Day : 1

○ The First Monday

Figure 108: Add Monthly Monitoring Time

Define the start and end time for auditing. Select the months and define the day on which the auditing will be performed.

- **One Time Only:** Select this option to run the auditing only once at the selected date and time.



Audit Duration : One Time Only

Start Time : 02:40:32 PM End Time : 03:40:32 PM

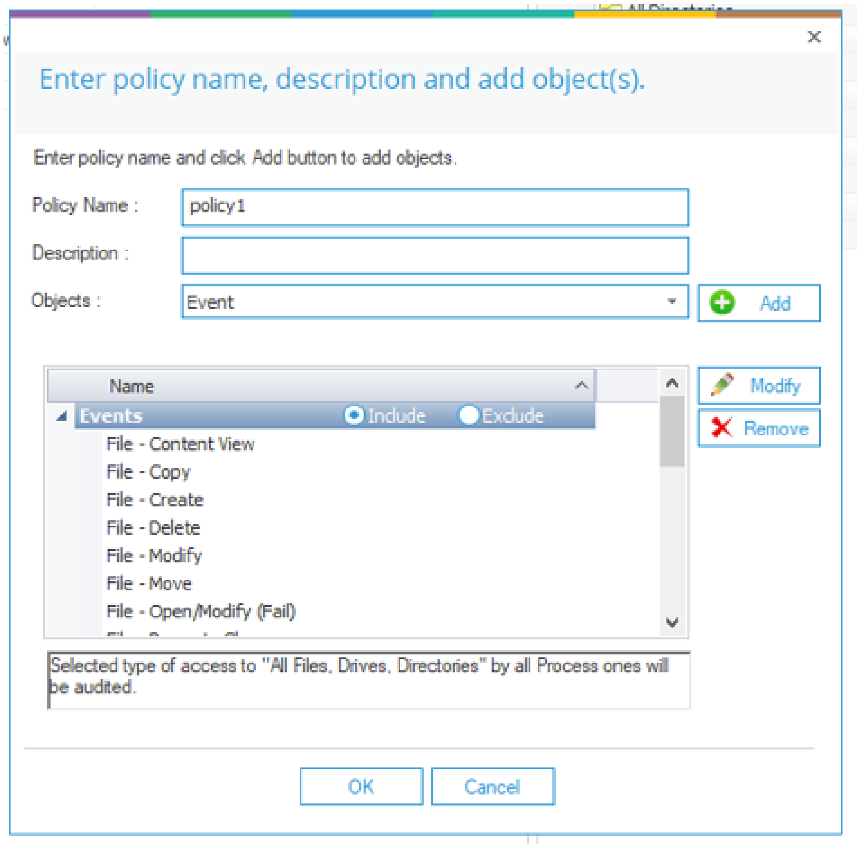
Set Date : 10/ 6/2022

Figure 109: Add One-Time Monitoring

iii. Select the required option and provide the necessary input for it as explained above.

iv. Click **OK** to add the selected monitoring time. It takes you back to **Add New Policy** wizard, which now shows the added monitoring time.

6. After you have added the required objects of the different categories such as directories, file masks, processes, and events, you can now select whether or not to include the entire category in the auditing.



Enter policy name, description and add object(s).

Enter policy name and click Add button to add objects.

Policy Name : policy1

Description :

Objects : Event

Name

Events ● Include ○ Exclude

File - Content View
File - Copy
File - Create
File - Delete
File - Modify
File - Move
File - Open/Modify (Fail)

Selected type of access to "All Files, Drives, Directories" by all Process ones will be audited.

Figure 110: Added Objects in Different Categories

7. The defined monitoring time specifies when the auditing will be done.
8. You can select a category and click **Remove** button to remove it from the auditing list.
9. Click **OK** to create the new audit policy.
10. If the notification appears, then you must update the agent as well.

