Lepide

QUICK START GUIDE

ACTIVE DIRECTORY AND GROUP POLICY

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 Active Directory. For information on installation, please see our Installation and Prerequisites Guide. For information on advanced configuration please refer to the Advanced Domain Configuration Guide.

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 Prerequisites to Audit Active Directory

- The Event Viewer for all domain controllers including the primary domain controller should be accessible from the application server.
- The required user rights to add a domain should meet the requirements that are listed in section 2.3.

2.2 Prerequisites to Audit Group Policy Objects

- Windows PowerShell 2.0 and .NET Framework 4.0 should be installed on both the server to be audited and the application server (the server where the Solution will be installed).
- GPMC (Group Policy Management Console) should be installed on the computer where the Solution is installed.

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 Active Directory. There are two approaches to configure Active Directory with Lepide Data Security Platform

- Least Privileges

- 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 membership of the following groups:

- Event Log Readers
- Administrators (on the application server)
- Organization Management (for Exchange auditing)

2.3.2 Full Privileges

To configure the Lepide Data Security Platform with full privileges the service account requires the membership from any of the following groups:

- Domain Admins
- Schema Admins
- Enterprise Admins

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. Port 135 for communication to Event Logs
    d. TCP/5985 (HTTP) and TCP/5986(HTTPS) for Remote PowerShell Communication
    e. Default Port for SQL Server Communication. In most cases, the default port for SQL is 1433.
2. The software also uses the following Microsoft functions, which use different ports:
    a. OpenEventLog, which uses Port 445 and Port 135
    b. ReadEventLog, which uses Port 445 and Port 135
    c. AdsOpenObject, which uses Port 389 and Port 636
3. Lepide Data Security Platform Web Console uses Port 7778 (HTTP).
4. Lepide Data Security Platform App uses Port 1051.

.

3. Adding an Active Directory Component

This guide will take you through the steps to add an Active Directory, Group Policy and Exchange Server component to the solution.

NOTE: Before continuing, ensure that the pre-requisites to audit the domain are met

