Lepide

USE CASE GUIDE

HOW TO RESTORE OBJECTS IN ACTIVE DIRECTORY

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 using the Lepide Data Security Platform to backup and restore the state of Active Directory and Group Policy.

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. Rollback Unwanted Changes

There are times when changes made to Active Directory or Group Policy are unauthorized or unwanted. In these cases, administrators need to be able to restore the changes back to their original state as quickly as possible to mitigate the effects that these changes have on the organization.

The Lepide Object Restore Wizard, which is part of the Lepide Data Security Platform, enables you to rollback these unwanted changes to their original state in a single click.

It does this by automatically capturing backup snapshots of Active Directory and Group Policy Objects at regular intervals and saving their state. Administrators can then use these snapshots to restore the deleted and modified objects. even if they have entered a recycled state or have been physically deleted from Active Directory.

3. Backup Snapshots

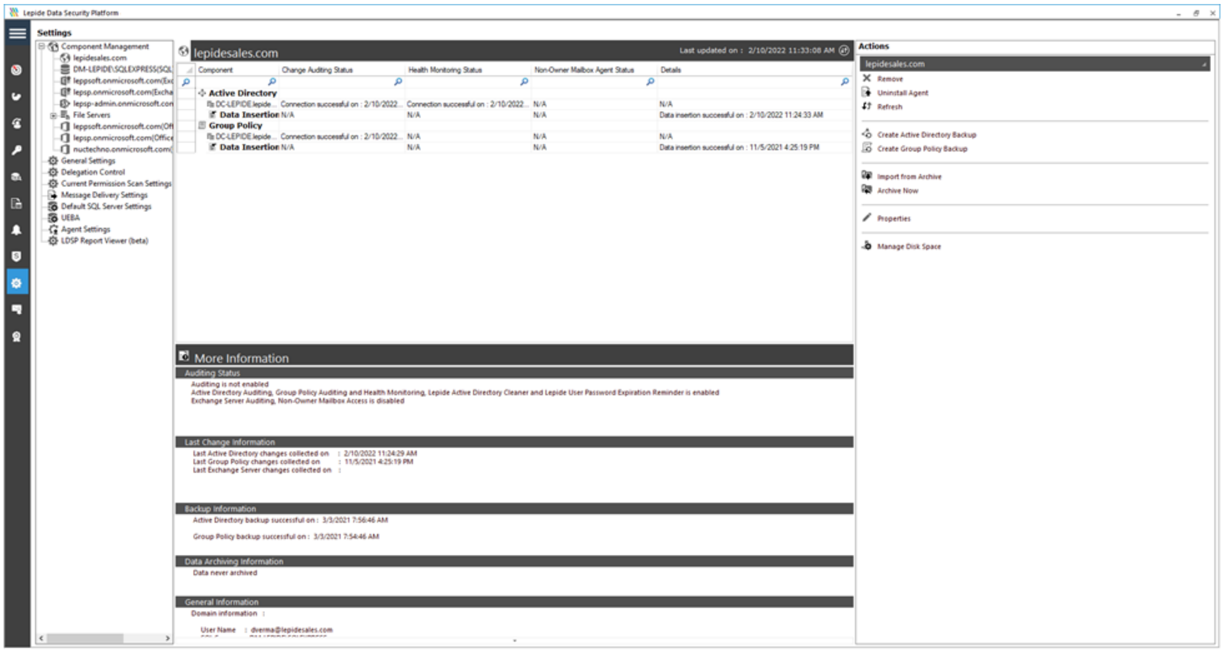
Backup Snapshots are backups of the state of Active Directory and Group Policy Objects at a point in time when the snapshot is captured. It is not the actual backup, which you would use to restore the Active Directory or Group Policies in the case of emergency when the server or Active Directory has crashed. A snapshot is used to restore the state of Active Directory, Group Policies, or their objects individually but only if Active Directory or the Server is in working condition.

4. Enabling Scheduled Backups

To enable backups for Active Directory and Group Policy:

1. Click the **Settings** icon

2. Click on the **Active Directory Component** and the following screen will be displayed:


Lepide Data Security Platform
Settings
Component Management
lepidesales.com
DM-LEPIDE\SQLEXPRESS(SQL
leppsoft.onmicrosoft.com(Exc
lepsp.onmicrosoft.com(Excha
lepsp-admin.onmicrosoft.con
File Servers
leppsoft.onmicrosoft.com(Off
lepsp.onmicrosoft.com(Office
nuctechno.onmicrosoft.com(
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Report Viewer (beta)
Actions
lepidesales.com
Remove
Uninstall Agent
Refresh
Create Active Directory Backup
Create Group Policy Backup
Import from Archive
Archive Now
Properties
Manage Disk Space

lepidesales.com Last updated on : 2/10/2022 11:33:08 AM

Component	Change Auditing Status	Health Monitoring Status	Non-Owner Mailbox Agent Status	Details
Active Directory				
DC-LEPIDE.lepide...	Connection successful on : 2/10/2022...	Connection successful on : 2/10/2022...	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 2/10/2022 11:24:33 AM
Group Policy				
DC-LEPIDE.lepide...	Connection successful on : 2/10/2022...	N/A	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 11/5/2021 4:25:19 PM

More Information

Auditing Status

Auditing is not enabled
Active Directory Auditing, Group Policy Auditing and Health Monitoring, Lepide Active Directory Cleaner and Lepide User Password Expiration Reminder is enabled
Exchange Server Auditing, Non-Owner Mailbox Access is disabled

Last Change Information

Last Active Directory changes collected on : 2/10/2022 11:24:29 AM
Last Group Policy changes collected on : 11/5/2021 4:25:19 PM
Last Exchange Server changes collected on :

Backup Information

Active Directory backup successful on : 3/3/2021 7:56:46 AM

Group Policy backup successful on : 3/3/2021 7:54:46 AM

Data Archiving Information

Data never archived

General Information

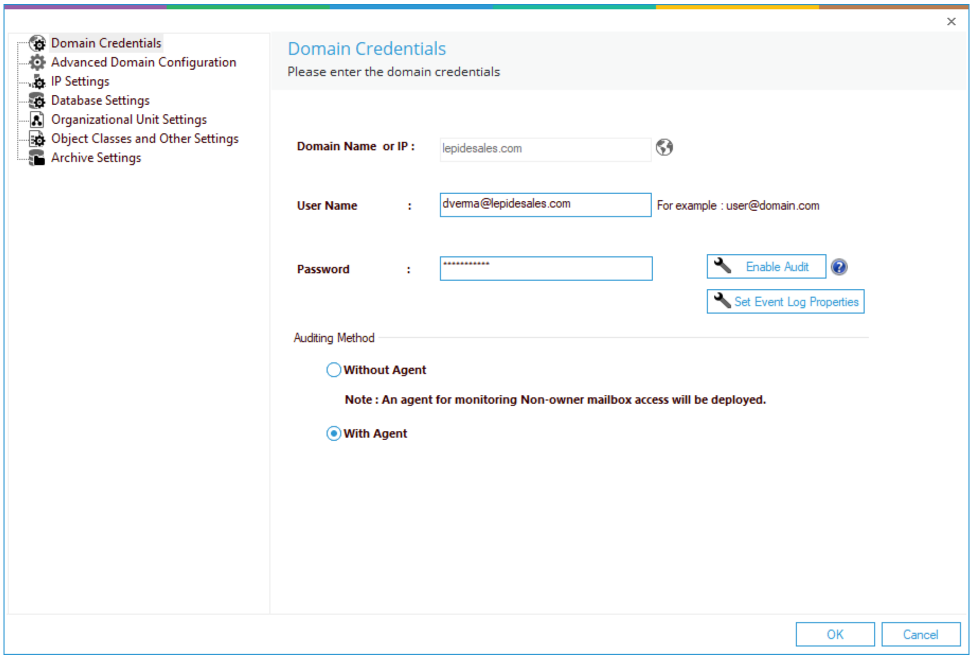
Domain information :

User Name : dverma@lepidesales.com

Figure 1: Active Directory Settings

3. Click **Properties** (found on the right-hand side of the screen)

The Domain Credentials dialog box is displayed:


Domain Credentials
Advanced Domain Configuration
IP Settings
Database Settings
Organizational Unit Settings
Object Classes and Other Settings
Archive Settings

Domain Credentials

Please enter the domain credentials

Domain Name or IP : lepidesales.com

User Name : dverma@lepidesales.com For example : user@domain.com

Password : ***********

Auditing Method

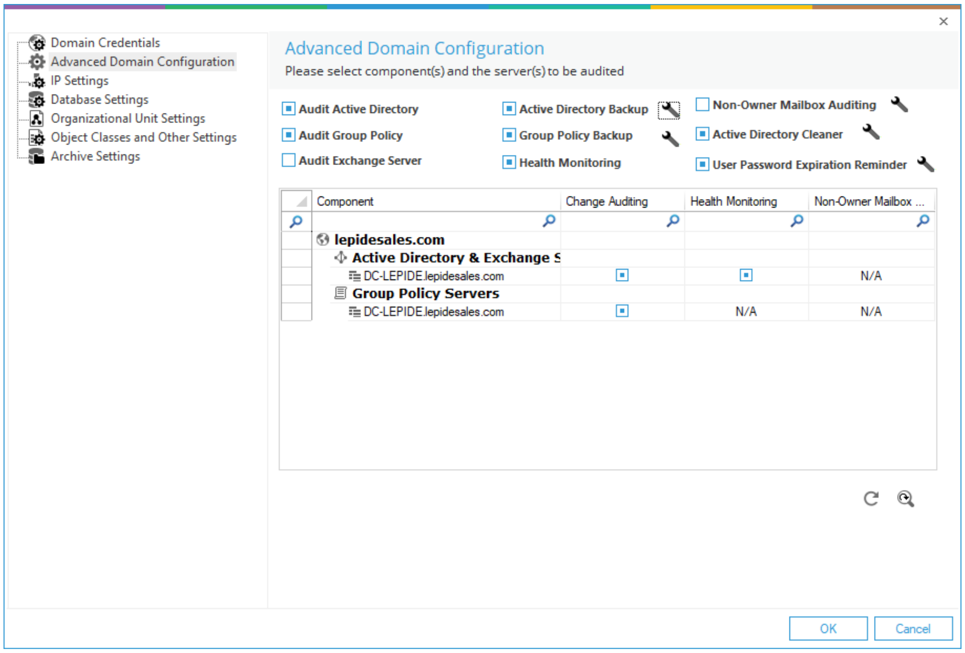
○ Without Agent

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

● With Agent

Figure 2: Domain Credentials

4. Choose Advanced Domain Configuration (from the left-hand list of options) and the Advanced Domain Configuration dialog box is displayed:


Domain Credentials
Advanced Domain Configuration
IP Settings
Database Settings
Organizational Unit Settings
Object Classes and Other Settings
Archive Settings

Advanced Domain Configuration

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

☑ Audit Active Directory ☑ Active Directory Backup ☐ Non-Owner Mailbox Auditing

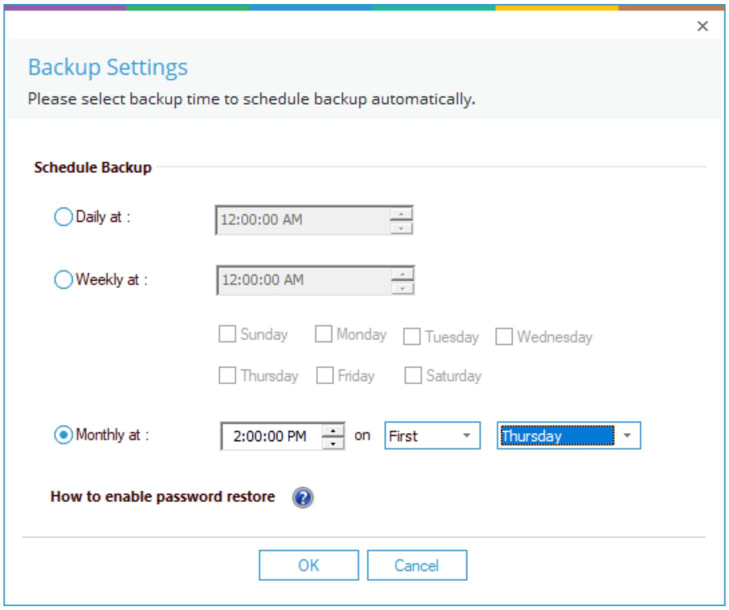
☑ Audit Group Policy ☑ Group Policy Backup ☑ Active Directory Cleaner

☐ Audit Exchange Server ☑ Health Monitoring ☑ User Password Expiration Reminder

Component	Change Auditing	Health Monitoring	Non-Owner Mailbox ...
lepidesales.com			
Active Directory & Exchange S			
DC-LEPIDE.lepidesales.com	☑	☑	N/A
Group Policy Servers			
DC-LEPIDE.lepidesales.com	☑	N/A	N/A

Figure 3: Advanced Domain Configuration

5. Check the **Active Directory Backup** and **Group Policy Backup** options to enable them
6. Once the backups are enabled, a backup will automatically run every month.
7. If you want to change the settings for the schedule of the backup, click the adjacent 🔧 icon to open the Backup Settings dialog box:



Backup Settings

Please select backup time to schedule backup automatically.

Schedule Backup

○ Daily at : 12:00:00 AM

○ Weekly at : 12:00:00 AM

□ Sunday □ Monday □ Tuesday □ Wednesday

□ Thursday □ Friday □ Saturday

● Monthly at : 2:00:00 PM on First Thursday

How to enable password restore

Figure 4: Schedule to Capture Backup of State of Objects

- Select the **Daily**, **Weekly**, or **Monthly** option from the dialog box.

  In the **Daily** settings you can customize the time

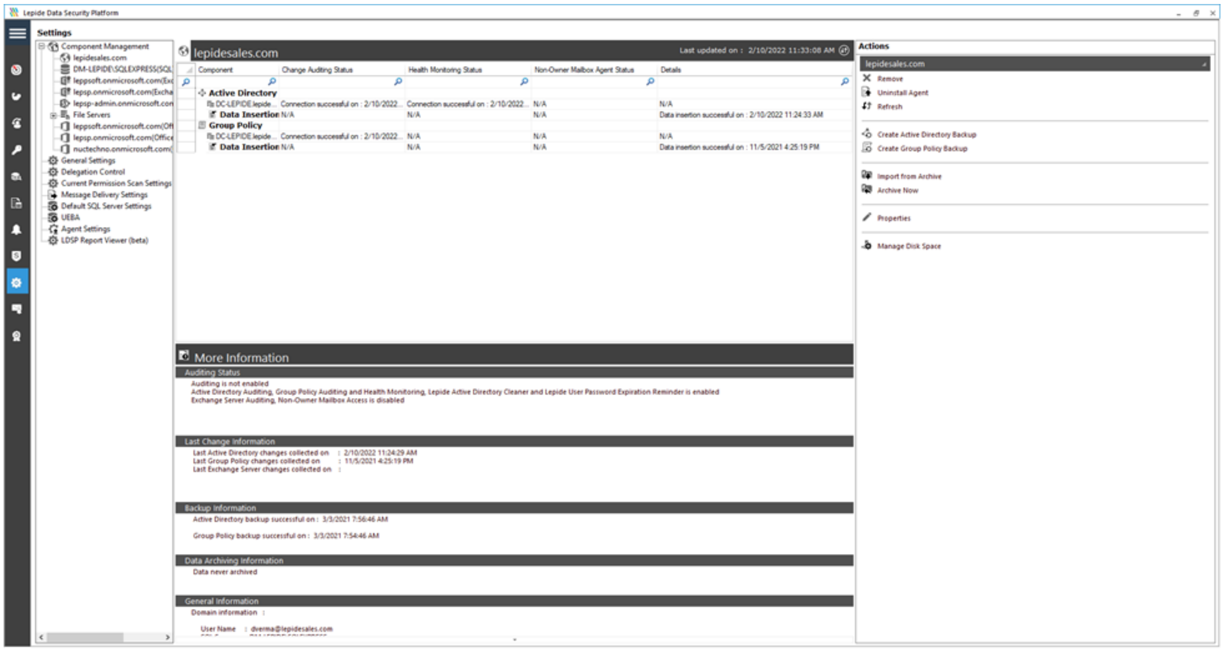
  In the **Weekly** settings, you can specify the time and the days on which backup snapshots will be captured

  In the **Monthly** settings you can specify the time and day of the month to run the backup snapshots

8. Click **OK** to apply the settings and return to the Advanced Domain Configuration dialog box.
9. Click **OK** to return to the Active Directory settings screen.

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

Backup Information can be seen on the lower part of the Active Directory Settings Screen:


Lepide Data Security Platform
Settings
Component Management
lepidesales.com
DM-LEPIDE\SQLEXPRESS(SQL
leppsoft.onmicrosoft.com(Exc
lepsp.onmicrosoft.com(Excha
lepsp-admin.onmicrosoft.con
File Servers
leppsoft.onmicrosoft.com(Off
lepsp.onmicrosoft.com(Office
nuctechno.onmicrosoft.com(
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Report Viewer (beta)
lepidesales.com
Last updated on : 2/10/2022 11:33:08 AM
Actions
lepidesales.com
Remove
Uninstall Agent
Refresh
Create Active Directory Backup
Create Group Policy Backup
Import from Archive
Archive Now
Properties
Manage Disk Space

Component	Change Auditing Status	Health Monitoring Status	Non-Owner Mailbox Agent Status	Details
Active Directory				
DC-LEPIDE.lepide...	Connection successful on : 2/10/2022...	Connection successful on : 2/10/2022...	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 2/10/2022 11:24:33 AM
Group Policy				
DC-LEPIDE.lepide...	Connection successful on : 2/10/2022...	N/A	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 11/5/2021 4:25:19 PM

More Information

Auditing Status

Auditing is not enabled
Active Directory Auditing, Group Policy Auditing and Health Monitoring, Lepide Active Directory Cleaner and Lepide User Password Expiration Reminder is enabled
Exchange Server Auditing, Non-Owner Mailbox Access is disabled

Last Change Information

Last Active Directory changes collected on : 2/10/2022 11:24:29 AM
Last Group Policy changes collected on : 11/5/2021 4:25:19 PM
Last Exchange Server changes collected on :

Backup Information

Active Directory backup successful on : 3/3/2021 7:56:46 AM

Group Policy backup successful on : 3/3/2021 7:54:46 AM

Data Archiving Information

Data never archived

General Information

Domain information :

User Name : dverma@lepidesales.com

Figure 5: Active Directory Settings

5. Capturing Backup Snapshots

Section 4 of this guide explained how to enable and schedule regular backup snapshots. However, there are times when you want to run a backup snapshot immediately to capture the present point in time. For example, as a precaution, before restoring an object it is important to create a backup so you can return to the point before the object was restored if necessary.

5.1. To Create a Backup Snapshot:

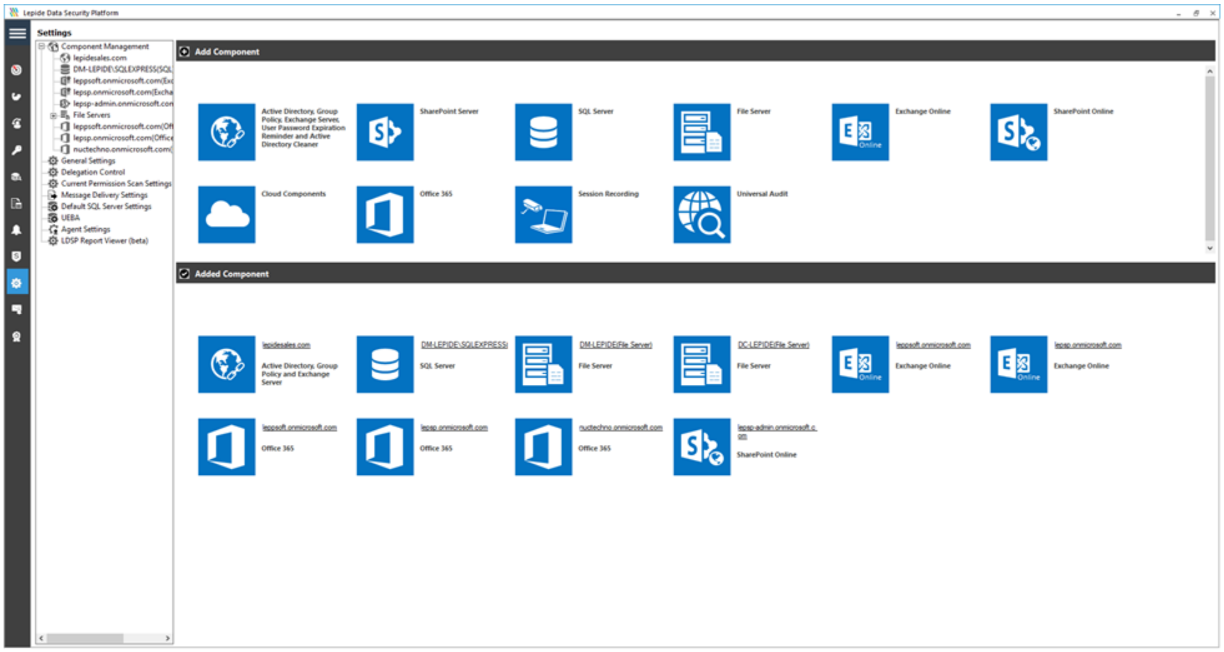
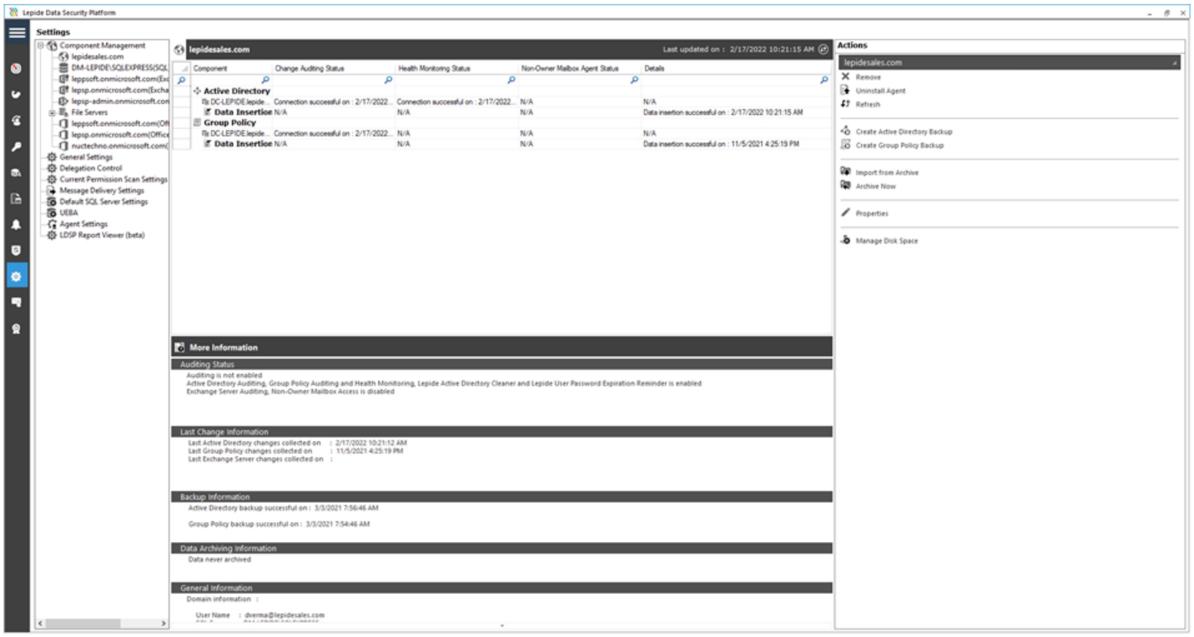


Figure 6: Component Management Window

1. From the Component Management window, click the Settings icon ⚙

2. Click on the **Active Directory Component** and the following screen will be displayed:


Lepide Data Security Platform
Settings
Component Management
lepidesales.com
DM-LEPIDE\SQLEXPRESS(SQL
leppsoft.onmicrosoft.com(Exc
lepsp.onmicrosoft.com(Excha
lepsp-admin.onmicrosoft.con
File Servers
leppsoft.onmicrosoft.com(Off
lepsp.onmicrosoft.com(Office
nuctechno.onmicrosoft.com(
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Report Viewer (beta)
lepidesales.com
Actions
lepidesales.com
Remove
Uninstall Agent
Refresh
Create Active Directory Backup
Create Group Policy Backup
Import from Archive
Archive Now
Properties
Manage Disk Space
More Information

Last updated on : 2/17/2022 10:21:15 AM

Component	Change Auditing Status	Health Monitoring Status	Non-Owner Mailbox Agent Status	Details
Active Directory				
DC-LEPIDE.lepide...	Connection successful on : 2/17/2022...	Connection successful on : 2/17/2022...	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 2/17/2022 10:21:15 AM
Group Policy				
DC-LEPIDE.lepide...	Connection successful on : 2/17/2022...	N/A	N/A	N/A
Data Insertion	N/A	N/A	N/A	Data insertion successful on : 11/5/2021 4:25:19 PM

Auditing Status

Auditing is not enabled
Active Directory Auditing, Group Policy Auditing and Health Monitoring, Lepide Active Directory Cleaner and Lepide User Password Expiration Reminder is enabled
Exchange Server Auditing, Non-Owner Mailbox Access is disabled

Last Change Information

Last Active Directory changes collected on : 2/17/2022 10:21:12 AM
Last Group Policy changes collected on : 11/5/2021 4:25:19 PM
Last Exchange Server changes collected on :

Backup Information

Active Directory backup successful on : 3/3/2021 7:56:46 AM

Group Policy backup successful on : 3/3/2021 7:54:46 AM

Data Archiving Information

Data never archived

General Information

Domain information :

User Name : dverma@lepidesales.com

Figure 7: Actions for a Domain

3. To the right-hand side of this window in the **Actions** pane there are two backup options:

- Click **Create Active Directory Backup** to create a backup snapshot of Active Directory
- Click **Create Group Policy Backup** link to create a backup snapshot of Group Policy

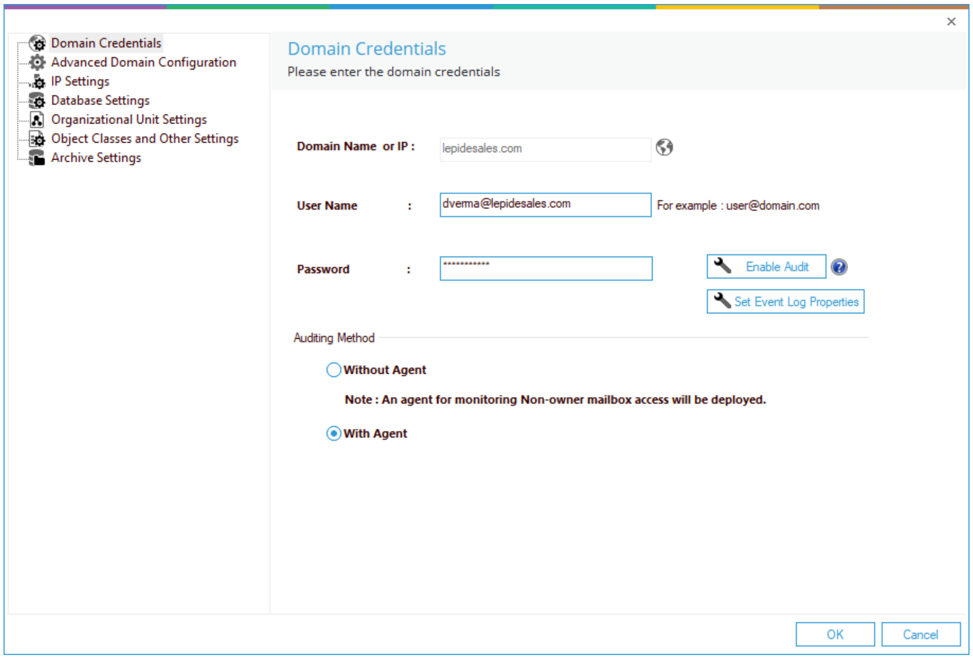
6. Move Backup Snapshot Data

The path for storing the backup snapshot data is set in the Database Settings dialog box. There are times when you may want to change the storage location for example if the storage gets full.

