Lepide

Active Directory.

Advanced configuration guide.

Contents

1 Introduction 2

2 Add an Active Directory Component with Advanced Configuration 2

2.1 Domain Credentials 4

2.2 Advanced Domain Configuration 10

2.2.1 Enable Auditing 11

2.2.2 Options for Domain Controllers: 11

2.3 IP Settings 13

2.4 Database Settings 15

2.4.1 Move Backup Snapshot Data 17

2.5 Organizational Unit Settings 20

2.6 Object Classes and other Settings 23

3 Advanced Domain Configuration Options 25

3.1 Active Directory and Group Policy Object Backup 25

3.2 Health Monitoring 26

3.3 Non-Owner Mailbox Auditing 26

3.4 Active Directory Cleaner 26

3.5 User Password Expiration Reminder 26

3.6 Restore Backed up Group Policy 27

3.7 Archive Database Settings 28

4 Support 29

5 Trademarks 29

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 advanced configuration of the Lepide Data Security Platform for Active Directory. For information on installation, please see our Installation and Prerequisites Guide. For information on standard configuration and prerequisites please refer to the Active Directory Quick Start 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 Add an Active Directory Component with Advanced Configuration

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

> **NOTE:** Before continuing, ensure that the prerequisites to audit the domain are met

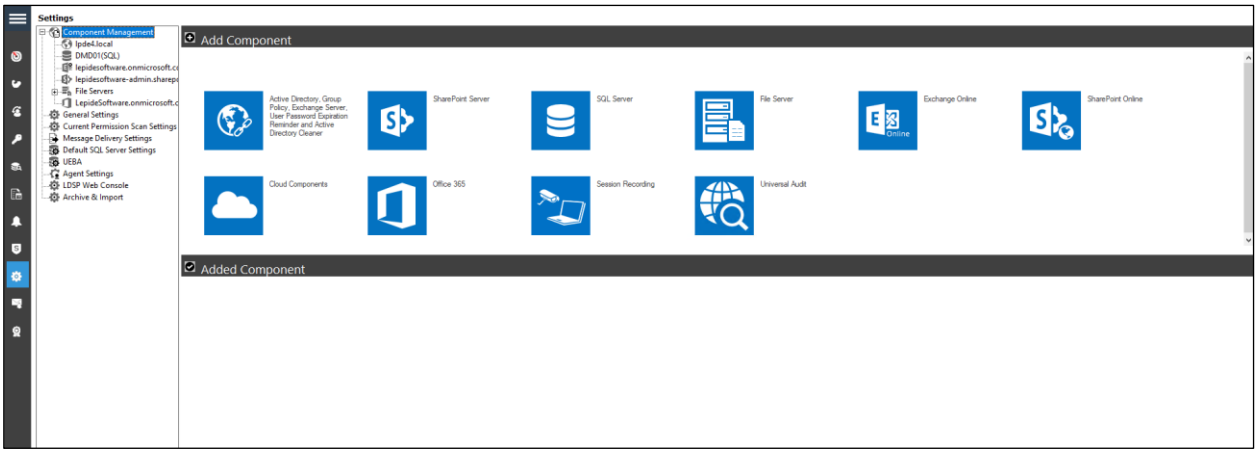


Figure 1: Component Management Window

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

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

1. **Express Configuration**: Add component with minimal recommended settings.
2. **Advanced Configuration**: Add component with customizable advanced settings.

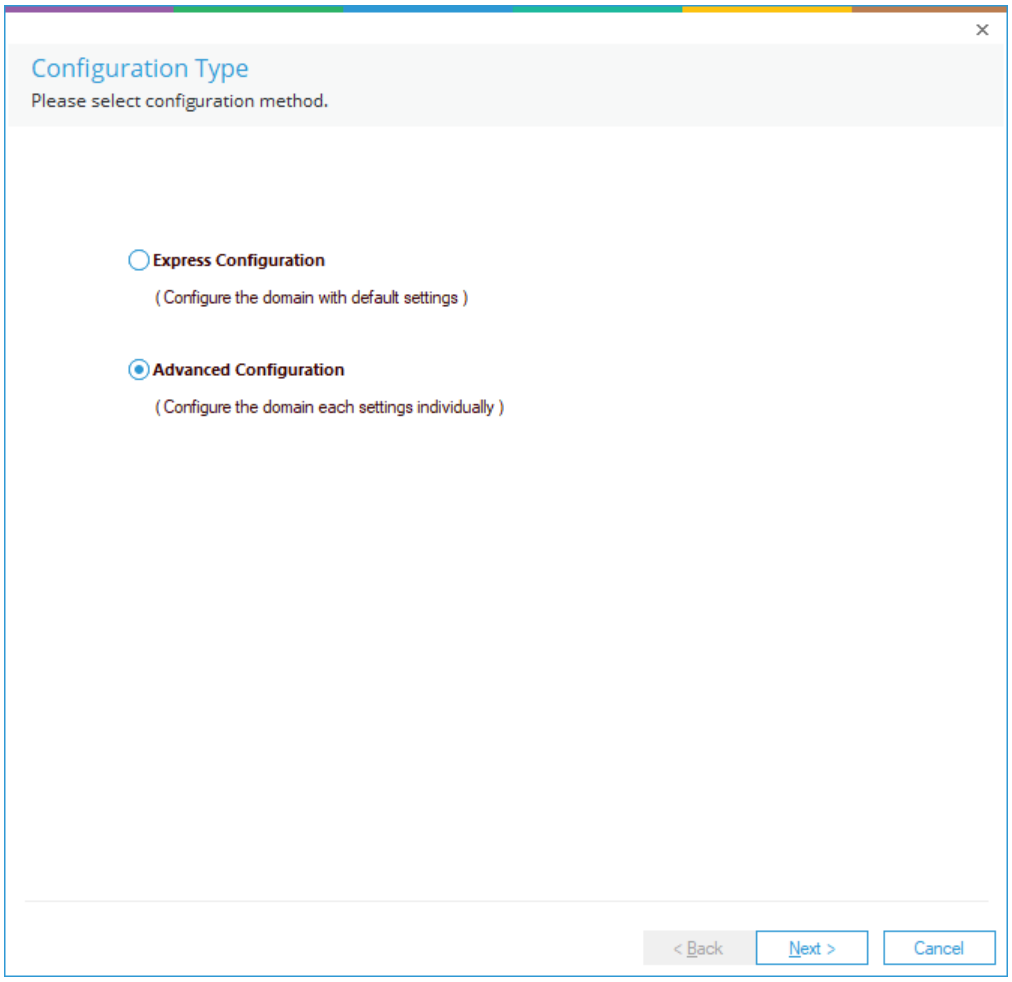


Figure 2: Configuration Wizard

- Select **Advanced Configuration** and click **Next**.

This takes you to the **Domain Credentials** dialog box.

2.1 Domain Credentials

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

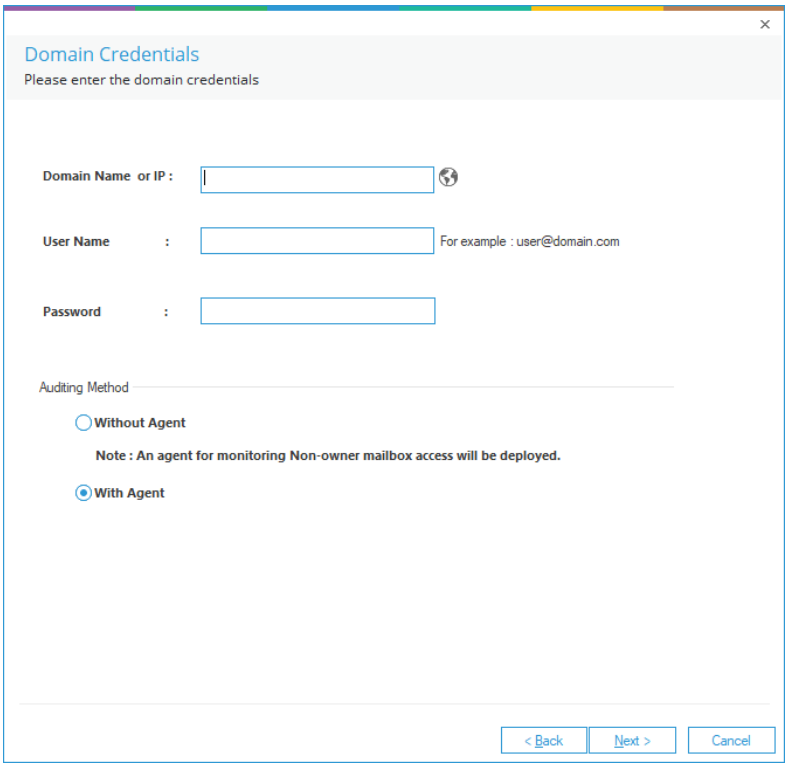


Figure 3: Add the Domain Credentials

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 Domain Controllers. 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:

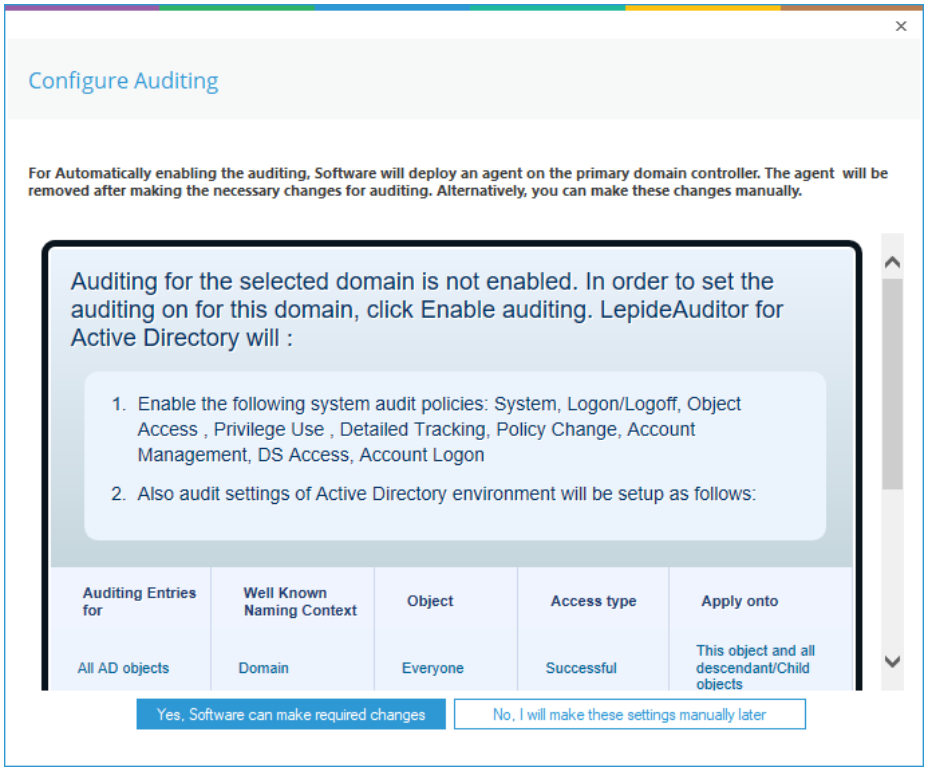


Figure 4:Configure Auditing

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 Enable Auditing Manually 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:

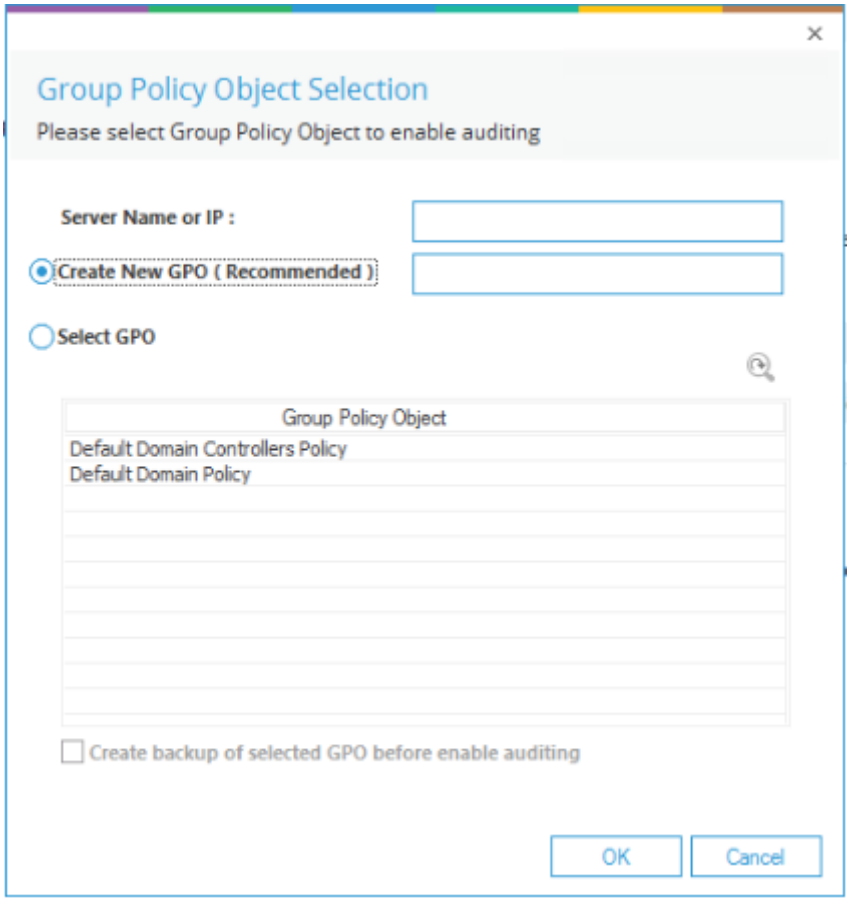


Figure 5: Enable Auditing

Server Name or IP: Enter either the **IP Address** or **Name** of any domain controller (PDC preferred)

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.