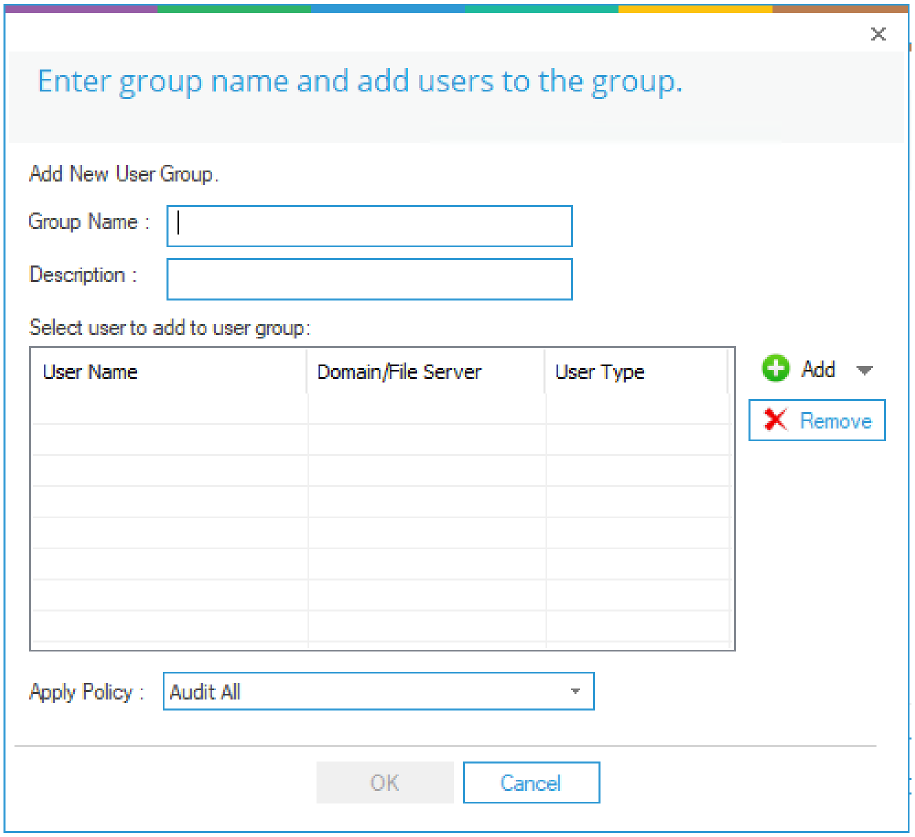
NOTE: You can follow the above similar steps to modify an existing user-created audit policy. The software also allows you deleting an audit policy.

11 Add User Group

You can create **Users Groups** of the selected users in an organization to apply similar policies over the groups. With the User Groups Section, you can create a group of individual users. The users of the user group are assigned a common policy and the users added to the User Group List are by default added to the User List.

Click **User Group** option on the Left Panel to add, modify, or delete the user group. Follow the steps below to add a new user group.

1. Click ⊕ icon, **Add New User Group** dialog appears.
2. Enter the name and description of the new user group.



Enter group name and add users to the group.

Add New User Group.

Group Name :

Description :

Select user to add to user group:

User Name	Domain/File Server	User Type

Apply Policy : Audit All

Figure 111: Add User

3. Click **Add** button and select any of the following options to add the users.

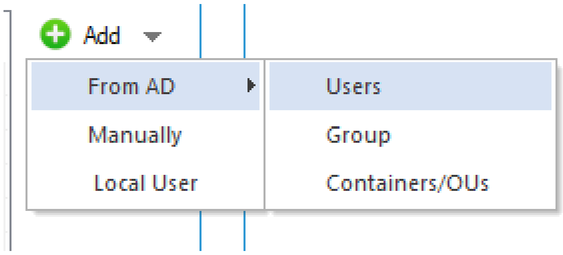
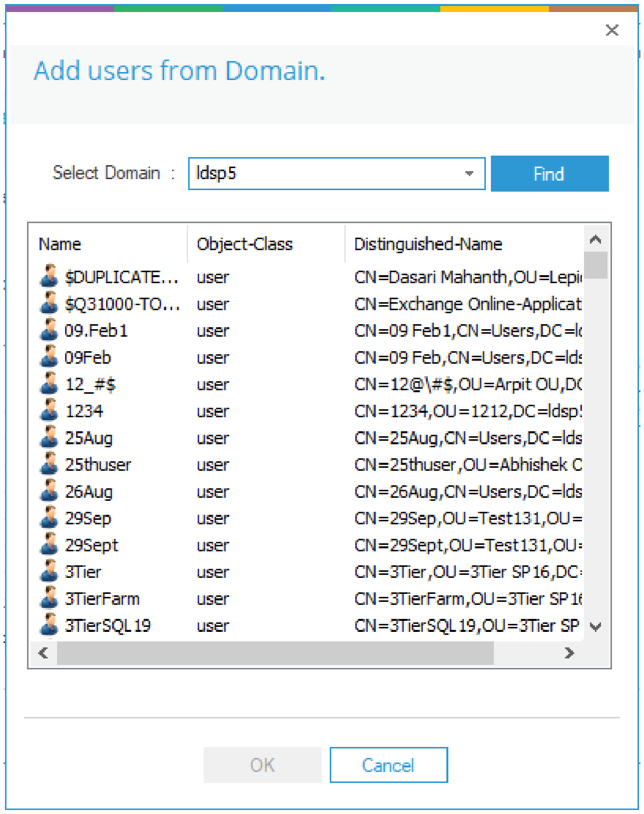


Figure 112: Options to add the user accounts

a. **From AD:** Select this option to obtain the users from Active Directory to form a user group. It contains the following options.

i. **Users**: You can select this option to add the users of Active Directory.


Add users from Domain.

Select Domain : ldsp5

Find

Name	Object-Class	Distinguished-Name
$DUPLICATE…	user	CN=Dasari Mahanth,OU=Lepi
$Q31000-TO…	user	CN=Exchange Online-Applicat
09.Feb1	user	CN=09 Feb1,CN=Users,DC=l
09Feb	user	CN=09 Feb,CN=Users,DC=lds
12_#$	user	CN=12@\#$,OU=Arpit OU,DC
1234	user	CN=1234,OU=1212,DC=ldsp!
25Aug	user	CN=25Aug,CN=Users,DC=lds
25thuser	user	CN=25thuser,OU=Abhishek C
26Aug	user	CN=26Aug,CN=Users,DC=lds
29Sep	user	CN=29Sep,OU=Test131,OU=
29Sept	user	CN=29Sept,OU=Test131,OU=
3Tier	user	CN=3Tier,OU=3Tier SP16,DC=
3TierFarm	user	CN=3TierFarm,OU=3Tier SP16
3TierSQL19	user	CN=3TierSQL19,OU=3Tier SP

OK Cancel

Figure 113: Add users from Active Directory

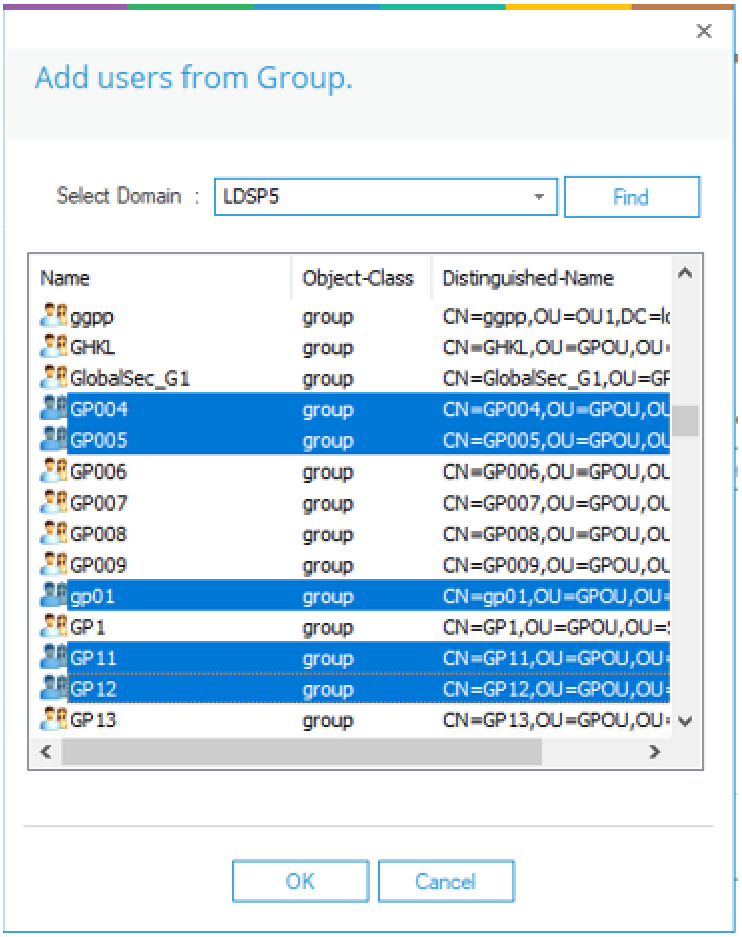
Follow the steps below to add the users:

- Select the domain from the drop-down menu or type a domain name manually.
- Click **Find** to list all available users.

  You can tap and hold CTRL button to select multiple users.
- Click **OK** to add the users.

It takes you back to **Add User** wizard, which now shows the list of added users.

ii. **Groups**: You can select this option to add the users from a group.



Add users from Group.

Select Domain : LDSP5

Name	Object-Class	Distinguished-Name
ggpp	group	CN=ggpp,OU=OU1,DC=l
GHKL	group	CN=GHKL,OU=GPOU,OU
GlobalSec_G1	group	CN=GlobalSec_G1,OU=GF
GP004	group	CN=GP004,OU=GPOU,OL
GP005	group	CN=GP005,OU=GPOU,OL
GP006	group	CN=GP006,OU=GPOU,OL
GP007	group	CN=GP007,OU=GPOU,OL
GP008	group	CN=GP008,OU=GPOU,OL
GP009	group	CN=GP009,OU=GPOU,OL
gp01	group	CN=gp01,OU=GPOU,OU
GP1	group	CN=GP1,OU=GPOU,OU=
GP11	group	CN=GP11,OU=GPOU,OU
GP12	group	CN=GP12,OU=GPOU,OU
GP13	group	CN=GP13,OU=GPOU,OU

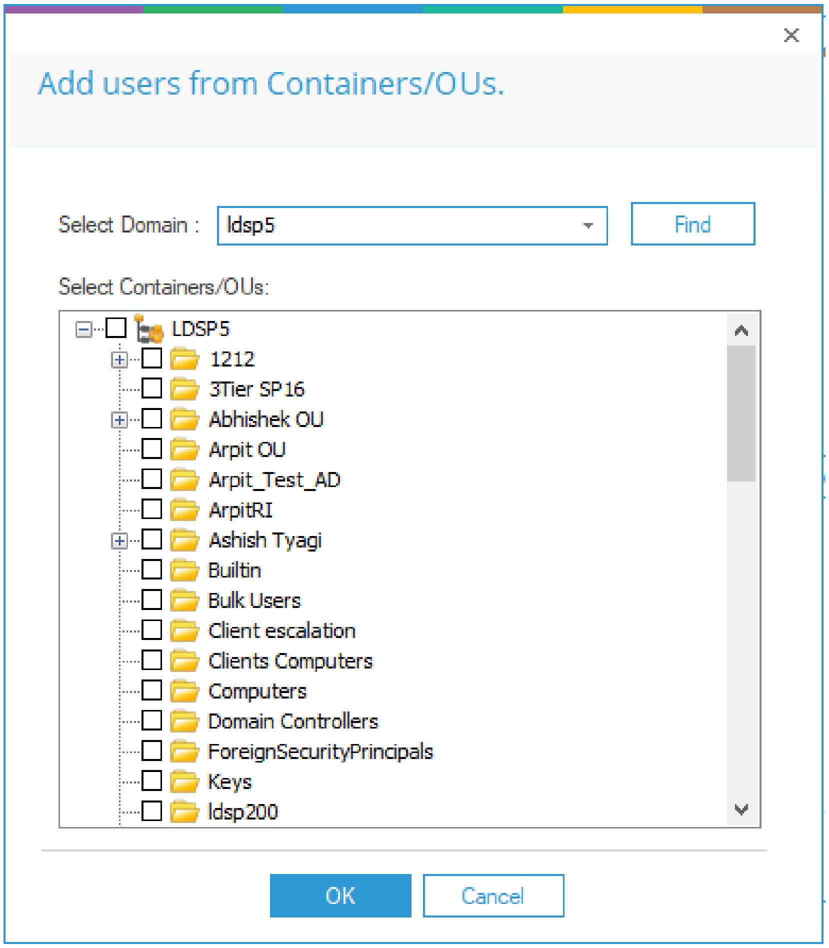
Figure 114: Select the Groups

Follow the steps below to select the group. All users in the selected group will be added.

- Select the domain from the drop-down menu or type a domain name manually.
- Click **Find** to list all available groups.
- You can tap and hold **CTRL** key to select the multiple groups.
- Click **OK** to add the groups.

It takes you back to **Add User** wizard, which now shows the list of users added from the selected group.

iii. Containers/OUs: You can select this option to add the users from a container or organizational unit.



Add users from Containers/OUs.

Select Domain : ldsp5

Select Containers/OUs:

- □ LDSP5
  - □ 1212
  - □ 3Tier SP16
  - □ Abhishek OU
  - □ Arpit OU
  - □ Arpit_Test_AD
  - □ ArpitRI
  - □ Ashish Tyagi
  - □ Builtin
  - □ Bulk Users
  - □ Client escalation
  - □ Clients Computers
  - □ Computers
  - □ Domain Controllers
  - □ ForeignSecurityPrincipals
  - □ Keys
  - □ ldsp200

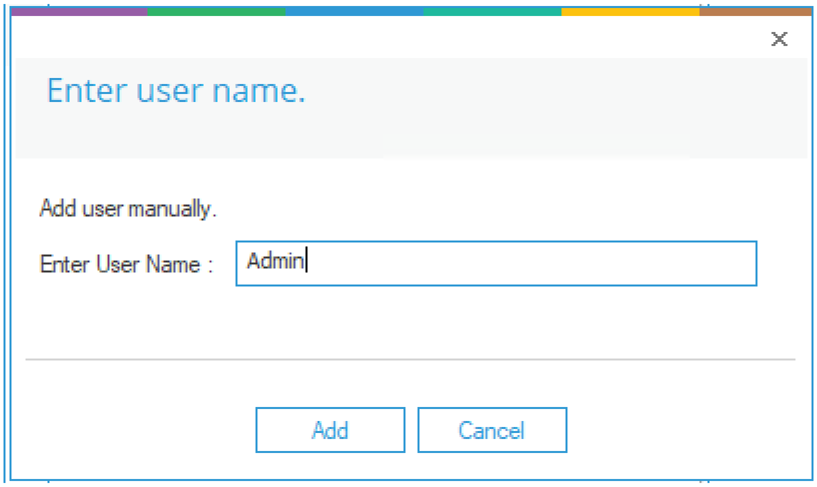
Figure 115: Add Users from the Container or Organizational Unit

Follow the steps below to select the container of which all users will be added.

- Select the domain from the drop-down menu or type a domain name manually.
- Click **Find** to list all available containers or Organizational Units.
- Check the boxes of containers or organizational units, from which you want to add the users.
- Click **OK**.

It takes you back to **Add User** wizard, which now shows the list of users added from the selected container.

b. **Manually**: Select this option to add the user manually by providing its username and name of its domain or computer.



Enter user name.

Add user manually.

Enter User Name : Admin

Figure 116: Add User Manually

Follow the steps below to add a user manually.