To view the current path and change the location do the following:

1. Click the **Settings** icon from the Component Management Screen
2. Click on the Active Directory Component
3. Click **Properties**

The Domain Credentials dialog box is displayed:



Domain Credentials

Please enter the domain credentials

Domain Name or IP : lepidesales.com

User Name : dverma@lepidesales.com For example : user@domain.com

Password : ***********

Auditing Method

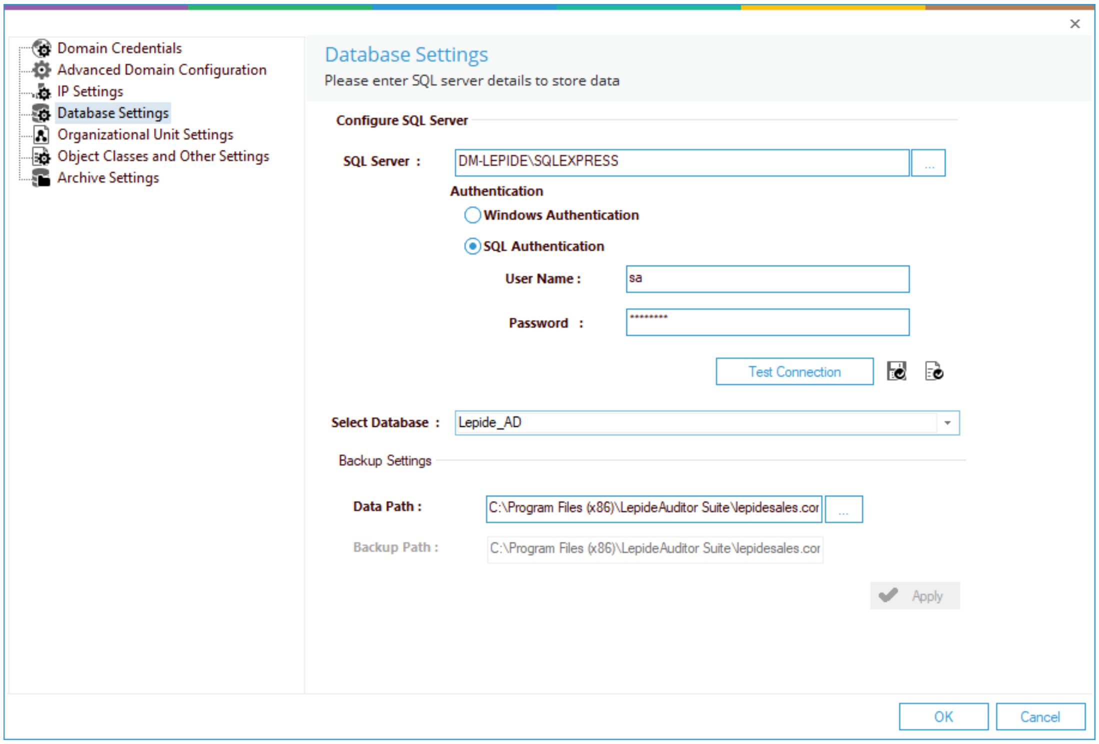
○ Without Agent

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

● With Agent

Figure 8: Domain Credentials

4. Choose **Database Settings** (from the left-hand list of options) and the Database Settings dialog box is displayed:



- Domain Credentials
- Advanced Domain Configuration
- IP Settings
- Database Settings
- Organizational Unit Settings
- Object Classes and Other Settings
- Archive Settings

Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : DM-LEPIDE\SQLEXPRESS

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

Select Database : Lepide_AD

Backup Settings

Data Path : C:\Program Files (x86)\LepideAuditor Suite\lepidesales.cor

Backup Path : C:\Program Files (x86)\LepideAuditor Suite\lepidesales.cor

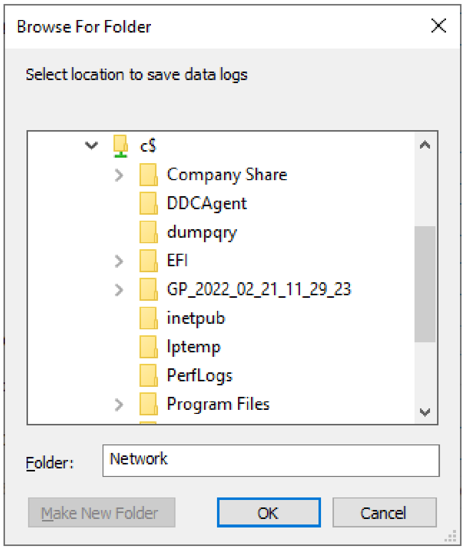
Figure 9: Database Settings

The **Data Path** is displayed under **Backup Settings**.

You can modify the path of both the 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.

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



Browse For Folder

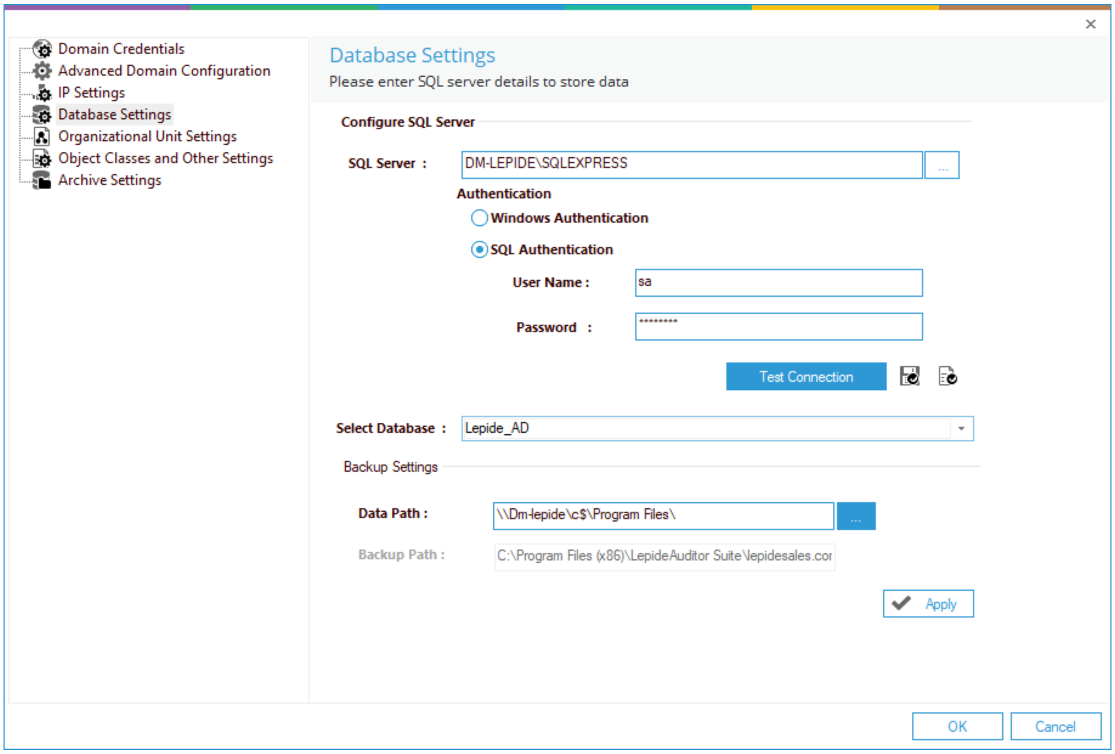
Select location to save data logs

c$
Company Share
DDCAgent
dumpqry
EFI
GP_2022_02_21_11_29_23
inetpub
lptemp
PerfLogs
Program Files

Folder: Network

Figure 10: 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



Domain Credentials
Advanced Domain Configuration
IP Settings
Database Settings
Organizational Unit Settings
Object Classes and Other Settings
Archive Settings

Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : DM-LEPIDE\SQLEXPRESS

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

Select Database : Lepide_AD

Backup Settings

Data Path : \\Dm-lepide\c$\Program Files\

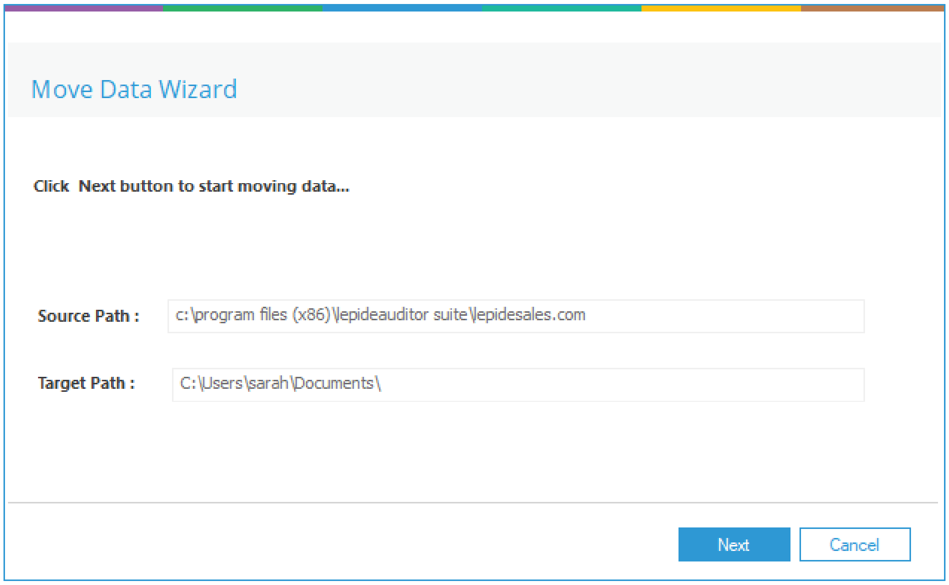
Backup Path : C:\Program Files (x86)\LepideAuditor Suite\lepidesales.cor

Test Connection
Apply
OK
Cancel

Figure 11: Sample Path of New Backup Location

3. Click Apply

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



Move Data Wizard

Click Next button to start moving data...

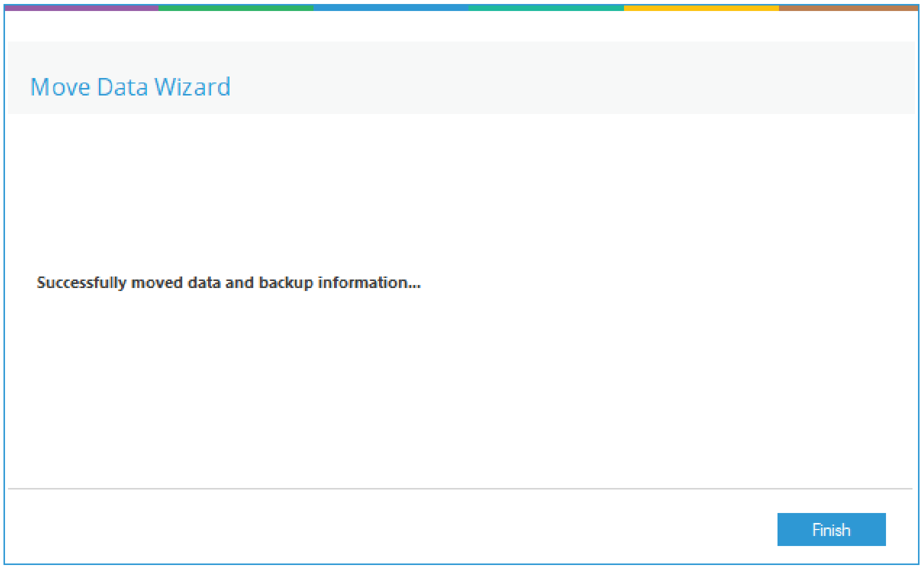
Source Path : c:\program files (x86)\lepideauditor suite\lepidesales.com

Target Path : C:\Users\sarah\Documents\

Figure 12: Utility to Move the Backup Data

4. Click Next to move old backup data to the new location. Select Cancel if you want to keep the old data in its existing location but change the location of new backup data.

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



Move Data Wizard

Successfully moved data and backup information...

Figure 13: 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**

7. Restore Active Directory Objects

There are two ways to restore Active Directory objects. Objects can be restored individually using **Active Directory Reports** or they can be restored using the **Restore Wizard** for larger numbers of objects.

7.1. Restore from Active Directory Reports

- From the Component Management Window, click the **User & Entity Behavior Analytics** icon
- To the left-hand side of the screen is a tree structure listing the reports

1. Expand the **file server name** (from the tree structure)
2. Expand **Active Directory Reports**
3. Expand **Active Directory Modification Reports**
4. Expand **All Modification Reports**
5. Select **Object Modifications**

The Object Modifications Report is displayed:

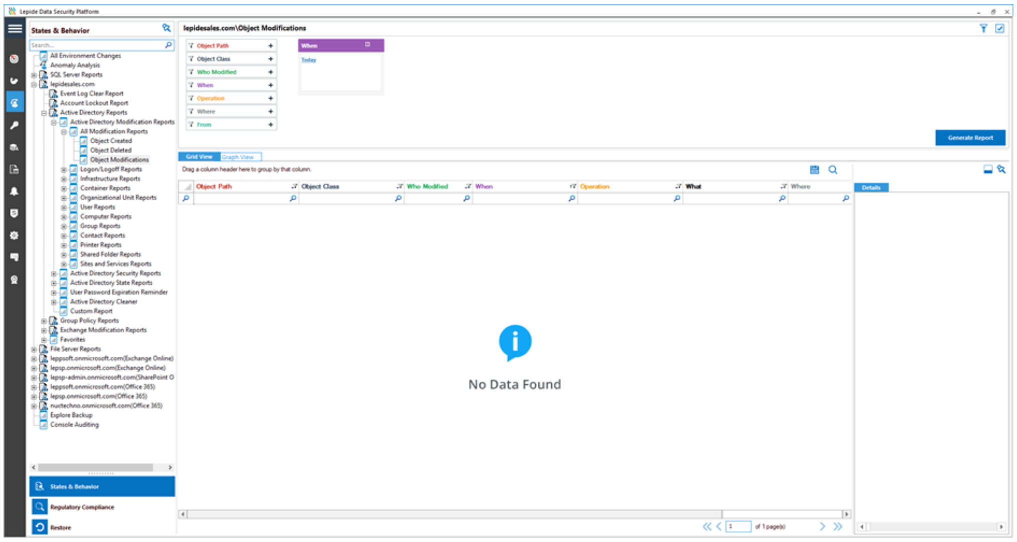
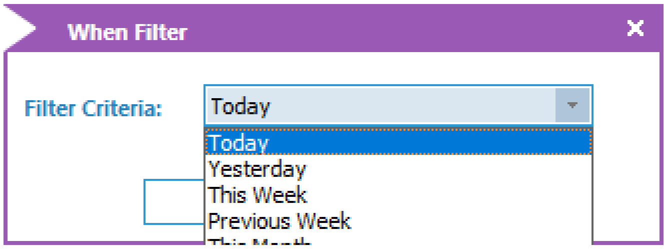


Figure 14: Object Modifications Report

6. From the **When** Box at the top, click on **Today**

The When Filter dialog box is displayed:

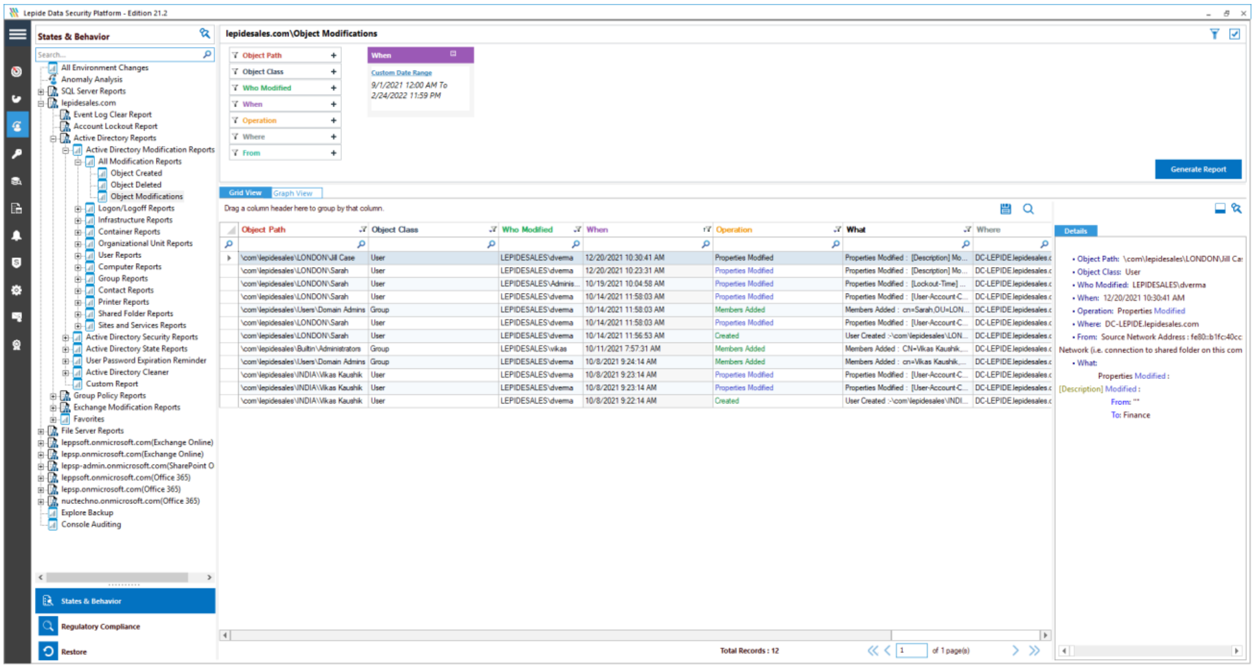


Filter Criteria: Today

Figure 15: When Filter

7. Choose a date range from the drop-down menu
8. Click OK
9. Click Generate

The report will run and will display information on all modifications made:



lepidesales.com\Object Modifications

When: Custom Date Range 9/1/2021 12:00 AM To 2/24/2022 11:59 PM

Drag a column header here to group by that column.

Object Path	Object Class	Who Modified	When	Operation	What	Where
\com\lepidesales\LONDON\Jill Case	User	LEPIDESALES\dverma	12/20/2021 10:30:41 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.c
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	12/20/2021 10:23:31 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.c
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\Adminis...	10/19/2021 10:04:58 AM	Properties Modified	Properties Modified : [Lockout-Time] ...	DC-LEPIDE.lepidesales.c
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.c
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Members Added	Members Added : cn=Sarah,OU=LON...	DC-LEPIDE.lepidesales.c
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.c
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:56:53 AM	Created	User Created :-\com\lepidesales\LON...	DC-LEPIDE.lepidesales.c
\com\lepidesales\Builtin\Administrators	Group	LEPIDESALES\vikas	10/11/2021 7:57:31 AM	Members Added	Members Added : CN=Vikas Kaushik,...	DC-LEPIDE.lepidesales.c
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/8/2021 9:24:14 AM	Members Added	Members Added : cn=Vikas Kaushik,...	DC-LEPIDE.lepidesales.c
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.c
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.c
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:22:14 AM	Created	User Created :-\com\lepidesales\INDI...	DC-LEPIDE.lepidesales.c

Total Records : 12

1 of 1 page(s)

- Object Path: \com\lepidesales\LONDON\Jill Ca
- Object Class: User
- Who Modified: LEPIDESALES\dverma
- When: 12/20/2021 10:30:41 AM
- Operation: Properties Modified
- Where: DC-LEPIDE.lepidesales.com
- From: Source Network Address : fe80::b1fc:40cc

Network (i.e. connection to shared folder on this com

- What:

Properties Modified :

[Description] Modified :

From: ""

To: Finance

Figure 16: Object Modifications Report

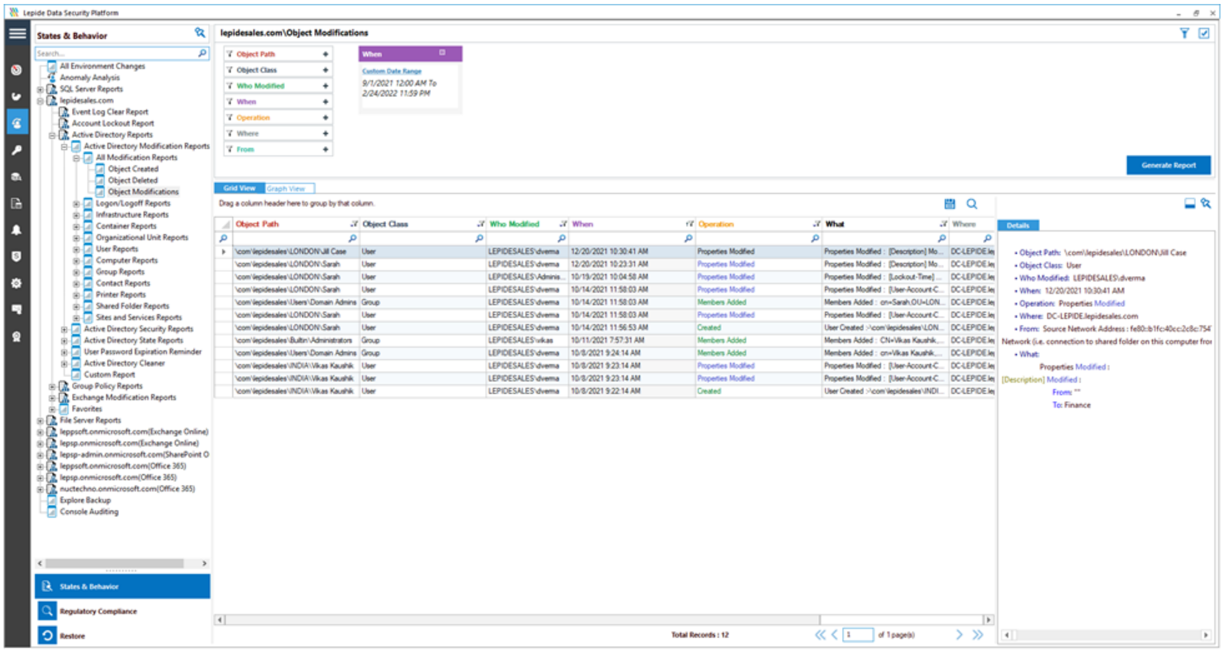
If no data is displayed, it could be because you need to run an Active Directory scan. For information on how to do this, see Section 7.2, Configure the Solution to Run a Scan.

The Object Modifications Report

This report lists information about each object modification with column headings including Object Path, Object Class, Who Modified, When and the Operation performed.

When a row is selected, further information as to what was modified is displayed in the Details section to the right-hand side of the report.

In the example below the first row has been selected. This shows that User Properties were modified. In the Details window to the right, there is more information on exactly what has been modified. It shows that the Description was changed from "" to Finance:



When
Custom Date Range
9/1/2021 12:00 AM To 2/24/2022 11:59 PM

Drag a column header here to group by that column.

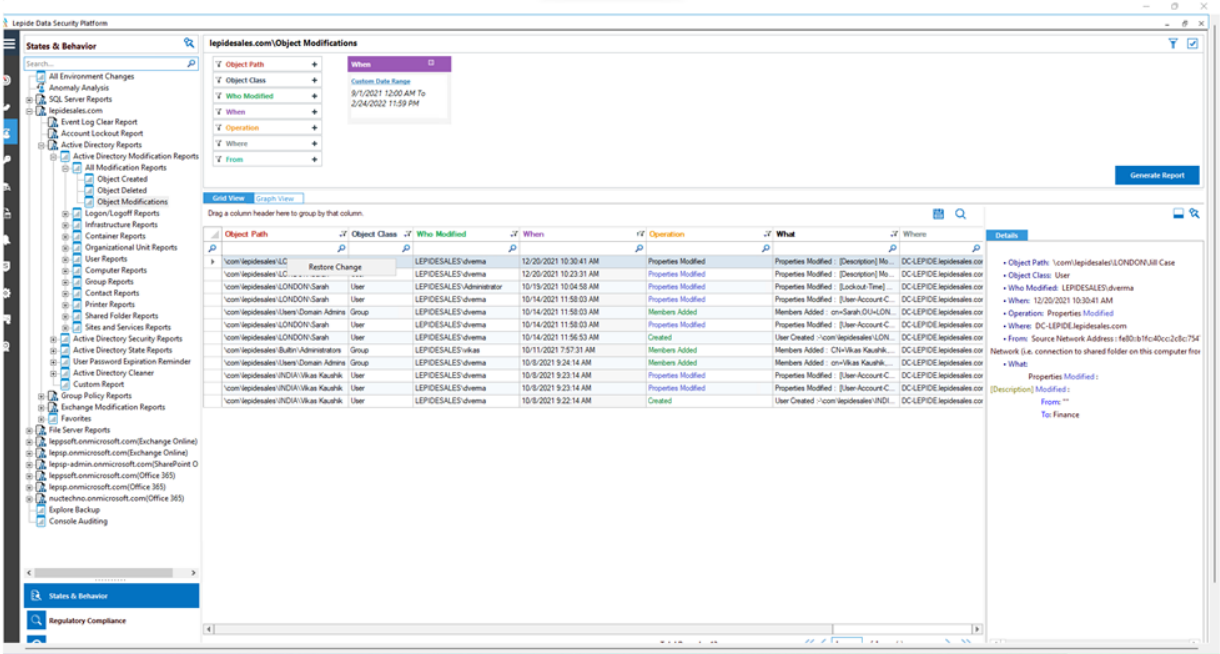
Object Path	Object Class	Who Modified	When	Operation	What	Where
\com\lepidesales\LONDON\Jill Case	User	LEPIDESALES\dverma	12/20/2021 10:30:41 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.le
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	12/20/2021 10:23:31 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.le
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\Adminis...	10/19/2021 10:04:58 AM	Properties Modified	Properties Modified : [Lockout-Time] ...	DC-LEPIDE.le
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.le
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Members Added	Members Added : cn=Sarah,OU=LON...	DC-LEPIDE.le
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.le
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:56:53 AM	Created	User Created :-\com\lepidesales\LON...	DC-LEPIDE.le
\com\lepidesales\Builtin\Administrators	Group	LEPIDESALES\vikas	10/11/2021 7:57:31 AM	Members Added	Members Added : CN=Vikas Kaushik,...	DC-LEPIDE.le
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/8/2021 9:24:14 AM	Members Added	Members Added : cn=Vikas Kaushik,...	DC-LEPIDE.le
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.le
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.le
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:22:14 AM	Created	User Created :-\com\lepidesales\INDI...	DC-LEPIDE.le

Total Records : 12 1 of 1 page(s)

- Object Path: \com\lepidesales\LONDON\Jill Case
- Object Class: User
- Who Modified: LEPIDESALES\dverma
- When: 12/20/2021 10:30:41 AM
- Operation: Properties Modified
- Where: DC-LEPIDE.lepidesales.com
- From: Source Network Address : fe80::b1fc:40cc:2c8c:754
Network (i.e. connection to shared folder on this computer fro
- What:
Properties Modified :
[Description] Modified :
From: ""
To: Finance

Figure 17: Object Modifications Report Showing Details Window

To restore this change, you can right click on the row:



Object Path	Object Class	Who Modified	When	Operation	What	Where
\com\lepidesales\LC		LEPIDESALES\dverma	12/20/2021 10:30:41 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LC		LEPIDESALES\dverma	12/20/2021 10:23:31 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\Administrator	10/19/2021 10:04:58 AM	Properties Modified	Properties Modified : [Lockout-Time] ...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Members Added	Members Added : cn=Sarah,OU=LON...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:56:53 AM	Created	User Created :-\com\lepidesales\LON...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Builtin\Administrators	Group	LEPIDESALES\vikas	10/11/2021 7:57:31 AM	Members Added	Members Added : CN=Vikas Kaushik,...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/8/2021 9:24:14 AM	Members Added	Members Added : cn=Vikas Kaushik,...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:22:14 AM	Created	User Created :-\com\lepidesales\INDI...	DC-LEPIDE.lepidesales.cor

- Object Path: \com\lepidesales\LONDON\Jill Case
- Object Class: User
- Who Modified: LEPIDESALES\dverma
- When: 12/20/2021 10:30:41 AM
- Operation: Properties Modified
- Where: DC-LEPIDE.lepidesales.com
- From: Source Network Address : fe80::b1fc:40cc:2c8c:754
Network (i.e. connection to shared folder on this computer fro
- What:
Properties Modified :
[Description] Modified :
From: ""
To: Finance

Figure 18: Restore Change Option

To Restore the change:

1. Right click on the row to be restored
2. Select Restore Change
3. The following message box will appear:

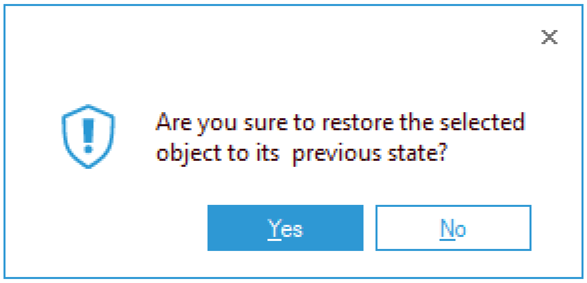
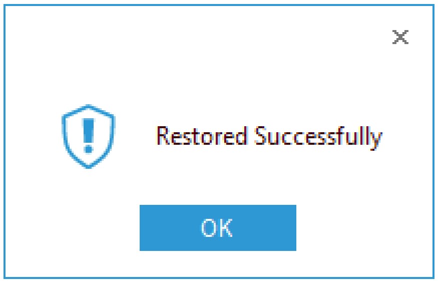

Are you sure to restore the selected object to its previous state?