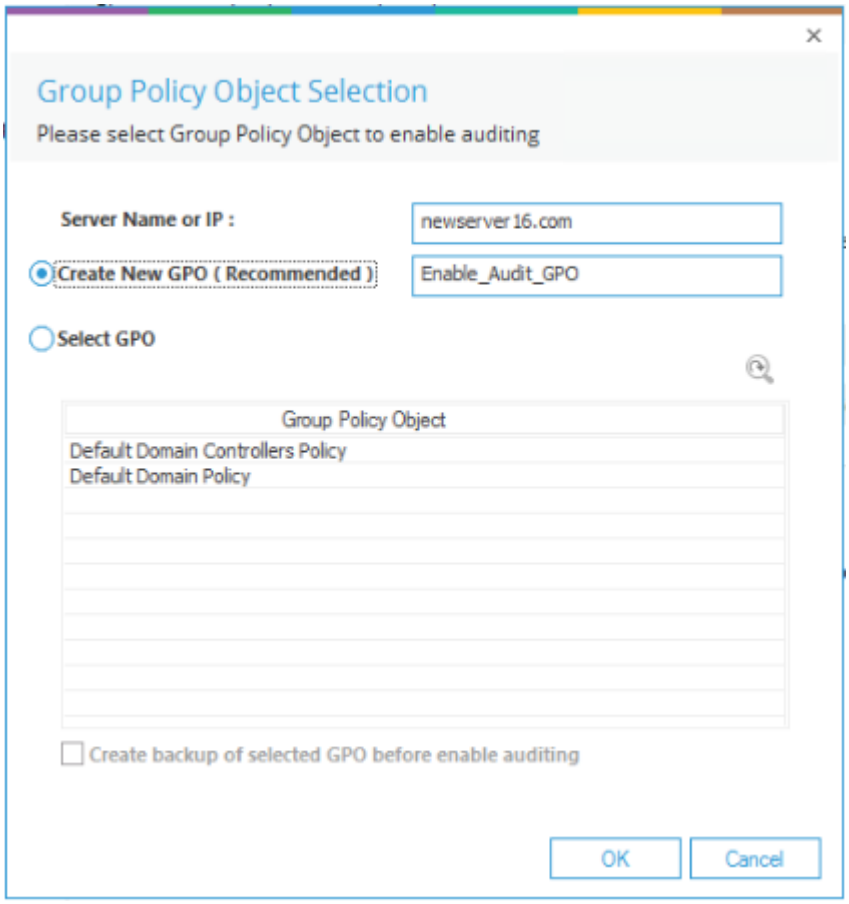


Figure 6: Creating a New Group Policy

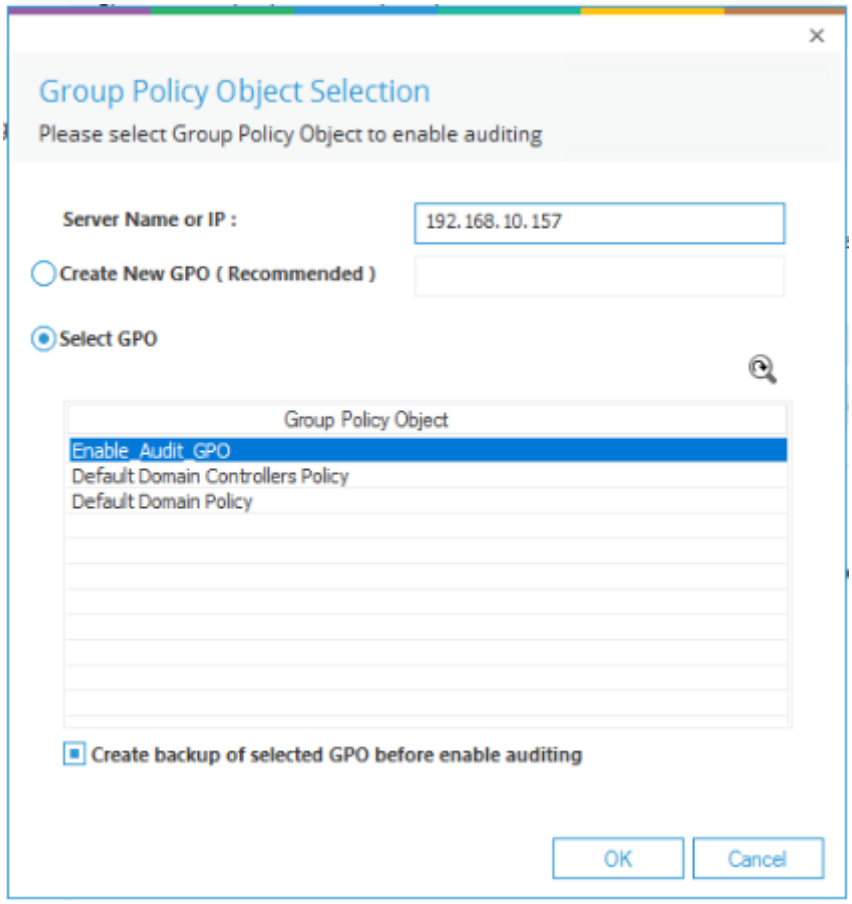


Figure 7: Select a Group Policy Object

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 will appear on the screen:

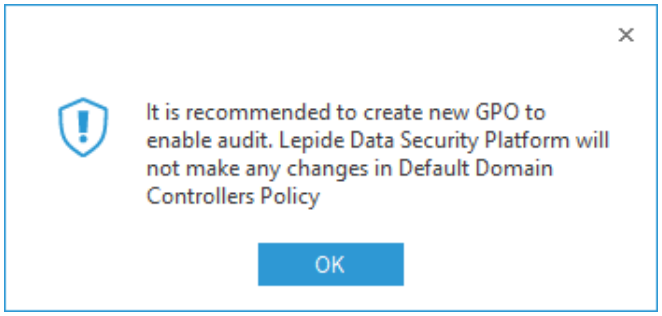


Figure 8: Error message while Enabling Auditing at Default Domain Controller

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_24-01-2022 18_13_35** folder.

   Here, 24-01-2022 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 Section 3.6 of this document 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:

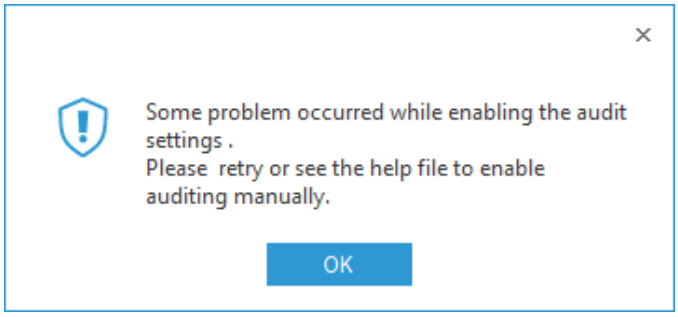


Figure 9: Error Message

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 Enable Auditing Manually Guide for information on enabling the auditing settings manually.

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

2.2 Advanced Domain Configuration

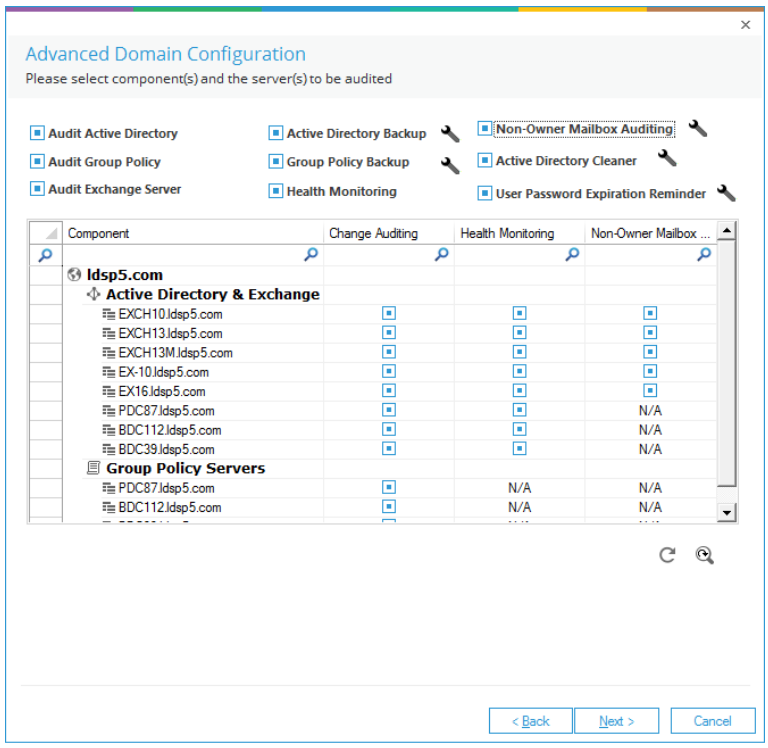


Figure 10: Advanced Domain Configuration

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

2.2.1 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 On-Premises.
d.	Non-owner Mailbox Auditing:	Enable/disable the mailbox access auditing of non-owners, delegated users, administrators, and owners themselves.
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.

2.2.2 Options for Domain Controllers:

Each domain controller will have the following options. Check or uncheck these options to enable or disable features and install or uninstall their corresponding agents for the target domain controller.

a.	Change Auditing:	Check this to enable Change Auditing for a domain controller and install its corresponding agent. Auditing agents will not be installed in the agentless auditing mode.
b.	Health Monitoring:	Check this to enable Health Monitoring for the Active Directory and Exchange component.
c.	Non-Owner Mailbox Auditing:	Check this to enable Non-Owner Mailbox Access Auditing

and to install the agent on the selected Exchange Server.

