Lepide

CONFIGURATION GUIDE

WINDOWS FILE SERVER QUICK START GUIDE

Table of Contents

1. Introduction

The Lepide Data Security Platform provides a comprehensive way to provide visibility across Active Directory, Group Policy, Exchange on-premises, M365, SharePoint, SQL Server, Windows File Server, NetApp Filer and every platform which can provide an integration with Syslogs and RestAPI.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for Windows File Servers.

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.

2. Requirements and Prerequisites

2.1 Basic System Requirements

- Required Processor
  - Minimum dual-core processor
  - Recommended quad-core processor
- Required RAM
  - Minimum 8 GB RAM
  - Recommended 16 GB RAM
- Required free disk space
  - Minimum 1 GB
  - Recommended 2 GB
- Network Bandwidth Recommendations:
  - We recommend the use of Giga switches and a Giga Lan adapter on your local network (on-premise) and you should have a Giga network plan supported on Azure as well. The internet

speed is also recommended to be in Giga (the more the better).

- The network speed between on-premise machines and Azure virtual machines should be similar to what we normally have when transferring data between two machine within local network.

- Any of the following 32 bit or 64 bit Windows Operating Systems:
  - Windows Server OS: 2016, 2019 and 2022 (latest)
- Any of the following SQL Servers (local or network hosted) for storing auditing logs:
  - Any SQL Server above and including SQL Server 2016 (standard or enterprise) as per current support from Microsoft
- .NET Framework 4.6.2 developer pack and above

2.2 Supported Servers for Auditing

- Supported Versions: All Windows Servers above Windows Server 2016

2.3 Required User Rights

To install and work with the Lepide Data Security Platform, you need to have appropriate rights to the system where it will be installed. Also, you need to have appropriate rights to access the file server. There are two approaches to configure Windows File Server with Lepide Data Security Platform:

- With Least Privileges
- With Full Privileges

NOTE: To understand the difference in the functionalities being offered with both these approaches please refer to The Principle of Least Privilege Document

2.3.1 Least Privileges

To configure the Lepide Data Security Platform with least privileges the service account requires the following rights:

- A domain user account.

- This account should have Db owner/Db_creator rights over the SQL databases. An SQL account with the mentioned privileges can also be used.
- This account should be a member of the Local Administrators Group on the File Server.
- This account should be a member of the Local Administrators Group on the Lepide Server.
- This account should have List Folder/Read Data, Traverse Folder/Execute File and Read Permissions rights on the Shares which are to be audited.
- This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.
- The SYSTEM account should have Modify rights on the folder where the agent is installed.

2.3.2 Full Privileges

To configure the Lepide Data Security Platform with full privileges the service account requires the following rights:

- Member of Domain Admins Group in Active Directory
- Should have access to the admin$ on the File Servers

2.4 Required SQL Server Rights

- For Windows Authentication: A login for the currently logged on Windows User should exist in SQL Server with the assigned role of dbcreator in SQL server.
- For SQL Authentication: A local SQL account with dbcreator permission.

NOTE: For using SQL authentication, the SQL server should be set to mixed authentication mode.

2.5 Required Ports

The software uses the following ports for different purposes.

1. Lepide Data Security Platform uses the following ports for communication:

    a. Port 389 and Port 636 for LDAP queries.

b. Port 445 for RPCS (Remote Procedure Call Services)

c. Default Port for SQL Server Communication. In most cases, the default port for SQL is 1433.

d. Port 3000 for data transfer between the file server and the Lepide Application Server.

2. Lepide Data Security Platform Web Console uses Port 7778 (HTTP).

3. Lepide Data Security Platform App uses Port 1051.

3. Adding a Windows File Server

After you have installed the Solution and configured Lepide service to run with administrative credentials, you can add a Windows File Server for auditing.