Figure 19: Asking to Confirm Restore of Object State

4. Choose Yes and the change will be restored.

   A message box will appear confirming it has been restored successfully:

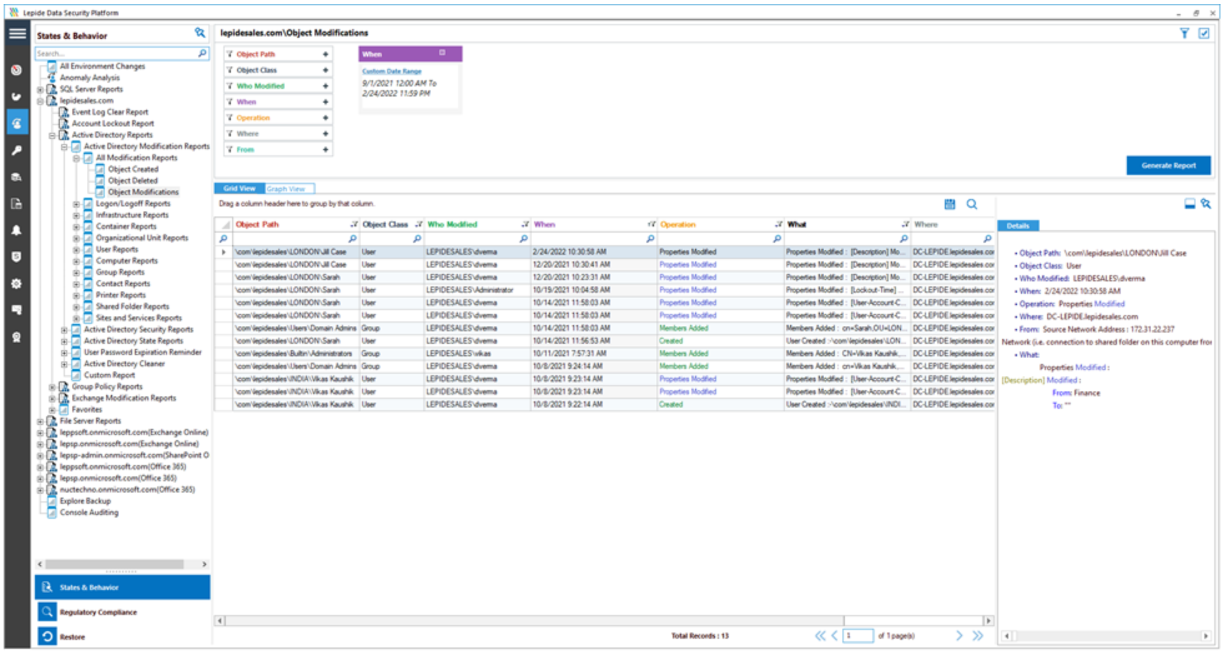


Restored Successfully

Figure 20: Restored Successfully

5. Click OK

Now when you run the Object Modifications Report you will see the modification listed showing it has been restored back to its previous state:



When
Custom Date Range
9/1/2021 12:00 AM To 2/24/2022 11:59 PM

Drag a column header here to group by that column.

Object Path	Object Class	Who Modified	When	Operation	What	Where
\com\lepidesales\LONDON\Jill Case	User	LEPIDESALES\dverma	2/24/2022 10:30:58 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Jill Case	User	LEPIDESALES\dverma	12/20/2021 10:30:41 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	12/20/2021 10:23:31 AM	Properties Modified	Properties Modified : [Description] Mo...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\Administrator	10/19/2021 10:04:58 AM	Properties Modified	Properties Modified : [Lockout-Time] ...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/14/2021 11:58:03 AM	Members Added	Members Added : cn=Sarah,OU=LON...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\LONDON\Sarah	User	LEPIDESALES\dverma	10/14/2021 11:56:53 AM	Created	User Created :-\com\lepidesales\LON...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Builtin\Administrators	Group	LEPIDESALES\vikas	10/11/2021 7:57:31 AM	Members Added	Members Added : CN=Vikas Kaushik,...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\Users\Domain Admins	Group	LEPIDESALES\dverma	10/8/2021 9:24:14 AM	Members Added	Members Added : cn=Vikas Kaushik,...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:23:14 AM	Properties Modified	Properties Modified : [User-Account-C...	DC-LEPIDE.lepidesales.cor
\com\lepidesales\INDIA\Vikas Kaushik	User	LEPIDESALES\dverma	10/8/2021 9:22:14 AM	Created	User Created :-\com\lepidesales\INDI...	DC-LEPIDE.lepidesales.cor

Total Records : 13

- Object Path: \com\lepidesales\LONDON\Jill Case
- Object Class: User
- Who Modified: LEPIDESALES\dverma
- When: 2/24/2022 10:30:58 AM
- Operation: Properties Modified
- Where: DC-LEPIDE.lepidesales.com
- From: Source Network Address : 172.31.22.237

Network (i.e. connection to shared folder on this computer fro

- What:

Properties Modified :
[Description] Modified :
From: Finance
To: ""

Figure 21: Object Modifications Report

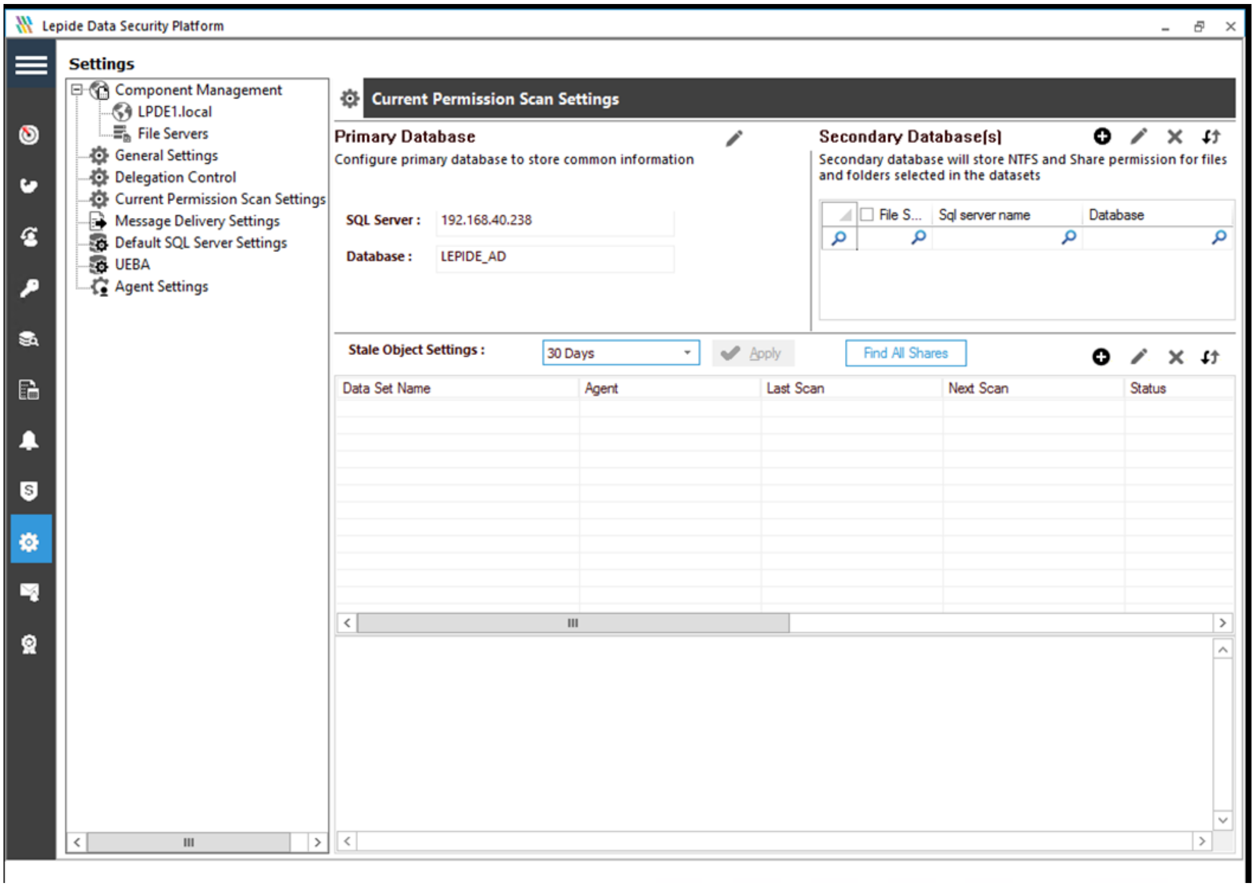
In the example above, the modification has been restored and the Description has changed back from Finance to "".

7.2. Configure the Solution to Run a Scan

The Lepide Data Security Platform needs to be configured to run an Active Directory scan before the report can be run and the steps to do this are as follows:

1. Click on the **Settings** icon ⚙
2. Click on **Current Permission Scan Settings**

The following screen will be displayed:



Lepide Data Security Platform
Settings
Component Management
LPDE1.local
File Servers
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
Current Permission Scan Settings
Apply
Find All Shares

Primary Database

Configure primary database to store common information

SQL Server : 192.168.40.238

Database : LEPIDE_AD

Secondary Database(s)

Secondary database will store NTFS and Share permission for files and folders selected in the datasets

File S...	Sql server name	Database

Stale Object Settings : 30 Days

Data Set Name	Agent	Last Scan	Next Scan	Status

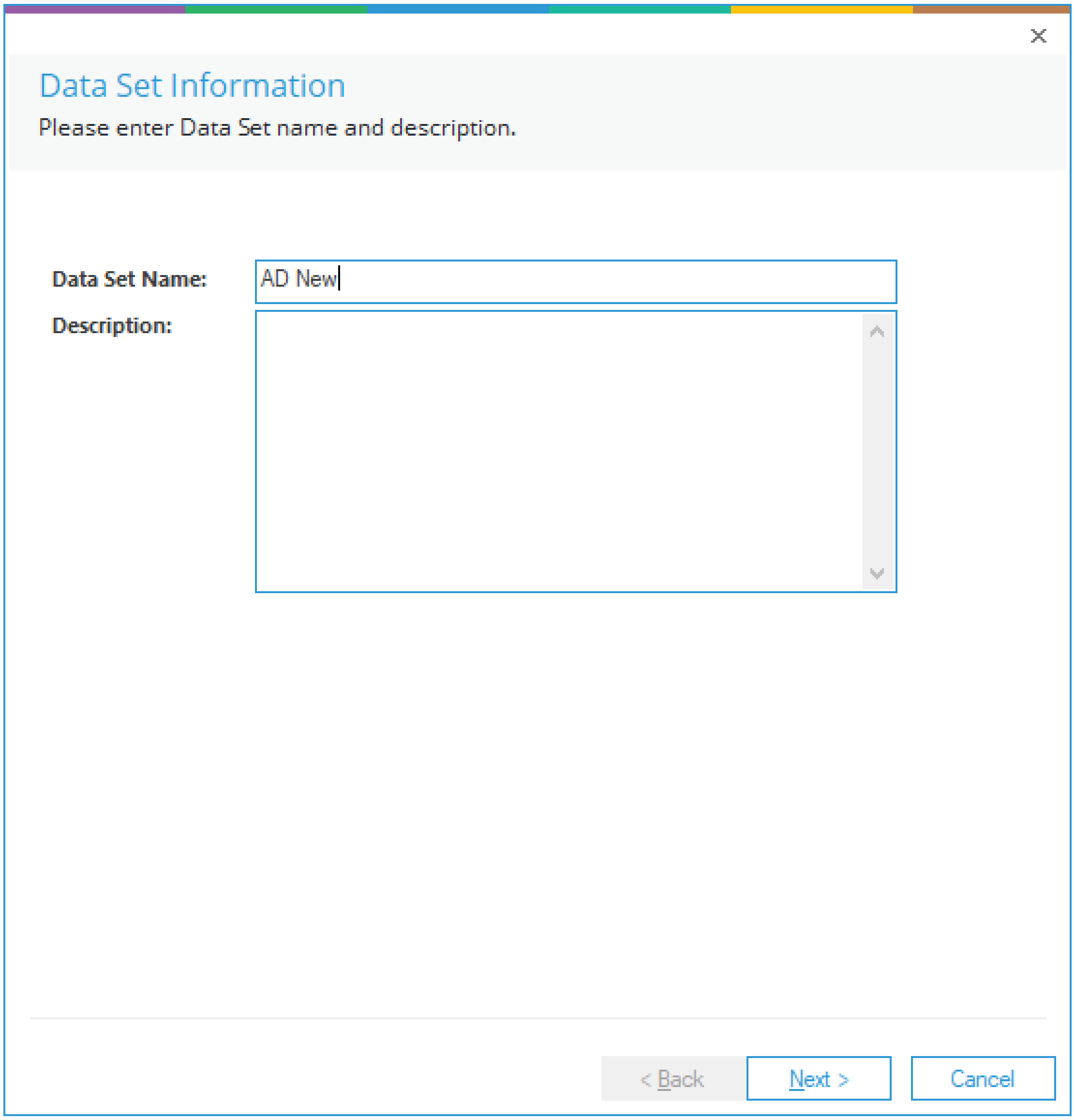
Figure 22: Current Permission Scan Settings

Adding a Dataset

The middle section of the screen will show the data set information.

3. To add a data set, click the ⊕ button (from the middle section of the screen)

The Data Set Information dialog box is displayed:



Data Set Information

Please enter Data Set name and description.

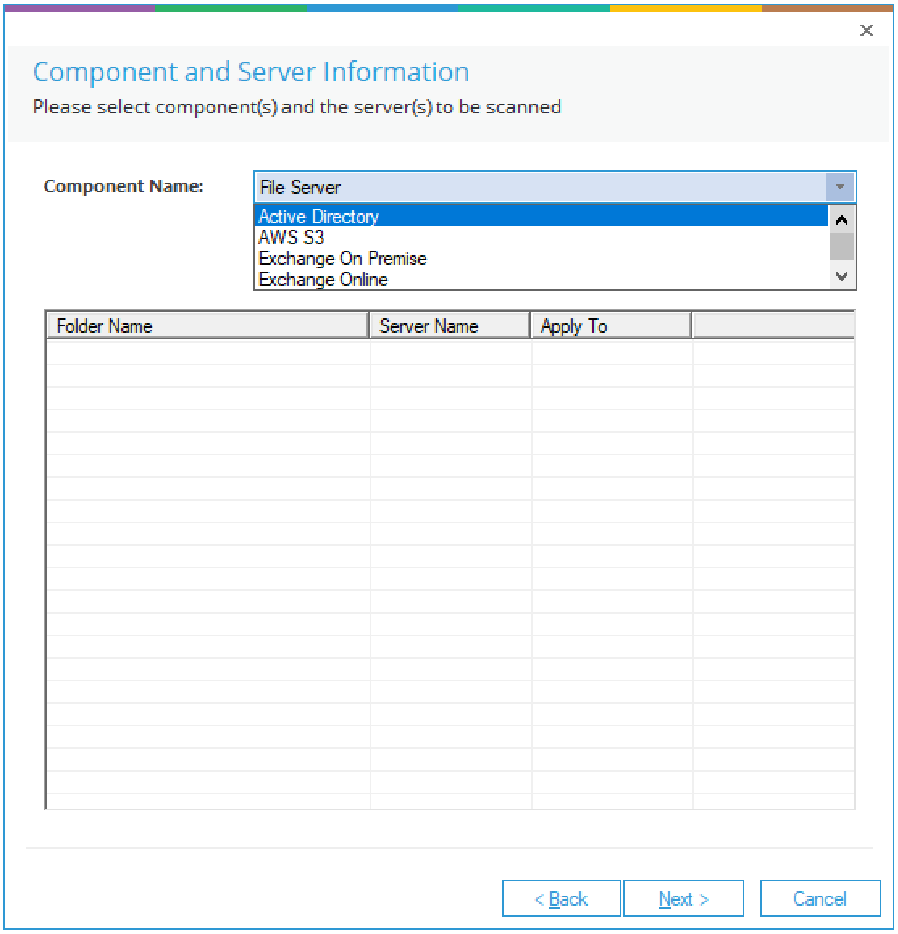
Data Set Name: AD New

Description:

Figure 23: Data Set Information

4. Type in a Data Set Name and a Description
5. Click Next

The Component and Server Information dialog box is displayed:



Component and Server Information

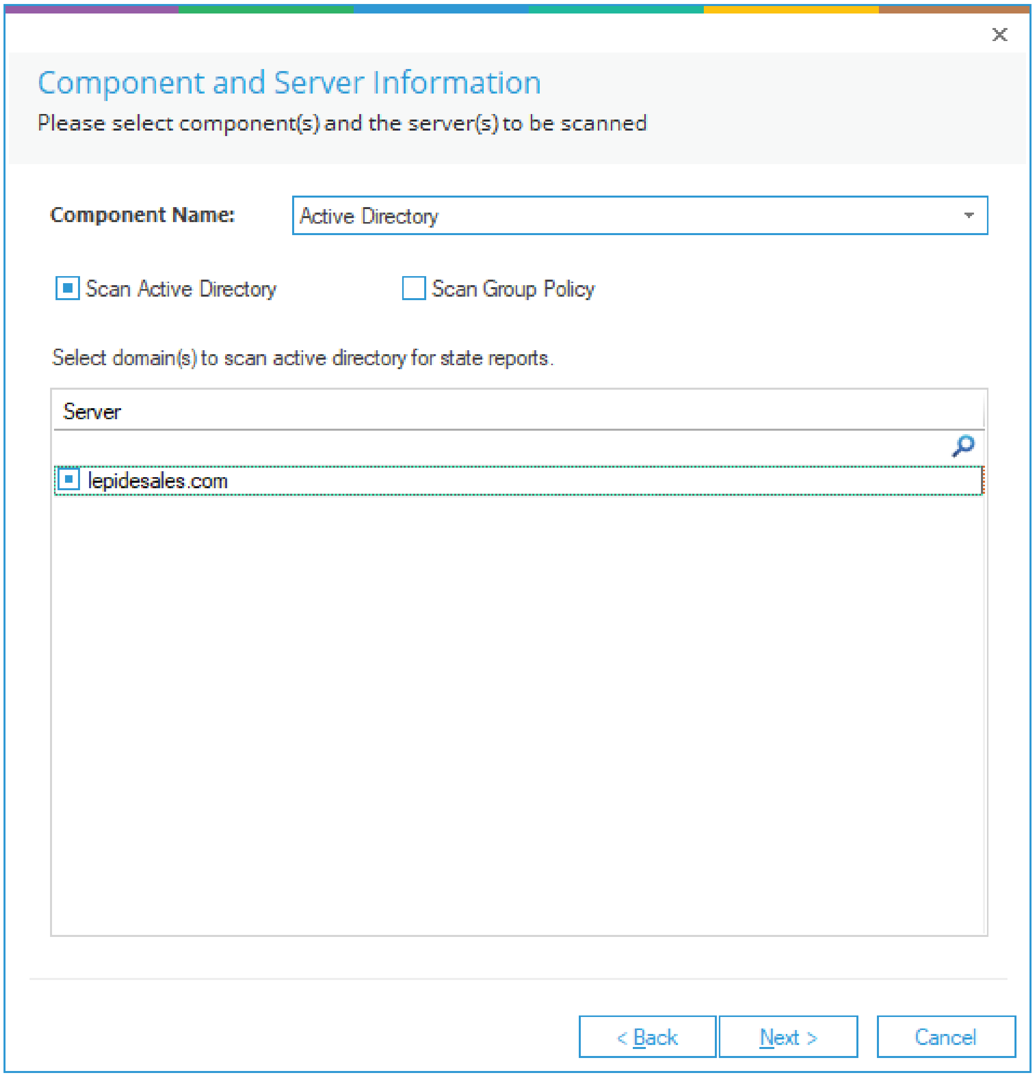
Please select component(s) and the server(s) to be scanned

Component Name: File Server

Figure 24: Component and Server Information

6. From the Component Name drop down, select Active Directory (you may need to scroll up to see Active Directory in the list).

The Active Directory options will now be displayed in the dialog box:



Component and Server Information

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

Component Name: Active Directory

■ Scan Active Directory □ Scan Group Policy

Select domain(s) to scan active directory for state reports.

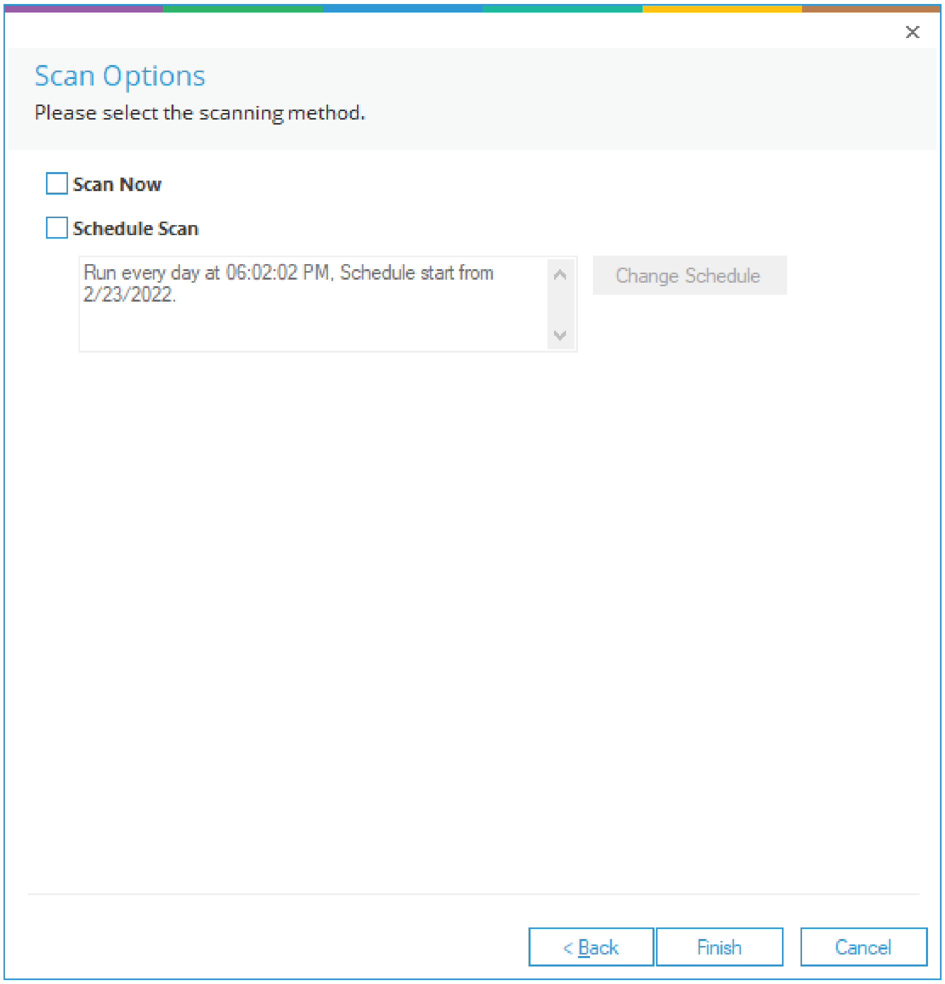
Server

■ lepidesales.com

Figure 25: Active Directory Options

7. Check the Scan Active Directory box
8. Select the domain(s) to scan active directory for state reports
9. Click Next

The Scan Options dialog box will be displayed:



Scan Options

Please select the scanning method.

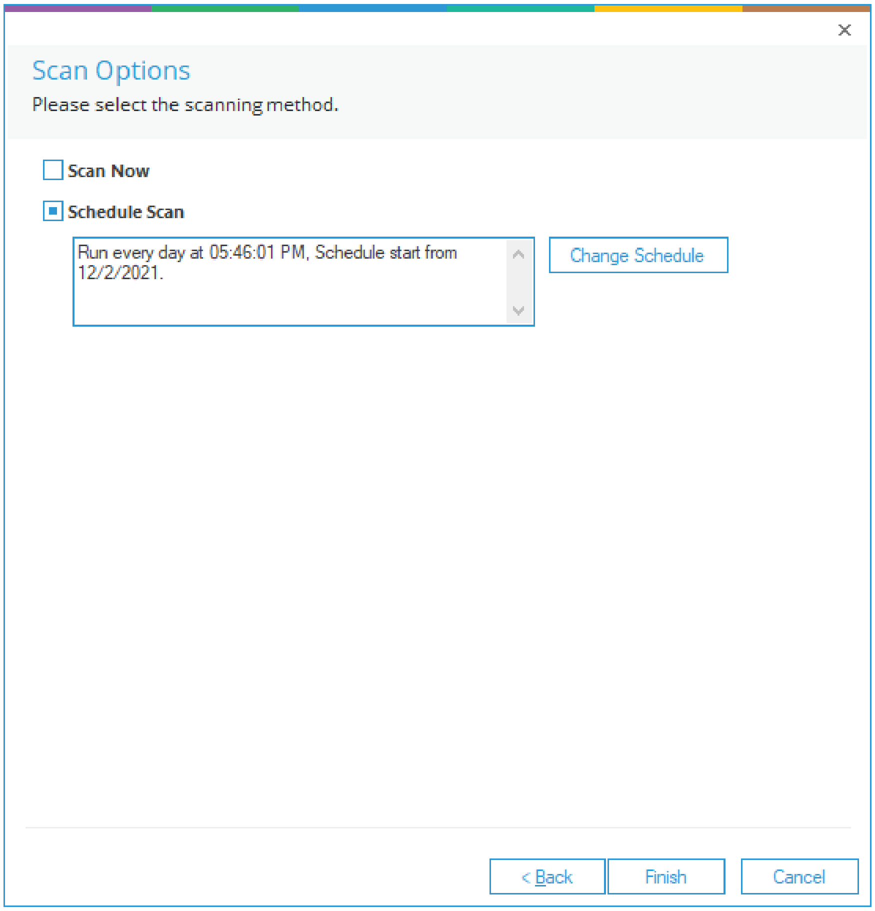
□ Scan Now

□ Schedule Scan

Run every day at 06:02:02 PM, Schedule start from 2/23/2022.

Figure 26: Scan Options

10. Select to Scan Now and/or Schedule Scan



Scan Options

Please select the scanning method.

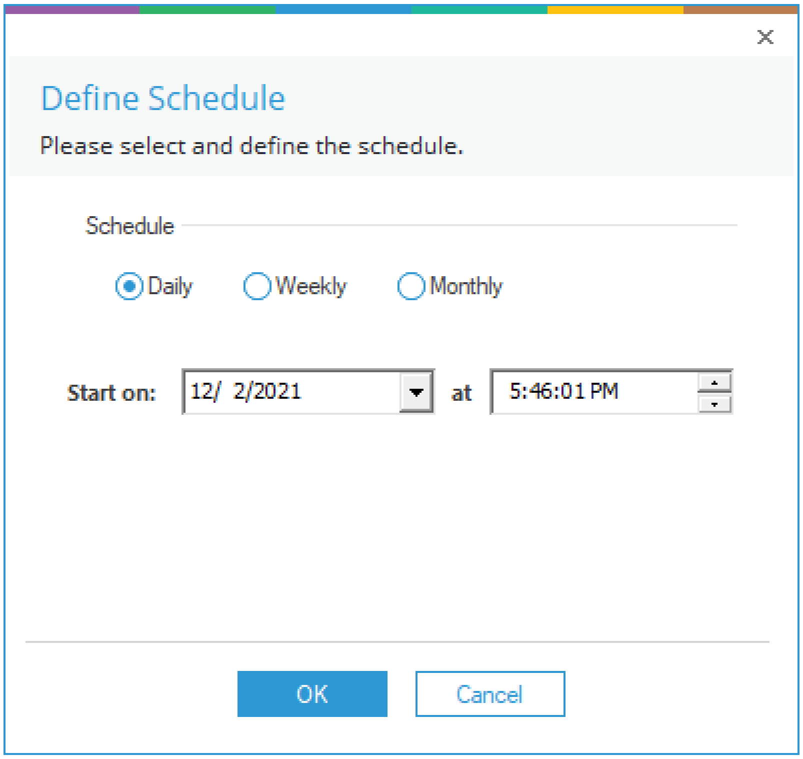
□ Scan Now

■ Schedule Scan

Run every day at 05:46:01 PM, Schedule start from 12/2/2021.

