Lepide

CONFIGURATION GUIDE

CURRENT PERMISSION REPORT

Table of Contents

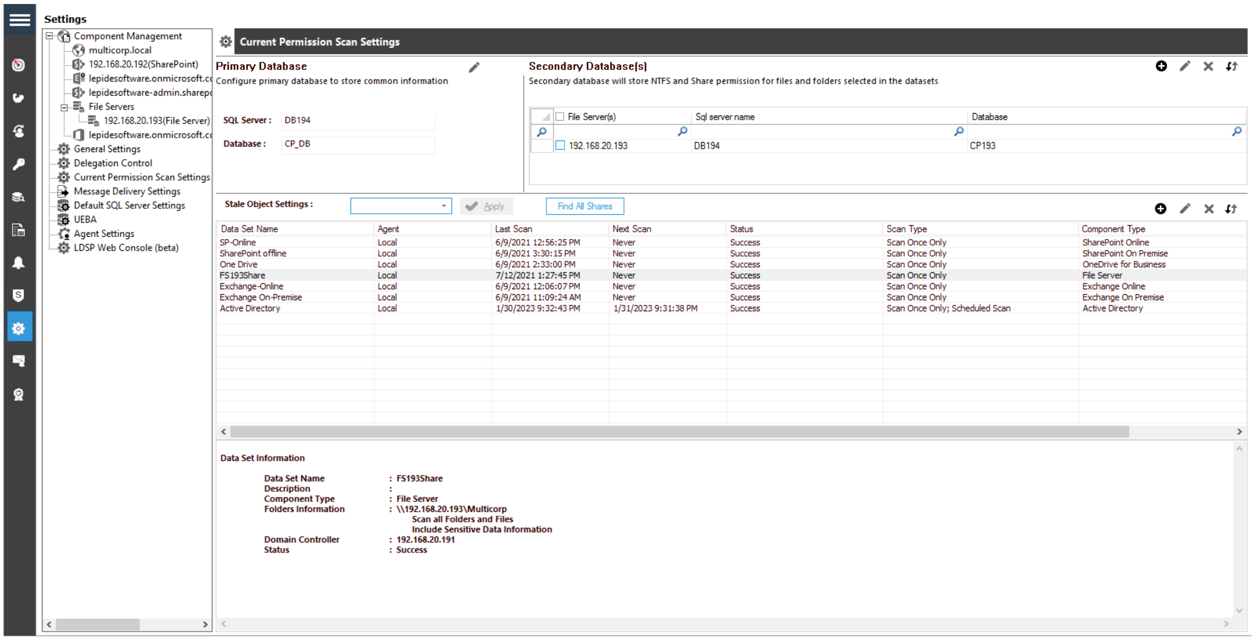
1 Introduction

The Lepide Data Security Platform provides a comprehensive means of auditing on-premise and cloud platforms.

This document is focused on how to run the Current Permission Report for File Server and for Exchange Online. It shows how to configure Current Permission Scan Settings, create a Data Set, scan the permissions, and generate the Current Permission Report.

2 Current Permission Scan Settings

You can use the Current Permission Scan Settings to create the Data Set containing those folders for which you want to monitor current permissions.


Settings
Component Management
multicorp.local
192.168.20.192(SharePoint)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
192.168.20.193(File Server)
lepidesoftware.onmicrosoft.c
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console (beta)
Current Permission Scan Settings
Apply
Find All Shares

Primary Database

Configure primary database to store common information

SQL Server : DB194

Database : CP_DB

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
192.168.20.193	DB194	CP193

Stale Object Settings :

Data Set Name	Agent	Last Scan	Next Scan	Status	Scan Type	Component Type
SP-Online	Local	6/9/2021 12:56:25 PM	Never	Success	Scan Once Only	SharePoint Online
SharePoint offline	Local	6/9/2021 3:30:15 PM	Never	Success	Scan Once Only	SharePoint On Premise
One Drive	Local	6/9/2021 2:33:00 PM	Never	Success	Scan Once Only	OneDrive for Business
FS193Share	Local	7/12/2021 1:27:45 PM	Never	Success	Scan Once Only	File Server
Exchange-Online	Local	6/9/2021 12:06:07 PM	Never	Success	Scan Once Only	Exchange Online
Exchange On-Premise	Local	6/9/2021 11:09:24 AM	Never	Success	Scan Once Only	Exchange On Premise
Active Directory	Local	1/30/2023 9:32:43 PM	1/31/2023 9:31:38 PM	Success	Scan Once Only; Scheduled Scan	Active Directory

Data Set Information

```
Data Set Name          : FS193Share
Description            :
Component Type         : File Server
Folders Information    : \\192.168.20.193\Multicorp
                              Scan all Folders and Files
                              Include Sensitive Data Information
Domain Controller      : 192.168.20.191
Status                 : Success
```

Figure 1: Current Permission Scan Settings

After configuring SQL Server, the Administrator can add, edit and delete the object lists.