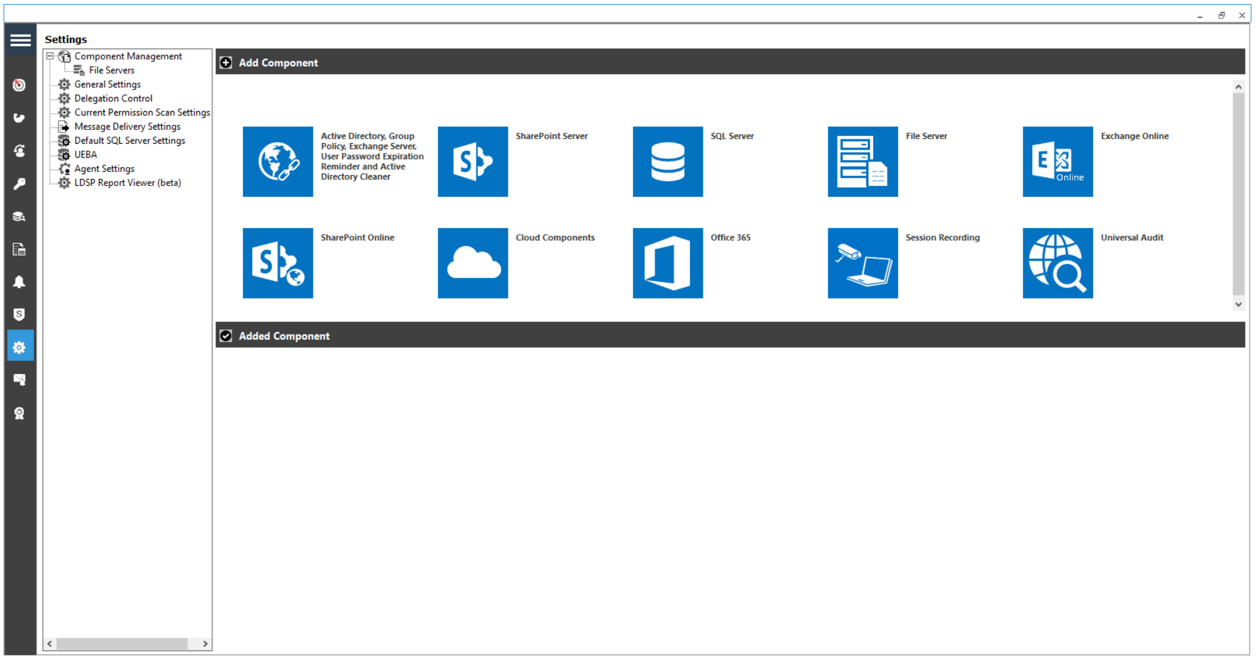
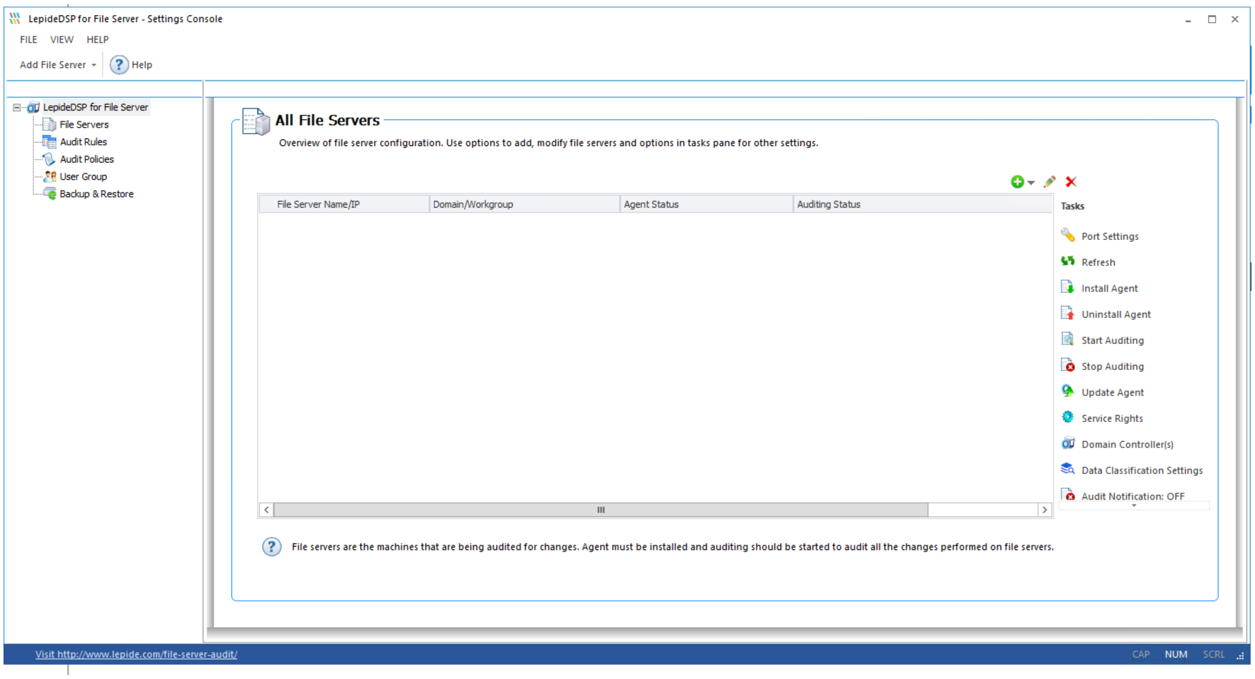