Figure 27: Scan Options, Schedule Scan

11. Choose Schedule Scan for the Change Schedule button to be enabled.
12. Click the Change Schedule button to change the frequency and times of the scan if required:



Define Schedule

Please select and define the schedule.

Schedule

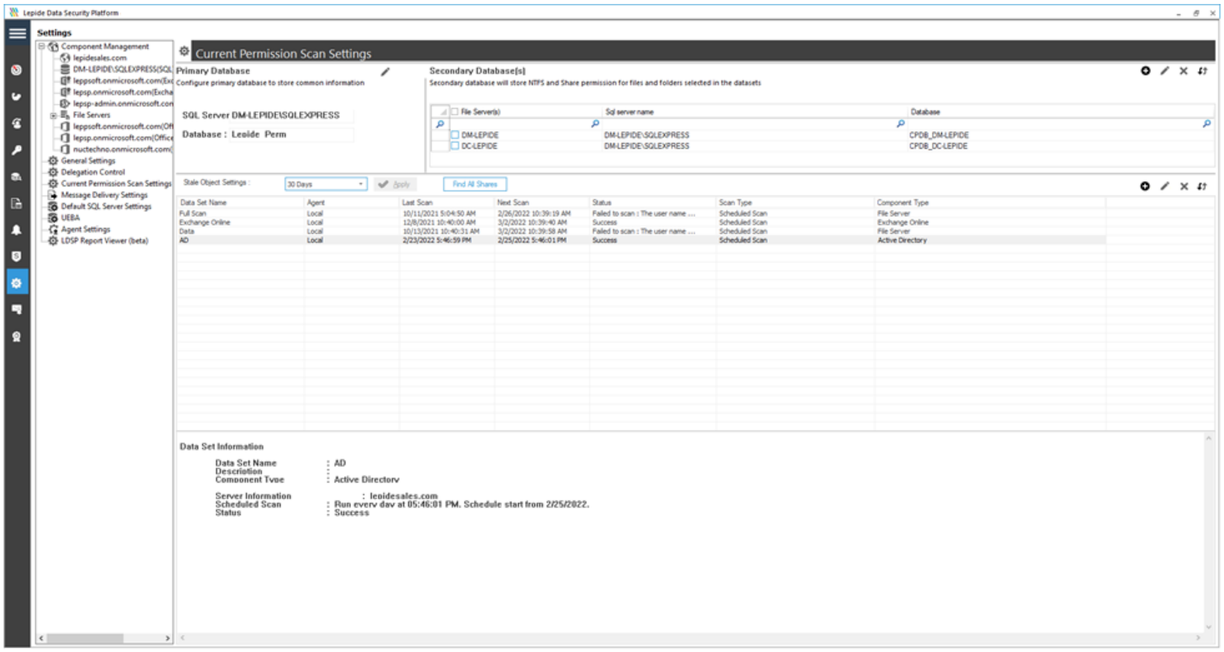
● Daily ○ Weekly ○ Monthly

Start on: 12/ 2/2021 at 5:46:01 PM

Figure 28: Define Schedule

13. Click OK once the schedule settings are updated.
14. Click Finish

The Data Set information is now displayed in the middle part of the screen:


Lepide Data Security Platform
Settings
Component Management
lepidesales.com
DM-LEPIDE\SQLEXPRESS(SQL
leppsoft.onmicrosoft.com(Exc
lepsp.onmicrosoft.com(Excha
lepsp-admin.onmicrosoft.con
File Servers
leppsoft.onmicrosoft.com(Off
lepsp.onmicrosoft.com(Office
nuctechno.onmicrosoft.com(
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Report Viewer (beta)
Current Permission Scan Settings
Apply
Find All Shares

Primary Database

Configure primary database to store common information

SQL Server DM-LEPIDE\SQLEXPRESS

Database : Leoide Perm

Secondary Database[s]

Secondary database will store NTFS and Share permission for files and folders selected in the datasets

□ File Server(s)	Sql server name	Database
□ DM-LEPIDE	DM-LEPIDE\SQLEXPRESS	CPDB_DM-LEPIDE
□ DC-LEPIDE	DM-LEPIDE\SQLEXPRESS	CPDB_DC-LEPIDE

Stale Object Settings : 30 Days

Data Set Name	Agent	Last Scan	Next Scan	Status	Scan Type	Component Type
Full Scan	Local	10/11/2021 5:04:50 AM	2/26/2022 10:39:19 AM	Failed to scan : The user name ...	Scheduled Scan	File Server
Exchange Online	Local	12/8/2021 10:40:00 AM	3/2/2022 10:39:40 AM	Success	Scheduled Scan	Exchange Online
Data	Local	10/13/2021 10:40:31 AM	3/2/2022 10:39:58 AM	Failed to scan : The user name ...	Scheduled Scan	File Server
AD	Local	2/23/2022 5:46:59 PM	2/25/2022 5:46:01 PM	Success	Scheduled Scan	Active Directory

Data Set Information

Data Set Name : AD
Descriotion :
Comoonent Tvoe : Active Directorv

Server Information : leoidesales.com
Scheduled Scan : Run everv dav at 05:46:01 PM. Schedule start from 2/25/2022.
Status : Success

Figure 29: Data Set Settings

7.3. The Lepide Object Restore Wizard

The Lepide Object Restore Wizard enables you to roll-back unwanted changes to their original state in a single click.

Follow the steps below to restore the added, deleted, modified, renamed, or moved objects from the Backup Snapshots:

> NOTE: It is essential to create a backup of the current Active Directory so that you can revert to this current state after restoring an object if required. See Section 4 of this document for the steps on how to create a backup.

- Click the User and Behavior Entity Analytics icon to display the States & Behavior window:

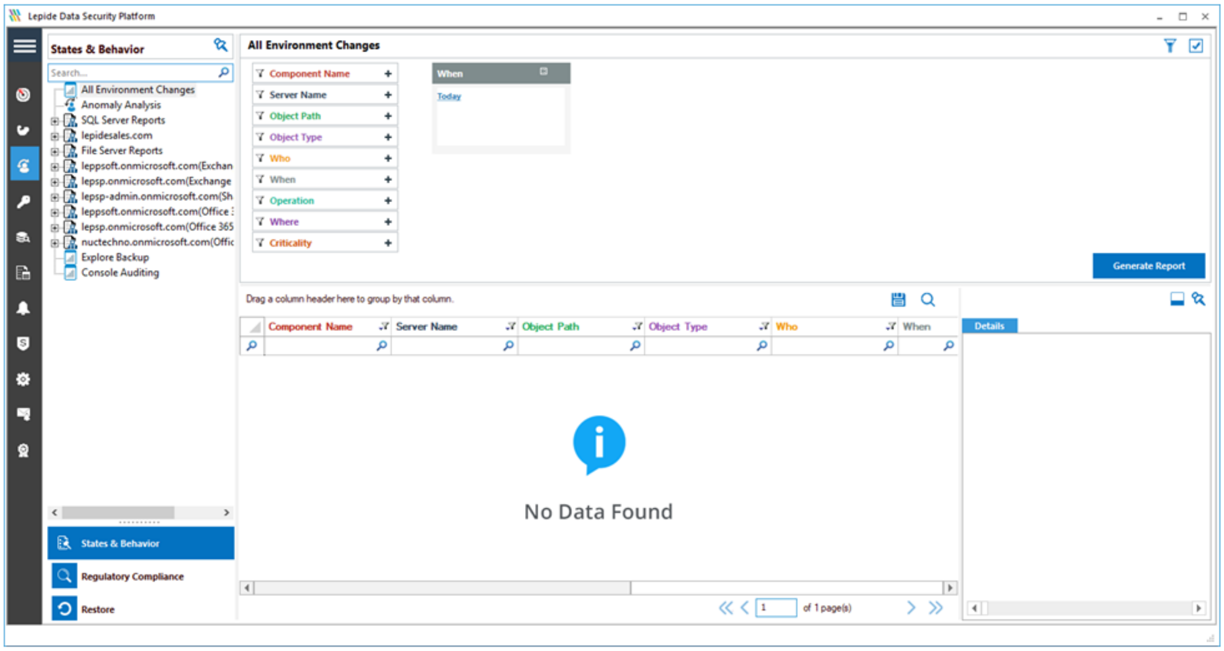
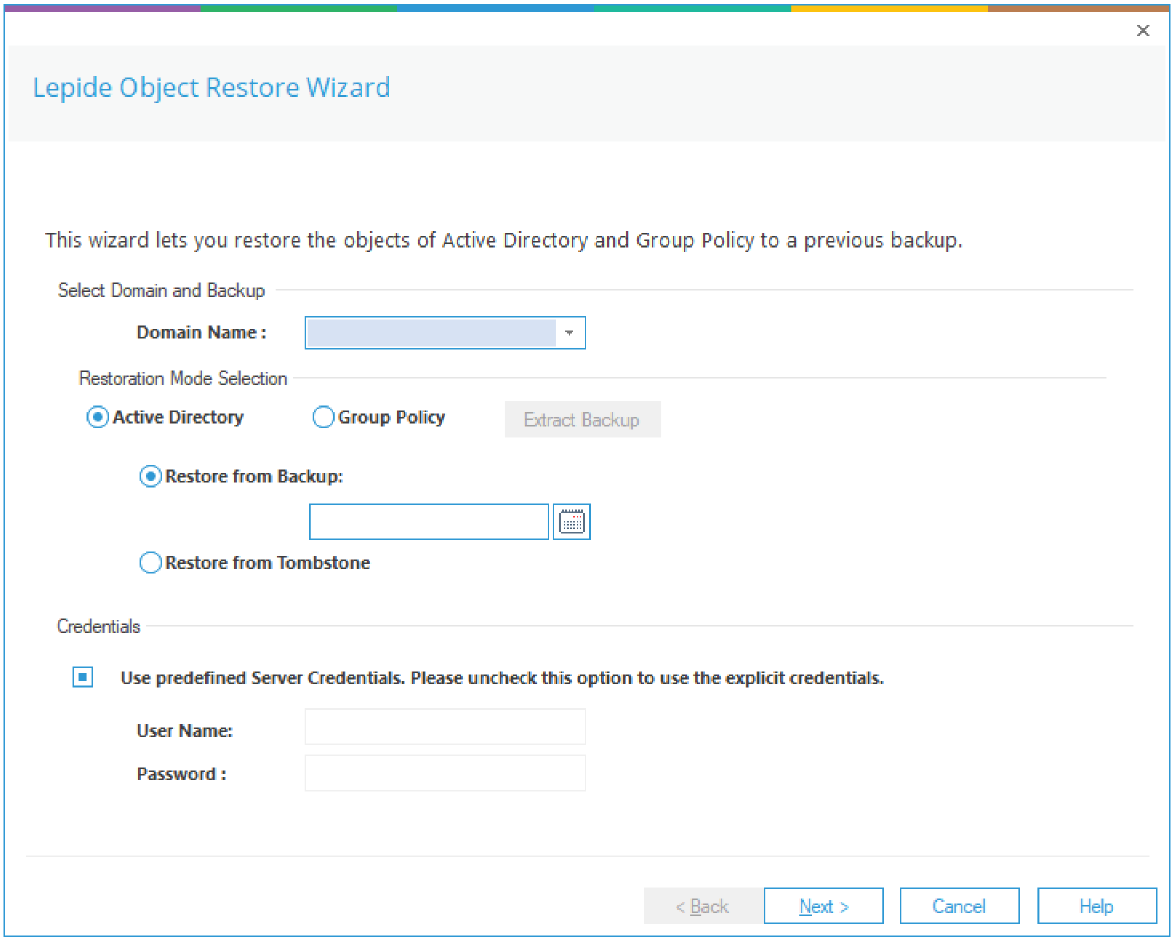


Figure 30: States & Behavior Window

- On the lower left of the window under **States & Behavior** is **Restore**
- Click the Restore icon

The Lepide Object Restore Wizard dialog box will be displayed:



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name :

Restoration Mode Selection

● Active Directory ○ Group Policy

● Restore from Backup:

○ Restore from Tombstone

Credentials

☑ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 31: Object Restore Wizard

1. Select the **Domain Name** from the drop-down list
2. From the **Restoration Mode Selection** section, choose **Active Directory**
3. Choose the **Restore from Backup** option to restore the objects using Backup Snapshots
4. Click the Calendar icon 📅 to choose a date. The following dialog box is displayed:

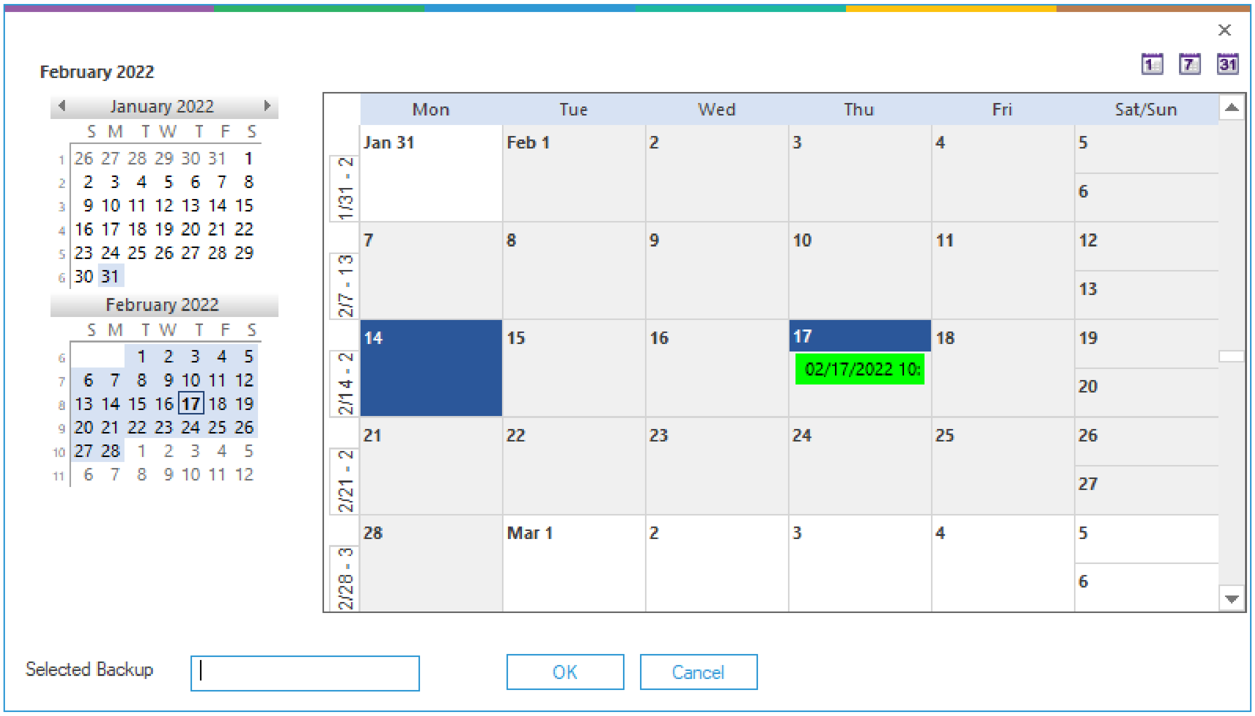


Figure 32: Selecting a Backup

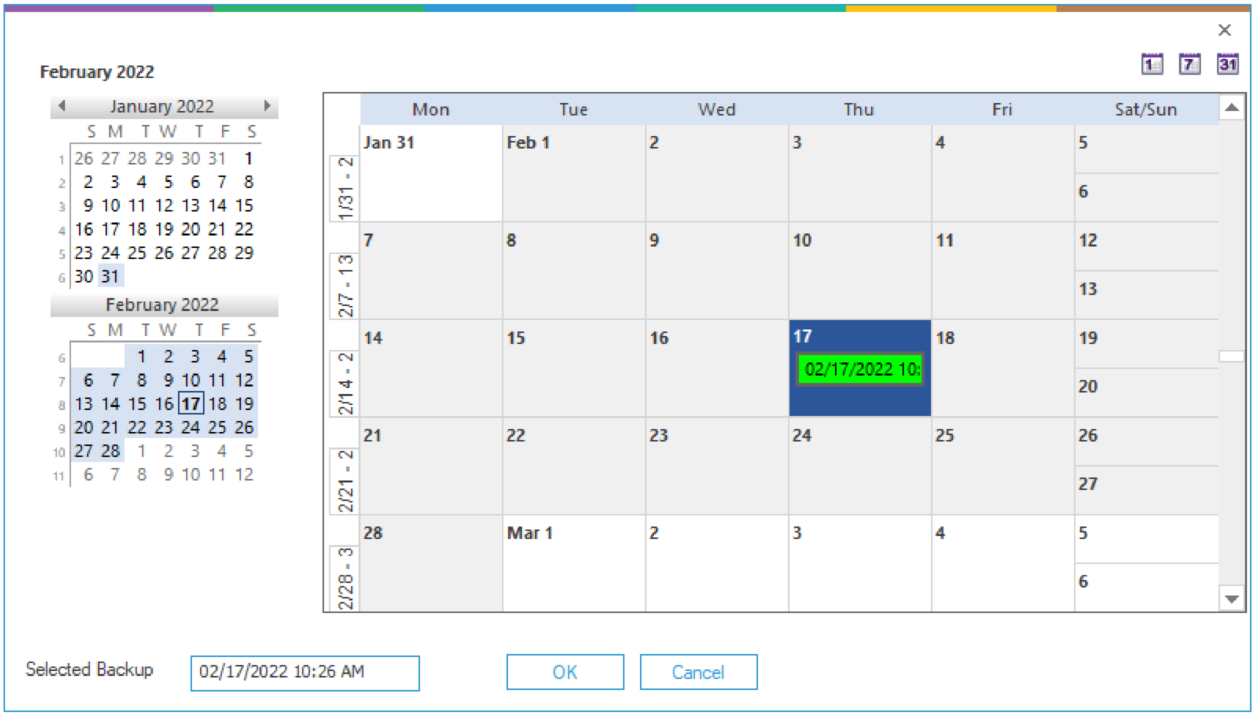
This dialog box provides a way to select the required backup with the left panel showing the calendars by months and the right panel displaying either month, week or day depending on which view has been selected.

The backups will be displayed in date and time format.

To change the calendar view, use one of the three buttons at the top:

1	24 hours
7	7 days
31	31 days

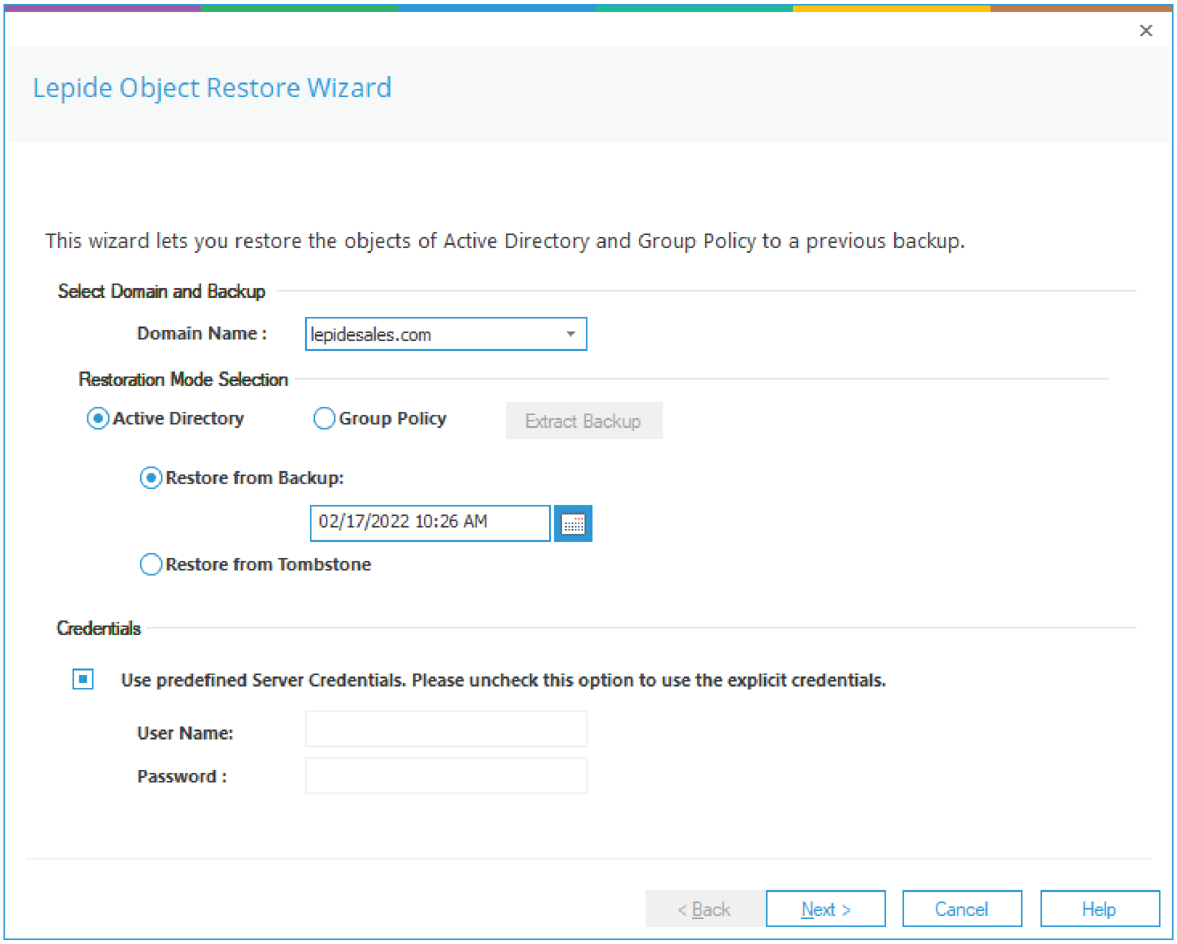
5. Find the backup you want to restore and click on it
6. The date and time will be displayed next to **Selected Backup** at the bottom of the dialog box:



Selected Backup 02/17/2022 10:26 AM

Figure 33: Selected Backup

7. Click **OK** to go back to the Lepide Object Restore Wizard:



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name : lepidesales.com

Restoration Mode Selection

● Active Directory ○ Group Policy

● Restore from Backup: 02/17/2022 10:26 AM

○ Restore from Tombstone

Credentials

☑ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 34: Restore Wizard with Backup Selected

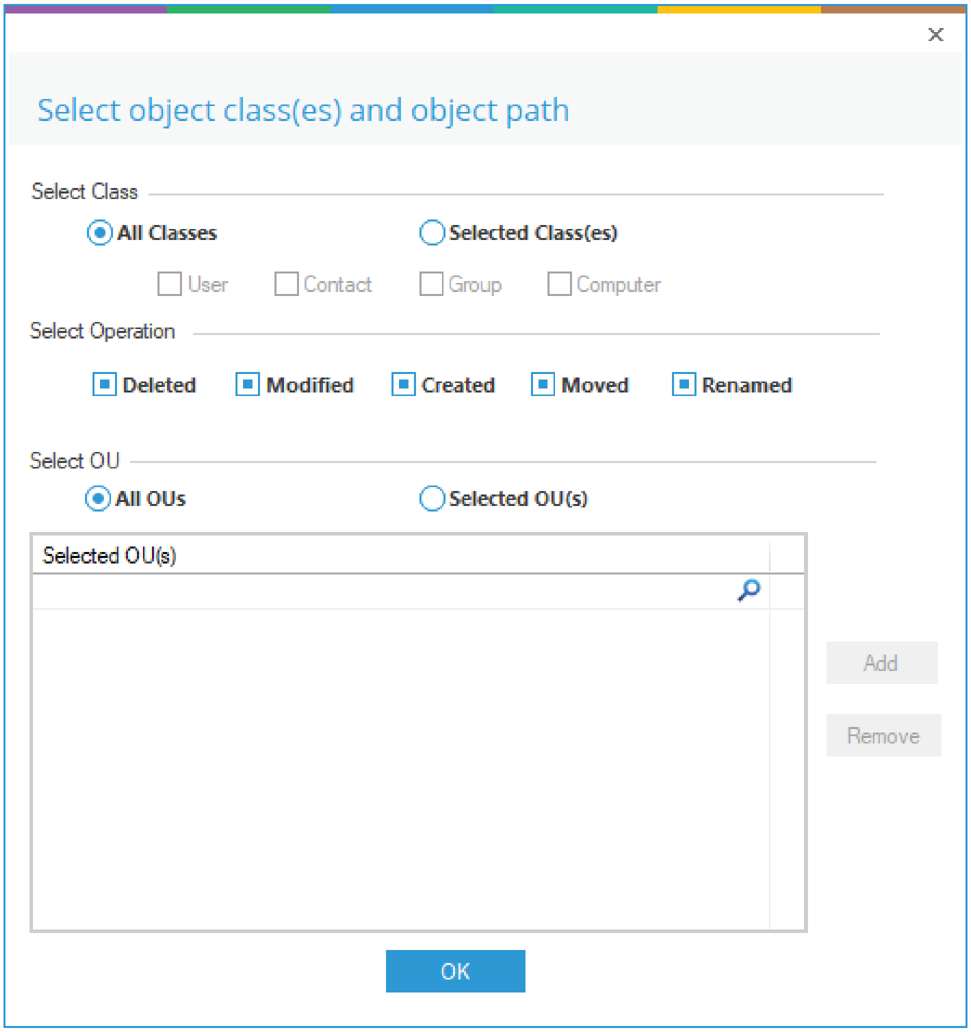
The selected backup date and time are now displayed.

8. If you want to use the same credentials as those provided while adding the domain, then keep the option Use predefined server credentials checked.

   Alternatively, uncheck it and provide the username and password for explicit login credentials to restore the object(s).

9. Click Next

The Select object class(es) and Object Path dialog box is displayed:



Select object class(es) and object path

Select Class

● All Classes ○ Selected Class(es)

□ User □ Contact □ Group □ Computer

Select Operation

☑ Deleted ☑ Modified ☑ Created ☑ Moved ☑ Renamed

Select OU

● All OUs ○ Selected OU(s)

Selected OU(s)

Figure 35: Object Classes and Object Path

This allows you to select filters to select which objects are to be restored. You can leave this with nothing selected to see all object modifications if required.