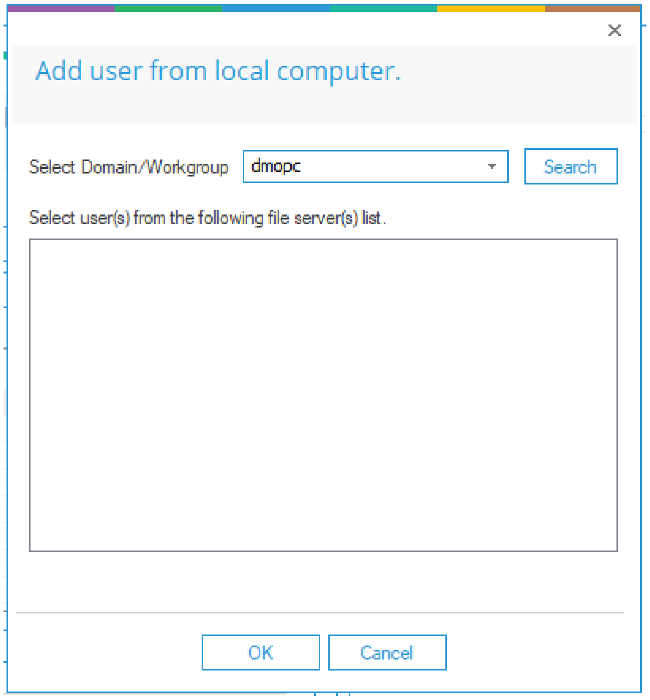
i. Enter the username.

ii. Enter the name of the domain or computer.

iii. Select whether it is a local user or a domain user.

iv. Click **OK** to add the user. It takes you back to **Add User** wizard that shows the added user.

c. **Local User**: Select this option to add the local users.



Add user from local computer.