Figure 1: Component Management Window

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

The File Server 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.

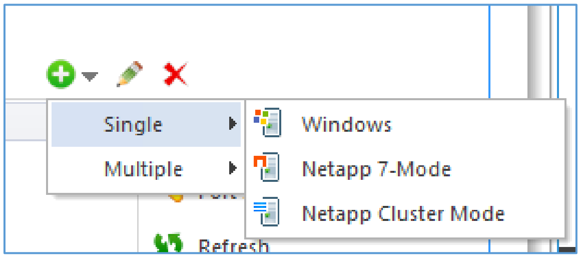
File servers are the machines that are being audited for changes. Agent must be installed and auditing should be started to audit all the changes performed on file servers.

Figure 2: File Server Settings Console

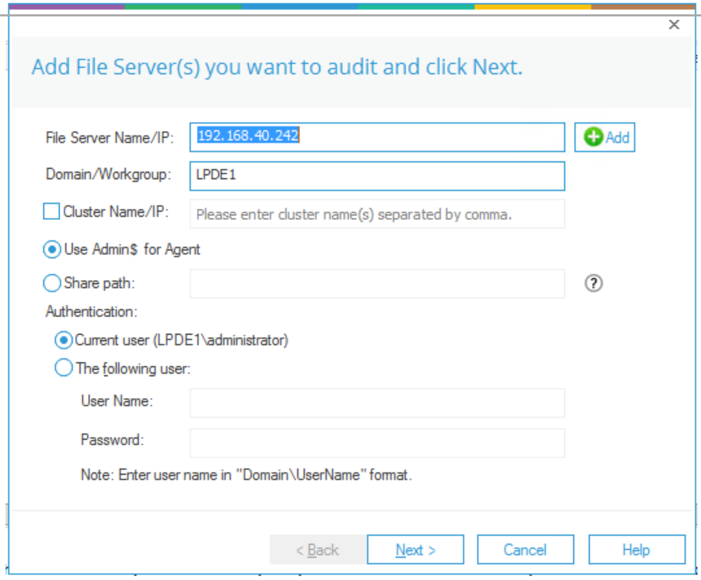
Here, you can click Add File Server icon ⊕▾ on the toolbar to add either of the following file servers:

- Windows File Server
- NetApp Filer

2. Click the Add File Server icon, ⊕▾ select Single then select Windows.



NOTE: This guide only explains the process for addition of a single windows file server. For adding multiple file servers, please refer to our Advanced Windows File Servers Configuration Guide.