1. Configure SQL Server

Follow the steps below to configure SQL Server Settings for accessing Current Permissions:

2. Configure the Solution to Run a Scan

The Lepide Data Security Platform needs to be configured to run a File Server scan before the report can be run and the steps to do this are as follows:

- Click on the **Settings** icon ⚙

- Click on **Current Permission Scan Settings**

The following screen will be displayed:

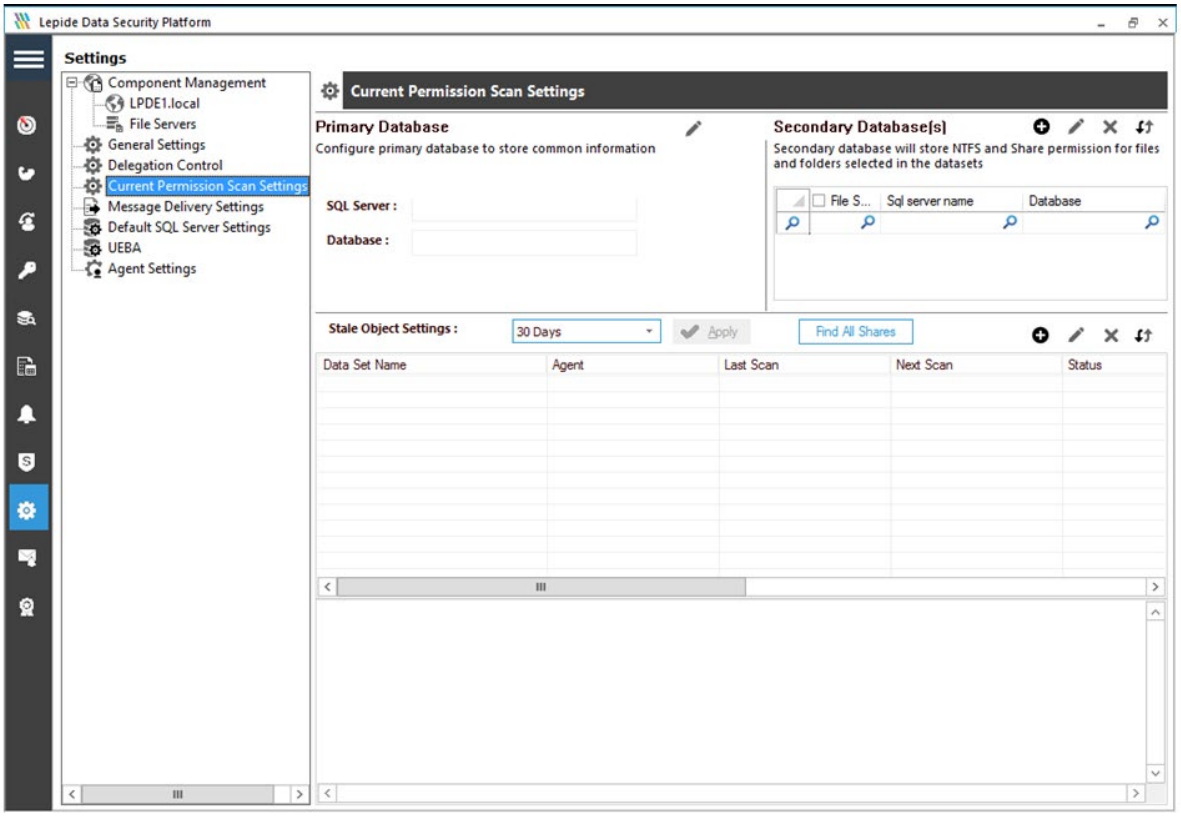
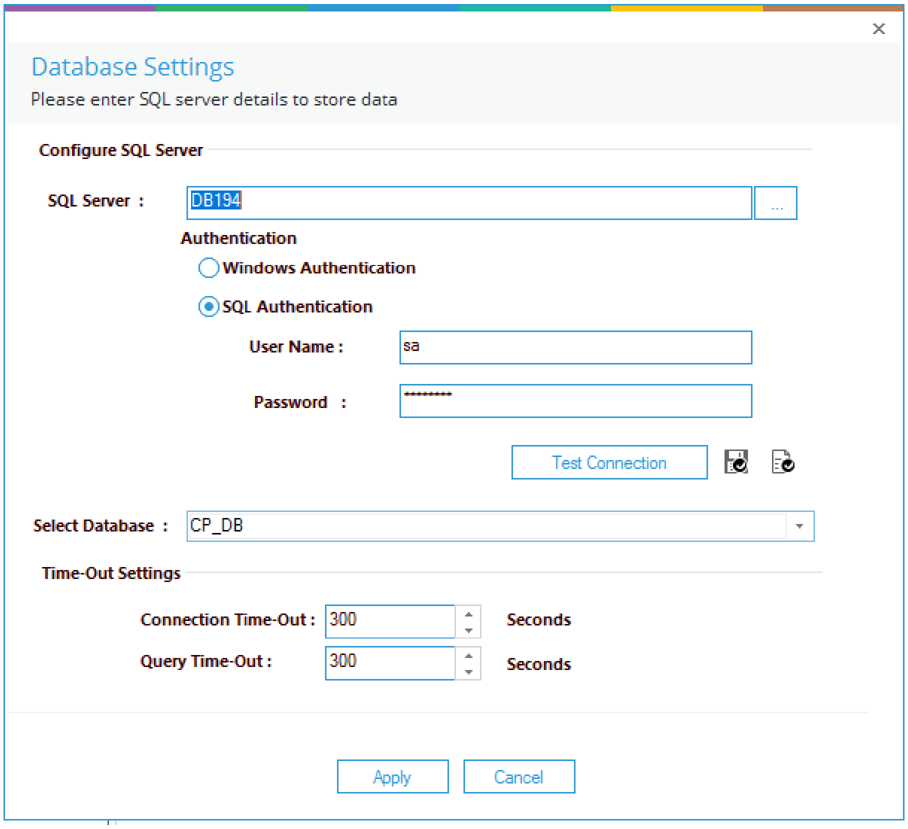