The following options are unchecked by default:

a. Active Directory Backup
b. Group Policy Backup
c. Health Monitoring
d. Non-Owner Mailbox Auditing
e. Active Directory Cleaner
f. User Password Expiration Reminder

These options need to be checked to enable them. All these options have been selected in this example:

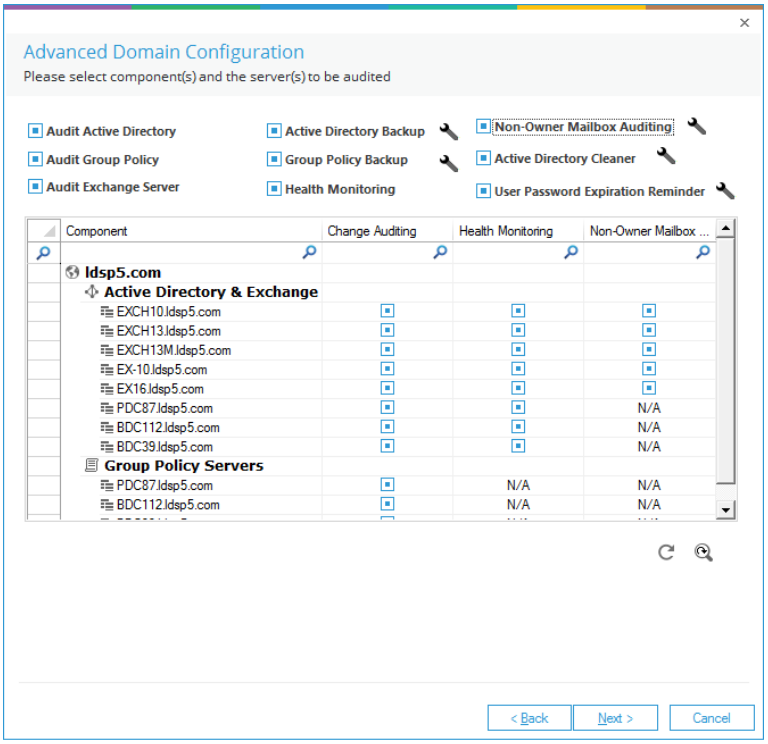


Figure 11: Configuring Advanced Domain Auditing Options

Further configuration options:

a. Click of **Non-Owner Mailbox Auditing** to configure the auditing options of Exchange Mailbox Accesses for both owner and non-owner users. Please refer to the Configure Mailbox Access Auditing Guide for more information.

b. Click for **Active Directory Cleaner** to configure its options. Click for more.

c. Click for **User Password Expiration** Reminder to configure its options. Click for more.

d. Click for **Active Directory Backup** to configure its options. Refer to Section 3.1of this document for further information.

e. Click **Next** to continue.

2.3 IP Settings

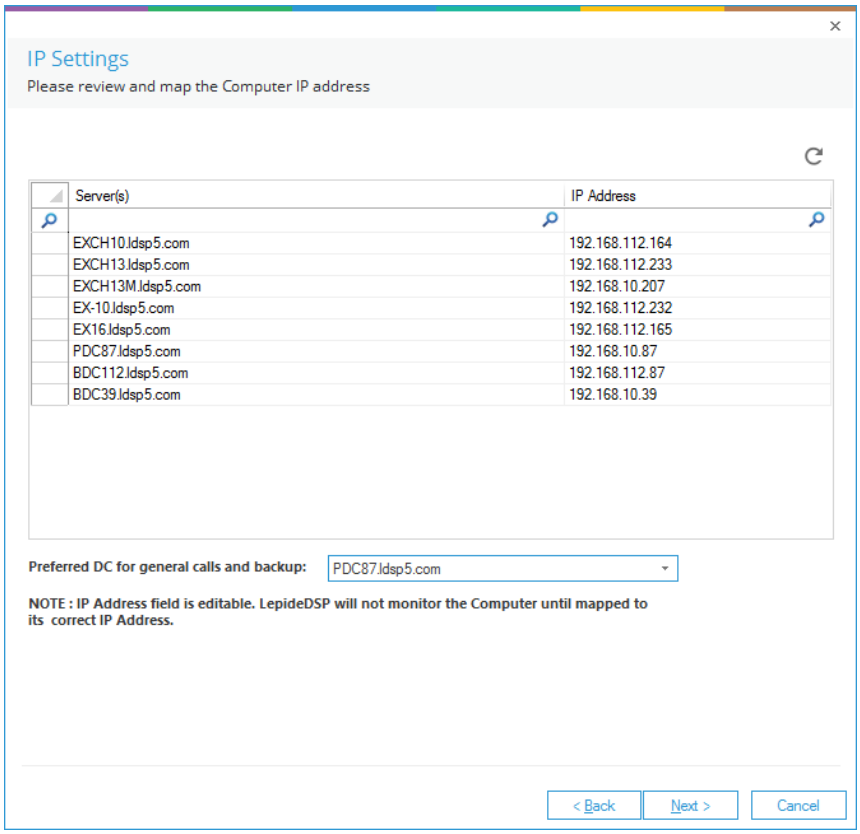


Figure 12: IP Settings

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

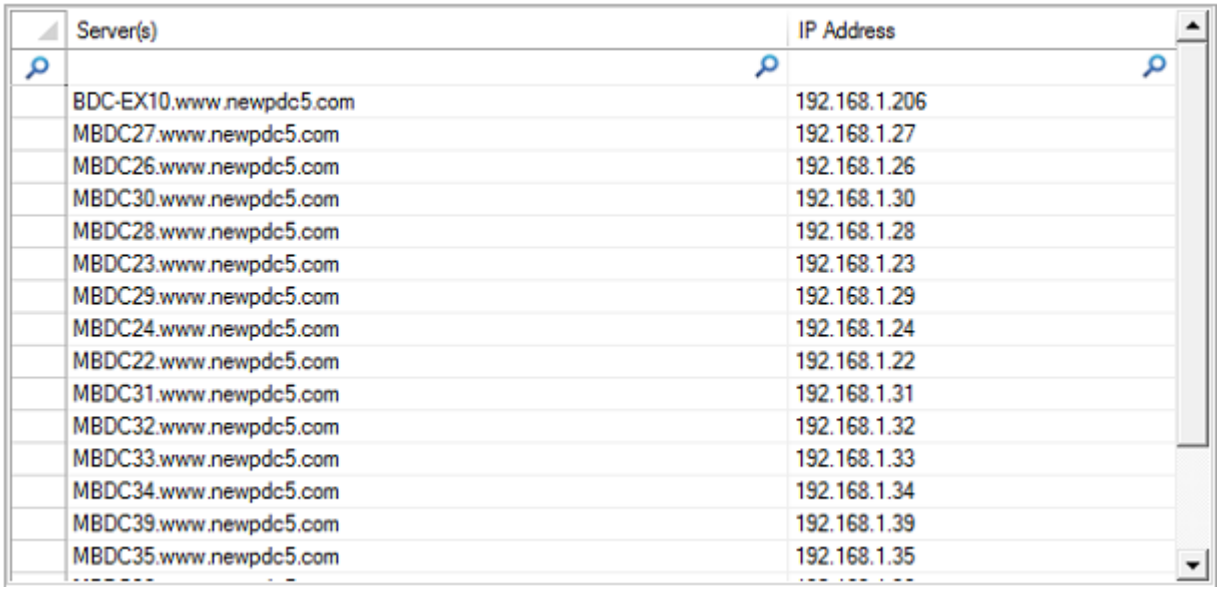
If the field is blank or IP Address is wrong, double click the cell containing IP Address to make this field editable. Enter the correct IP Address and press **ENTER.**

You can click the 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. 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 13: List of Domain Controllers

When finished, click **Next** to continue.

2.4 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.