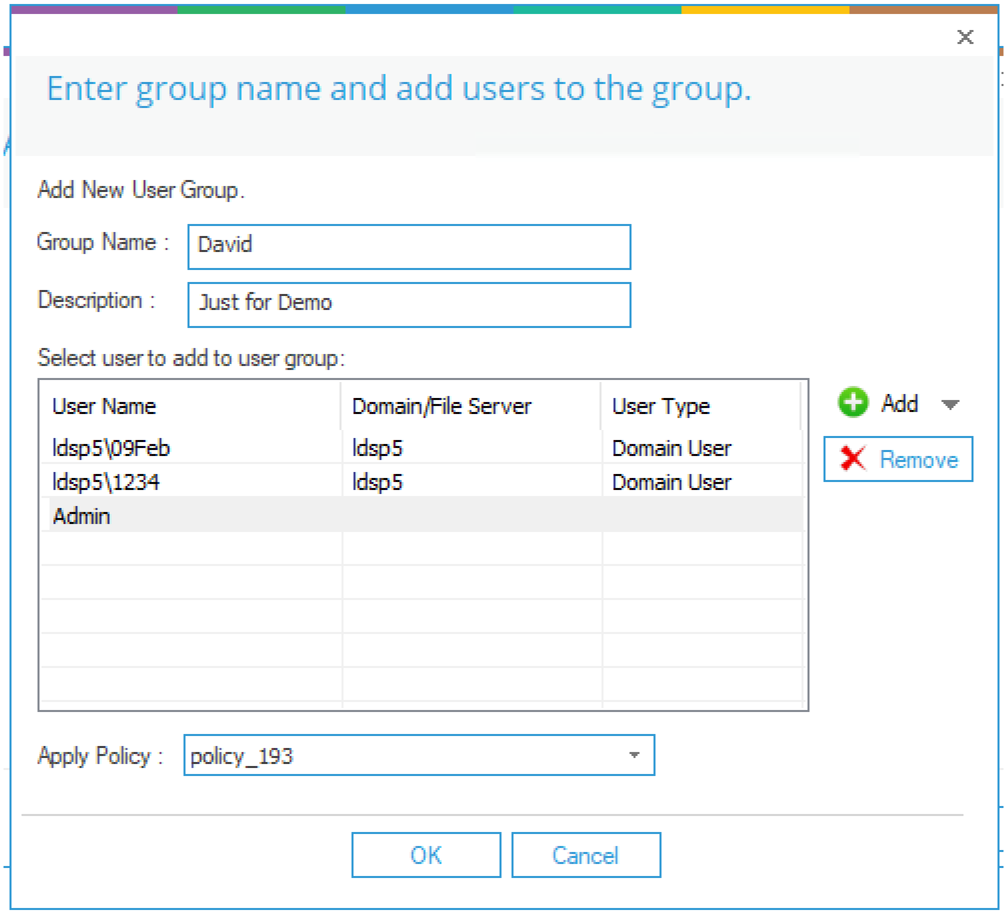
Select Domain/Workgroup dmopc

Select user(s) from the following file server(s) list.

Figure 117: Add Local User

Follow the steps below to add the local user.

- Select the domain from the drop-down menu or type a domain name manually.
- Click **Find** to list all available computers and their local users.
- Check the boxes of the users, which you want to add.
- Click **OK**. It takes you back to **Add User** wizard, which now shows the list of added users.



Enter group name and add users to the group.

Add New User Group.

Group Name : David

Description : Just for Demo

Select user to add to user group:

User Name	Domain/File Server	User Type
ldsp5\09Feb	ldsp5	Domain User
ldsp5\1234	ldsp5	Domain User
Admin		

Apply Policy : policy_193

Figure 118: List of Added Users

4. To remove the user(s), you can select the user(s) and click **Remove** button.
5. You can use the drop-down menu of **Apply Policy** to select the audit policy applicable for the added users. It lists three default audit policies (Audit all, audit shares only, and audit all but shares) and all customized audit policies created in the software.
6. Click **OK**. It creates the user group for the selected policy.
7. The notification appears on screen to update the agent. You have to update the agent to make the modifications in the auditing of the File server.

NOTE: Perform the same steps, mentioned above, to modify an existing user group. The software also allows you deleting a user group.

12 Support

If you are facing any issues whilst installing, configuring, or using the solution, you can connect with our team using the contact information below.

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91(0)-991-085-4291

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

13 Trademarks

Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.

Microsoft®, Active Directory®, Group Policy Object®, Exchange Server®, Exchange Online®, SharePoint®, and SQL Server® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

NetApp® is a trademark of NetApp, Inc., registered in the U.S. and/or other countries.