Lepide Data Security Platform
Settings
Component Management
LPDE1.local
File Servers
General Settings
Delegation Control
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
Current Permission Scan Settings
Primary Database
Configure primary database to store common information
SQL Server :
Database :
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
Apply
Find All Shares
Data Set Name
Agent
Last Scan
Next Scan
Status

Figure 2: Current Permission Scan Settings

2.1.1 Configure the Primary Database

- From the Primary Database area of the screen, click the ✎ icon to configure the **Primary Database**. It displays the following dialog box:



Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : DB194

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : *********

Select Database : CP_DB

Time-Out Settings

Connection Time-Out : 300 Seconds

Query Time-Out : 300 Seconds

Figure 3: Database Settings

NOTE: You can click 🗎 icon to show the SQL Server Settings from **Default SQL Server Settings**.

- The Solution lets you connect to a local or networked SQL Server. You can either enter the name of SQL Server manually in the text box or click … icon access a dialog box, which enumerates all SQL Servers in a list.
- Click the ⊞ icon to expand the listings for local and network servers. You can click ⊟ icon to collapse the list.
- Select a server and click **OK** to go back to the **SQL Server Settings** box, which now shows the selected SQL Server.
- Select any of the following authentication types.

  a. **Windows Authentication:** It lets the software login at SQL Server using the credentials of that user with which you are logged into the computer currently.

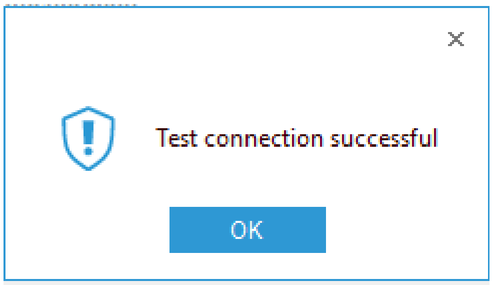
  b. **SQL Server Authentication:** It lets you provide the username and password of an SQL Server user.

NOTE: The selected user should have **dbcreator** role in SQL Server.

- Type a database name in the text box saying **Database**. If you are reinstalling the software, then you can reuse the earlier database.

- Click Test Connection to test the connection between the software and the selected SQL Server using the provided details. It either displays an error if failed to connect or shows the following message confirming the successful connection.

NOTE: The software does not create this database until you add a Data Set and start its scanning.

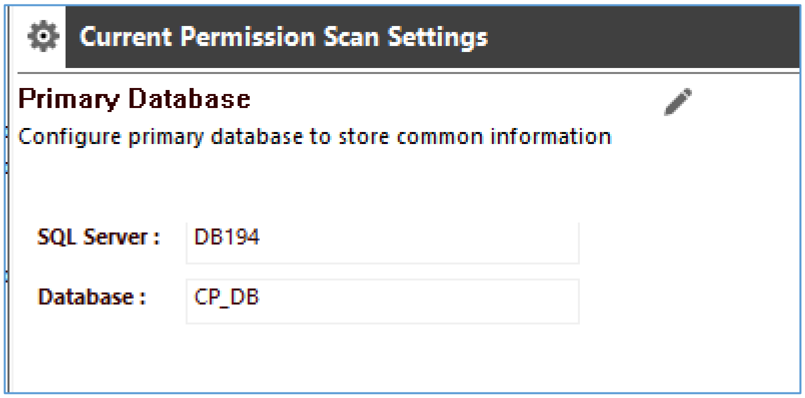


Test connection successful

Figure 4: SQL Server Connection is Successful

NOTE: You can click the icon to save the current SQL Server Settings as default in **Default SQL Server**

- Click **Apply** to save the database settings. It takes you back to **Current Permission Scan Settings** that shows the details of selected SQL Server and database.