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

File Server Name/IP: 192.168.40.242

Domain/Workgroup: LPDE1

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

● Use Admin$ for Agent

○ Share path:

Authentication:

● Current user (LPDE1\administrator)

○ The following user:

User Name:

Password:

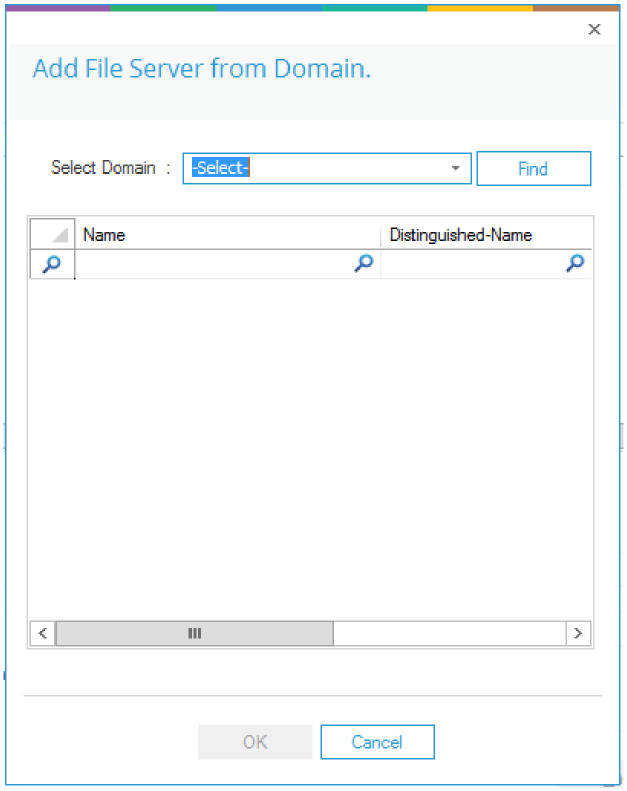
Note: Enter user name in "Domain\UserName" format.

Figure 4: Add File Server Wizard

3. The Add File Server wizard starts.

4. Enter the name or IP Address of the server along with its Domain or Workgroup name.

5. 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.

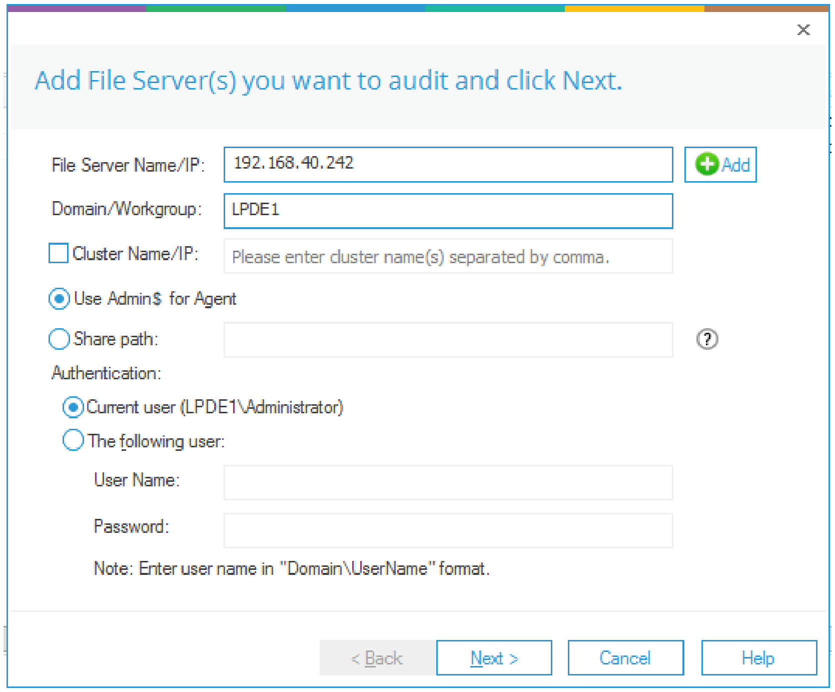
Select Domain : -Select-

Figure 5: Add File Server from Domain

6. Type the name of the domain in the Select Domain Window.
7. Click the Find button to list its computers in the blank area.
8. 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.
9. Select the user with which you want to add the File Server.
10. If you are logged in as a user that has the above rights, then you can select Current User.