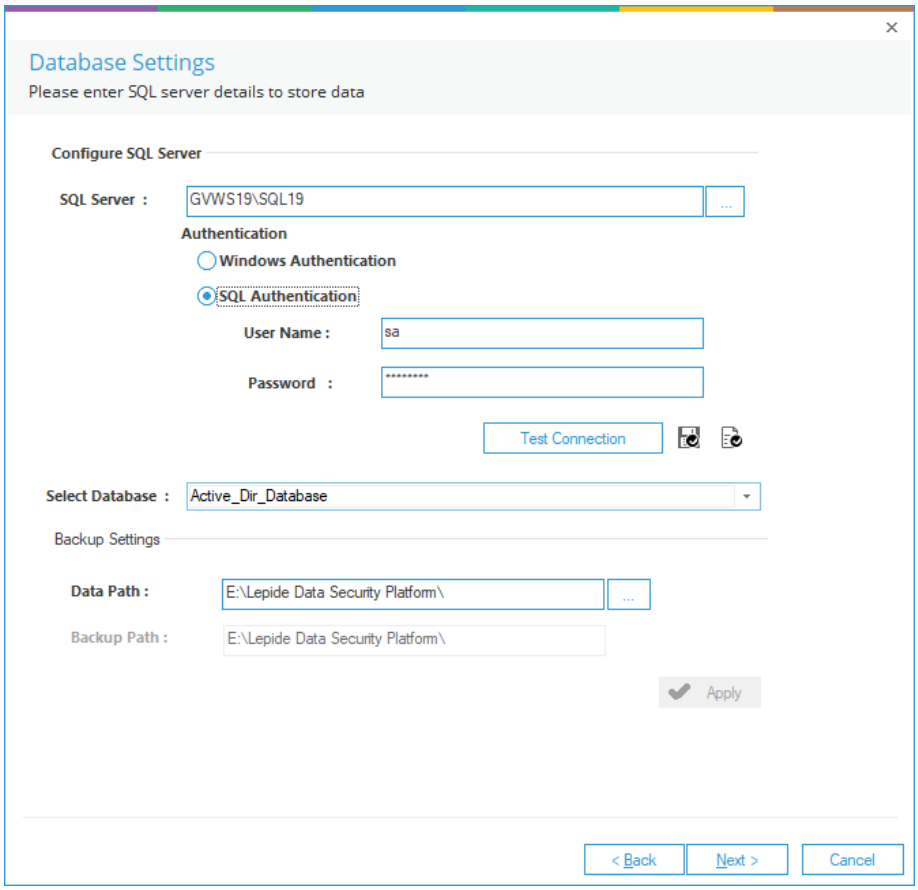


Figure 14: Database Settings

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 by 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.

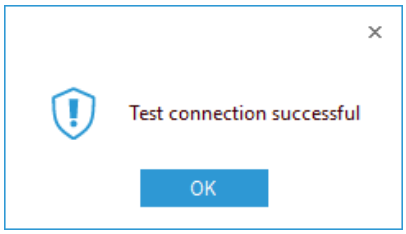


Figure 15: Test Connection is Successful

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

2.4.1 Move Backup Snapshot Data

You can modify the path of both Reference Backup and Complete Backup. If you are modifying their paths, then you can use the **Move Data** utility to move the backup from the previous location to the new location.

Follow the steps below to modify the path of the Reference Backup or Complete Backup.

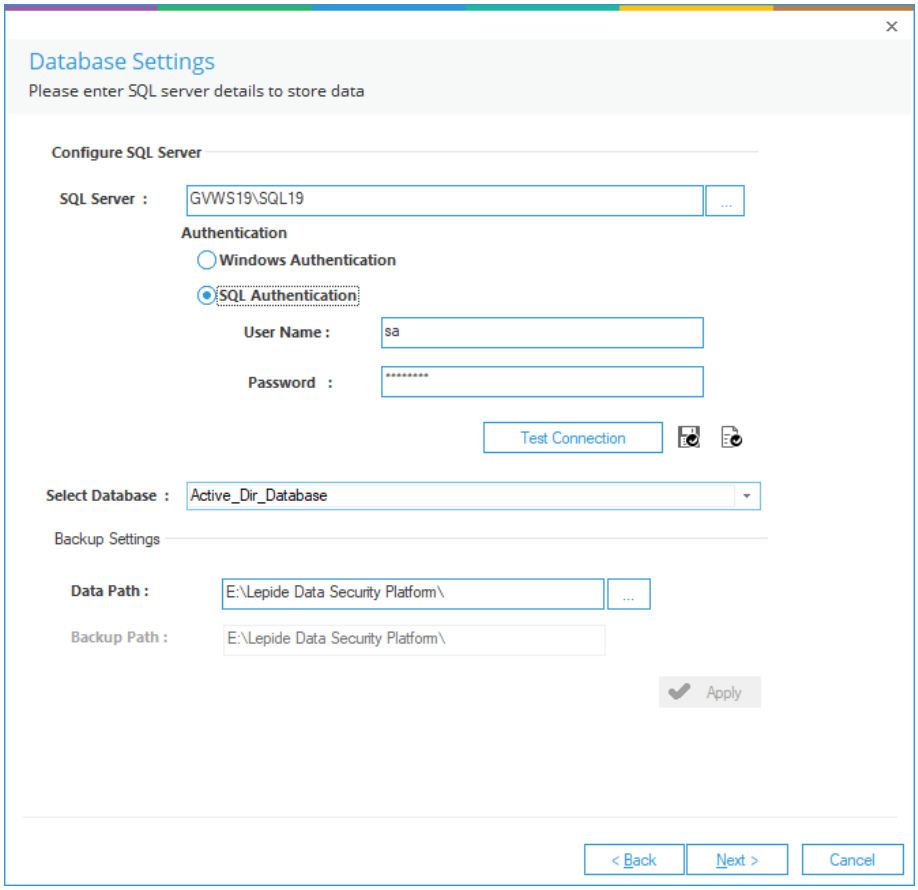


Figure 16: Database Settings

1. From the Database Settings dialog box, click the ... icon (under Backup Settings) to access the following dialog box to select the new folder to save the Active Directory or Group Policy Backup:

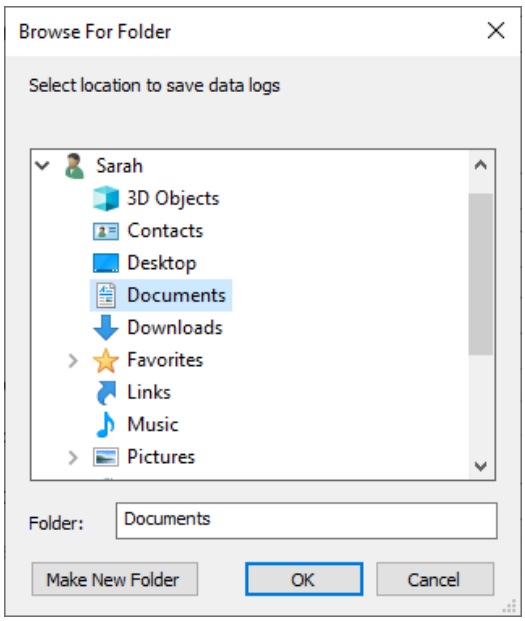


Figure 17: Dialog Box to Select the Folder

2. Select a folder and click **OK**. You will return to the **Database Settings** dialog box which now shows the newly selected folder in the **Data Path** box

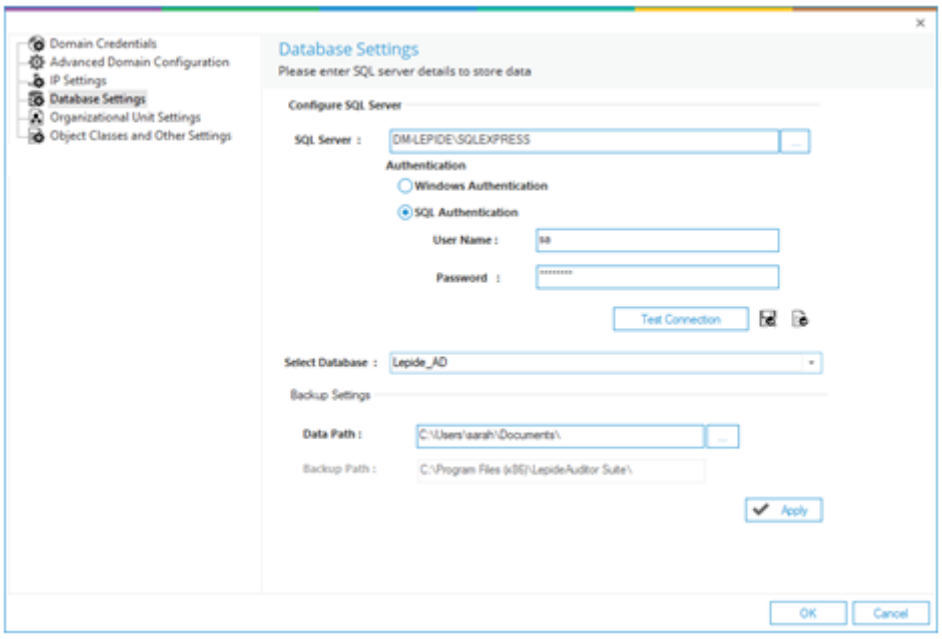


Figure 18: Sample Path of New Backup Location

3. Click **Apply**.

   This starts the **Move Data Wizard** which provides the steps to move the backup data from the old location to the newly selected location.