Current Permission Scan Settings

Primary Database

Configure primary database to store common information

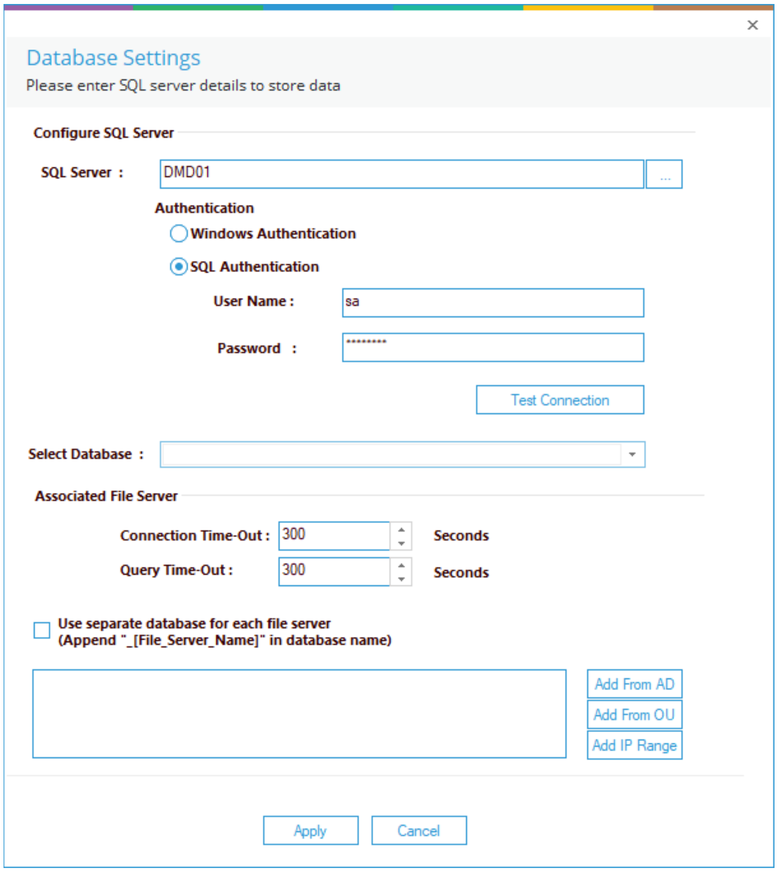
SQL Server : DB194

Database : CP_DB

Figure 5: Selected SQL Server and its Database

2.1.2 Add a Secondary Database

- From the Secondary Database area of the screen, click the (+) icon to configure the **Secondary Database**. It displays the following dialog box:



Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : DMD01

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

Select Database :

Associated File Server

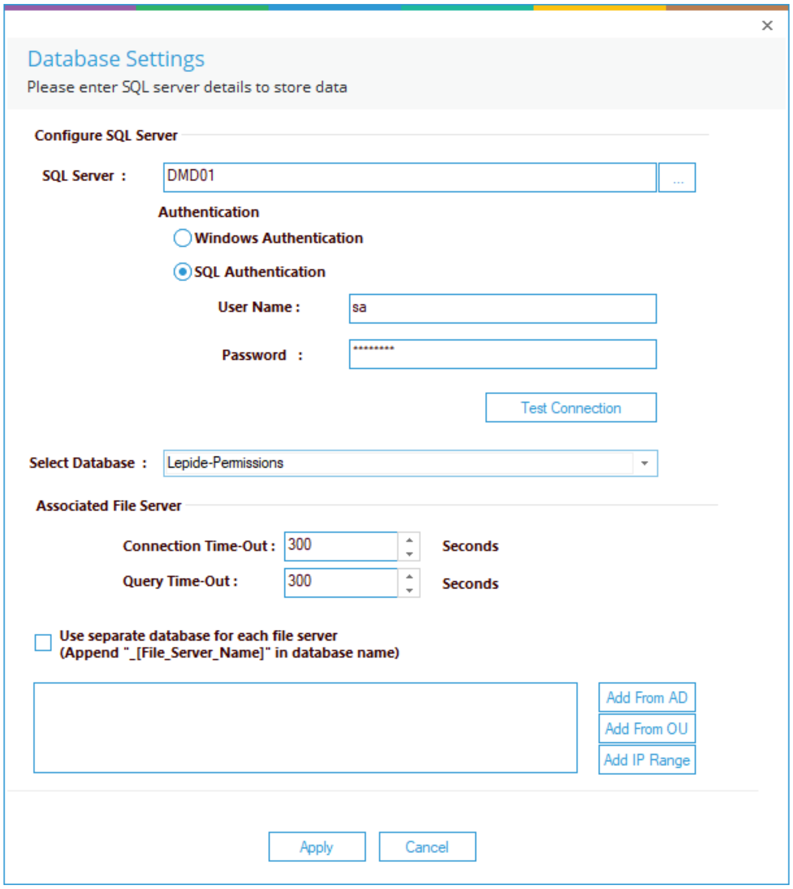
Connection Time-Out : 300 Seconds

Query Time-Out : 300 Seconds

□ Use separate database for each file server
(Append "_[File_Server_Name]" in database name)

Figure 6: Database Settings for Secondary Database

- Add the Database Name and click **Apply**



Database Settings

Please enter SQL server details to store data

Configure SQL Server

SQL Server : DMD01

Authentication

○ Windows Authentication

● SQL Authentication

User Name : sa

Password : ********

Select Database : Lepide-Permissions

Associated File Server

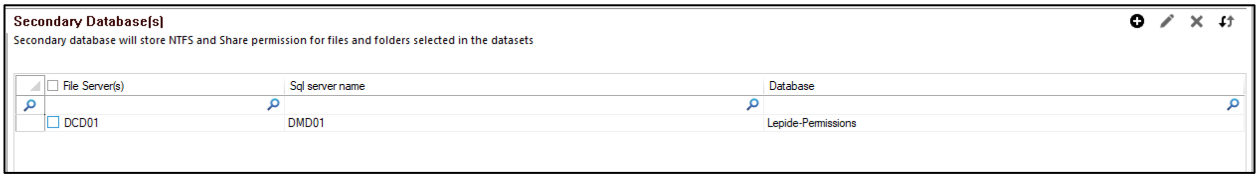
Connection Time-Out : 300 Seconds

Query Time-Out : 300 Seconds

□ Use separate database for each file server
(Append "_[File_Server_Name]" in database name)

Figure 7: Database Settings with Secondary Database Name

The secondary database information is displayed:



Secondary Database[s]