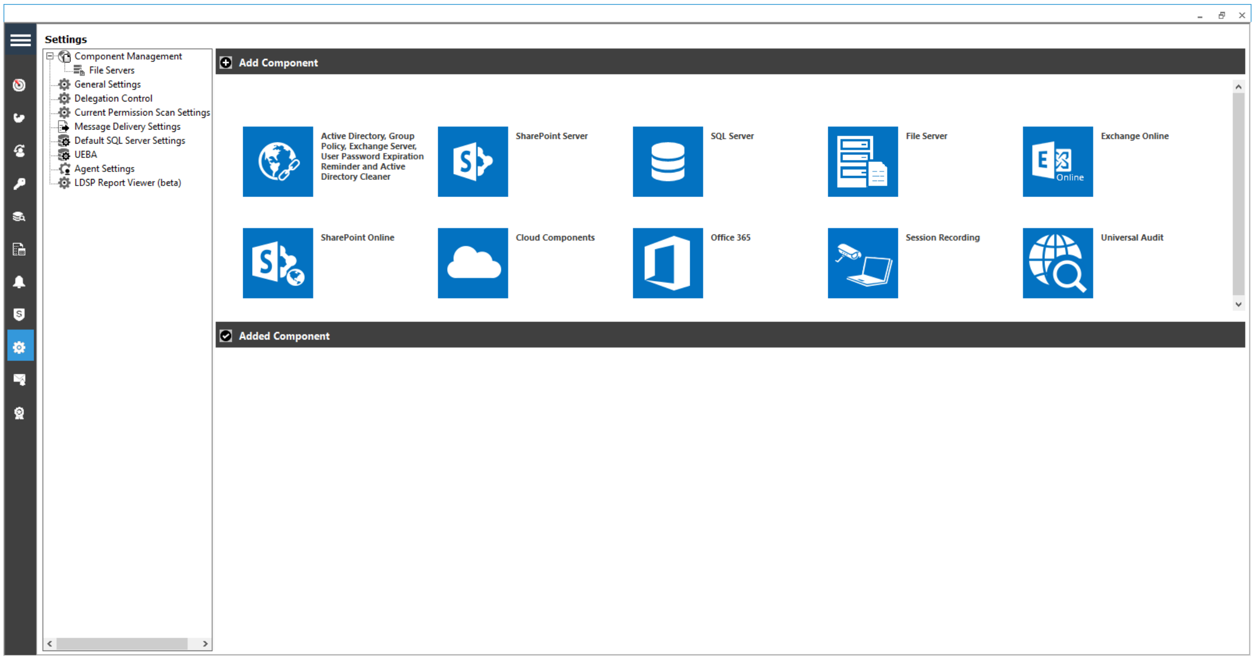


Figure 1: Component Management Window

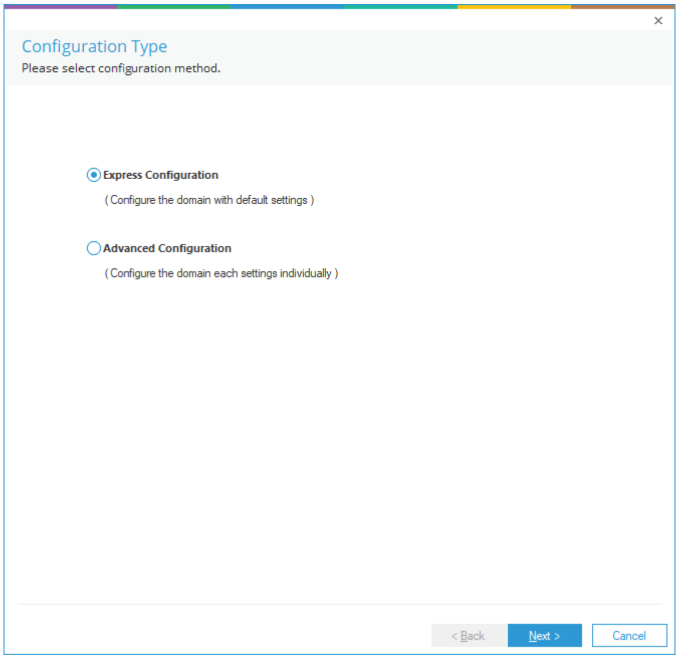
From the Component Management window, click on the icon which says *Active Directory, Group Policy & Exchange* to add these components to the solution.

A wizard will start with two configuration options available for adding a component. These are:

1. **Express Configuration**: Add with minimal recommended settings.

2. **Advanced Configuration**: Add with customizable advanced settings.

3.1 Add a Component with Express Configuration



Configuration Type

Please select configuration method.

● Express Configuration

(Configure the domain with default settings)

○ Advanced Configuration

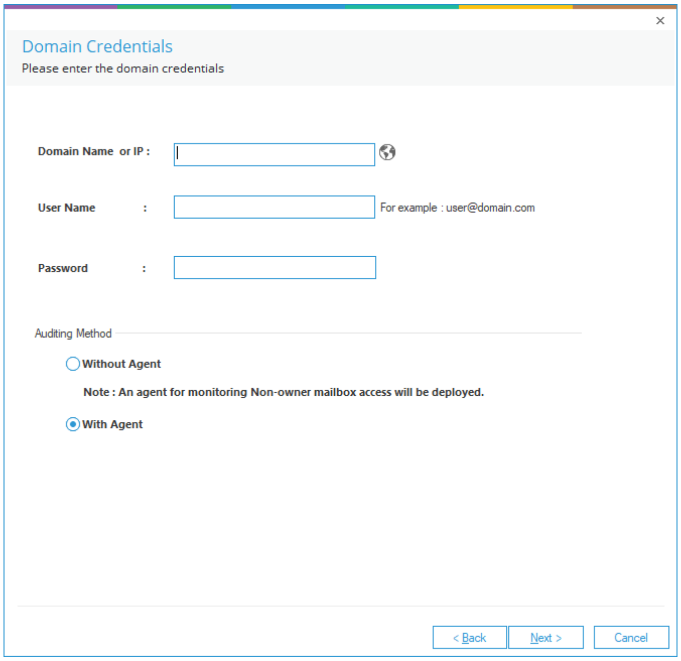
(Configure the domain each settings individually)

Figure 2: Configuration Type

1. From the **Configuration Type** dialog box, select **Express Configuration** and click **Next**
2. This takes you to the **Domain Credentials** dialog box

Domain Credentials

In this section, you will provide details of the component to be added.



Domain Credentials

Please enter the domain credentials

Domain Name or IP :

User Name : For example : user@domain.com

Password :

Auditing Method

○ Without Agent

Note : An agent for monitoring Non-owner mailbox access will be deployed.

● With Agent

Figure 3: Add the Domain Credentials

1. **Domain Name or IP:** Enter the domain name or its IP Address. Click 🌐 to let the solution discover the current domain in which it is installed. This will auto-fill the domain name in the text box.
2. **Username:** Enter the username in the format **Username@domain.com**. Ensure that you provide the complete username with the domain name.
3. **Password:** Enter the correct password for the selected user.
4. **Auditing Method**
   - **Without Agent:** In this approach. there is no need to install agents on the Domain Controllers. The auditing will be done completely agentless by making real time connections to the DCs. The least privilege configuration needs to use this approach as the agent can't be installed with least privilege account.