To select filters:

10. Select **Class**:

    Select either:

    - All Classes or
    - Selected Classes

    If you choose selected Classes, you can select one or more of the following:

    - User
    - Contact
    - Group
    - Computer

11. Select **Operation:**

    Select one or more of the following:

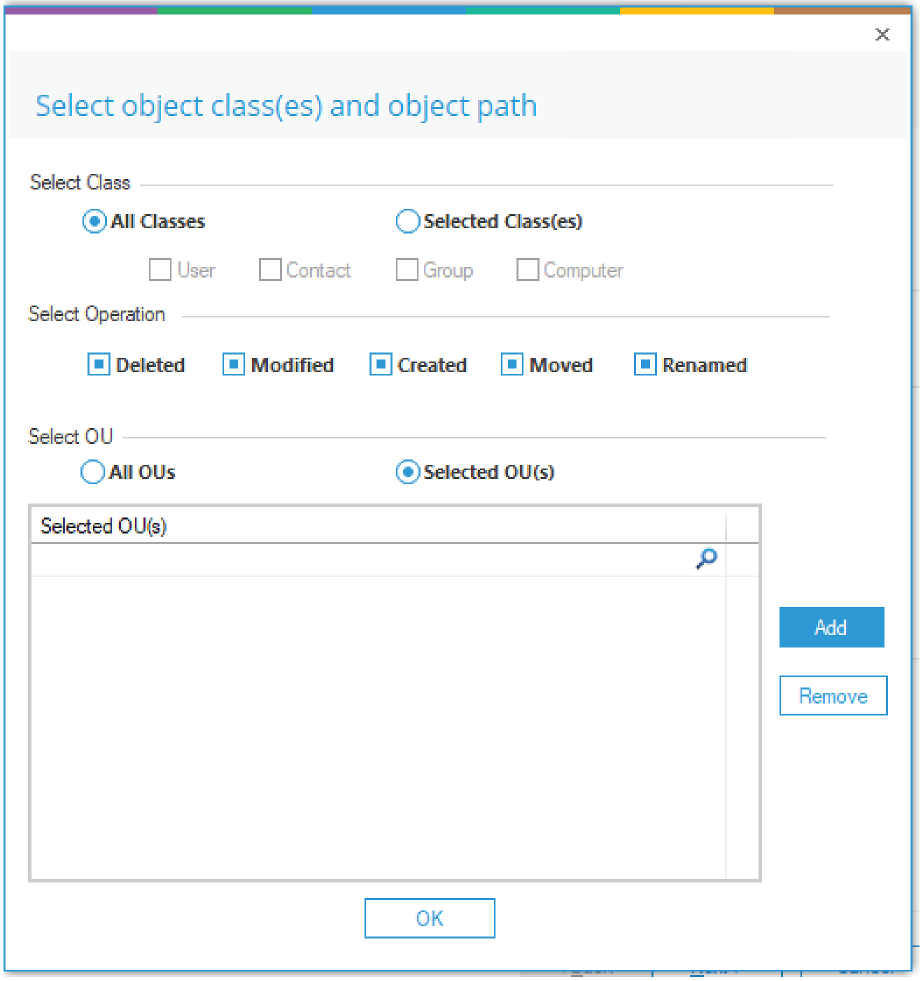
    - Deleted
    - Modified
    - Created
    - Moved
    - Renamed

12. Select **OU**

    Select either:

    - All OUs or
    - Selected OUs

If you choose specific OUs, the **Add** button becomes available:



Select object class(es) and object path

Select Class

● All Classes ○ Selected Class(es)

□ User □ Contact □ Group □ Computer

Select Operation

☒ Deleted ☒ Modified ☒ Created ☒ Moved ☒ Renamed

Select OU

○ All OUs ● Selected OU(s)

Figure 36: Object Classes and Object Path

To add selected OUs:

- Click **Add**

The Explore Backup dialog box is displayed:

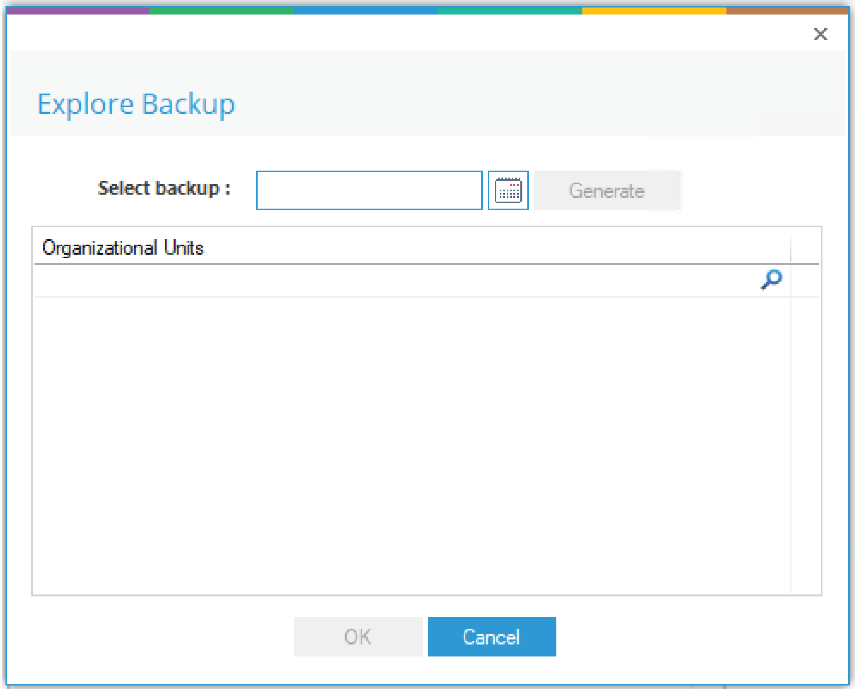
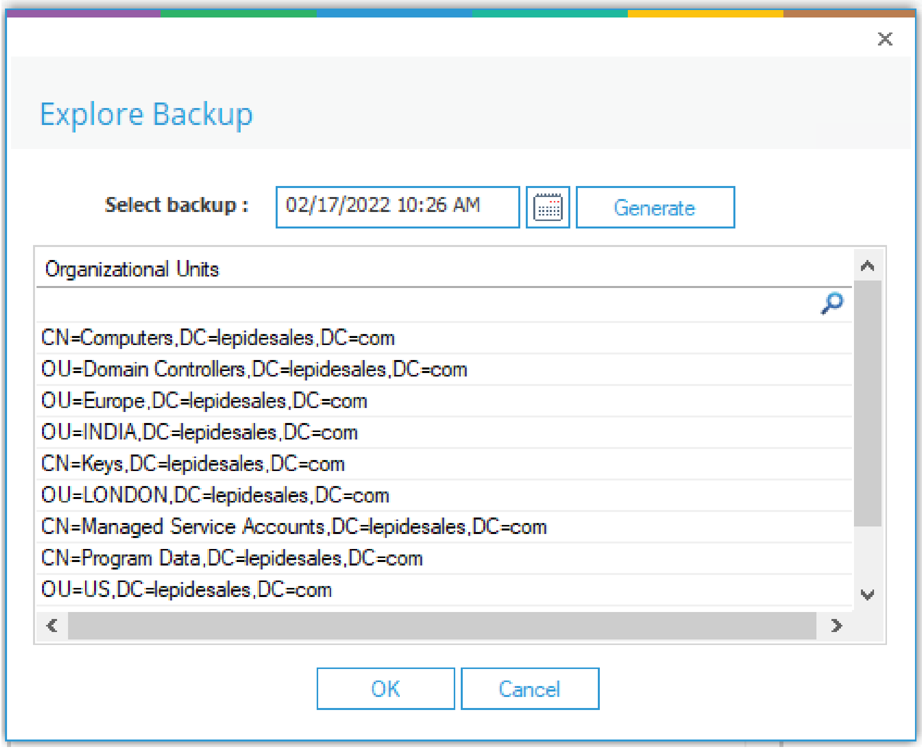


Figure 37: Explore Backup

- Click the Calendar icon ▦ to select a backup
- Choose a Backup and click **OK**
- Click **Generate**

A list of Organizational Units is displayed:

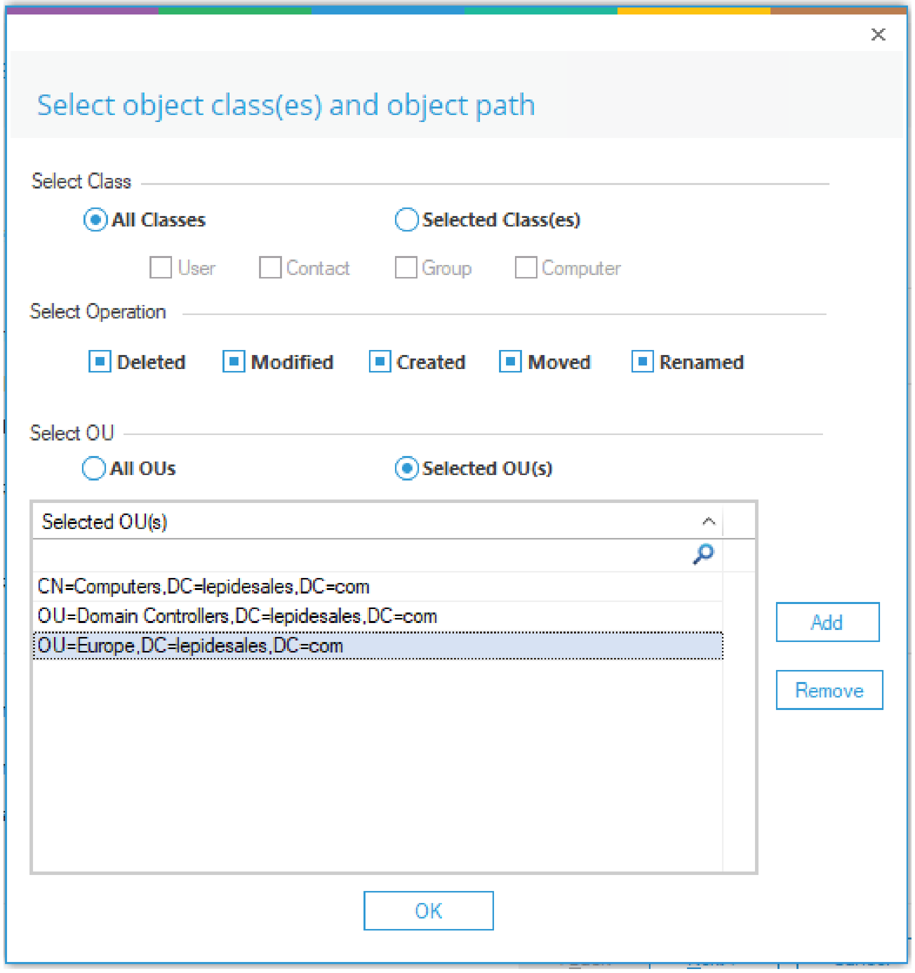


CN=Computers,DC=lepidesales,DC=com
OU=Domain Controllers,DC=lepidesales,DC=com
OU=Europe,DC=lepidesales,DC=com
OU=INDIA,DC=lepidesales,DC=com
CN=Keys,DC=lepidesales,DC=com
OU=LONDON,DC=lepidesales,DC=com
CN=Managed Service Accounts,DC=lepidesales,DC=com
CN=Program Data,DC=lepidesales,DC=com
OU=US,DC=lepidesales,DC=com

Figure 38: Explore Backup with OUs Displayed

- Select the organizational units required
- Click OK

The selected units are displayed in the Select object class(es) and object path dialog box:



Select object class(es) and object path

Select Class

● All Classes ○ Selected Class(es)

□ User □ Contact □ Group □ Computer

Select Operation

☑ Deleted ☑ Modified ☑ Created ☑ Moved ☑ Renamed

Select OU

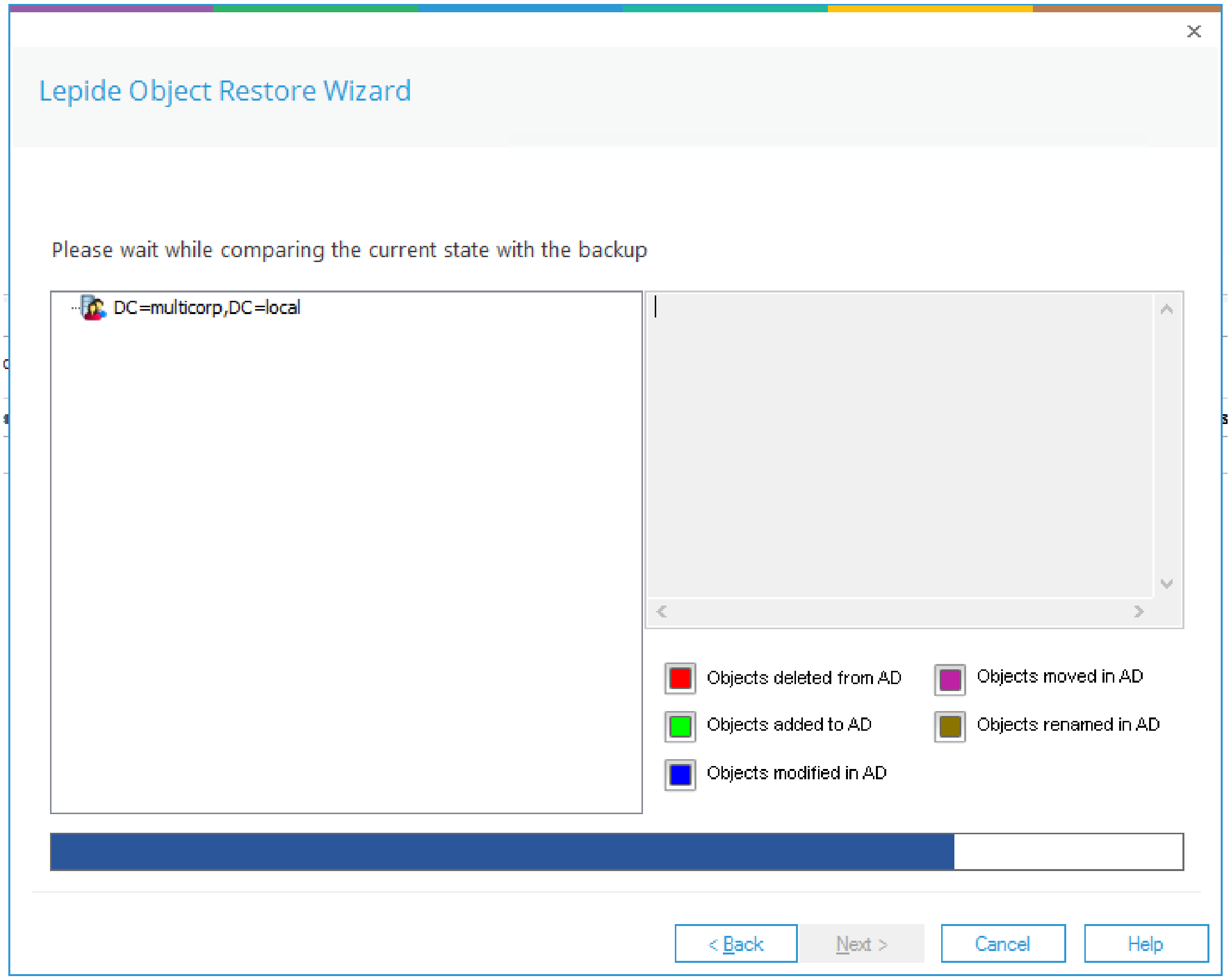
○ All OUs ● Selected OU(s)

Selected OU(s)
CN=Computers,DC=lepidesales,DC=com
OU=Domain Controllers,DC=lepidesales,DC=com
OU=Europe,DC=lepidesales,DC=com

Figure 39: Selected OUs Displayed

13. Click OK

    The following dialog box will be displayed where the wizard will compare the current state of Active Directory with the state stored in the selected snapshot:



Lepide Object Restore Wizard

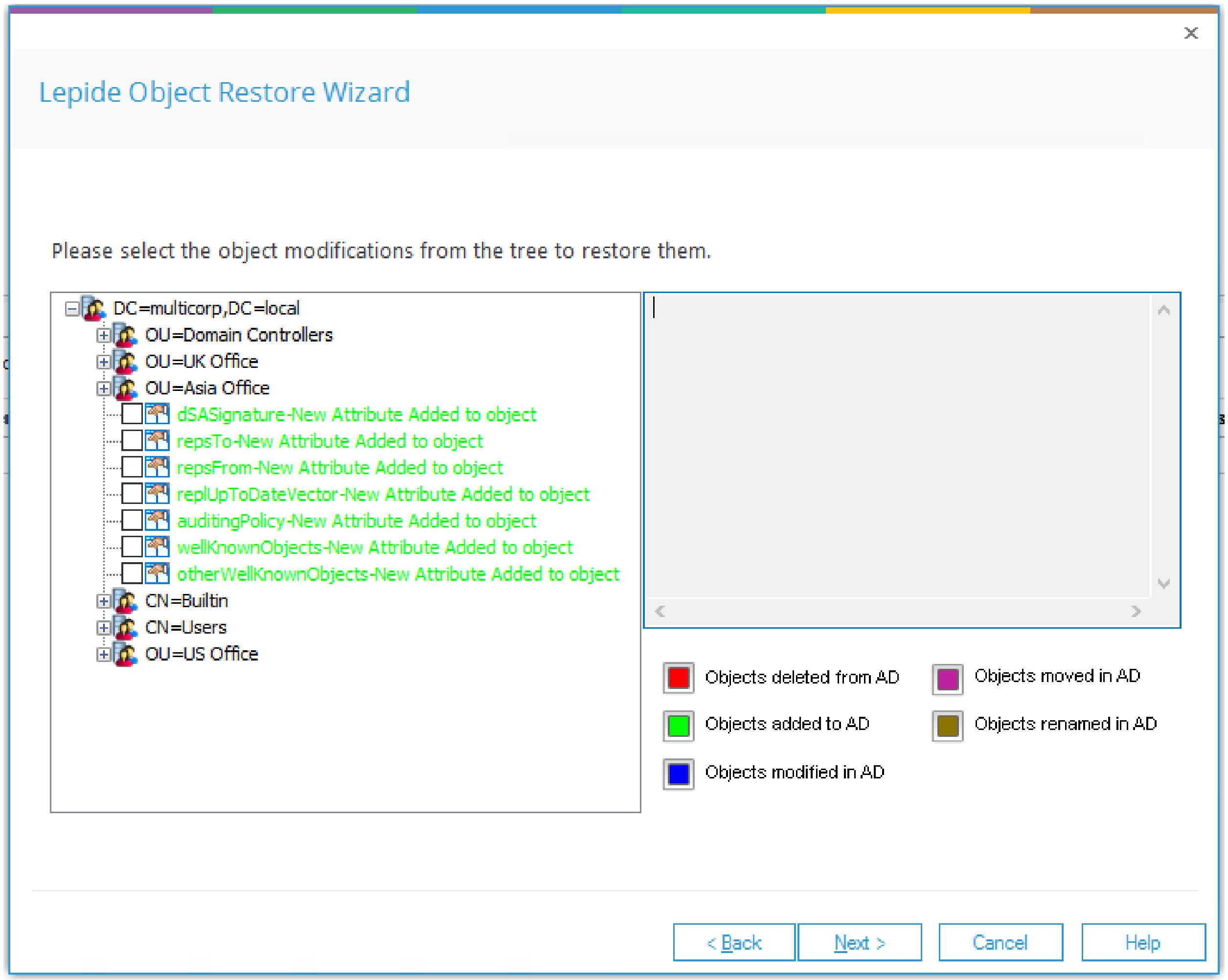
Please wait while comparing the current state with the backup

DC=multicorp,DC=local

🟥 Objects deleted from AD
🟪 Objects moved in AD
🟩 Objects added to AD
🟫 Objects renamed in AD
🟦 Objects modified in AD

Figure 40: Restore Wizard Comparing States

Once finished, a list of object modifications will be displayed:



Lepide Object Restore Wizard

Please select the object modifications from the tree to restore them.

- DC=multicorp,DC=local
  - OU=Domain Controllers
  - OU=UK Office
  - OU=Asia Office
    - □ dSASignature-New Attribute Added to object
    - □ repsTo-New Attribute Added to object
    - □ repsFrom-New Attribute Added to object
    - □ replUpToDateVector-New Attribute Added to object
    - □ auditingPolicy-New Attribute Added to object
    - □ wellKnownObjects-New Attribute Added to object
    - □ otherWellKnownObjects-New Attribute Added to object
  - CN=Builtin
  - CN=Users
  - OU=US Office

🟥 Objects deleted from AD

🟪 Objects moved in AD

🟩 Objects added to AD

🟫 Objects renamed in AD

🟦 Objects modified in AD

Figure 41: Object Modifications

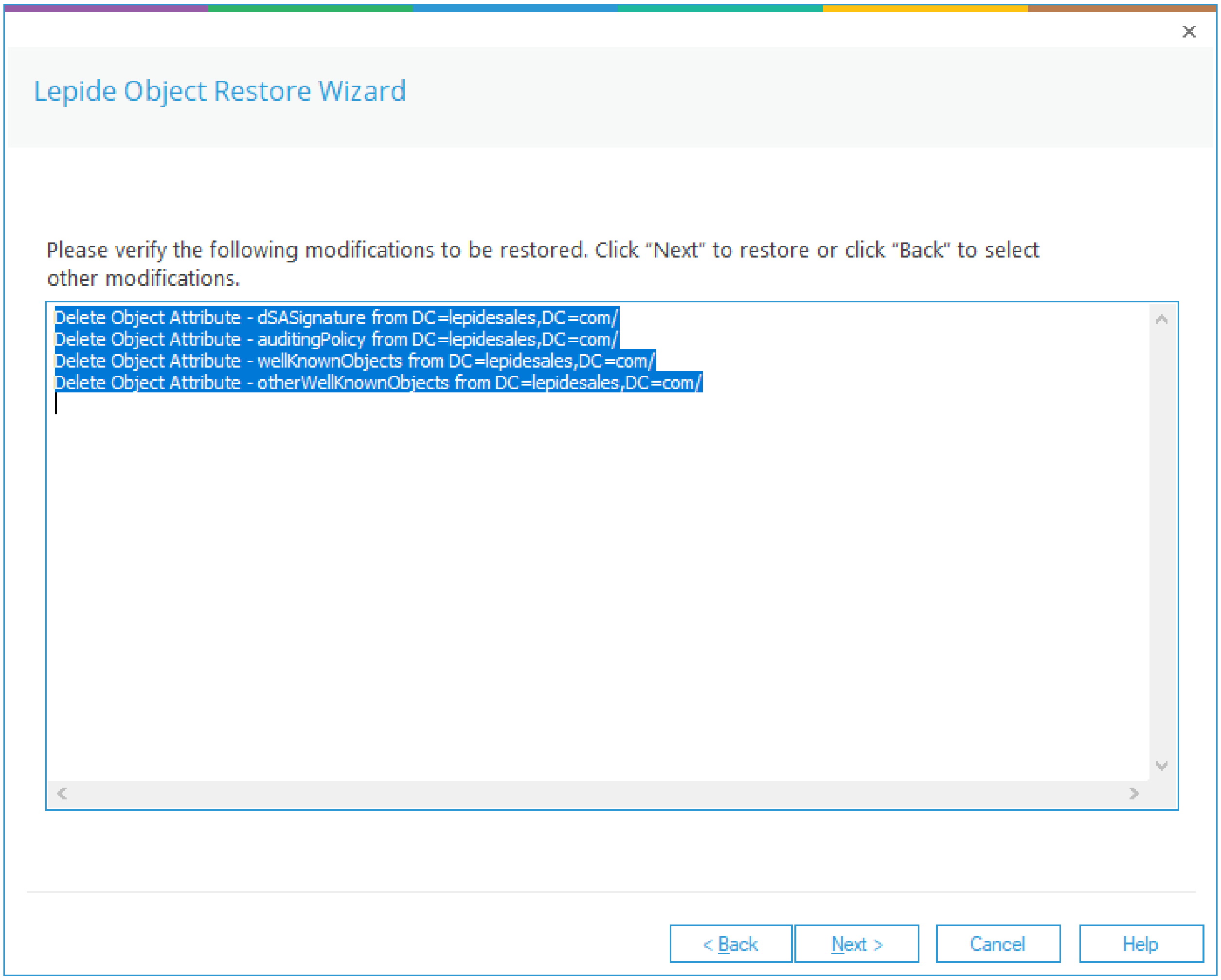
- The actions which can be selected are listed in a tree structure
- The text describing these actions is color coded according to the color key on the right-hand side of the dialog box
- In the example above, the text is green which shows that these objects have been added to Active Directory.

14. Check the boxes for the objects that you want to restore

NOTE: It is essential to create a backup of the current Active Directory so that you can revert to this current state after restoring an object if required. See Section 4 of this document for the steps on how to create a backup.

15. Click **Next** once you have selected the objects to be restored

The following dialog box is displayed:



Please verify the following modifications to be restored. Click "Next" to restore or click "Back" to select other modifications.

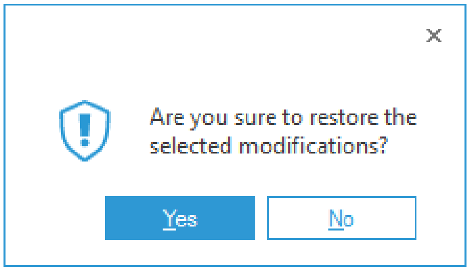
```
Delete Object Attribute - dSASignature from DC=lepidesales,DC=com/
Delete Object Attribute - auditingPolicy from DC=lepidesales,DC=com/
Delete Object Attribute - wellKnownObjects from DC=lepidesales,DC=com/
Delete Object Attribute - otherWellKnownObjects from DC=lepidesales,DC=com/
```

Figure 42: Summary of Selected Objects to be Restored

- This dialog box lists the changes about to be restored.

16. Click **Next** to restore these changes or click **Back** to go back to the previous dialog box and make different selections.

Once you click **Next**, a message box will be displayed for confirmation of the action:



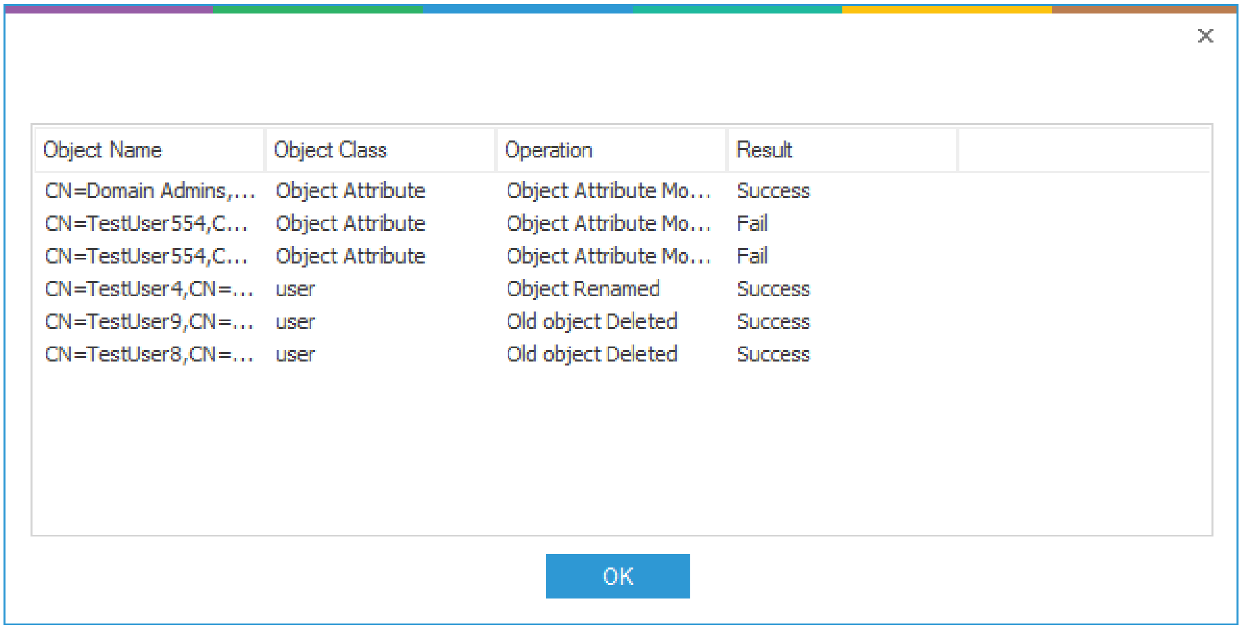
Are you sure to restore the selected modifications?