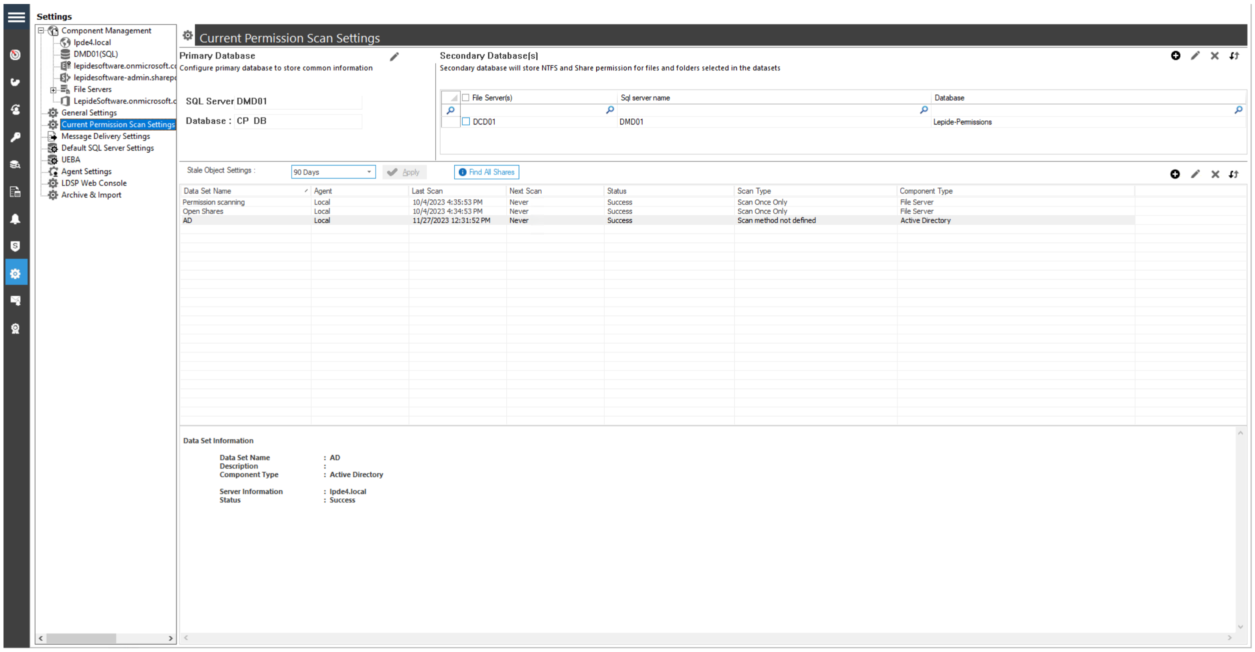
Secondary database will store NTFS and Share permission for files and folders selected in the datasets

File Server(s)	Sql server name	Database
□ DCD01	DMD01	Lepide-Permissions

Figure 8: Secondary Database Information

3. Add a Data Set for a File Server Permission Report

- From the Settings Screen
- Select the **Current Permission Scan Settings** option


Settings
Component Management
lpde4.local
DMD01(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
LepideSoftware.onmicrosoft.c
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Apply
Find All Shares

Current Permission Scan Settings

Primary Database
Configure primary database to store common information

SQL Server DMD01
Database : CP DB

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
□ DCD01	DMD01	Lepide-Permissions

Stale Object Settings : 90 Days

Data Set Name	Agent	Last Scan	Next Scan	Status	Scan Type	Component Type
Permission scanning	Local	10/4/2023 4:35:53 PM	Never	Success	Scan Once Only	File Server
Open Shares	Local	10/4/2023 4:34:53 PM	Never	Success	Scan Once Only	File Server
AD	Local	11/27/2023 12:31:52 PM	Never	Success	Scan method not defined	Active Directory

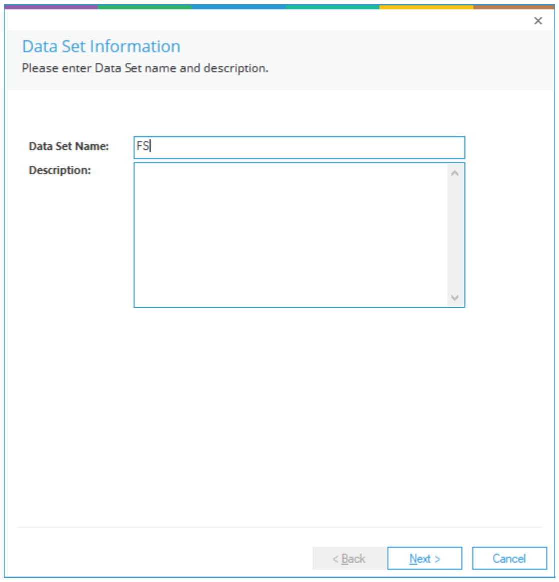
Data Set Information

Data Set Name : AD
Description :
Component Type : Active Directory

Server Information : lpde4.local
Status : Success

Figure 9: Current Permission Scan Settings

- Create a new **Data Set Profile** by clicking the (+) icon and give the Data Set a name
- Click **Next**

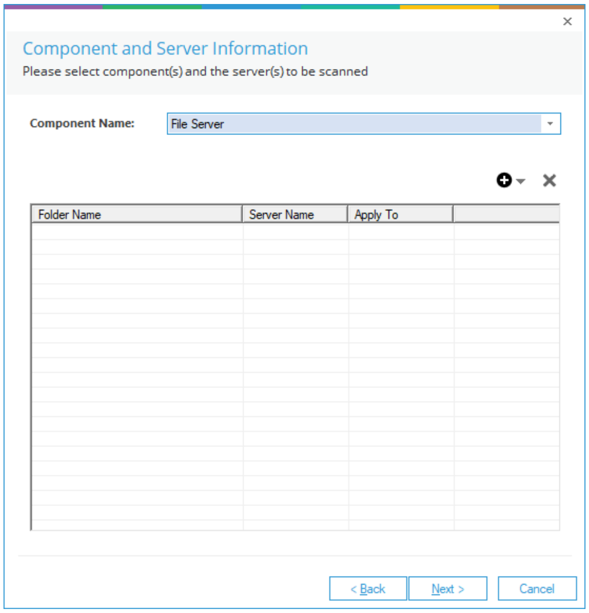


Data Set Information
Please enter Data Set name and description.