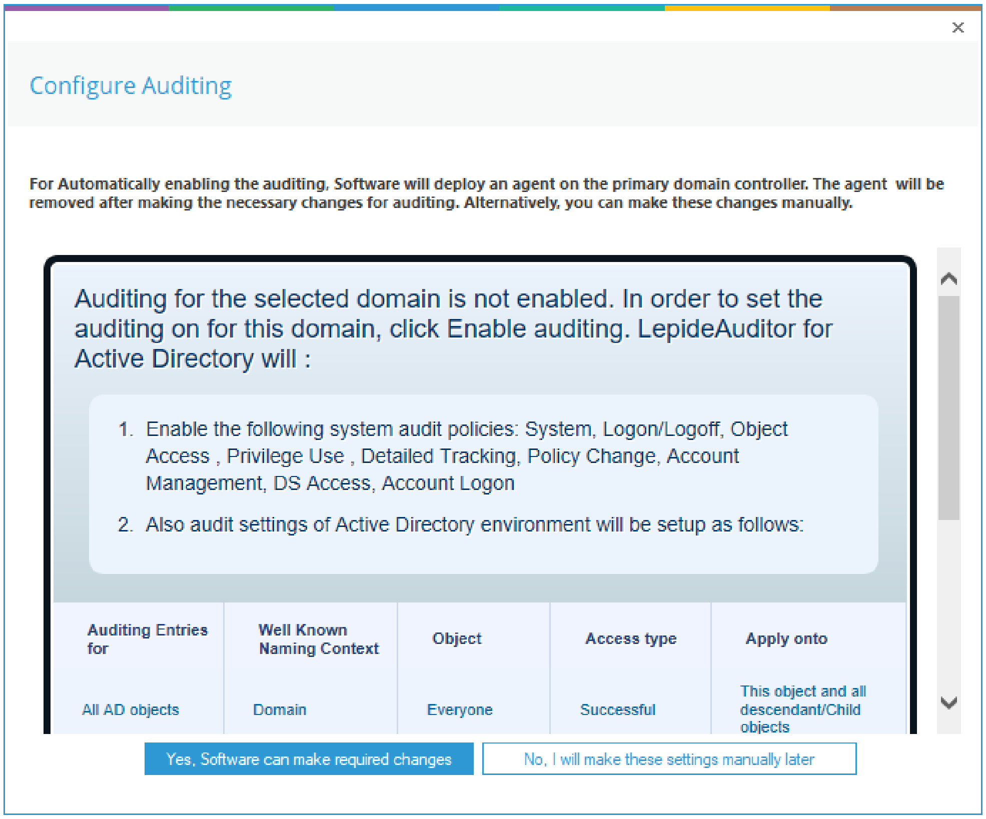
NOTE: If you are configuring with least privileges. please select Without Agent.

   - **With Agent:** With Agent approach is recommended in the following scenarios:

- ✓ When the domain controllers are placed in different geographical locations which have slow network connections.
- ✓ When the event log retention size is smaller than 1 GB on the DCs.

Click **Next** once you have provided all the details for the **Domain Credentials** dialog box.

If native auditing is not enabled at the domain level by default, the following dialog box appears:



Configure Auditing

For Automatically enabling the auditing, Software will deploy an agent on the primary domain controller. The agent will be removed after making the necessary changes for auditing. Alternatively, you can make these changes manually.

Auditing for the selected domain is not enabled. In order to set the auditing on for this domain, click Enable auditing. LepideAuditor for Active Directory will :

1. Enable the following system audit policies: System, Logon/Logoff, Object Access , Privilege Use , Detailed Tracking, Policy Change, Account Management, DS Access, Account Logon
2. Also audit settings of Active Directory environment will be setup as follows:

Auditing Entries for	Well Known Naming Context	Object	Access type	Apply onto
All AD objects	Domain	Everyone	Successful	This object and all descendant/Child objects

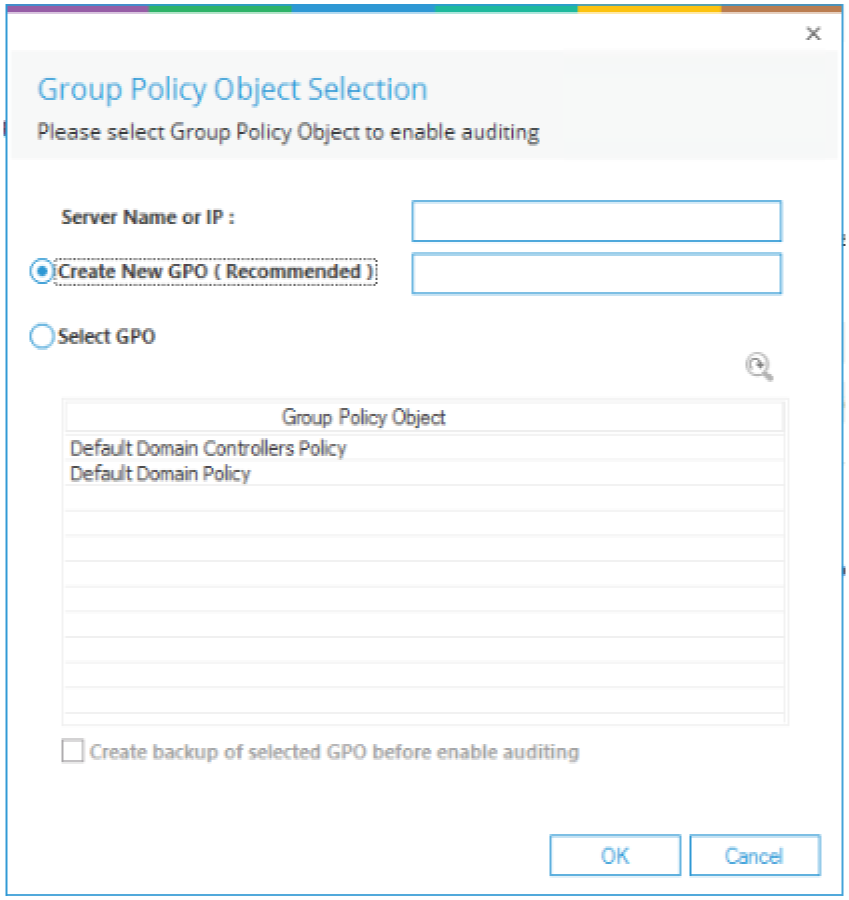
×
Yes, Software can make required changes
No, I will make these settings manually later

The user account will need at least **Schema Admin** permission to enable the auditing automatically. You can temporarily elevate the permissions of the user account to Schema Admins and then click **Yes**, to enable the auditing automatically.