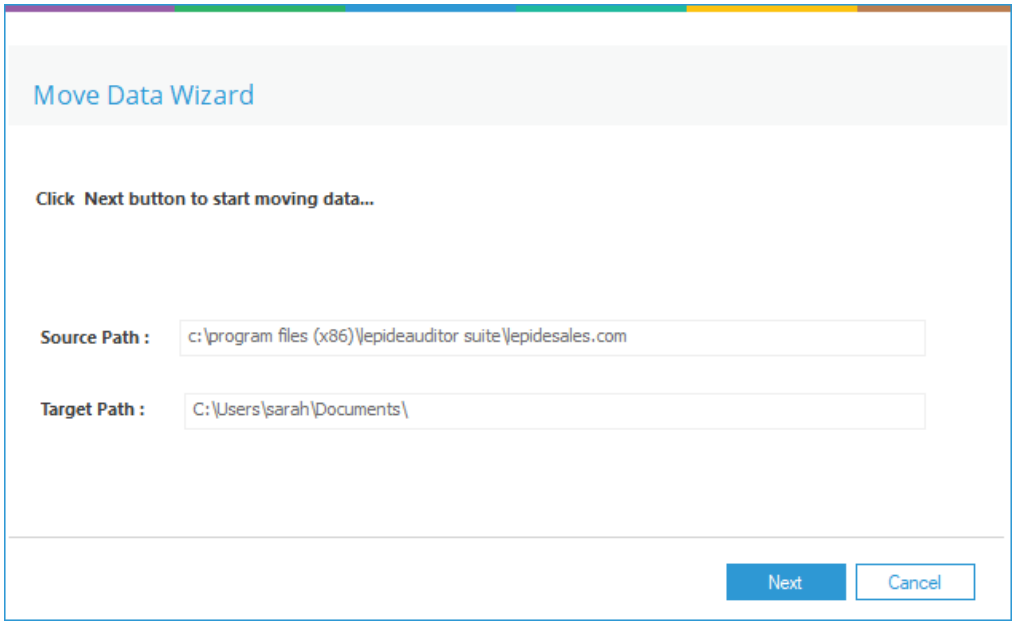


Figure 19: Utility to Move the Backup Data

4. Click **Next**. It starts to move the data.

   Once the backup data is moved successfully, the following message box appears on the screen:

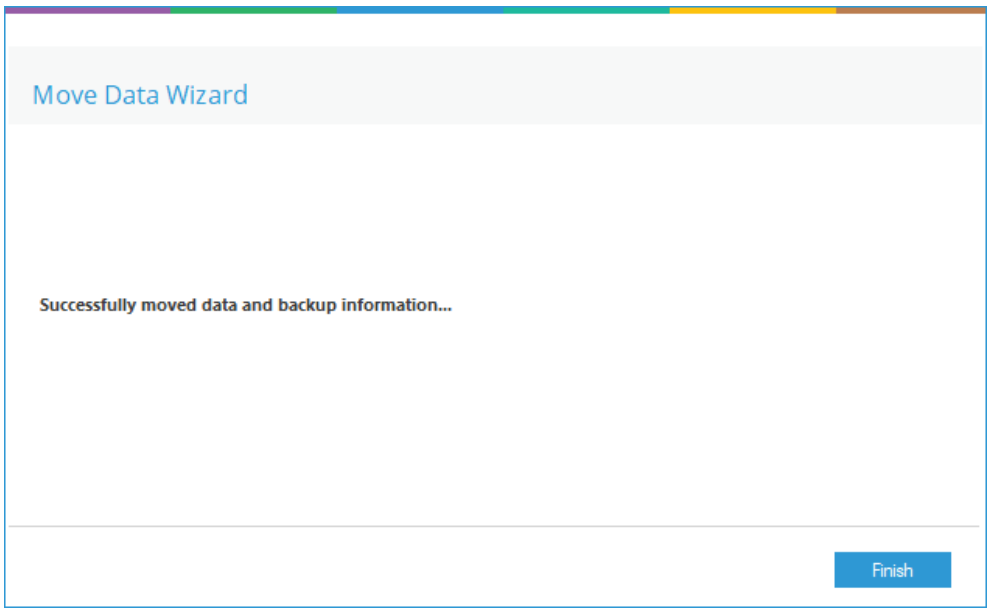


Figure 20: Data has been Moved Successfully

5. Click **Finish** to close the wizard. It takes you back to the Database Settings dialog box.
6. Click **OK**.

2.5 Organizational Unit Settings

In this step, you can select the Organizational Units that you wish to audit.

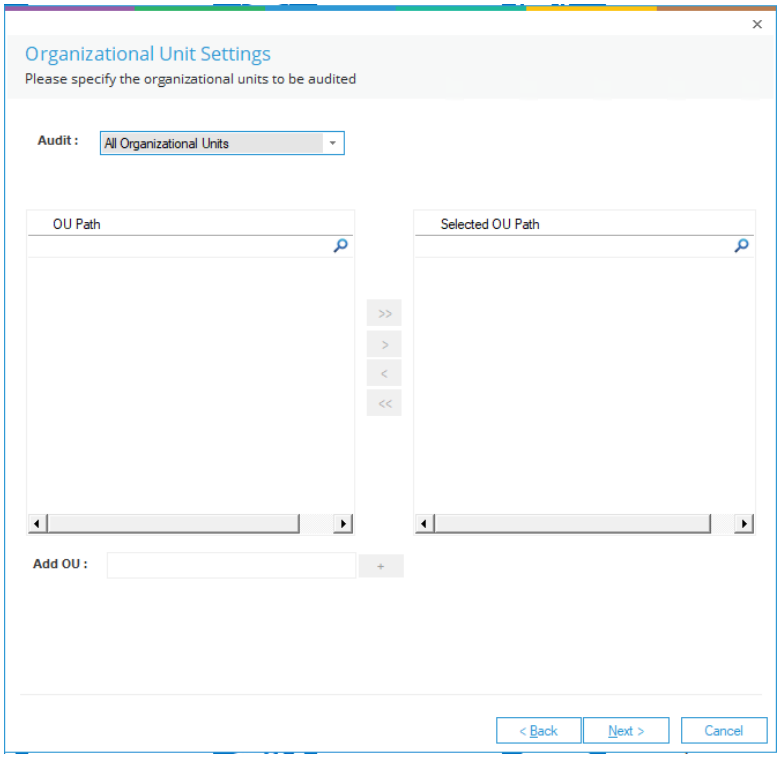


Figure 21: Organizational Unit Settings

Use the **Audit** drop-down menu to select any of the following options:

- **All Organizational Units:** Select this option to audit all Organizational Units. By default, the Audit All Organizational Units option is selected. If you wish to audit all Organizational Units click **Next** to proceed.
- **Only selected Organizational Units:** Select this option to point the solution to audit specific OUs instead of all OUs in the domain. Select the OUs from the list and then move them to the right section and then press Next.

To add Organizational Units manually, enter the name of the new Organizational Unit in Add OU box and click the + button.