Data Set Name: FS
Description:

Figure 10: Add a Data Set Name

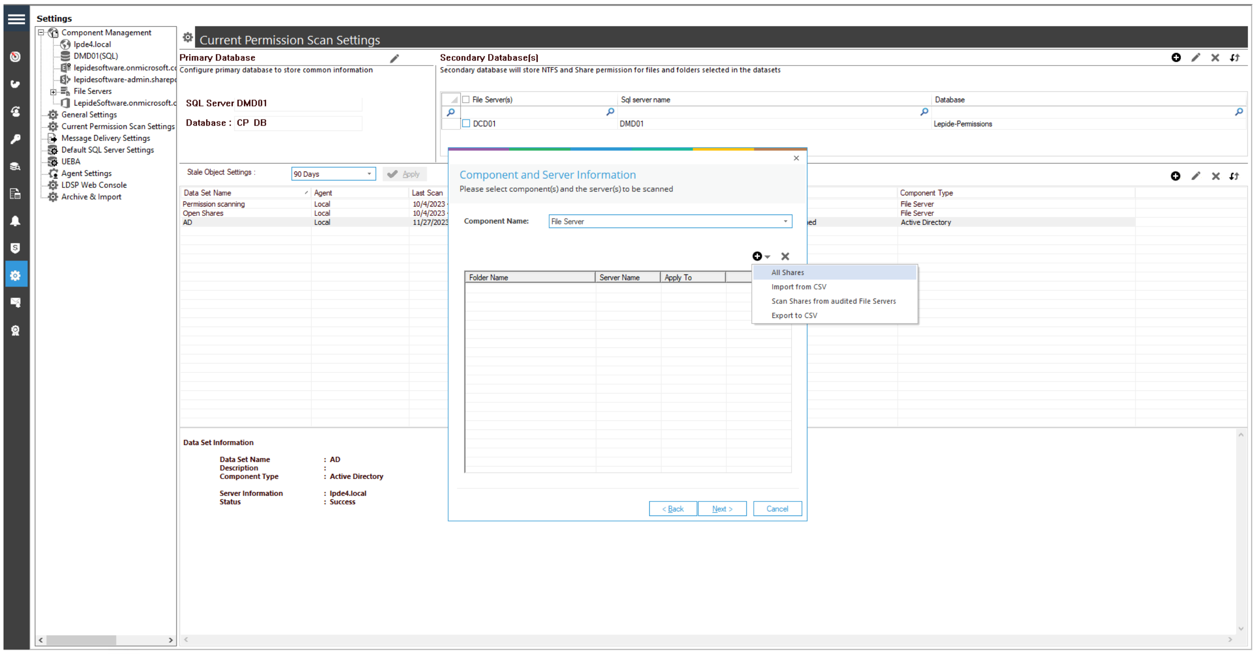
- Choose **File Server** as the Component Name
- Click on the (+) icon


×
Component and Server Information
Please select component(s) and the server(s) to be scanned
< Back
Next >
Cancel

Component Name: File Server

Folder Name	Server Name	Apply To	

Figure 11: Add Component and Server Information


Settings
Component Management
lpde4.local
DMD01(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
LepideSoftware.onmicrosoft.c
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Current Permission Scan Settings
Primary Database
Configure primary database to store common information
Secondary Database[s]
Secondary database will store NTFS and Share permission for files and folders selected in the datasets
Apply
Component and Server Information
Please select component(s) and the server(s) to be scanned
All Shares
Import from CSV
Scan Shares from audited File Servers
Export to CSV
< Back
Next >
Cancel

SQL Server DMD01

Database : CP DB

File Server(s)	Sql server name	Database
DCD01	DMD01	Lepide-Permissions

Stale Object Settings : 90 Days

Data Set Name	Agent	Last Scan	Component Type
Permission scanning	Local	10/4/2023	File Server
Open Shares	Local	10/4/2023	File Server
AD	Local	11/27/2023	Active Directory

Component Name: File Server

Folder Name	Server Name	Apply To	

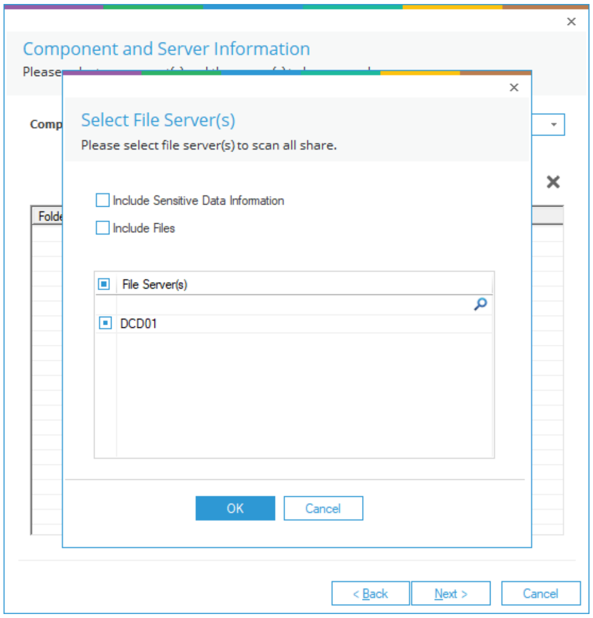
Data Set Information

Data Set Name	: AD
Description	:
Component Type	: Active Directory
Server Information	: lpde4.local
Status	: Success

Figure 12: Choose All Shares from the Menu

- Choose **All Shares**.