11. If the logged in user does not have the required rights, then you must 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: 192.168.40.242

Domain/Workgroup: LPDE1

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

● Use Admin$ for Agent

○ Share path:

Authentication:

● Current user (LPDE1\Administrator)

○ The following user:

User Name:

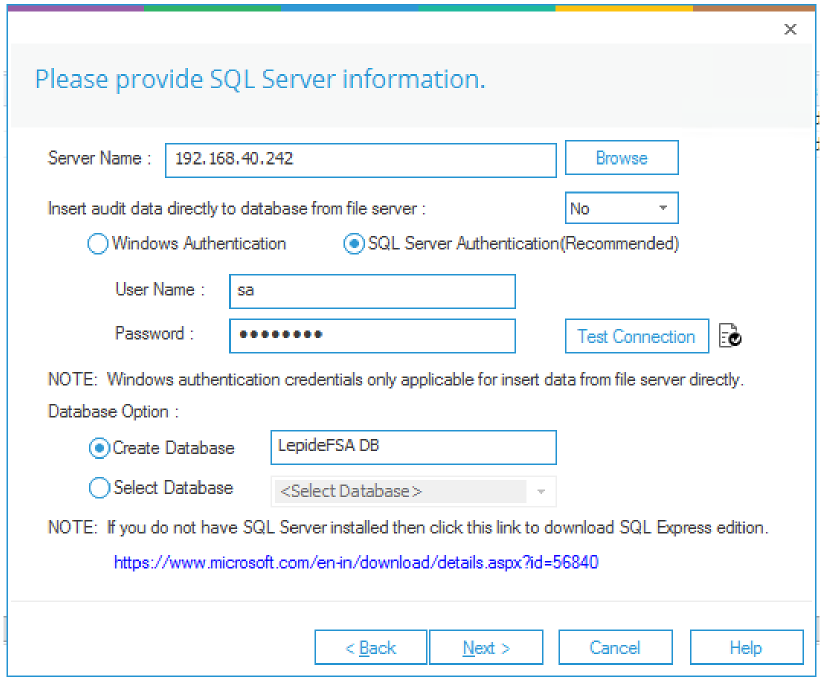
Password:

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

Figure 6: Enter File Server Details

12. After entering the details, click Next.

13. The next step is to provide the SQL Server details:



Please provide SQL Server information.

Server Name : 192.168.40.242

Insert audit data directly to database from file server : No

○ 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.

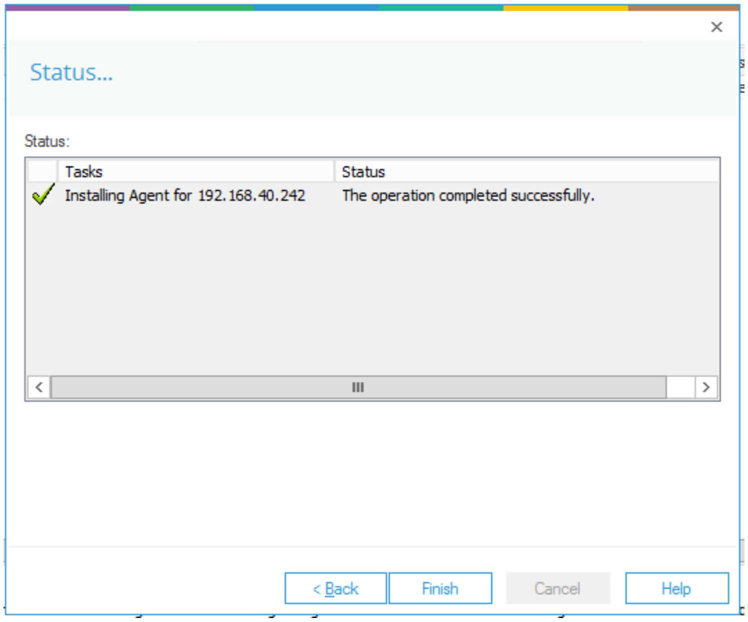
https://www.microsoft.com/en-in/download/details.aspx?id=56840

Figure 7: SQL Server Details

14. Please set the *"Insert audit data directly to database from file server"* option to NO, if the port 1433 is not open from the file server to the SQL server.
15. Type the Server Name or click Browse to select the desired SQL Server.
16. There are two authentication options:
    - Windows Authentication:. Please put in the domain account which has at least dbowner rights on the SQL server.
    - 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.
17. Enter a database name in the Create Database field to create a new database or leave it as default. You can also select an existing database created by Lepide or another application.
18. Click Next to start installing the auditing agent on the Windows File Server.