Figure 43: Message Box asking for Confirmation

17. Click **Yes** to start the restoration of modified or deleted objects

- The Lepide Object Restore Wizard runs to restore the objects

Once done, the following dialog box appears on the screen:

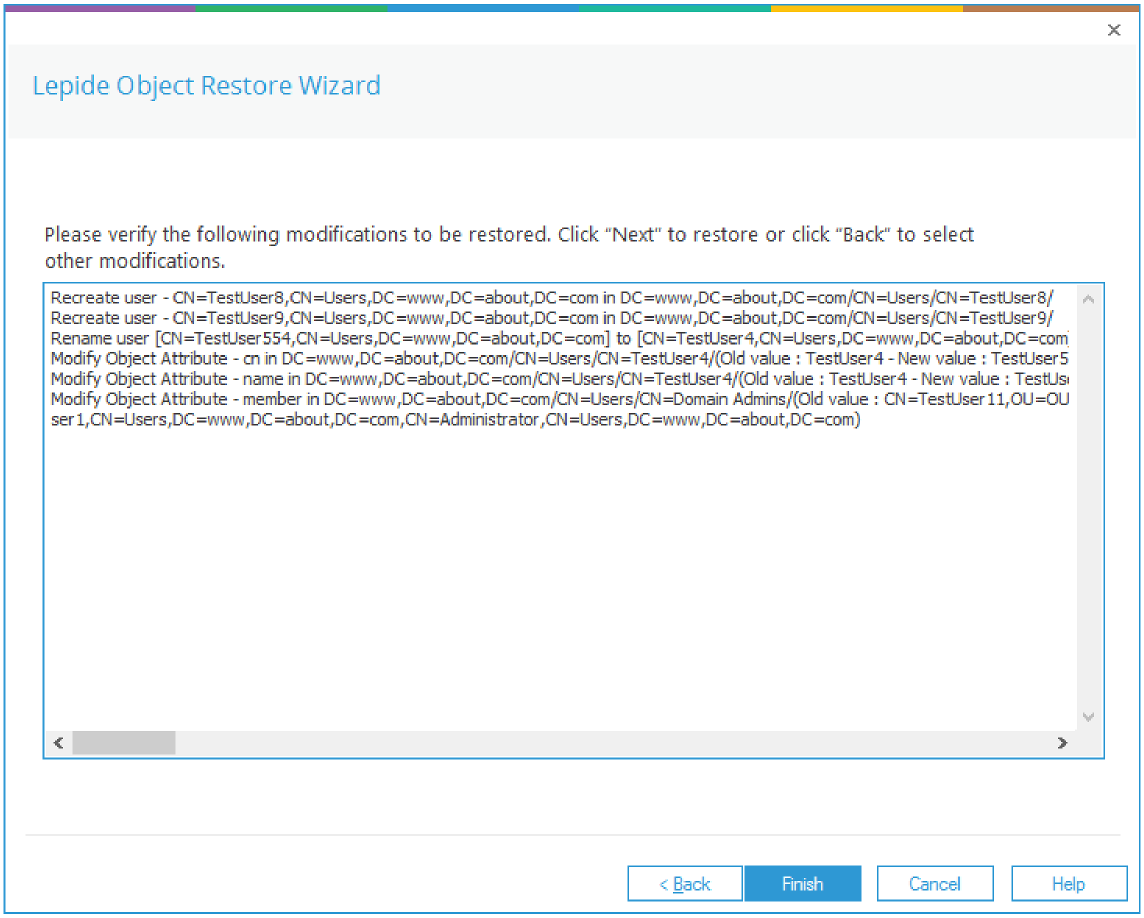


Object Name	Object Class	Operation	Result
CN=Domain Admins,...	Object Attribute	Object Attribute Mo...	Success
CN=TestUser554,C...	Object Attribute	Object Attribute Mo...	Fail
CN=TestUser554,C...	Object Attribute	Object Attribute Mo...	Fail
CN=TestUser4,CN=...	user	Object Renamed	Success
CN=TestUser9,CN=...	user	Old object Deleted	Success
CN=TestUser8,CN=...	user	Old object Deleted	Success

Figure 44: Summary of Object Restoration

- The objects that have been restored successfully will display the result **Success**. Their status will be **Fail** if they cannot be restored.

18. Click **OK** to close this summary box. It takes you back to the restore wizard



Please verify the following modifications to be restored. Click "Next" to restore or click "Back" to select other modifications.

```
Recreate user - CN=TestUser8,CN=Users,DC=www,DC=about,DC=com in DC=www,DC=about,DC=com/CN=Users/CN=TestUser8/
Recreate user - CN=TestUser9,CN=Users,DC=www,DC=about,DC=com in DC=www,DC=about,DC=com/CN=Users/CN=TestUser9/
Rename user [CN=TestUser554,CN=Users,DC=www,DC=about,DC=com] to [CN=TestUser4,CN=Users,DC=www,DC=about,DC=com
Modify Object Attribute - cn in DC=www,DC=about,DC=com/CN=Users/CN=TestUser4/(Old value : TestUser4 - New value : TestUser5
Modify Object Attribute - name in DC=www,DC=about,DC=com/CN=Users/CN=TestUser4/(Old value : TestUser4 - New value : TestUs
Modify Object Attribute - member in DC=www,DC=about,DC=com/CN=Users/CN=Domain Admins/(Old value : CN=TestUser11,OU=OU
ser1,CN=Users,DC=www,DC=about,DC=com,CN=Administrator,CN=Users,DC=www,DC=about,DC=com)
```

Figure 45: Final Status of Object Restoration

19. Click **Finish** to close the wizard

7.4. Restore Active Directory Objects from Tombstone

- Click the User and Behavior Entity Analytics icon to display the States & Behavior window:

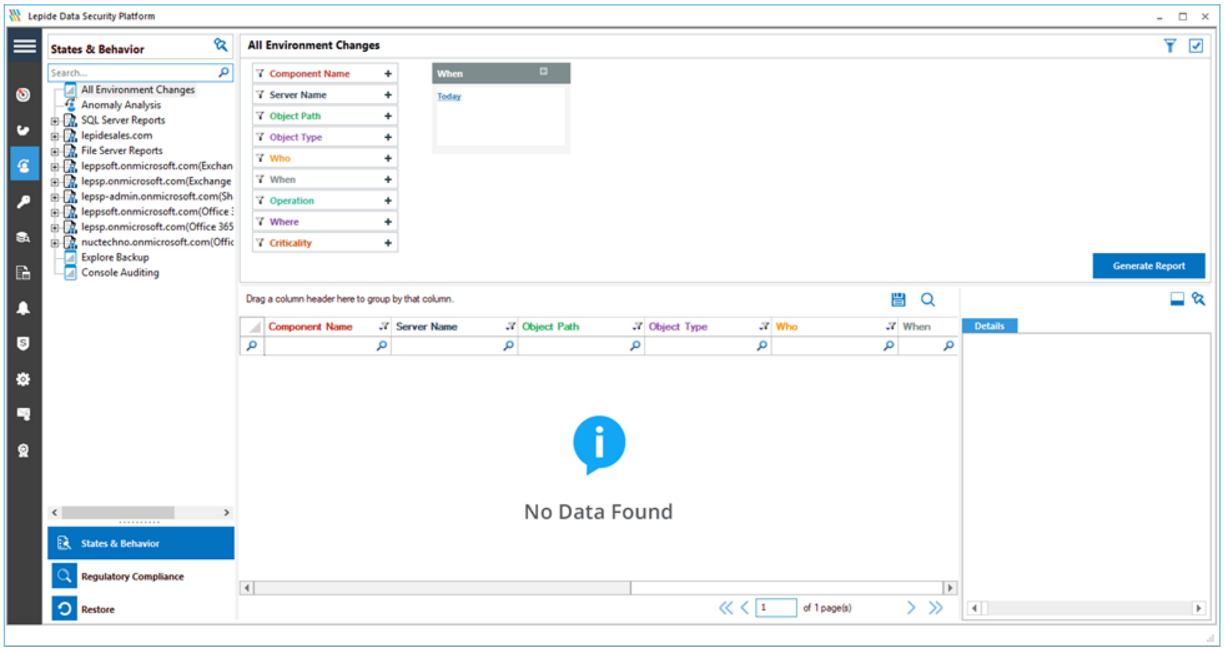
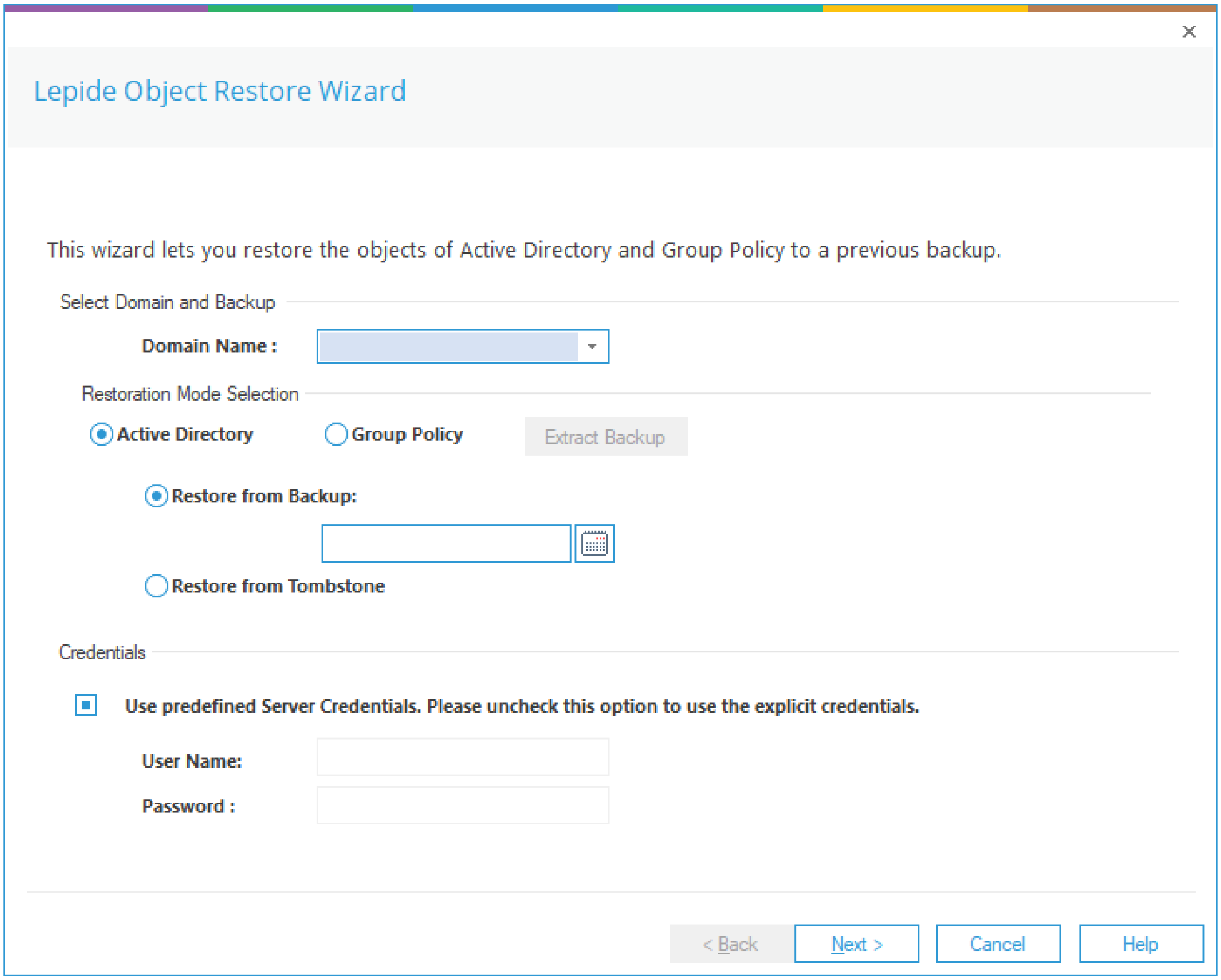


Figure 46: States & Behavior Window

- On the lower left of the screen under **States & Behavior** is **Restore**
- Click the Restore icon to start the **Lepide Object Restore Wizard**



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name :

Restoration Mode Selection

● Active Directory ○ Group Policy

● Restore from Backup:

○ Restore from Tombstone

Credentials

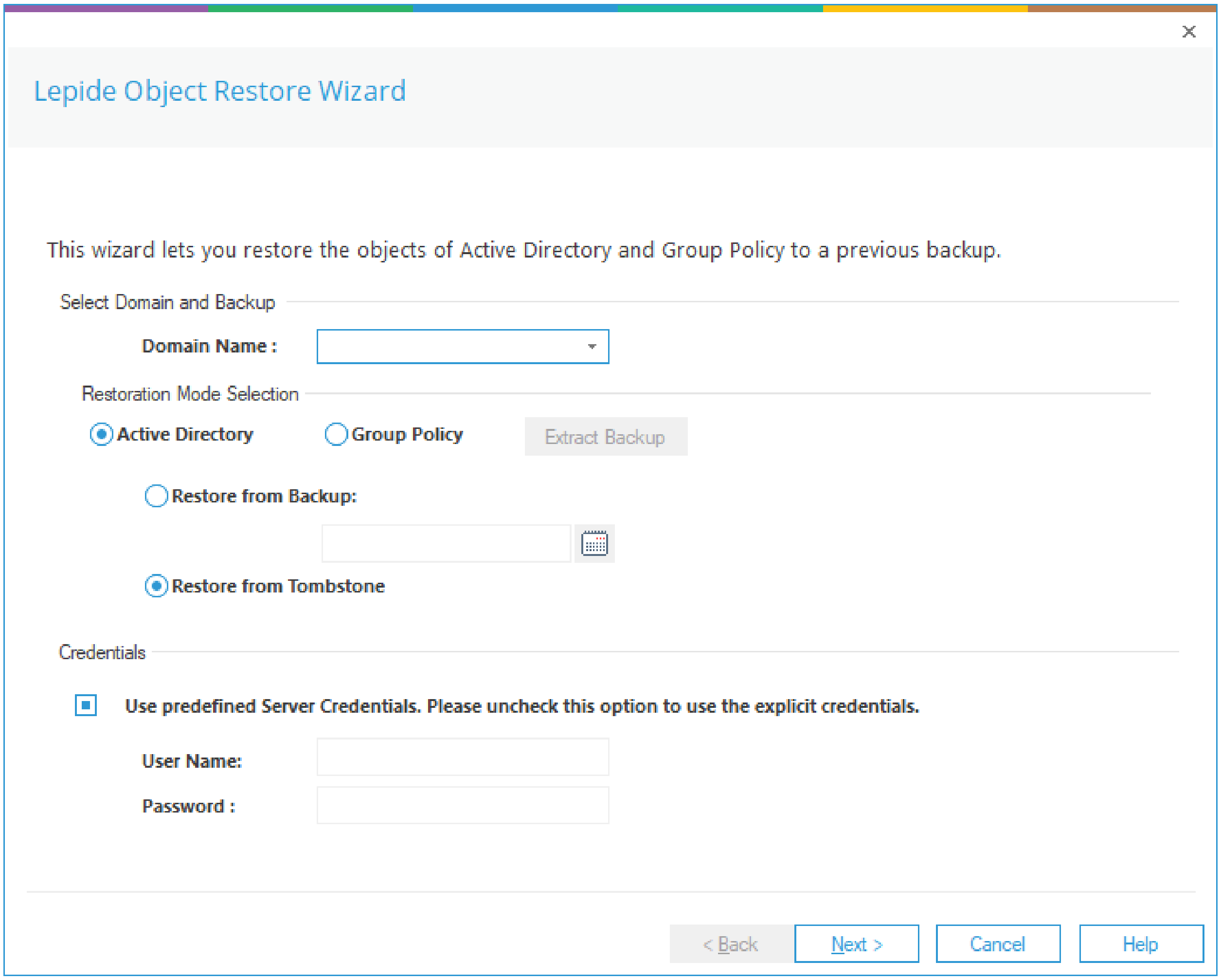
☑ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 47: Lepide Object Restore Wizard

1. Select the Domain Name from the drop-down list
2. From the Restoration Mode Selection section, select Restore from Tombstone



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name :

Restoration Mode Selection

● **Active Directory** ○ **Group Policy**

○ **Restore from Backup:**

● **Restore from Tombstone**

Credentials

☑ **Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.**

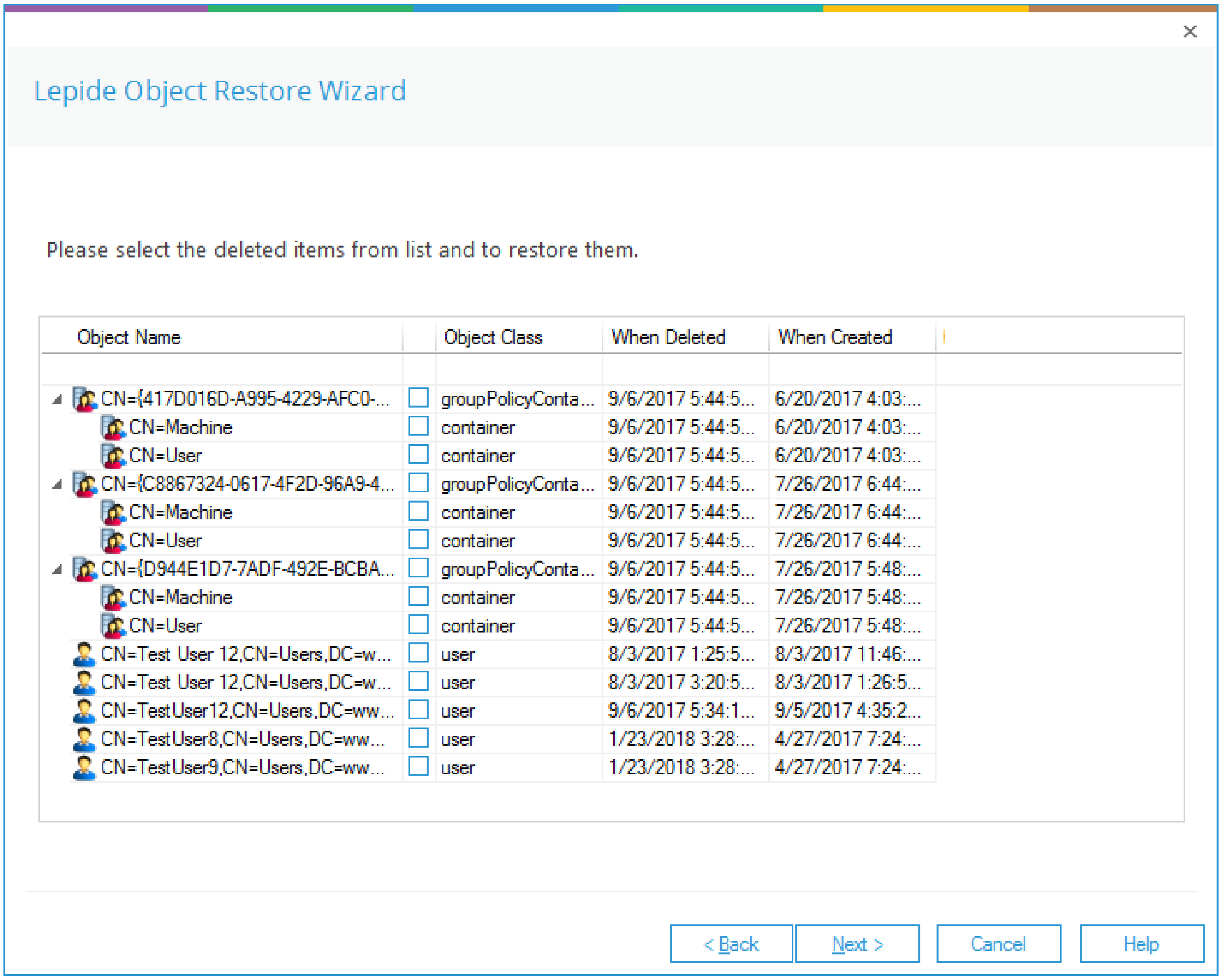
User Name:

Password :

Figure 48: Restore Wizard - Restore from Tombstone

3. Click Next

This will read the tombstone folder and display the objects from this folder:



Lepide Object Restore Wizard

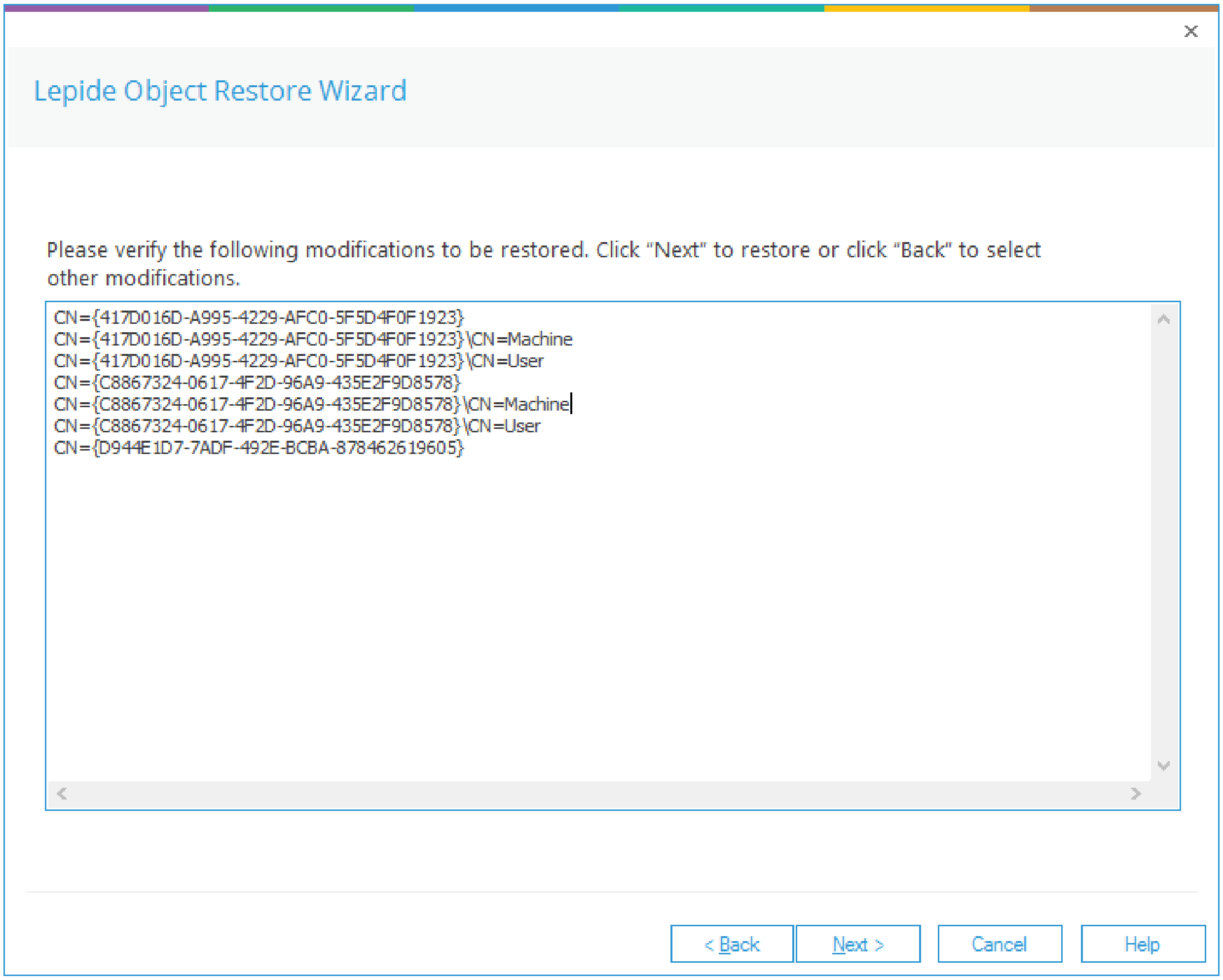
Please select the deleted items from list and to restore them.

Object Name		Object Class	When Deleted	When Created
CN={417D016D-A995-4229-AFC0-...	□	groupPolicyConta...	9/6/2017 5:44:5...	6/20/2017 4:03:...
CN=Machine	□	container	9/6/2017 5:44:5...	6/20/2017 4:03:...
CN=User	□	container	9/6/2017 5:44:5...	6/20/2017 4:03:...
CN={C8867324-0617-4F2D-96A9-4...	□	groupPolicyConta...	9/6/2017 5:44:5...	7/26/2017 6:44:...
CN=Machine	□	container	9/6/2017 5:44:5...	7/26/2017 6:44:...
CN=User	□	container	9/6/2017 5:44:5...	7/26/2017 6:44:...
CN={D944E1D7-7ADF-492E-BCBA...	□	groupPolicyConta...	9/6/2017 5:44:5...	7/26/2017 5:48:...
CN=Machine	□	container	9/6/2017 5:44:5...	7/26/2017 5:48:...
CN=User	□	container	9/6/2017 5:44:5...	7/26/2017 5:48:...
CN=Test User 12,CN=Users,DC=w...	□	user	8/3/2017 1:25:5...	8/3/2017 11:46:...
CN=Test User 12,CN=Users,DC=w...	□	user	8/3/2017 3:20:5...	8/3/2017 1:26:5...
CN=TestUser12,CN=Users,DC=ww...	□	user	9/6/2017 5:34:1...	9/5/2017 4:35:2...
CN=TestUser8,CN=Users,DC=ww...	□	user	1/23/2018 3:28:...	4/27/2017 7:24:...
CN=TestUser9,CN=Users,DC=ww...	□	user	1/23/2018 3:28:...	4/27/2017 7:24:...

Figure 49: Objects Available to be Restored

4. Select the objects that you want to restore

5. Click **Next** once you've selected the objects. This will display the details of the selected objects to be restored:



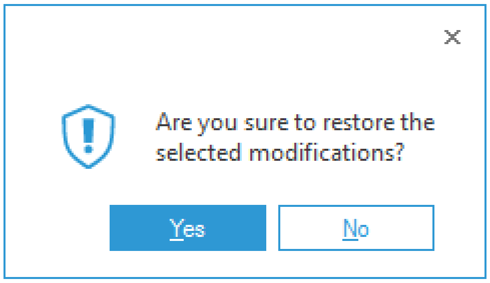
Please verify the following modifications to be restored. Click "Next" to restore or click "Back" to select other modifications.

```
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=Machine
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=User
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=Machine
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=User
CN={D944E1D7-7ADF-492E-BCBA-878462619605}
```

Figure 50: Summary of Selected Objects to be Restored

6. Click **Next** to restore these changes or click **Back** to go back to the previous dialog box

Once you click **Next**, the Solution will ask to confirm your action:

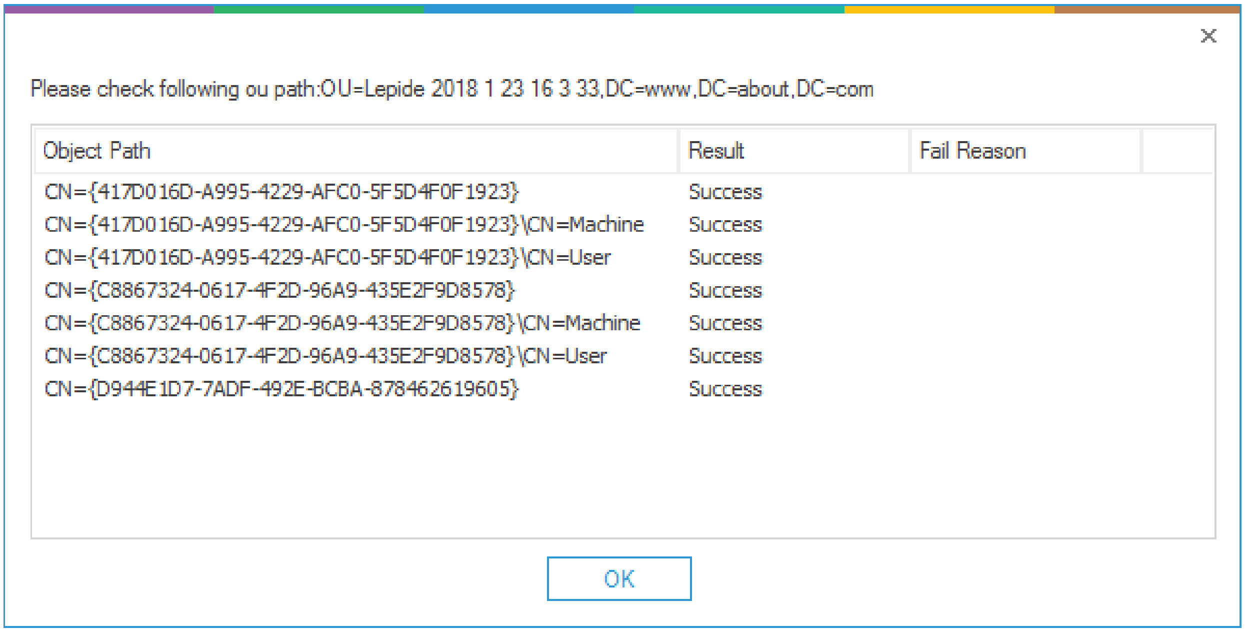


Are you sure to restore the selected modifications?

Figure 51: Message Box asking for Confirmation

7. Click **Yes** to start the process of restoring the selected objects to the real Active Directory environment from the tombstone folder.

The Lepide Object Restore Wizard will process to restore the objects. Once done, you'll receive the following screen.