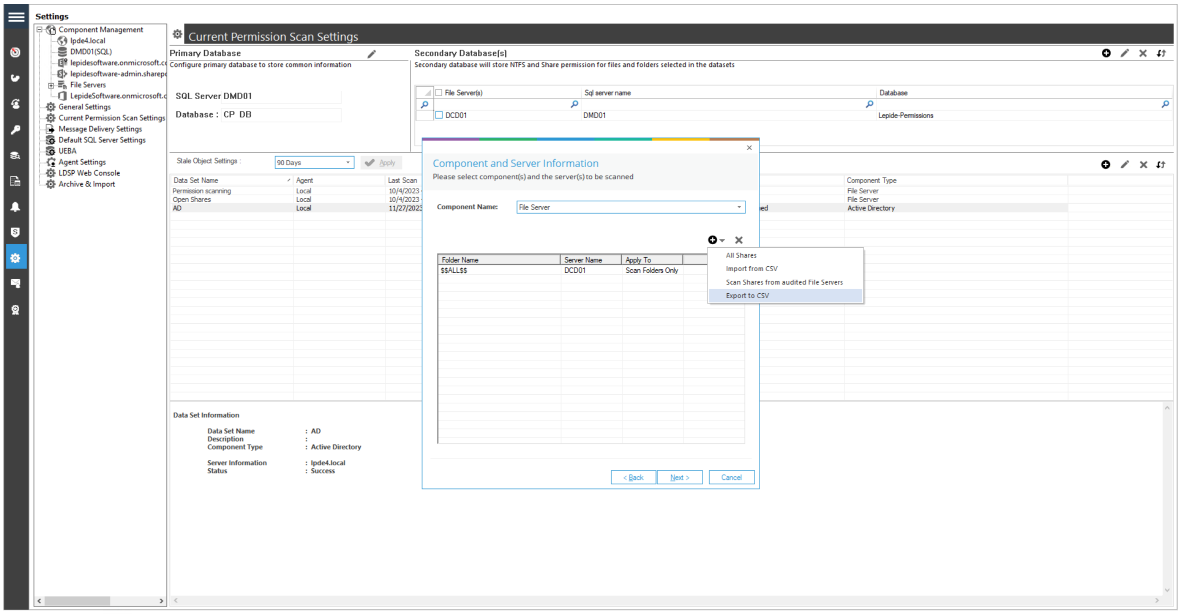
- Select the File Server from the list for which you want to add the All Shares option and click **OK**



Component and Server Information
Please
Comp
Folde
Select File Server(s)
Please select file server(s) to scan all share.
□ Include Sensitive Data Information
□ Include Files
File Server(s)
DCD01
OK
Cancel
< Back
Next >
Cancel

Figure 13: Select the File Server(s)

- If you want to export to CSV, click the (+) icon again and choose **Export to CSV (+)**


Settings
Component Management
lpde4.local
DMD01(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
LepideSoftware.onmicrosoft.c
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Current Permission Scan Settings
All Shares
Import from CSV
Scan Shares from audited File Servers
Export to CSV
< Back
Next >
Cancel
Apply

Primary Database

Configure primary database to store common information

SQL Server DMD01

Database : CP DB

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
□ DCD01	DMD01	Lepide-Permissions

Stale Object Settings : 90 Days

Data Set Name	Agent	Last Scan	Component Type
Permission scanning	Local	10/4/2023	File Server
Open Shares	Local	10/4/2023	File Server
AD	Local	11/27/2023	Active Directory

Data Set Information

Data Set Name : AD
Description :
Component Type : Active Directory

Server Information : lpde4.local
Status : Success

Component and Server Information

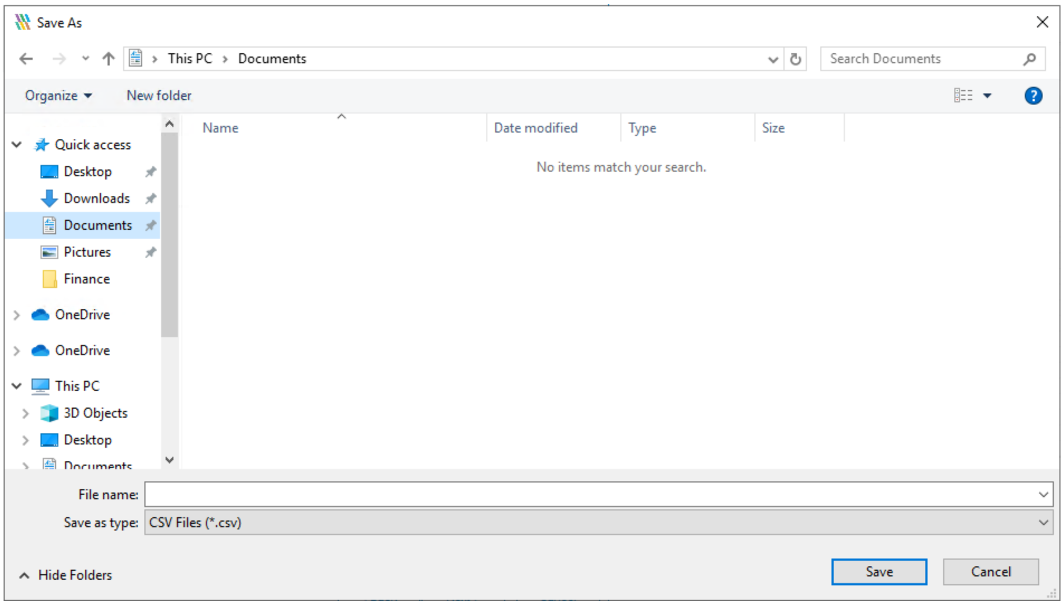
Please select component(s) and the server(s) to be scanned

Component Name: File Server

Folder Name	Server Name	Apply To
$$ALL$$	DCD01	Scan Folders Only

Figure 14: Export to CSV

- Specify the path where you want to export to and then click **Save**



No items match your search.