Figure 1: Component Management Window 4
Figure 2: File Server Console 5
Figure 3: Option to add File Server 5
Figure 4: Add File Server Wizard 6
Figure 5: Add File Server from Domain 7
Figure 6: Enter File Server Details 8
Figure 7: SQL Server Details........ 9
Figure 8: Auditing Agent is Installed 10
Figure 9: Option to Create a Rule........ 11
Figure 10: Highlighting Group Policies for NetApp Filer........ 12
Figure 11: Group Policy Management Editor........ **Error! Bookmark not defined.**
Figure 12: Option to Add NetApp 7-Mode File Server 13
Figure 13: Select File Server Type........ 14
Figure 14: Select a NetApp Filer 14
Figure 15: SQL Server Details to add NetApp Filer........ 15
Figure 16: NetApp Agent Information 16
Figure 17: List of Changes to be made for Auditing NetApp Filer........ 18
Figure 18: Installing the Agent for NetApp Filer 19
Figure 19: Option to Add File Server........ 19
Figure 20: Wizard to Add NetApp Cluster Mode 20
Figure 21: Audit Log Configuration Settings 21
Figure 22: Commands to Set Auditing and Show its Status........ 23
Figure 23: Commands to Set Auditing and Show its Status........ 23
Figure 24: Manual Auditing Selected 24
Figure 25: Audit Log Message........ 24
Figure 26: Selected Automatic Auditing for NetApp 25
Figure 27: Error Message while Enabling Automatic Auditing........ 26
Figure 28: SQL Server Details to Add NetApp Cluster Mode 27
Figure 29: Install Agent on NetApp Cluster Mode........ 28
Figure 30: Starting Add Rule to the File Server Wizard........ 28
Figure 31: Message to Restart the Software........ 29
Figure 32: File Server Management........ 29
Figure 33: Displaying the Added File Servers 30
Figure 34: Component Management Window 31
Figure 35: File Server Console 32
Figure 36: Option to add Multiple File Servers........ 32
Figure 37: Add File Server Wizard 33
Figure 38: Add File Server from Domain........ 34
Figure 39: Add File Server from OU 35
Figure 40: Selected File Servers........ 36
Figure 41: File Servers added Manually........ 37
Figure 42: Add File Server Manually 37