Or you can click **No**, if you wish to do it later manually with the help of our Advanced Configuration guide.

Click **Yes, Software can make required changes** (only if the permission of the user account is elevated to Schema Admins)

The following dialog box will be displayed:



Group Policy Object Selection

Please select Group Policy Object to enable auditing

Server Name or IP :

● Create New GPO (Recommended)

○ Select GPO

Group Policy Object
Default Domain Controllers Policy
Default Domain Policy

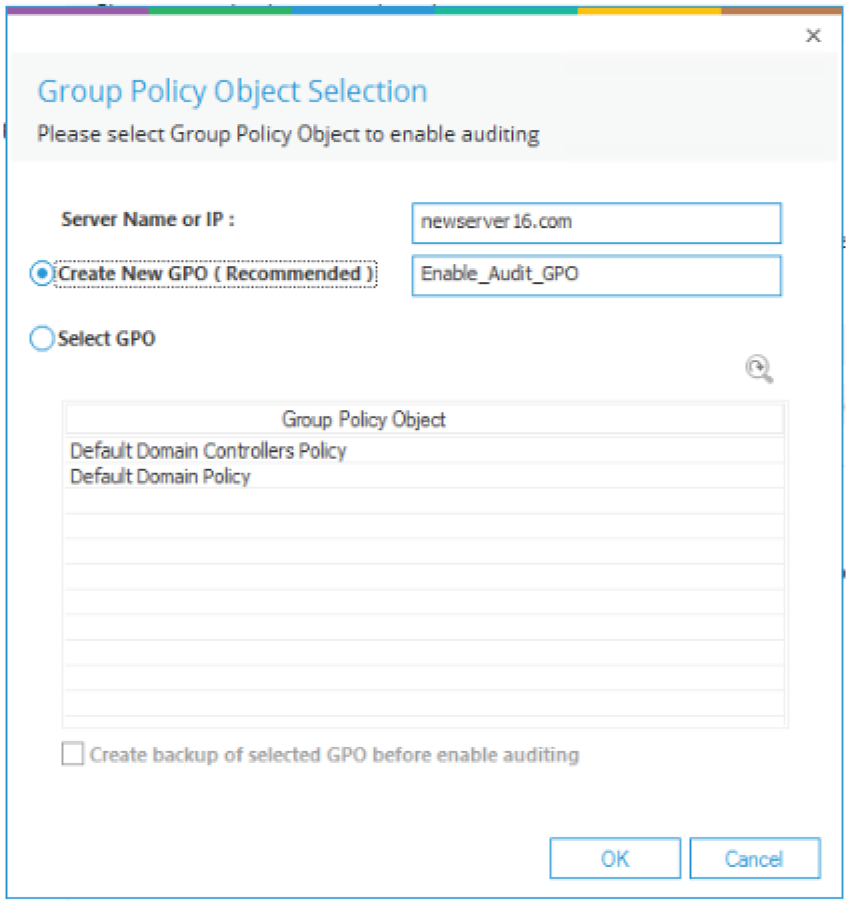
□ Create backup of selected GPO before enable auditing

Figure 5: Enable Auditing

Server Name or IP: Enter either the **IP Address** of the primary domain controller or the **name** of the domain.

Then select any of the following options:

- **Create New GPO (Recommended):**
  Select this to create a new **Group Policy Object**. Once selected, you need to provide the name of new Group Policy to be created.
  Click **OK** to create a new Group Policy at the domain to enable the auditing.
- **Select GPO:**
  This option lets you select a **Group Policy Object** to enable auditing. Select this option to enable the adjoining section.



Group Policy Object Selection

Please select Group Policy Object to enable auditing

Server Name or IP : newserver16.com

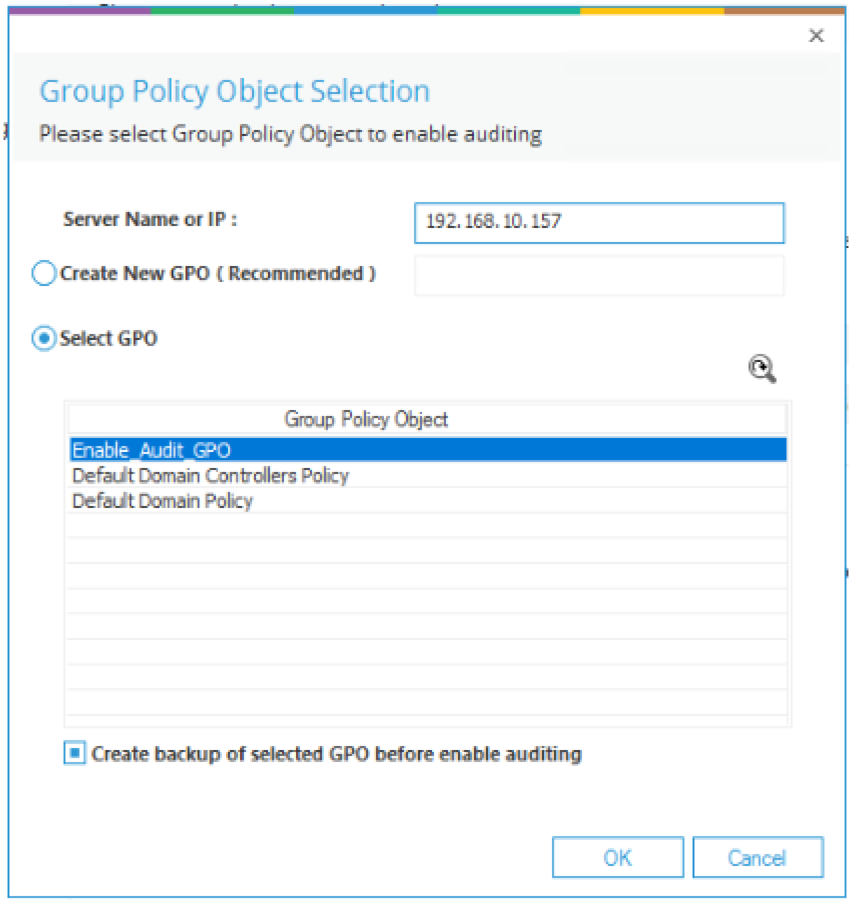
● Create New GPO (Recommended) Enable_Audit_GPO