Press and hold **CTRL** key to select the multiple organizational units to be added and click the > button to add the selected organizational units to the **Selected OU Path** list.

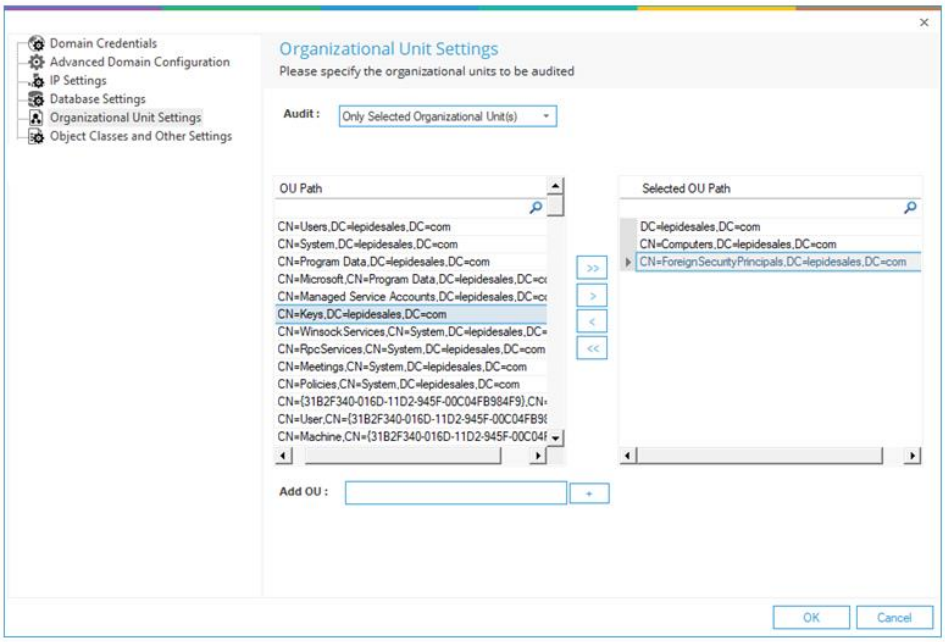


Figure 22: Adding the required Organizational Units

The selected OUs will be listed in the table. Click **Next** to continue.

2.6 Object Classes and other Settings

In this step, you can select the Object Classes that you wish to audit:

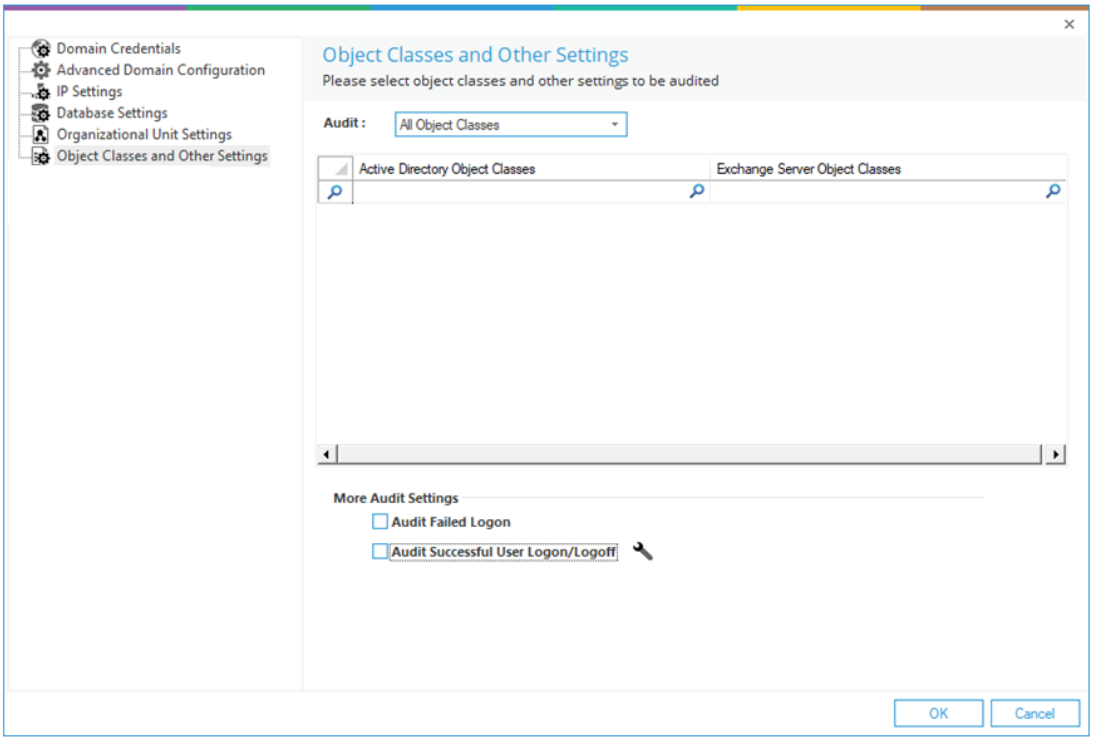


Figure 24: Object Classes and Other Settings

By default, the **Audit All Object Classes** option is selected. If you want to audit specific object classes, then you can select those manually. This section is divided into two parts:

1. **Object Classes**: In this section, you can choose any of the following two options:
    a. **All Object Classes**: Select this option to audit all Object Classes of both Active Directory and Exchange Server.
    b. **Only selected Classes**: Select this option to audit only the specific Object Classes of Active Directory and Exchange Server.
    c. **All but excluding selected classes**: Select this option to audit all Active Directory and Exchange Server Object Classes except the selected classes. It is the default option while adding the domain. It means the following 13 object classes remain excluded from the auditing by default. You need to uncheck these classes in **All but excluding selected classes** or select **All Object Classes** to start their auditing.
        - CRLDistributionPoint

- CrossRef
- CrossRefContainer
- DnsNode
- InfrastructureUpdate
- LinkTrackOMTEntry
- LinkTrackVolEntry
- MSMQConfiguration
- NTFRSMember
- PrintQueue
- RIDManager
- Secret
- ServiceConnectionPoint

2. **More Audit Settings**: This section allows you to enable and configure the Logon Auditing for the domain. It contains the following options:
    a. **Audit Failed Logon**: Select this option to audit all failed login attempts.
    b. **Audit Successful Logon/Logoff:** Select this option to audit all logon/logoff attempts. These events will not be collected until this module is configured from the icon.

Refer to the Enable logon/logoff monitoring guide for more information.

3 Advanced Domain Configuration Options

For advanced configuration options, click the icon next to the relevant option:

3.1 Active Directory and Group Policy Object Backup

The **Active Directory Backup** option is available while adding a domain or modifying an already added domain. This can be found in **Advanced Domain Configuration** screen:

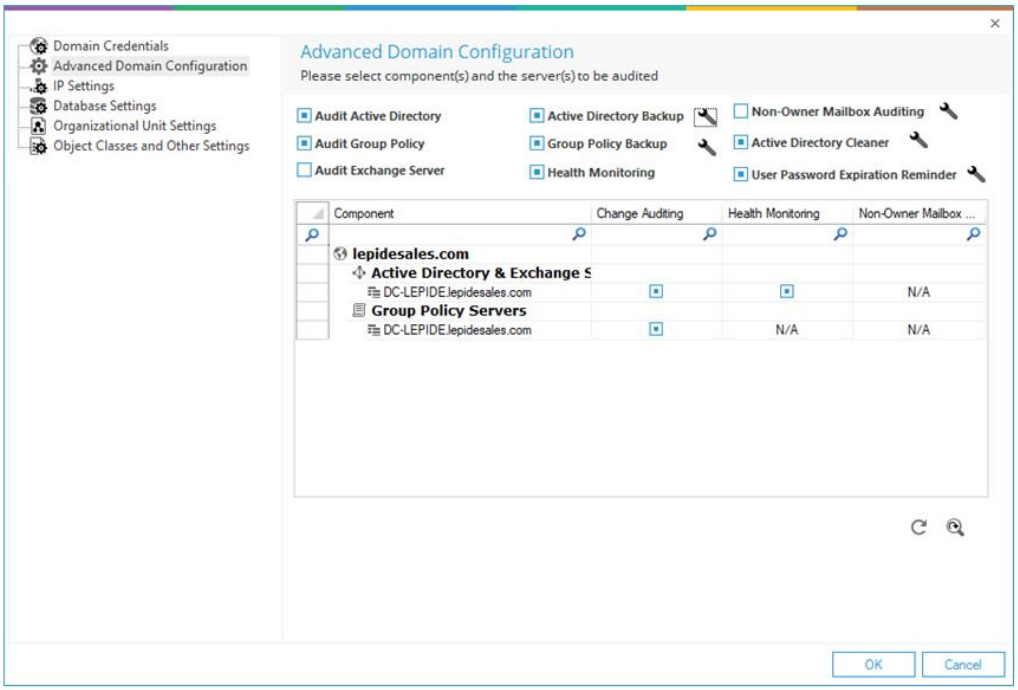


Figure 25: Active Directory Backup Option

You need to check the **Active Directory Backup** option to enable this feature. Once enabled, you can click the adjacent icon to open its settings.