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



Status...

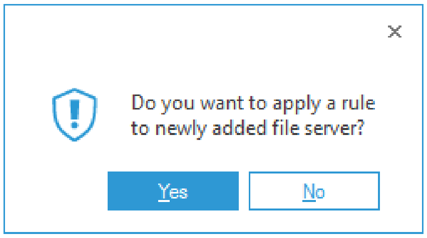
Status:

	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.

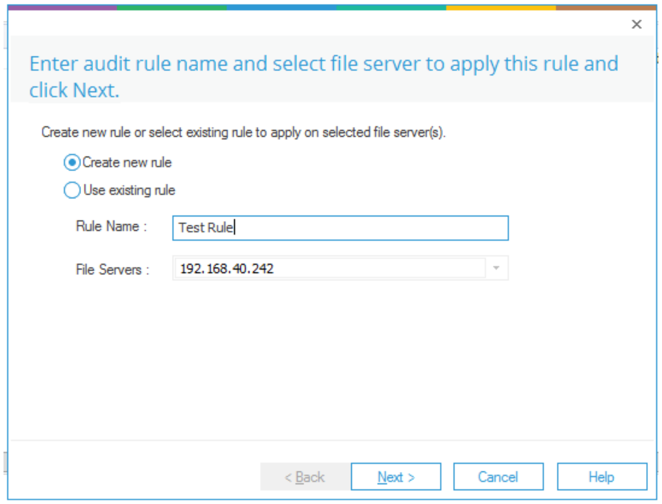
A dialog box is displayed asking whether you want to apply a rule to the newly added file server:



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

Figure 9: Option to Create a Rule

20. Click Yes and create a new rule from the next window.



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

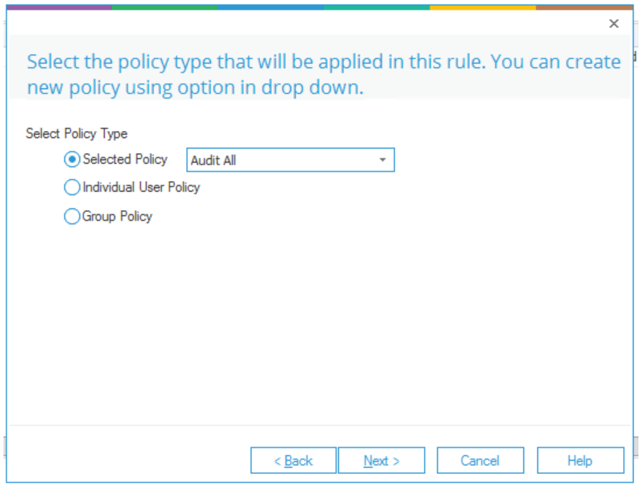
Rule Name : Test Rule

File Servers : 192.168.40.242

Figure 10: Enter Rule Name and Select File Server

21. 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.