○ Select GPO

Group Policy Object
Default Domain Controllers Policy
Default Domain Policy

□ Create backup of selected GPO before enable auditing

Figure 6: Creating a New Group Policy



Group Policy Object Selection

Please select Group Policy Object to enable auditing

Server Name or IP : 192.168.10.157

○ Create New GPO (Recommended)

● Select GPO

Group Policy Object
Enable_Audit_GPO
Default Domain Controllers Policy
Default Domain Policy

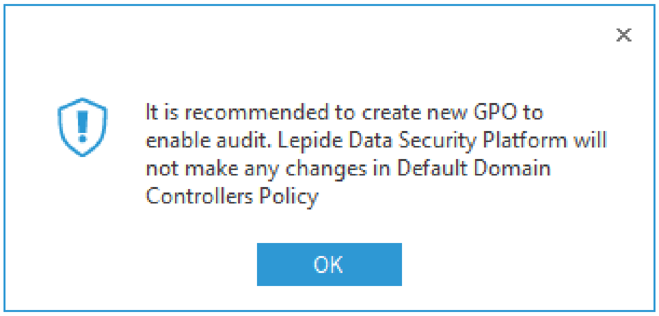
☑ Create backup of selected GPO before enable auditing

Figure 7: Select a Group Policy Object

Perform the following steps to select an existing Group Policy.

a. If a Group Policy is not listed here, you can click 🔍 to rescan the domain for an updated set of Group Policies.

b. You cannot select Default Domain Controller Group Policy or Default Domain Group Policy to enable the auditing using Lepide Data Security Platform. If you try to do this, the following error message appears on the screen:



It is recommended to create new GPO to enable audit. Lepide Data Security Platform will not make any changes in Default Domain Controllers Policy

Figure 8: Error Message while Enabling Auditing at Default Domain Controller Policy

c. Select a custom Group Policy created at the Domain Level or Domain Controller Level upon which the auditing setting must be applied.

d. Make sure to check the **Create a backup of selected Group Policy Object before enable auditing** box if you are enabling the auditing on an existing Group Policy. This backup allows you to restore the previous default Domain Controller Policy if any issue persists after enabling the auditing.

e. To avoid such an issue, create a new Domain Controller Policy to enable the auditing.

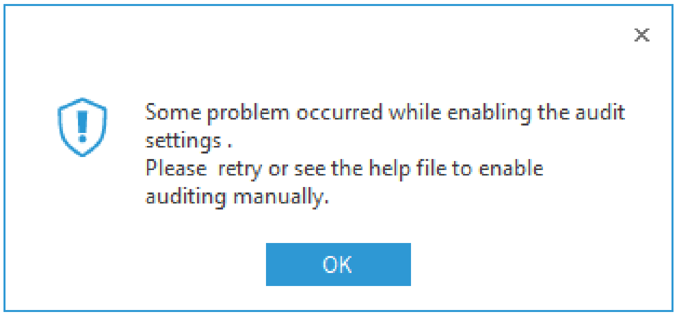
f. Click **OK**. The software tries to enable the auditing and create the backup of the selected group policy on the server in the **%systemdrive%\Windows\Lepide\GPOBKP_24-01-2017 18_13_35** folder.

   Here, 24-01-2017 will be replaced with the date and 18_13_35 will be replaced with the time when you have clicked **OK** to enable auditing on the selected policy.

g. If you face any issue in future, you can use this backup to restore the policy to an earlier state.
   Refer to the Advanced Configuration Guide to restore the group policy.

h. You will need to wait a short time until the auditing is enabled.

If there is a problem enabling the audit, you may receive the following or another error message:



Some problem occurred while enabling the audit settings .
Please retry or see the help file to enable auditing manually.