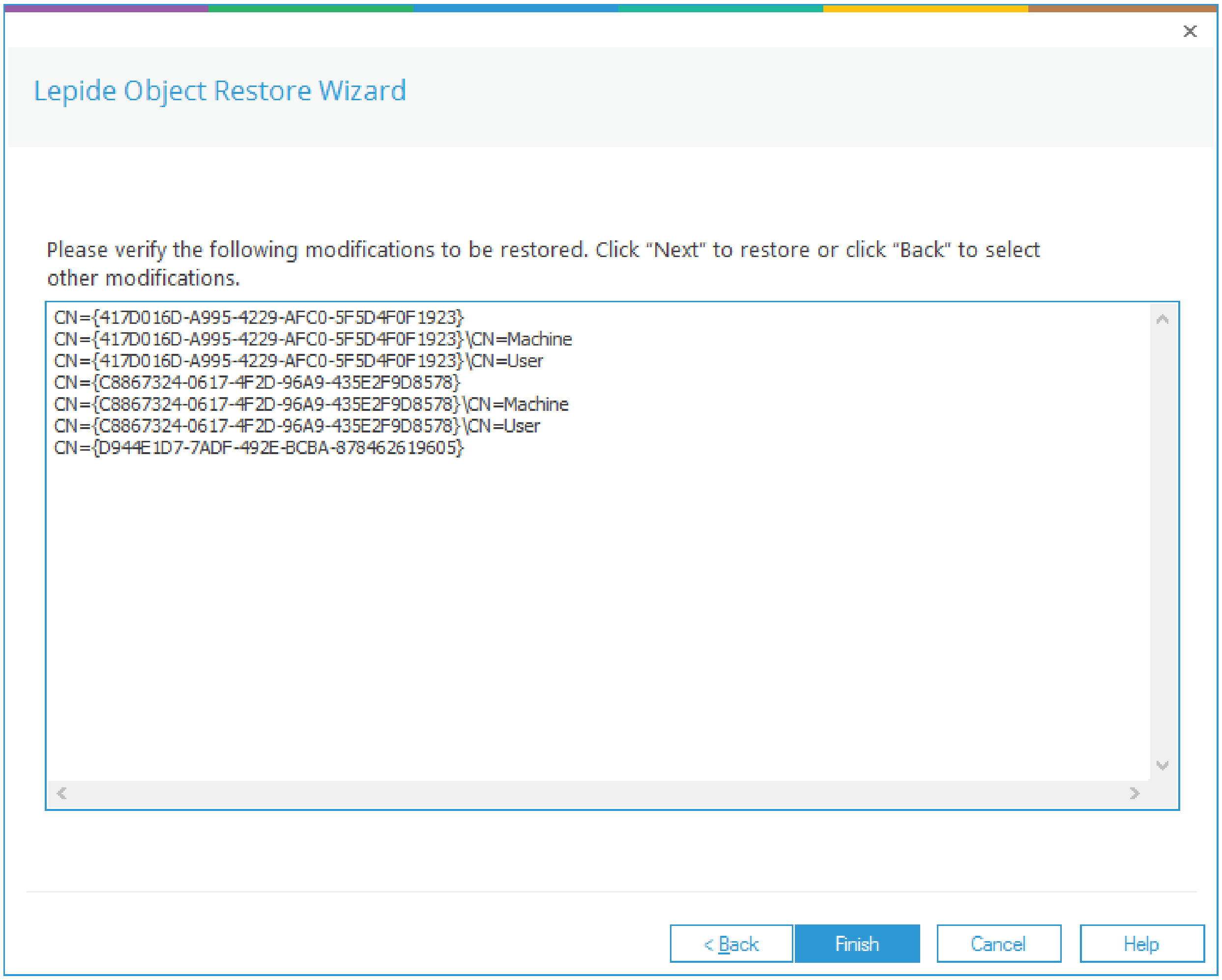
Please check following ou path:OU=Lepide 2018 1 23 16 3 33,DC=www,DC=about,DC=com

Object Path	Result	Fail Reason
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}	Success	
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=Machine	Success	
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=User	Success	
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}	Success	
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=Machine	Success	
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=User	Success	
CN={D944E1D7-7ADF-492E-BCBA-878462619605}	Success	

Figure 52: Summary of Object Restoration

The objects that have been restored successfully will display the result **Success**. Their status will be **Fail** if they cannot be restored.

8. Click **OK** to close this summary box. This will take you back to the wizard



Lepide Object Restore Wizard

Please verify the following modifications to be restored. Click "Next" to restore or click "Back" to select other modifications.

```
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=Machine
CN={417D016D-A995-4229-AFC0-5F5D4F0F1923}\CN=User
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=Machine
CN={C8867324-0617-4F2D-96A9-435E2F9D8578}\CN=User
CN={D944E1D7-7ADF-492E-BCBA-878462619605}
```

Figure 53: Final Status of Object Restoration

9. Click **Finish** to close the wizard

8. Restore Group Policy Objects

You can restore the state of complete Group Policy Objects at the domain level or the domain controller level. Please note that you cannot restore the individual group policies.

The current state of the Group Policy Objects at the domain level or the domain controller level can be restored with a state stored in the selected snapshot using the following steps.

NOTE: It is essential to create a backup of the current state of Group Policies so that you can revert to this current state after restoring a backup if required. See Section 4 of this document for the steps on how to create a backup.

Follow the steps below to restore the added, deleted, renamed, or modified Group Policy Objects from a backup.

- Click the User and Behavior Entity Analytics icon to display the States & Behavior window:

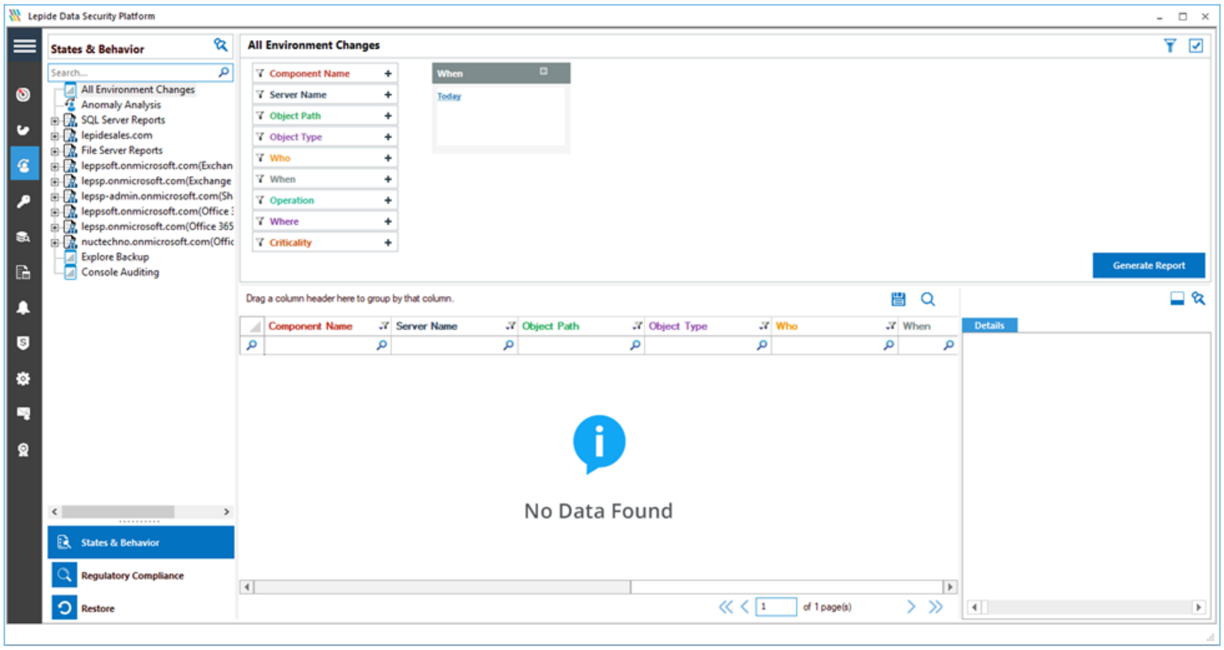
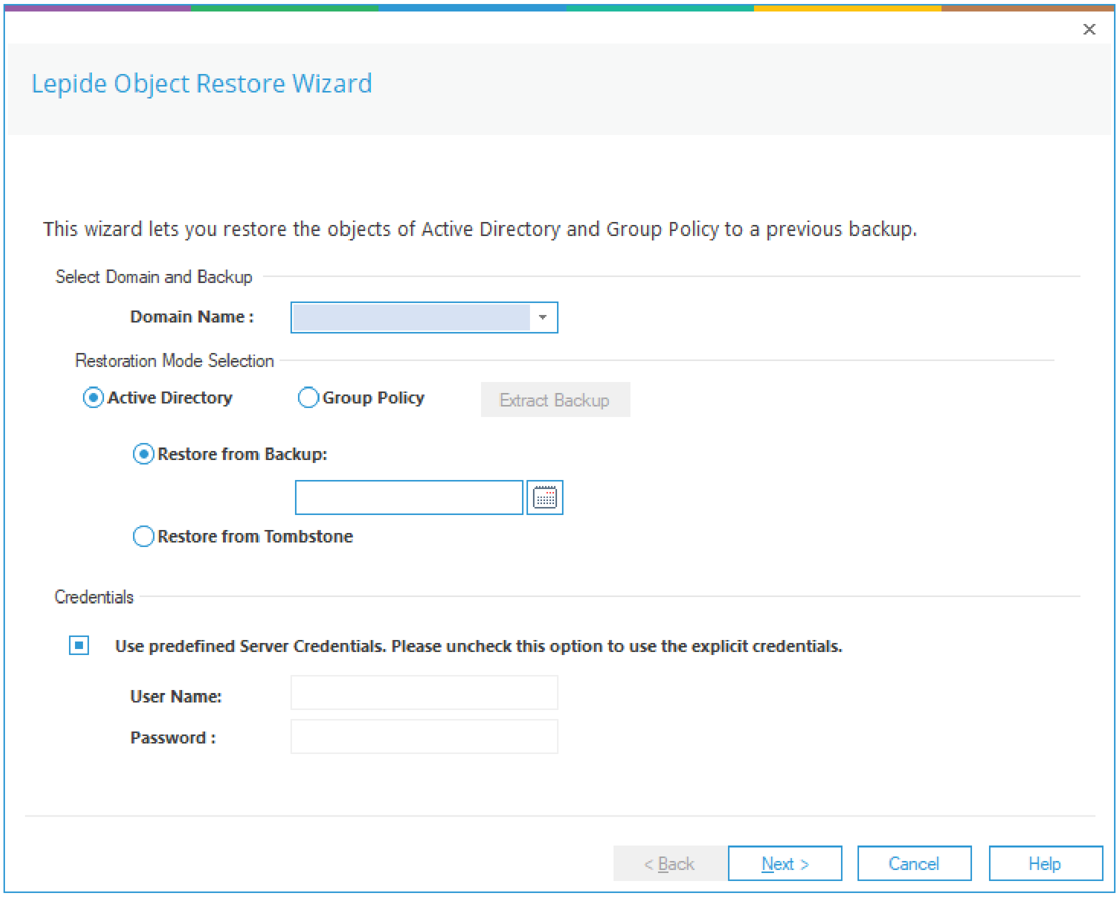


Figure 54: States & Behavior Window

- On the lower left of the screen under States & Behavior is Restore

- Click the Restore icon ⟲ to start the Lepide Object Restore Wizard:



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name :

Restoration Mode Selection

● Active Directory ○ Group Policy

● Restore from Backup:

○ Restore from Tombstone

Credentials

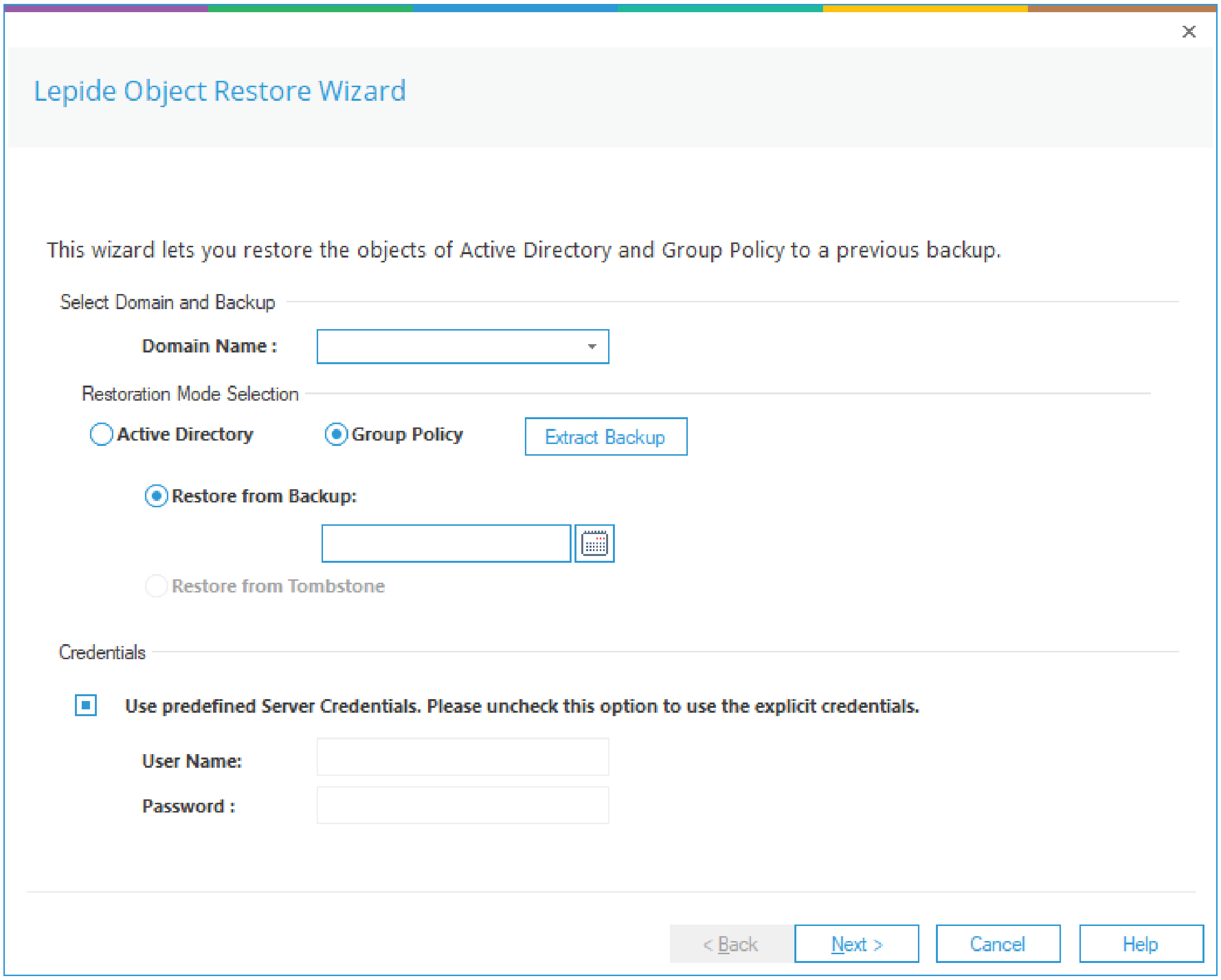
☑ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 55: Object Restore Wizard

1. Select the Domain Name from the drop-down list
2. From the Restoration Mode Selection section, choose Group Policy



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name :

Restoration Mode Selection

○ Active Directory ● Group Policy

● Restore from Backup:

○ Restore from Tombstone

Credentials

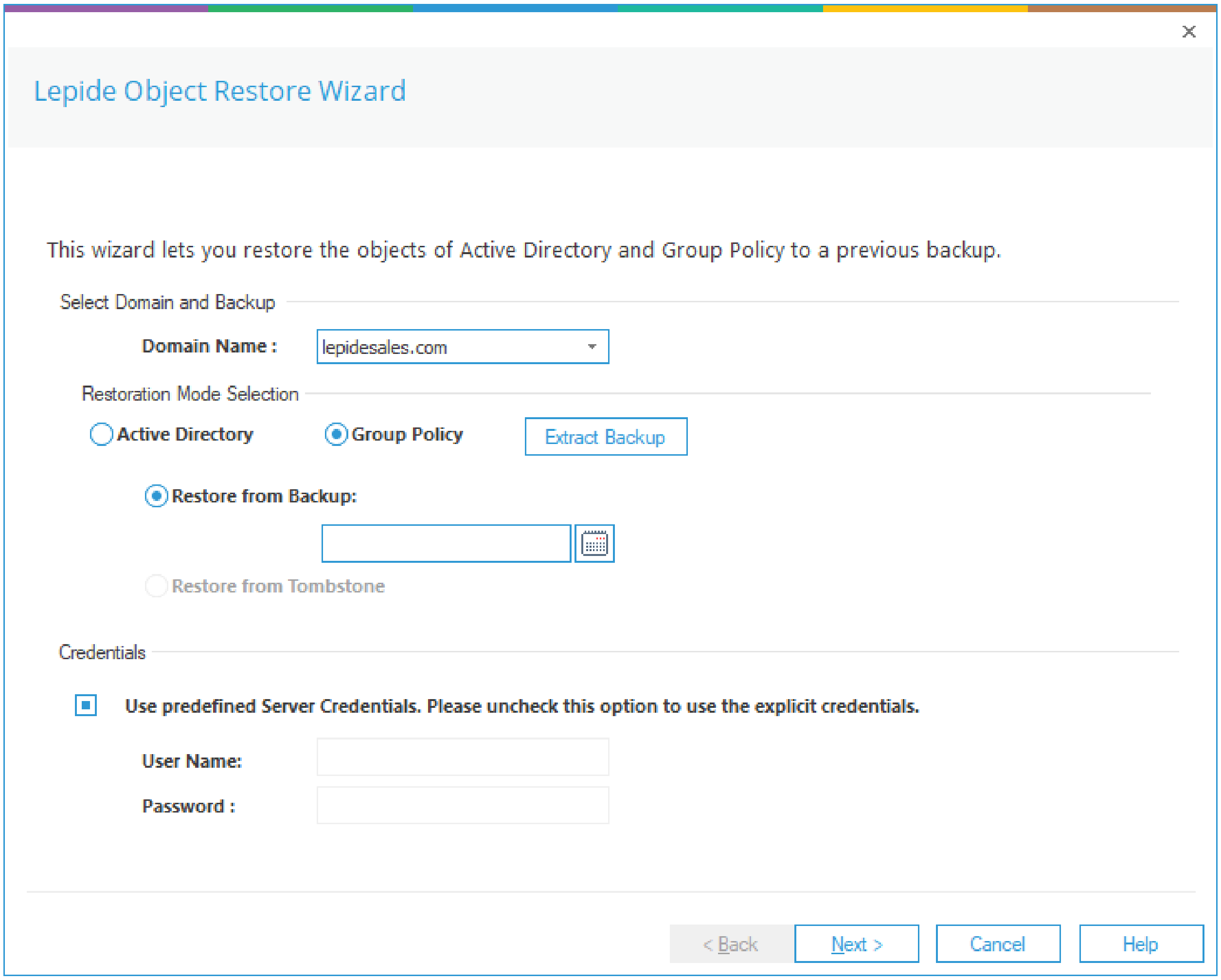
▣ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 56: Object Restore Wizard with Group Policy Selected

The Extract Backup button becomes enabled. For instructions on using the Group Policy Backup Extractor, please see Section 8.1 Group Policy Backup Extractor .



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name : lepidesales.com

Restoration Mode Selection

○ Active Directory ● Group Policy

● Restore from Backup:

○ Restore from Tombstone

Credentials

☑ Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.

User Name:

Password :

Figure 57: Object Restore Wizard

3. Click the Calendar icon ▦ to choose a date. The following dialog box is displayed:

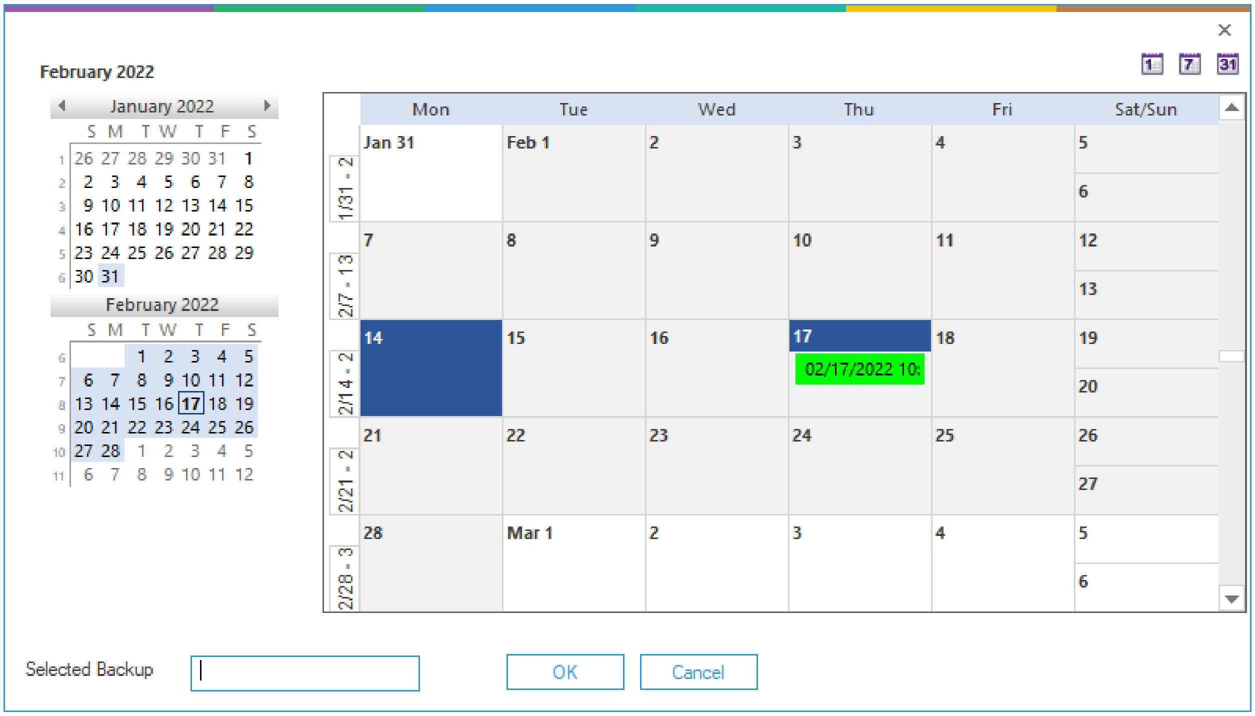


Figure 58: Selecting a Backup

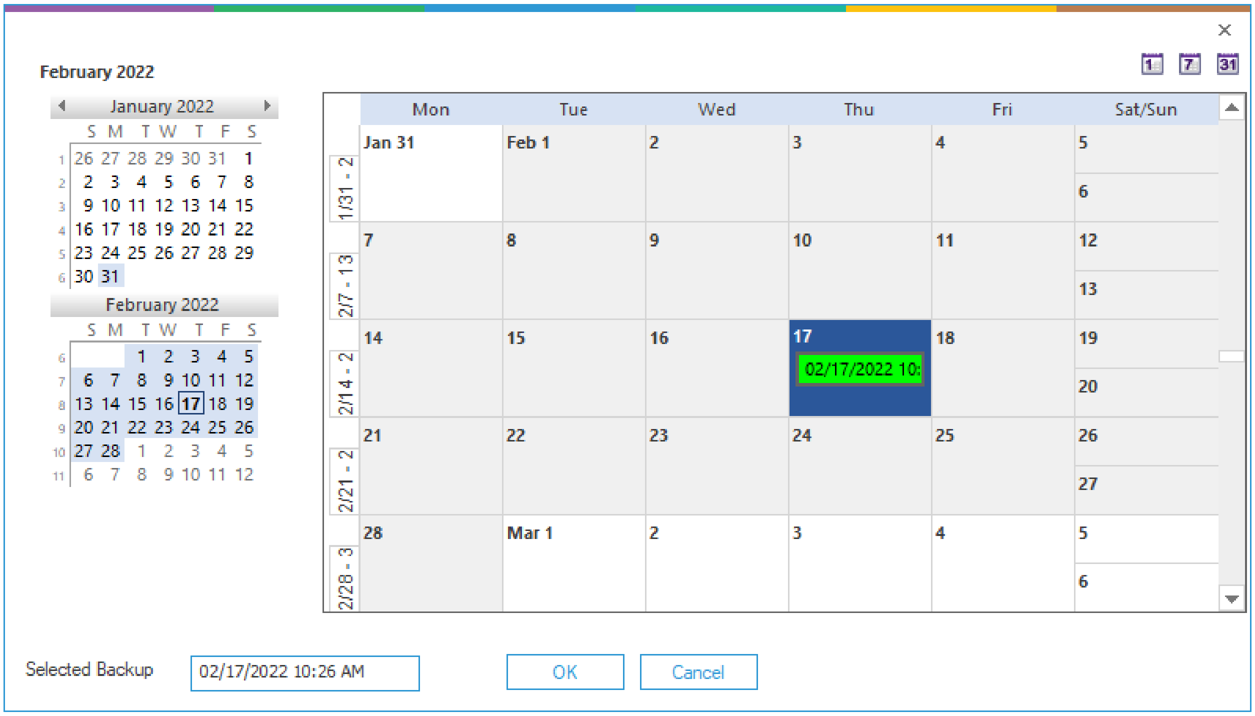
This dialog box provides a way to select the required backup with the left panel showing the calendars by months and the right panel displaying either month, week or day depending on which view has been selected.

The backups will be displayed in date and time format.

To change the calendar view, use one of the three buttons at the top:

1	24 hours
7	7 days
31	31 days

4. Find the backup you want to restore and click on it
5. The date and time will be displayed next to **Selected Backup** at the bottom of the dialog box:



Selected Backup 02/17/2022 10:26 AM

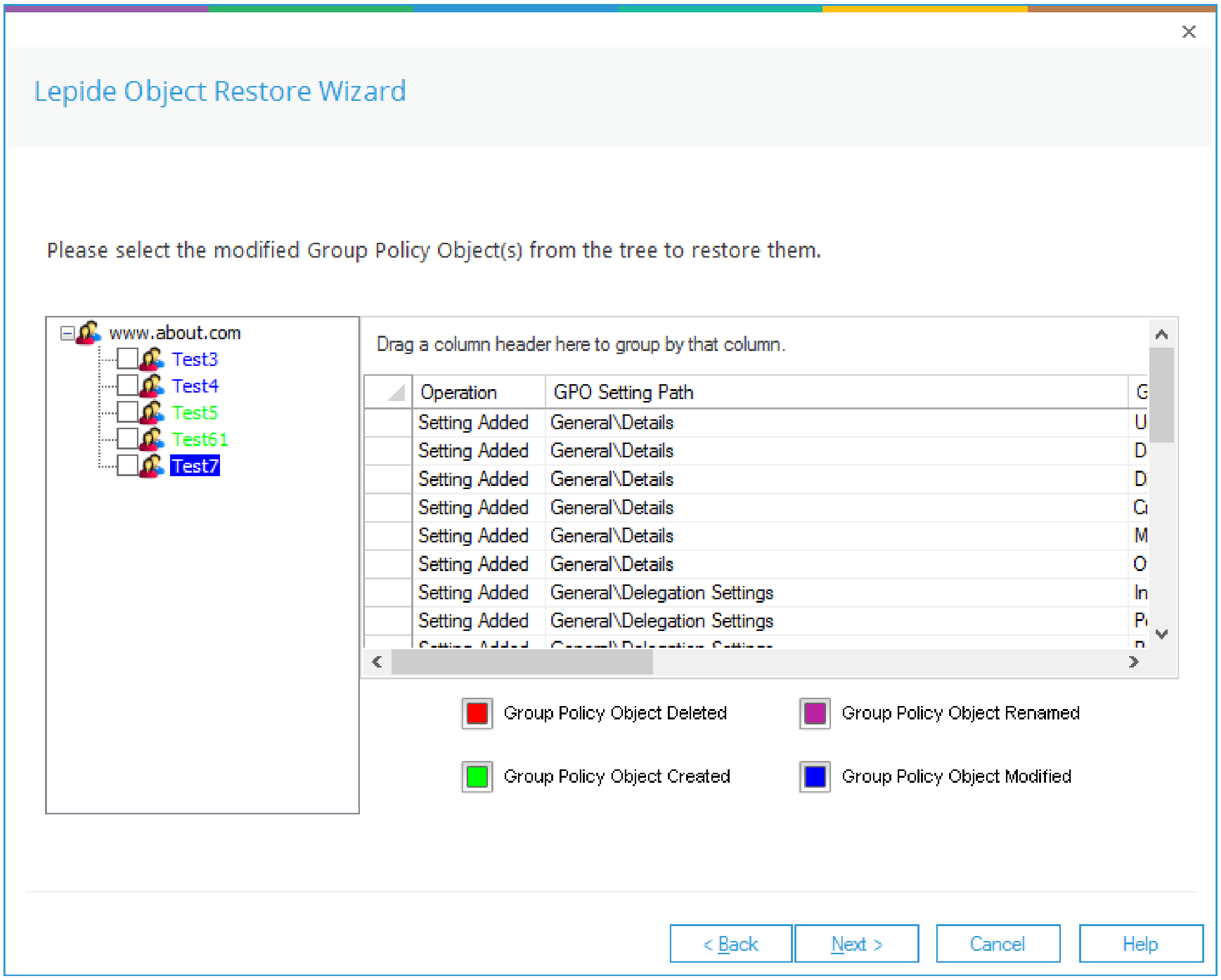
Figure 59: Selected Backup

6. Click **OK** to go back to the **Lepide Object Restore Wizard**:

7. If you want to use the same credentials as those provided while adding the domain, then keep the option **Use predefined server credentials** checked.