22. 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

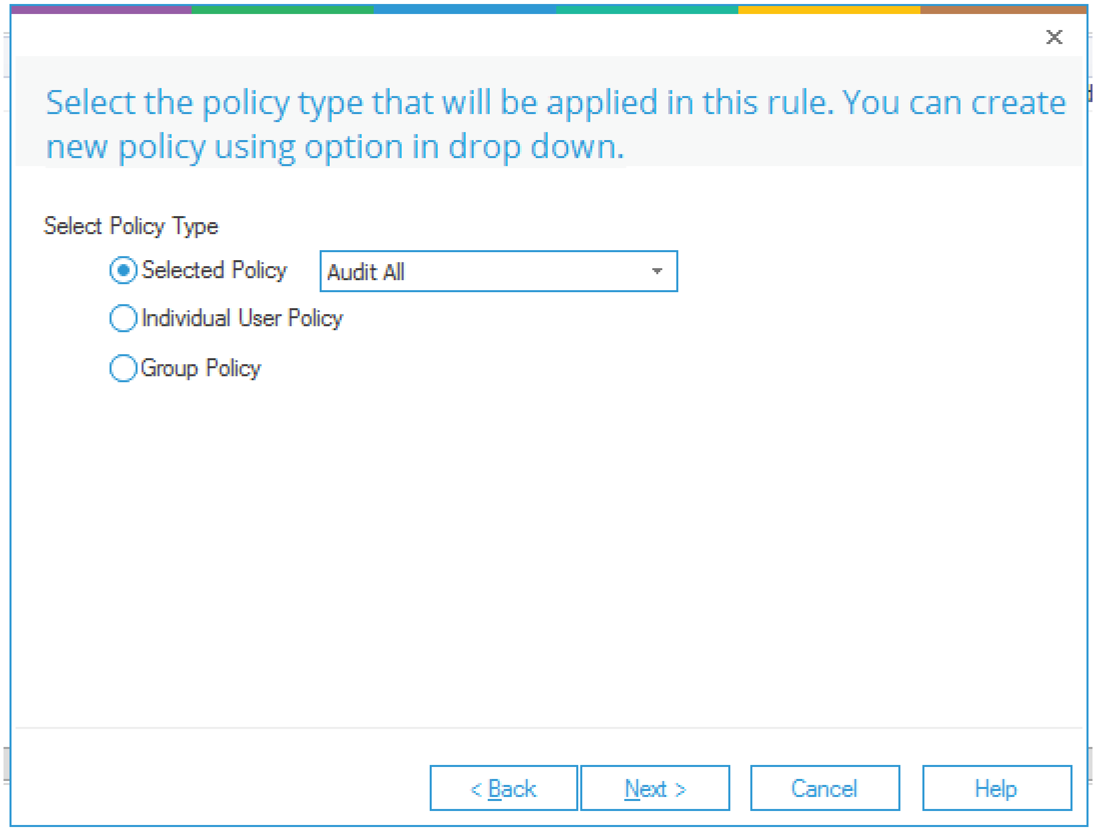
○ Individual User Policy

○ Group Policy

Figure 11: Audit Policies

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 Advanced File Server Configuration Guide.