Figure 9: Error Message

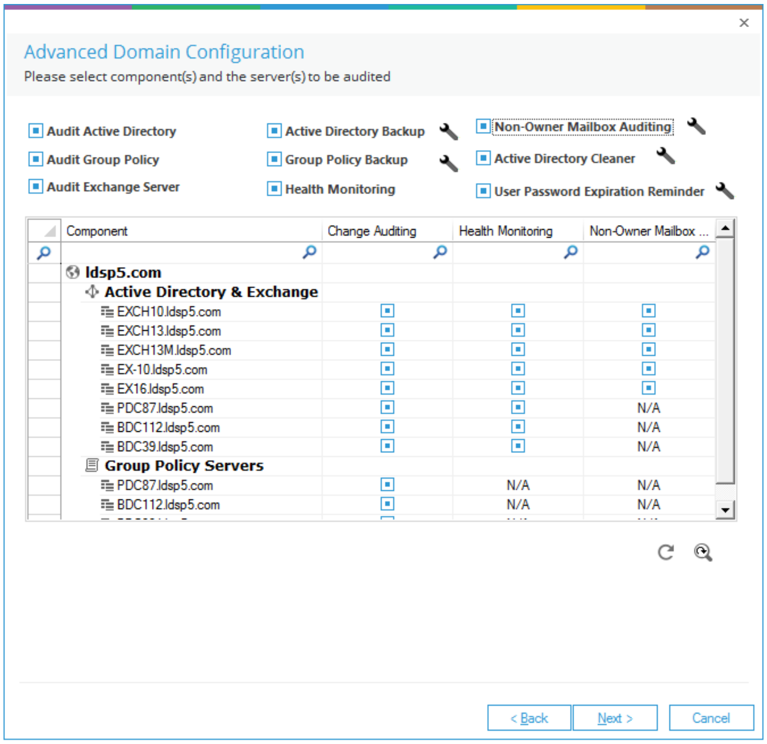
In the case of the above error or a different problem, you will have to enable the auditing settings manually on the Windows Server.

In this case, please select **No** from the next dialog box and proceed further.

Please refer to the [Advanced Configuration Guide]() for information on enabling the auditing settings manually.

Once auditing is enabled, the solution displays the next step to configure the auditing.

3.2 Advanced Domain Configuration



Advanced Domain Configuration

Please select component(s) and the server(s) to be audited

☑ Audit Active Directory
☑ Audit Group Policy
☑ Audit Exchange Server
☑ Active Directory Backup
☑ Group Policy Backup
☑ Health Monitoring
☑ Non-Owner Mailbox Auditing
☑ Active Directory Cleaner
☑ User Password Expiration Reminder

Component	Change Auditing	Health Monitoring	Non-Owner Mailbox ...
ldsp5.com			
Active Directory & Exchange			
EXCH10.ldsp5.com	☑	☑	☑
EXCH13.ldsp5.com	☑	☑	☑
EXCH13M.ldsp5.com	☑	☑	☑
EX-10.ldsp5.com	☑	☑	☑
EX16.ldsp5.com	☑	☑	☑
PDC87.ldsp5.com	☑	☑	N/A
BDC112.ldsp5.com	☑	☑	N/A
BDC39.ldsp5.com	☑	☑	N/A
Group Policy Servers			
PDC87.ldsp5.com	☑	N/A	N/A
BDC112.ldsp5.com	☑	N/A	N/A

Figure 10: Advanced Domain Configuration

All domain controllers in the domain will be listed here. You can select which modules are required:

Enable Auditing

Check or uncheck the following options to enable or disable auditing, backup snapshots and Health Monitoring.

a. Audit Active Directory: Enable/disable the Auditing of Active Directory.

b. Audit Group Policy: Enable/disable the Auditing of Group Policy Objects.

c. Audit Exchange Server: Enable/disable the Auditing of Exchange Server.

d. Non-owner Mailbox Auditing: Enable/disable the mailbox access auditing of non-owner users and owners.

e. Health Monitoring: Enable/disable the Health Monitoring of Active Directory and Exchange Servers.

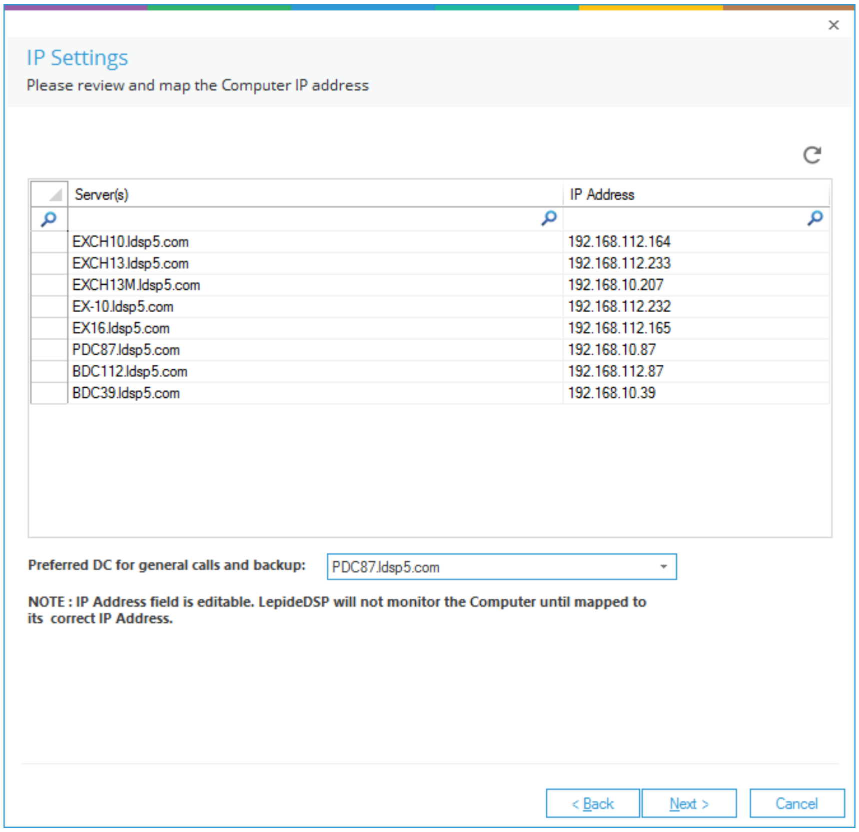
f. Active Directory Backup: Enable/disable the backup snapshot feature to create snapshots of Active Directory.

g. Group Policy Backup: Enable/disable the backup snapshot feature to create snapshots of Group Policy Objects.