   Alternatively, uncheck it and provide the username and password for explicit login credentials to restore the object(s).

8. Click **Next**



Lepide Object Restore Wizard

Please select the modified Group Policy Object(s) from the tree to restore them.

- www.about.com
  - □ Test3
  - □ Test4
  - □ Test5
  - □ Test61
  - □ Test7

Drag a column header here to group by that column.

Operation	GPO Setting Path	G
Setting Added	General\Details	U
Setting Added	General\Details	D
Setting Added	General\Details	D
Setting Added	General\Details	C
Setting Added	General\Details	M
Setting Added	General\Details	O
Setting Added	General\Delegation Settings	In
Setting Added	General\Delegation Settings	P

🟥 Group Policy Object Deleted

🟪 Group Policy Object Renamed

🟩 Group Policy Object Created

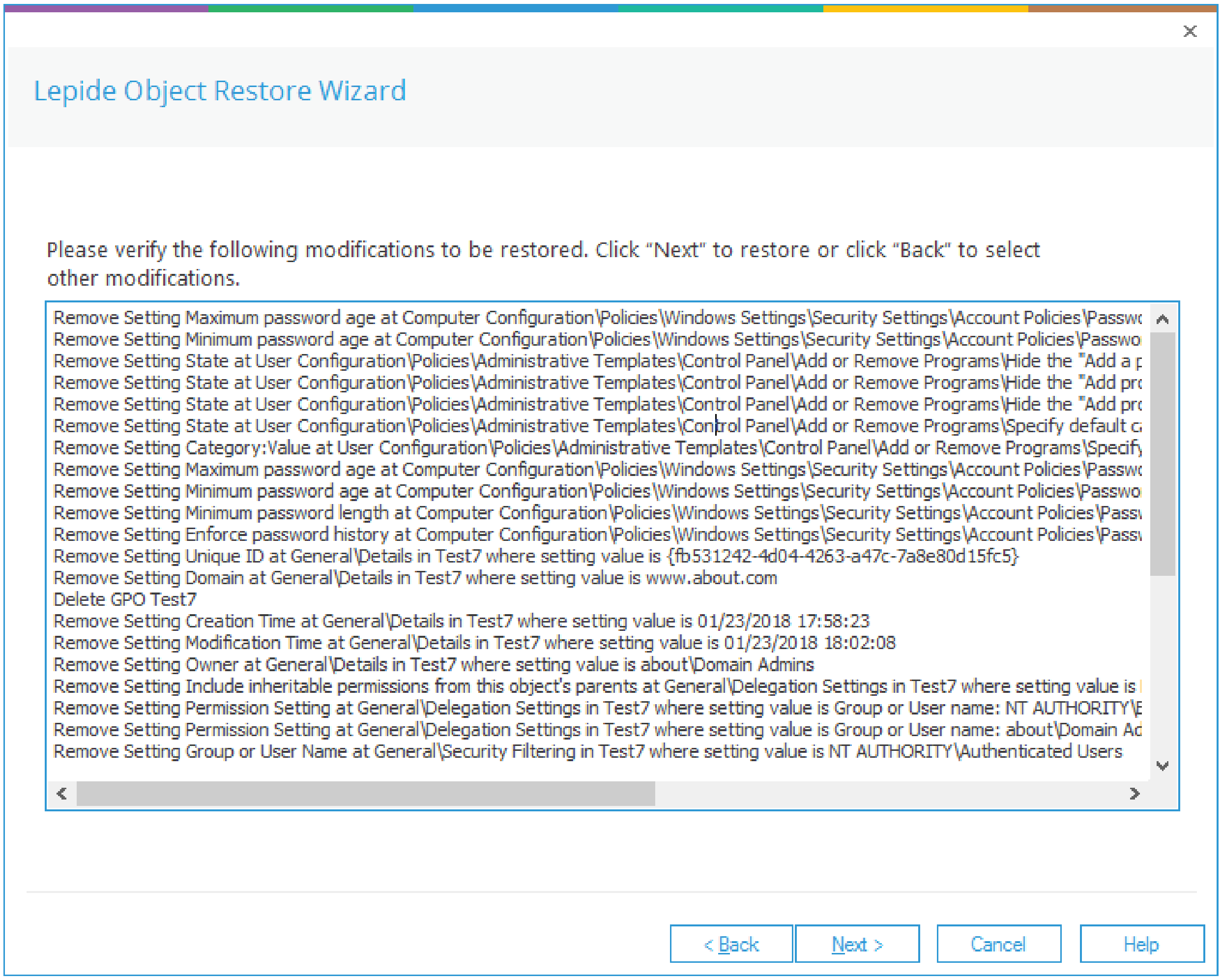
🟦 Group Policy Object Modified

Figure 60: Object Modifications

- The actions which can be selected are listed in a tree structure
- Click an object from the hierarchical tree to view the change details in the top right section
- The text describing these actions is color coded according to the colors code key

9. Check the boxes for the objects that you want to restore
10. Click **Next** once you have selected the objects to be restored.

The following dialog box is displayed:



Please verify the following modifications to be restored. Click "Next" to restore or click "Back" to select other modifications.

```
Remove Setting Maximum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwc
Remove Setting Minimum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwo
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add a p
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add prc
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add prc
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Specify default c
Remove Setting Category:Value at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Specify
Remove Setting Maximum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwc
Remove Setting Minimum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwo
Remove Setting Minimum password length at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passv
Remove Setting Enforce password history at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passv
Remove Setting Unique ID at General\Details in Test7 where setting value is {fb531242-4d04-4263-a47c-7a8e80d15fc5}
Remove Setting Domain at General\Details in Test7 where setting value is www.about.com
Delete GPO Test7
Remove Setting Creation Time at General\Details in Test7 where setting value is 01/23/2018 17:58:23
Remove Setting Modification Time at General\Details in Test7 where setting value is 01/23/2018 18:02:08
Remove Setting Owner at General\Details in Test7 where setting value is about\Domain Admins
Remove Setting Include inheritable permissions from this object's parents at General\Delegation Settings in Test7 where setting value is
Remove Setting Permission Setting at General\Delegation Settings in Test7 where setting value is Group or User name: NT AUTHORITY\E
Remove Setting Permission Setting at General\Delegation Settings in Test7 where setting value is Group or User name: about\Domain Ac
Remove Setting Group or User Name at General\Security Filtering in Test7 where setting value is NT AUTHORITY\Authenticated Users
```

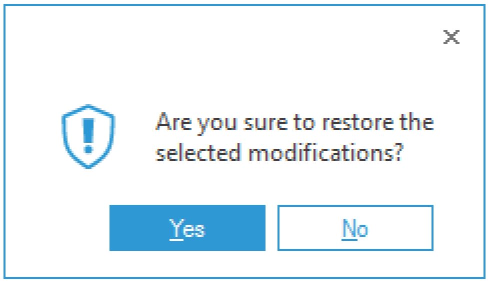
Figure 61: Summary of Selected Objects to be Restored

- This dialog box lists the changes about to be restored.

NOTE: It is essential to create a backup of the entire state of Group Policiy Objects so that you can revert to this current state after restoring a backup if required. See Section 4 of this document for the steps on how to create a backup.

11. Click **Next** to restore these changes or click **Back** to go back to the previous dialog box

A message box will be displayed for confirmation of the action:



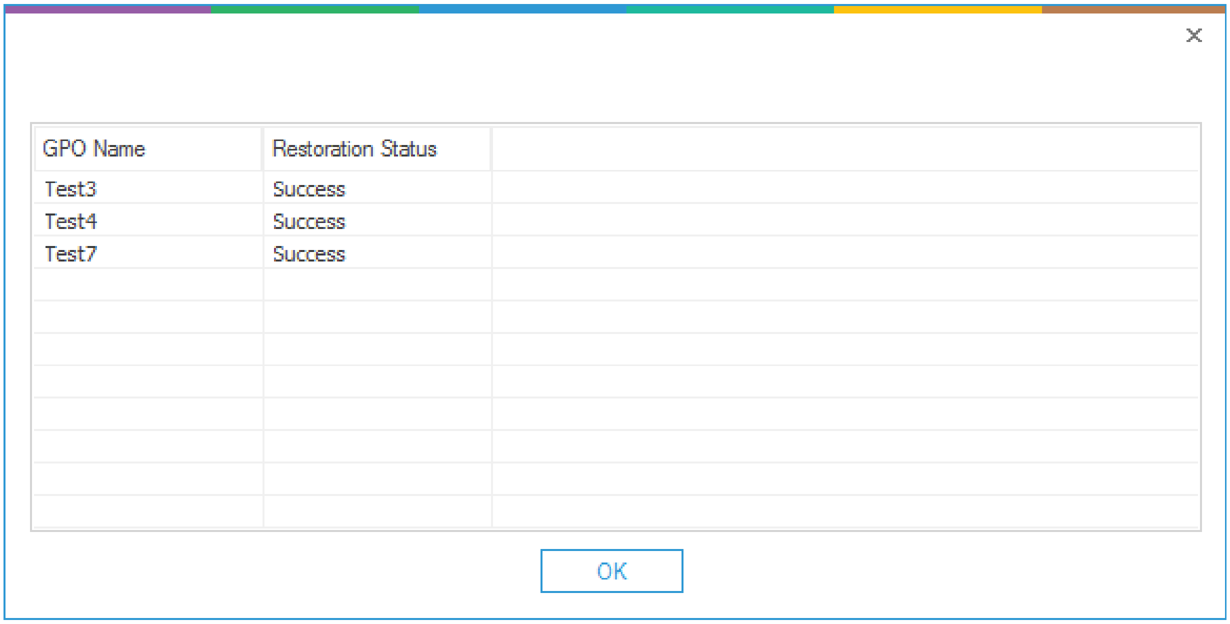
Are you sure to restore the selected modifications?

Figure 62: Message Box asking for Confirmation

12. Click **Yes** to start the restoration of modified or deleted objects

The Lepide Object Restore Wizard processes to restore the objects.

Once finished, the following screen will be displayed:

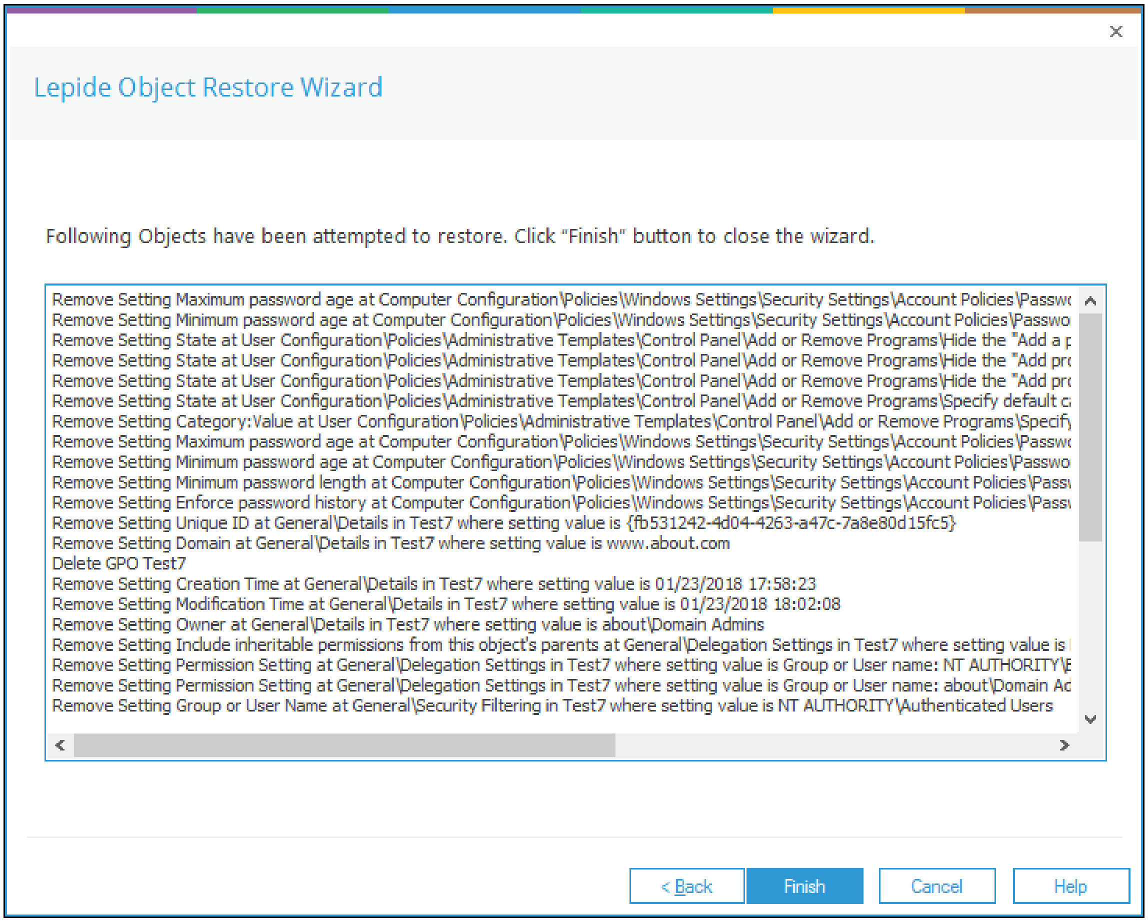


GPO Name	Restoration Status
Test3	Success
Test4	Success
Test7	Success

Figure 63: Summary of Object Restoration

- The objects that have been restored successfully displays the result **Success**. Their status will be **Fail** if they cannot be restored.

13. Click **OK** to close this summary box. It takes you back to the restore wizard:



Following Objects have been attempted to restore. Click "Finish" button to close the wizard.

```
Remove Setting Maximum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passw
Remove Setting Minimum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwo
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add a
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add pr
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Hide the "Add pr
Remove Setting State at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Specify default c
Remove Setting Category:Value at User Configuration\Policies\Administrative Templates\Control Panel\Add or Remove Programs\Specify
Remove Setting Maximum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passw
Remove Setting Minimum password age at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Passwo
Remove Setting Minimum password length at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Pass
Remove Setting Enforce password history at Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Pass
Remove Setting Unique ID at General\Details in Test7 where setting value is {fb531242-4d04-4263-a47c-7a8e80d15fc5}
Remove Setting Domain at General\Details in Test7 where setting value is www.about.com
Delete GPO Test7
Remove Setting Creation Time at General\Details in Test7 where setting value is 01/23/2018 17:58:23
Remove Setting Modification Time at General\Details in Test7 where setting value is 01/23/2018 18:02:08
Remove Setting Owner at General\Details in Test7 where setting value is about\Domain Admins
Remove Setting Include inheritable permissions from this object's parents at General\Delegation Settings in Test7 where setting value is
Remove Setting Permission Setting at General\Delegation Settings in Test7 where setting value is Group or User name: NT AUTHORITY\
Remove Setting Permission Setting at General\Delegation Settings in Test7 where setting value is Group or User name: about\Domain Ad
Remove Setting Group or User Name at General\Security Filtering in Test7 where setting value is NT AUTHORITY\Authenticated Users
```

Figure 64: Final Status of Object Restoration

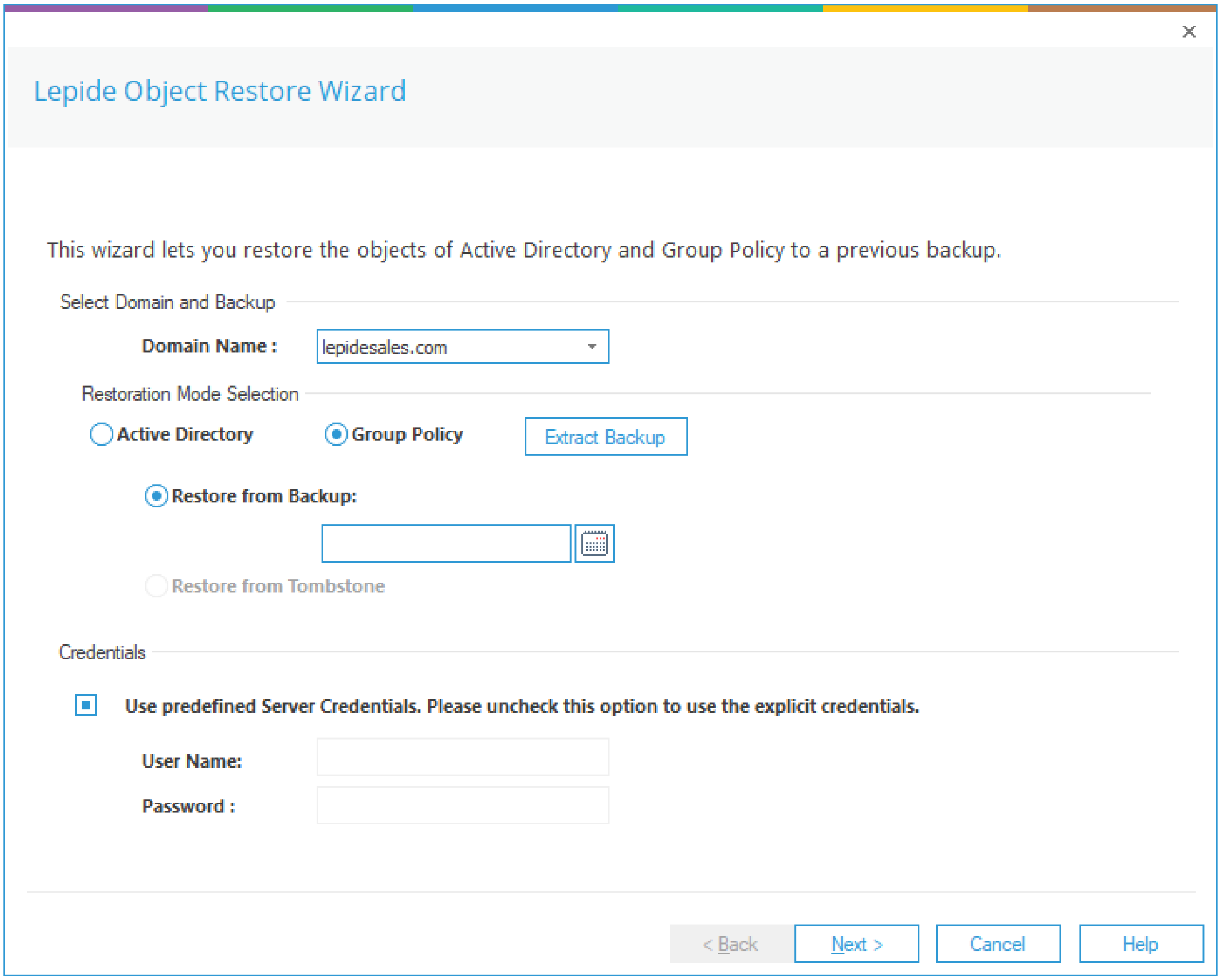
14. Click **Finish** to close the wizard

8.1. Group Policy Backup Extractor

As an alternative to restoring Group Policy Objects using the Object Restore Wizard, it is possible to extract Group Policy Objects to create a native file format and restore them outside of the Lepide Data Security Platform. To do this, the steps are as follows:

From the Lepide Object Restore Wizard dialog box, choose **Group Policy**

Click the **Extract Backup** button Extract Backup to extract a section of a group policy object:



Lepide Object Restore Wizard

This wizard lets you restore the objects of Active Directory and Group Policy to a previous backup.

Select Domain and Backup

Domain Name : lepidesales.com

Restoration Mode Selection

○ **Active Directory** ● **Group Policy** Extract Backup

● **Restore from Backup:**

○ Restore from Tombstone

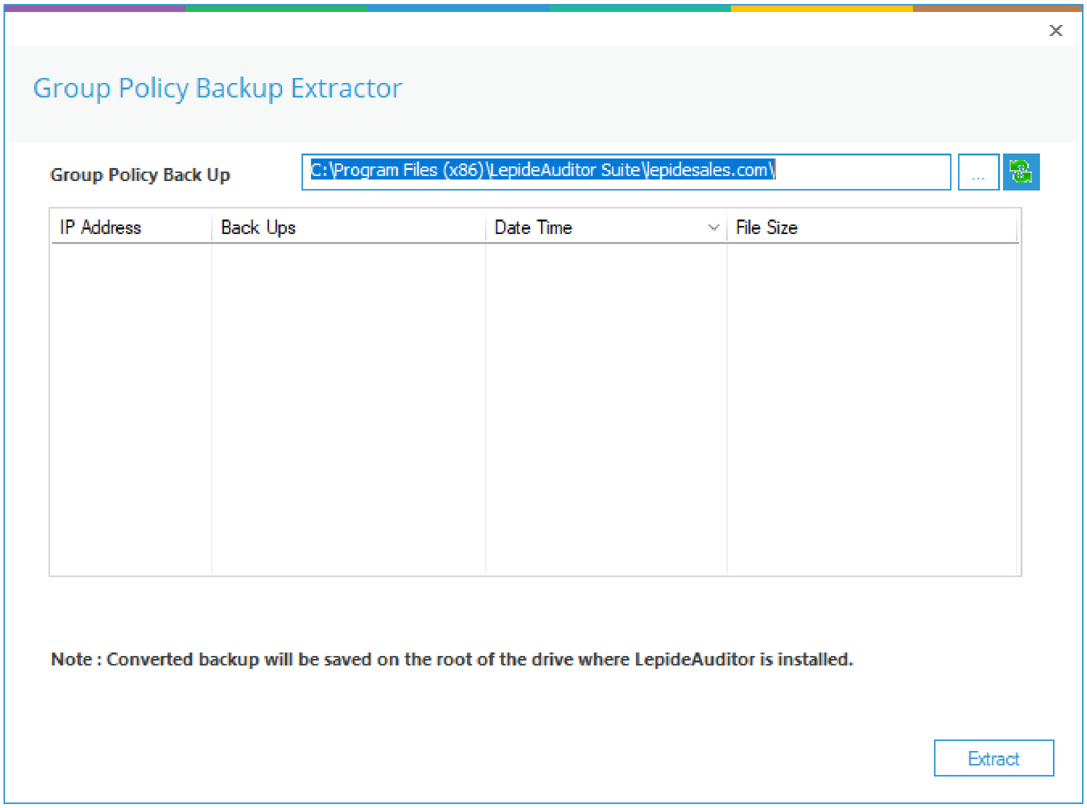
Credentials

☑ **Use predefined Server Credentials. Please uncheck this option to use the explicit credentials.**

User Name:

Password :

Figure 65: Lepide Object Restore Wizard


Group Policy Backup Extractor
Group Policy Back Up
C:\Program Files (x86)\LepideAuditor Suite\lepidesales.com\
...
IP Address
Back Ups
Date Time
File Size
Extract

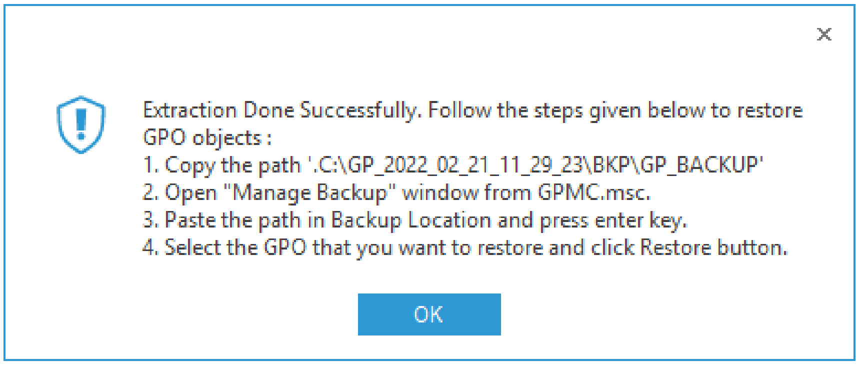
Note : Converted backup will be saved on the root of the drive where LepideAuditor is installed.

Figure 66: Group Policy Extractor

This will extract the Group Policy in a format that can be used by a native Group Policy Management Console to restore the group policy objects.

- Select the backup
- Click **Extract**

The following message box appears:

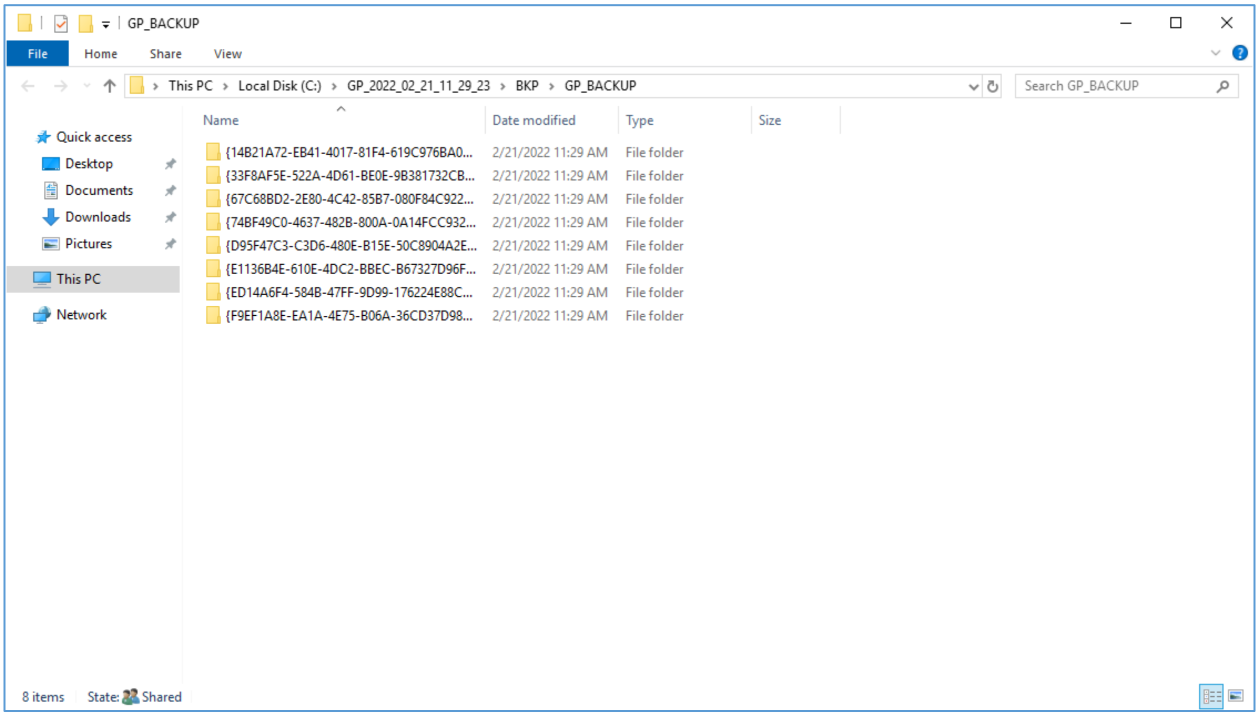


Extraction Done Successfully. Follow the steps given below to restore GPO objects :
1. Copy the path '.C:\GP_2022_02_21_11_29_23\BKP\GP_BACKUP'
2. Open "Manage Backup" window from GPMC.msc.
3. Paste the path in Backup Location and press enter key.
4. Select the GPO that you want to restore and click Restore button.

Figure 67: Successful Extraction of GPO Backup

- Click OK

The extracted file will be displayed in the location it has been stored:



Name	Date modified	Type	Size
{14B21A72-EB41-4017-81F4-619C976BA0...	2/21/2022 11:29 AM	File folder	
{33F8AF5E-522A-4D61-BE0E-9B381732CB...	2/21/2022 11:29 AM	File folder	
{67C68BD2-2E80-4C42-85B7-080F84C922...	2/21/2022 11:29 AM	File folder	
{74BF49C0-4637-482B-800A-0A14FCC932...	2/21/2022 11:29 AM	File folder	
{D95F47C3-C3D6-480E-B15E-50C8904A2E...	2/21/2022 11:29 AM	File folder	
{E1136B4E-610E-4DC2-BBEC-B67327D96F...	2/21/2022 11:29 AM	File folder	
{ED14A6F4-584B-47FF-9D99-176224E88C...	2/21/2022 11:29 AM	File folder	
{F9EF1A8E-EA1A-4E75-B06A-36CD37D98...	2/21/2022 11:29 AM	File folder	

Figure 68: Extracted File and Location

- Follow the instructions given above in the message box, Figure 67 to restore the Group Policy Object.

9. 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/.

10. Trademarks

Lepide Data Security Platform, 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.