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

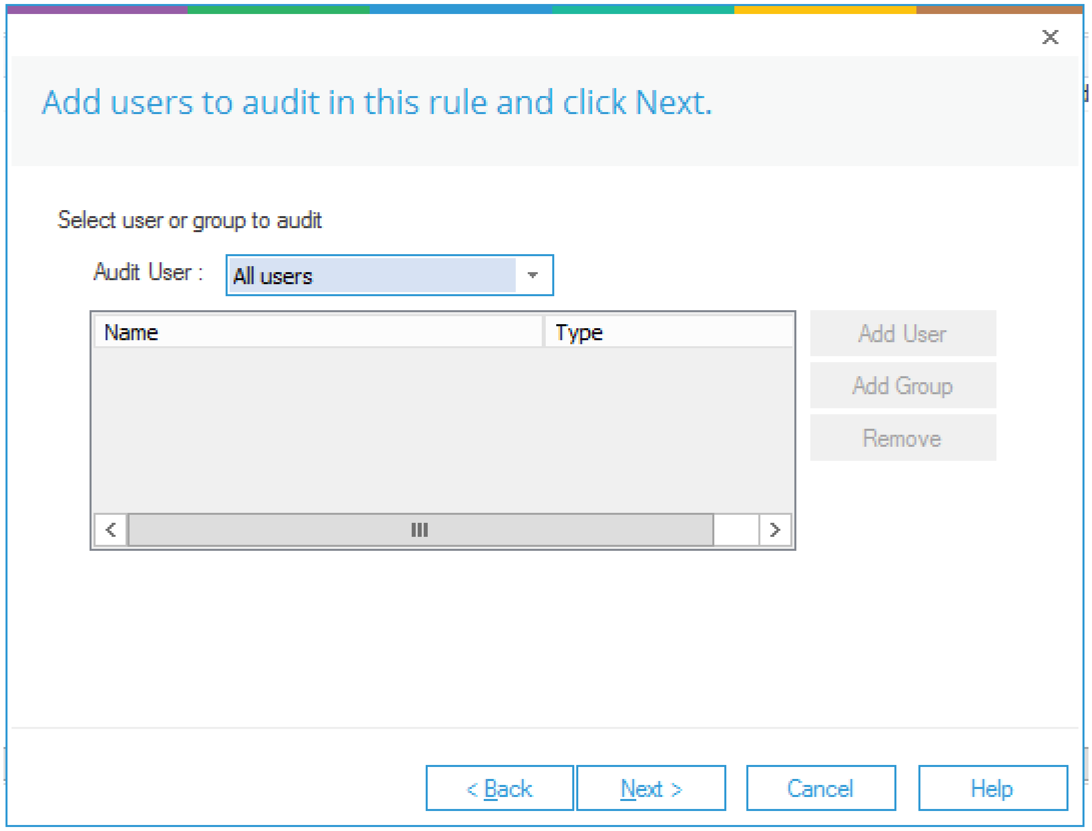
● Selected Policy Audit All

○ Individual User Policy

○ Group Policy

Figure 12: Select Policy Type

23. Click Next



Add users to audit in this rule and click Next.

Select user or group to audit

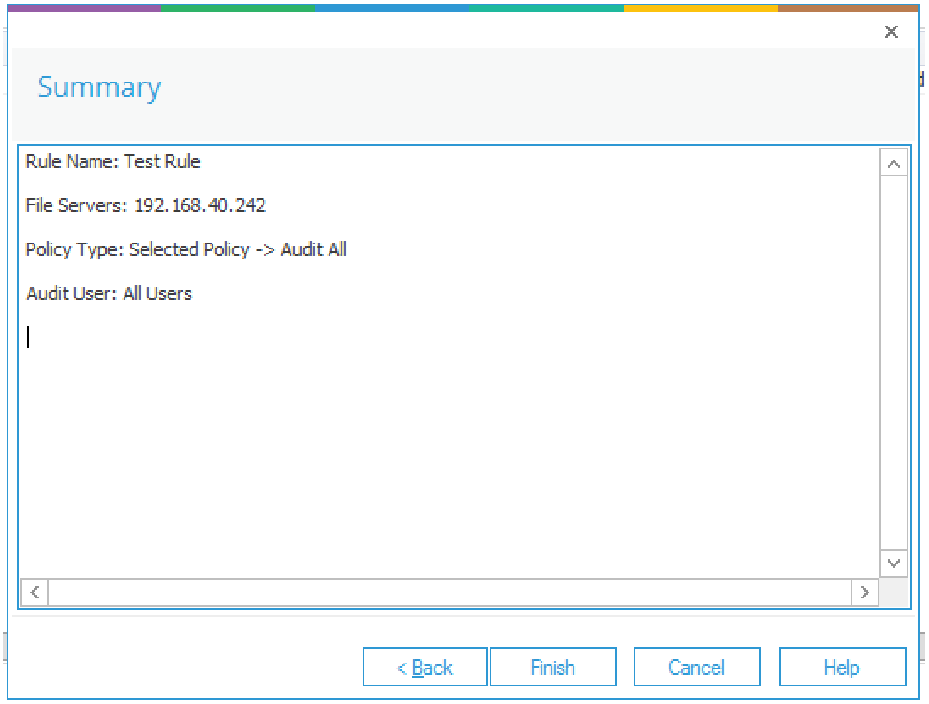
Audit User : All users

Name	Type

Figure 13: Add Users to Audit

24. Select All Users in the Audit User Tab and click Next. The rule is applied to all users in this case.
25. 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 14: Summary

26. Click Finish to complete the process. The newly added audit rule is displayed in the list.
27. 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.

28. After you have created the auditing rules, Restart the main console, and go to the Audit Reports tab in the main panel to view the reports.

4. Support

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

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/.

5. 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.