Figure 43: Add File Server using IP Range 38
Figure 44: File Servers added using IP Range 38
Figure 45: Add File Server using CSV File 39
Figure 46: Add File Server using CSV File 40
Figure 47: Enter User Name Details 41
Figure 48: SQL Server Details 41
Figure 49: Enter the details of SQL Server and database 41
Figure 50: Auditing Agent is Installed 42
Figure 51: Option to Create a Rule 43
Figure 52: Component Management Window 43
Figure 53: File Server Console 44
Figure 54: Option to add Multiple File Servers 44
Figure 55: Add File Server Wizard 45
Figure 56: Enter File Server Name 46
Figure 57: SQL Server Details 47
Figure 58: Enter the details of SQL Server and database 47
Figure 59: Enter Agent Server Details 48
Figure 60: Status of Agent Installation 49
Figure 61: Option to Create a Rule 49
Figure 62: Component Management Window 50
Figure 63: File Server Console 51
Figure 64: Option to add Multiple File Servers 51
Figure 65: Add NetApp File Server Wizard 52
Figure 66: NetApp Filer to be Added 52
Figure 67: Add NetApp Filer with Agent IP Selected 53
Figure 68: SQL Server Details 54
Figure 69: Enter the details of SQL Server and database 54
Figure 70: Status of Agent Installation 55
Figure 71: Option to Create a Rule 56
Figure 72: Option to Add Rule 56
Figure 73: Settings Console 57
Figure 74: Create New Rule 57
Figure 75: Audit Policies 58
Figure 76: Select Policy Type 60
Figure 77: Add Users to Audit 61
Figure 78: Add Users to Rule 62
Figure 79: Select User Group from the List 63
Figure 80: Added Users 64
Figure 81: Summary 65
Figure 82: Audit Rule Summary 65
Figure 83: Rules Management 67
Figure 84: Set Priority 67

Figure 85: Audit Policies section....69
Figure 86: Add New Policy Wizard....70
Figure 87: Add Directory....71
Figure 88: Add Directory Manually....71
Figure 89: Scan and Add Directory....72
Figure 90: Add the Default User Directories....73
Figure 91: Displaying the Added Directories....74
Figure 92: List of Added Directories....75
Figure 93: Add Files to Policy....76
Figure 94: Add File Mask Manually....76
Figure 95: Scan and Add....77
Figure 96: Add File Masks....78
Figure 97: Enter Policy Name....79
Figure 98: Add Processes....80
Figure 99: Add Process Manually....80
Figure 100: Add Processes....81
Figure 101: Add Process to Policy....82
Figure 102: List of added processes....83
Figure 103: Add Folder Event....84
Figure 104: Add File Event....84
Figure 105: List of Added Events....85
Figure 106: Add Monitoring Time....86
Figure 107: Add Daily Monitoring Time....87
Figure 108: Add Weekly Monitoring Time....87
Figure 109: Add Monthly Monitoring Time....88
Figure 110: Add One-Time Monitoring....88
Figure 111: Added Objects in Different Categories....89
Figure 112: Add User....90
Figure 113: Options to add the user accounts....91
Figure 114: Add users from Active Directory....91
Figure 115: Select the Groups....92
Figure 116: Add Users from the Container or Organizational Unit....93
Figure 117: Add User Manually....94
Figure 118: Add Local User....95
Figure 119: List of Added Users....96