To configure these components, please refer to the Advanced Configuration Guide.

Click **Next** to continue.

3.3 IP Settings



IP Settings

Please review and map the Computer IP address

Server(s)	IP Address
EXCH10.ldsp5.com	192.168.112.164
EXCH13.ldsp5.com	192.168.112.233
EXCH13M.ldsp5.com	192.168.10.207
EX-10.ldsp5.com	192.168.112.232
EX16.ldsp5.com	192.168.112.165
PDC87.ldsp5.com	192.168.10.87
BDC112.ldsp5.com	192.168.112.87
BDC39.ldsp5.com	192.168.10.39

Preferred DC for general calls and backup: PDC87.ldsp5.com

NOTE : IP Address field is editable. LepideDSP will not monitor the Computer until mapped to its correct IP Address.

Figure 11: IP Settings

Please verify the IP Addresses resolved by the solution in this wizard.

If the field is blank or IP Address is wrong, double click the cell containing IP Address to make this field editable. Enter the correct IP Address and press the **ENTER** key.

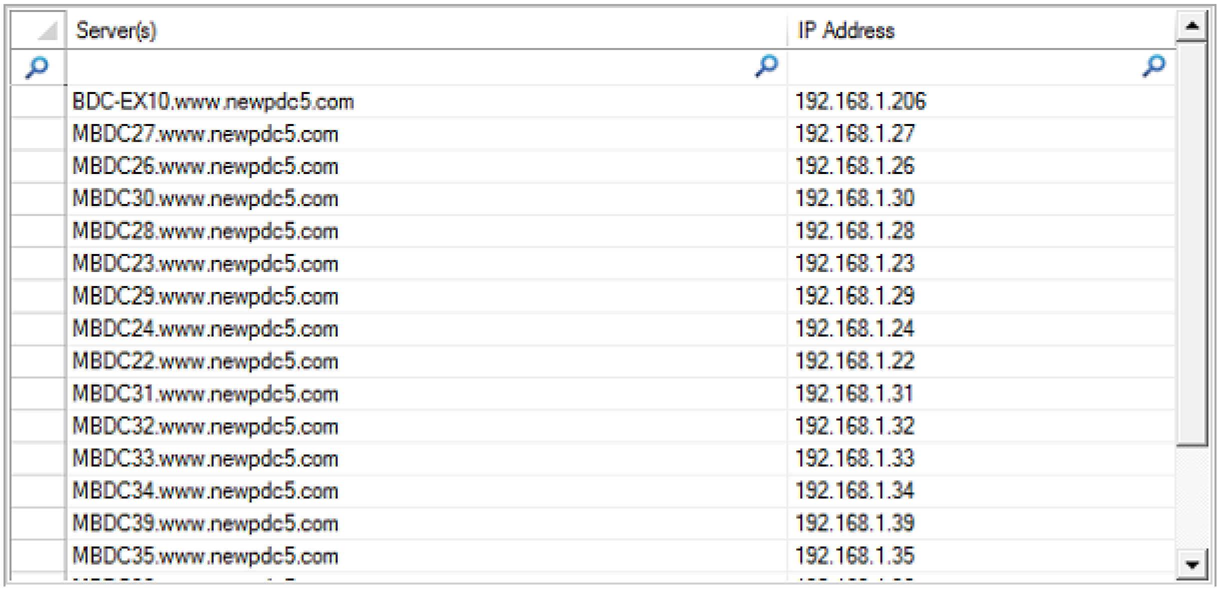
You can click ↻ icon to restore the default options for this step.

You can also select the preferred domain controller, to which the calls related to backup snapshots will be sent.

NOTE: The selected domain controller should be located nearby to the application server, so that the actions related to these calls can be performed first. You can also select a domain controller which is comparatively idle or has lesser load.

If there is a long list of domain controllers, then you can use the top filtration row to filter for the required domain controllers that have to be modified.

The following image shows an example:



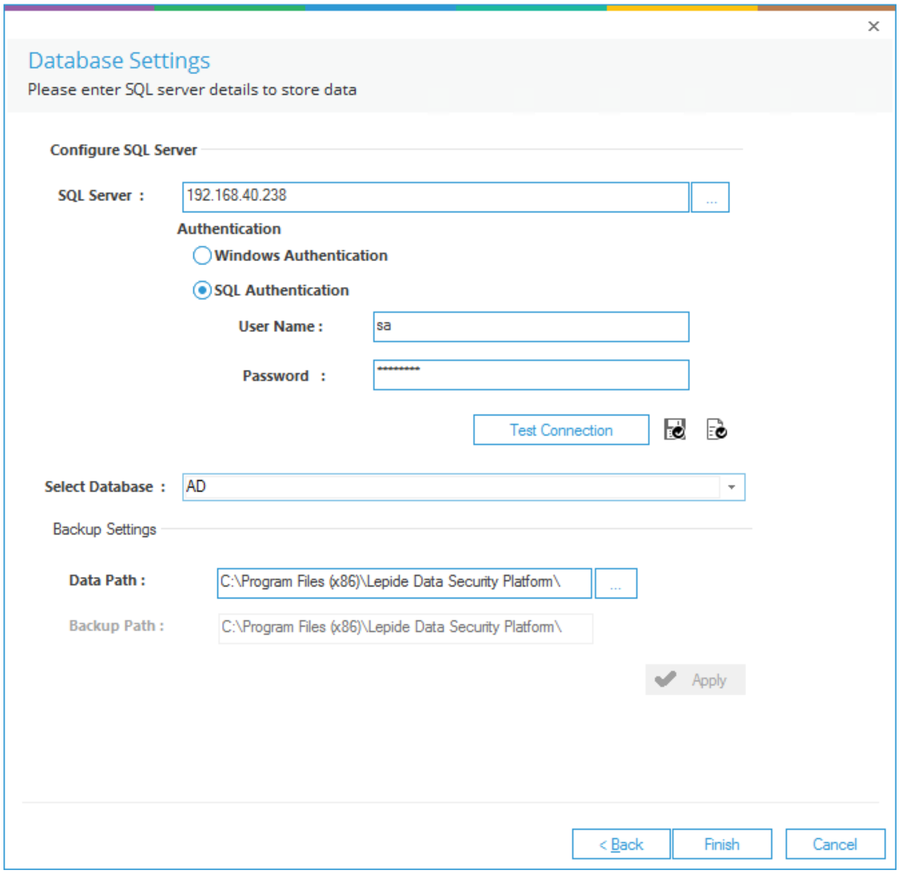
Server(s)	IP Address
BDC-EX10.www.newpdc5.com	192.168.1.206
MBDC27.www.newpdc5.com	192.168.1.27
MBDC26.www.newpdc5.com	192.168.1.26
MBDC30.www.newpdc5.com	192.168.1.30
MBDC28.www.newpdc5.com	192.168.1.28
MBDC23.www.newpdc5.com	192.168.1.23
MBDC29.www.newpdc5.com	192.168.1.29
MBDC24.www.newpdc5.com	192.168.1.24
MBDC22.www.newpdc5.com	192.168.1.22
MBDC31.www.newpdc5.com	192.168.1.31
MBDC32.www.newpdc5.com	192.168.1.32
MBDC33.www.newpdc5.com	192.168.1.33
MBDC34.www.newpdc5.com	192.168.1.34
MBDC39.www.newpdc5.com	192.168.1.39
MBDC35.www.newpdc5.com	192.168.1.35

Figure 12: List of Domain Controllers

When finished click **Next** to continue.

3.4 Database Settings

In this step, you need to provide the details of SQL Server and database that will be used to store the audit data. The solution lets you connect both to a locally hosted or a networked SQL Server.



Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : 192.168.40.238

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

Select Database : AD

Backup Settings

Data Path : C:\Program Files (x86)\Lepide Data Security Platform\

Backup Path : C:\Program Files (x86)\Lepide Data Security Platform\

Figure 13: Database Settings

Enter the SQL Server name manually or click ... button to show all SQL Servers on the network and select any one from the list.

NOTE: Click to load the SQL Server Settings from Default SQL Server Settings Page

Provide the SQL Server username and password to allow the solution to access SQL using these credentials.

NOTE: Here, the selected user should have **dbcreator** role in SQL Server.

Provide the database name where the Lepide Data Security Platform will store the auditing logs.

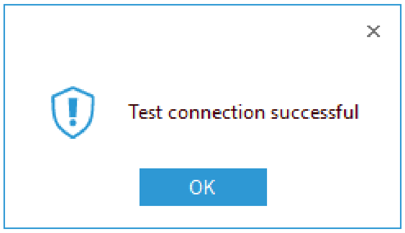
NOTE: Lepide Data Security Platform connects to a database created by the solution itself. The solution alerts when you try to use an existing database.

If you are using the solution for the first time, you can provide a name for the new database that will be created with the solution. In the case of reinstallation, you can use a database created earlier by the solution.

You must test the connection between the solution and the selected SQL Server. This helps to authenticate the database connection.

Click **Test Connection**.

It displays either an error if failed to connect or the following message confirming the successful connection.



Test connection successful

Figure 14: Test Connection is Successful

NOTE: Click 💾 icon to save the current SQL Server Settings as default in Default SQL Server Settings Page

Click **Finish** to add the domain with the above settings.

A message box to restart the solution appears on the screen:

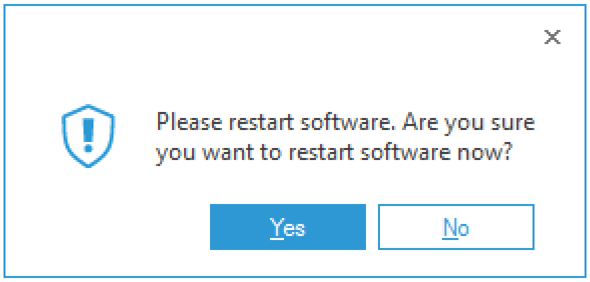

Please restart software. Are you sure you want to restart software now?

Figure 15: Restart the Solution

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.