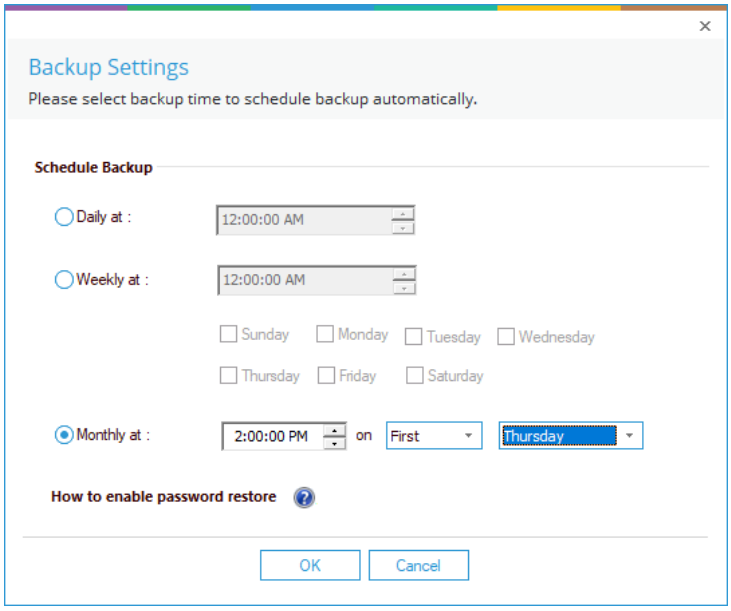


Figure 26: Monthly Schedule to Capture Backup of State of Objects

- Select the **Daily**, **Weekly**, or **Monthly** option from the dialog box. You can customize the time in **Daily** settings. Upon selecting **Weekly at**, you can specify the days on which backup snapshots will be captured.
- If the **Monthly at** option is selected, you can specify the time and day options. Click **OK** to apply the settings.

Similarly, you click icon for **Group Policy Backup** and use above steps to configure the Group Policy Backup.

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

Click icon to rescan the domain and to load the updated information.

3.2 Health Monitoring

Check the box to enable Health Monitoring. To view the health monitoring dashboard, click on the icon.

3.3 Non-Owner Mailbox Auditing

Please refer to the Configure Mailbox Auditing Guide for further information on how to configure this.

3.4 Active Directory Cleaner

Please refer to the Active Directory Cleaner Guide for further information on how to configure this. Click here.

3.5 User Password Expiration Reminder

Please refer to the User Password Expiration Reminder Guide for further information on how to configure this. Click here.

3.6 Restore Backed up Group Policy

While enabling the auditing, Lepide Data Security Platform lets you select an existing Group Policy or create a new one. If you are selecting an existing Group Policy, the solution allows you to take its backup. For further information see Section 2.2 page 10 of this guide.

The backup is created on the server in the **%systemdrive%\Windows\Lepide\GPOBKP_24-01-2017 18_13_35** folder. Here, 24-01-2022 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.

You can perform the following steps to restore the Group Policy using this backup to restore to its earlier state before enabling the auditing.

1. Go to **Start** → **Administrative Tools** → **Group Policy Management Console** to access its console.
2. In the left panel of **Group Policy Management Console**, browse to **Forest** → **www.domain.com**.
3. Right click on **Group Policy Objects** node and click **Manage Backups** option.

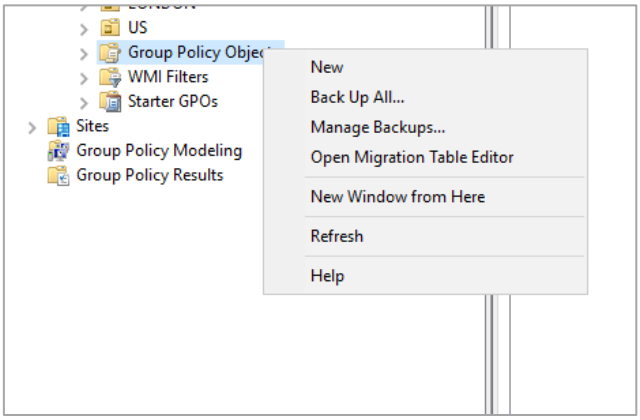


Figure 27: Option to Manage the Group Policy Backups

4. The **Manage Backups** dialog box appears on the screen:

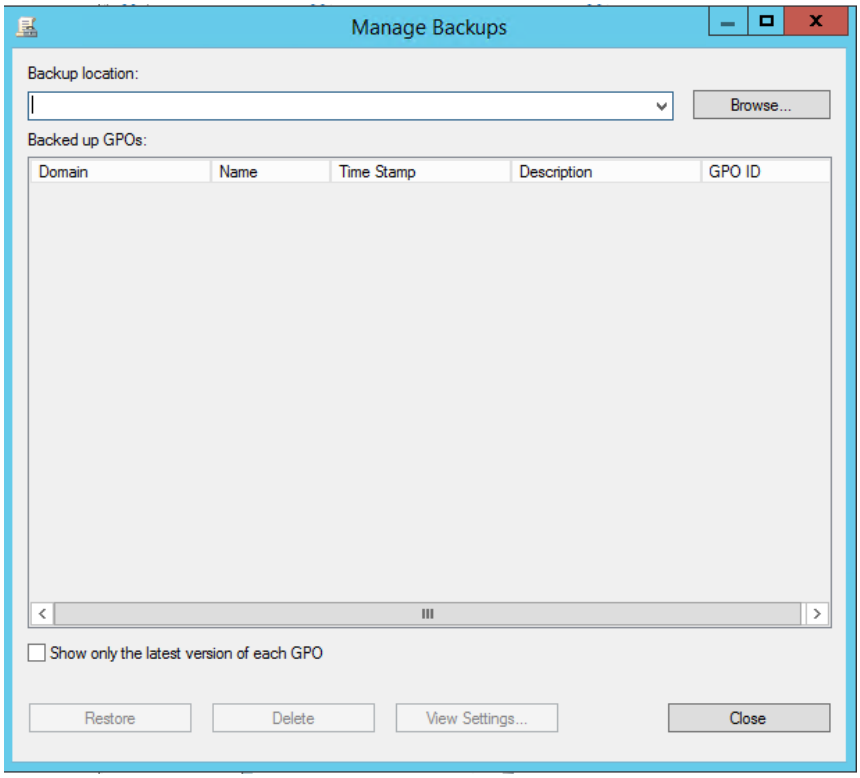


Figure 28: Manage the Backups of Group Policies

5. Click **Browse** and open the **%systemdrive%\Windows\Lepide** folder.
6. Now select **GPOBKP_*** folder of that date and time when you have selected to create the backup while enabling the auditing.
7. Click **OK.**. It takes you back to **Manage Backups** dialog box that shows the Group Policy from the selected backup.
8. Click **Restore** to restore this backup.

3.7 Archive Database Settings

Please refer to our Data Retention Configuration Guide for information on how to set up the archiving process.

4 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/.

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.