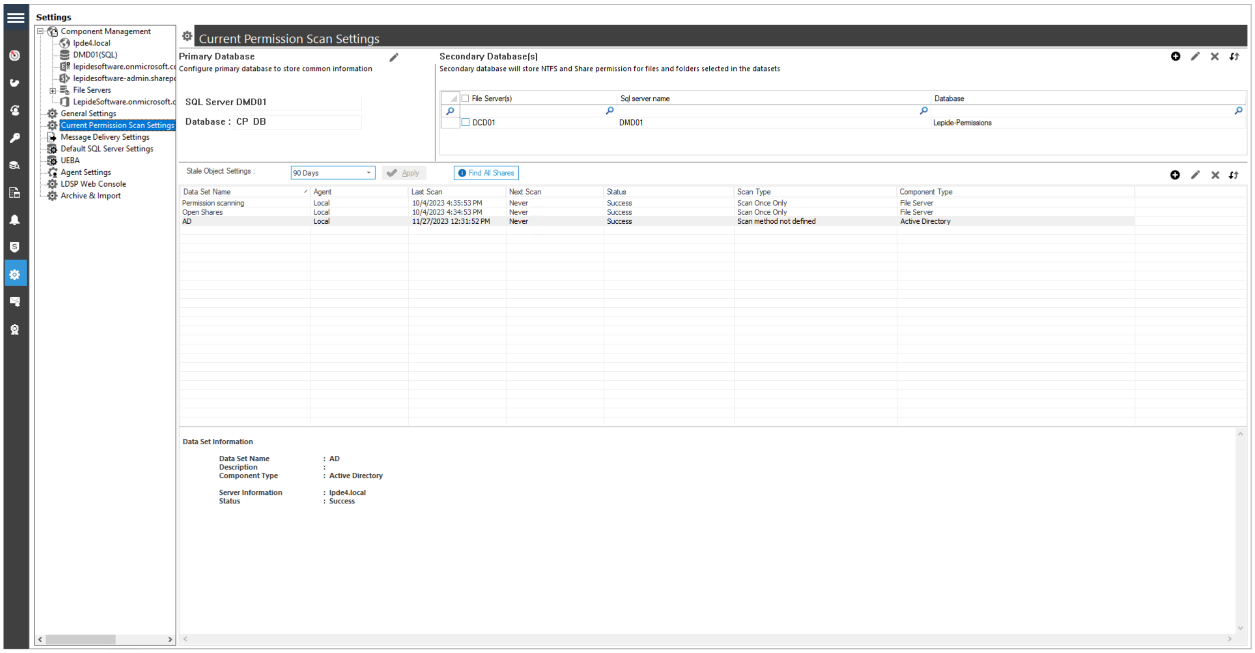
File name:

Save as type: CSV Files (*.csv)

Figure 15: Specify the Path

4. Add a Data Set for Exchange Online

- From the Settings Screen
- Select the **Current Permission Scan Settings** option:


Settings
Component Management
lpde4.local
DMD01(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
LepideSoftware.onmicrosoft.c
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Current Permission Scan Settings
Apply
Find All Shares

Primary Database
Configure primary database to store common information

SQL Server DMD01
Database : CP DB

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
□ DCD01	DMD01	Lepide-Permissions

Stale Object Settings : 90 Days

Data Set Name	Agent	Last Scan	Next Scan	Status	Scan Type	Component Type
Permission scanning	Local	10/4/2023 4:35:53 PM	Never	Success	Scan Once Only	File Server
Open Shares	Local	10/4/2023 4:34:53 PM	Never	Success	Scan Once Only	File Server
AD	Local	11/27/2023 12:31:52 PM	Never	Success	Scan method not defined	Active Directory

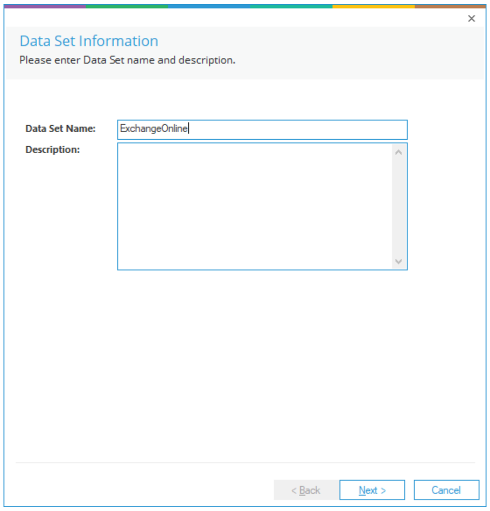
Data Set Information

Data Set Name : AD
Description :
Component Type : Active Directory

Server Information : lpde4.local
Status : Success

Figure 16: Current Permission Scan Settings

- Create a new **Data Set Profile** by clicking the (+) icon and give the Data Set a name

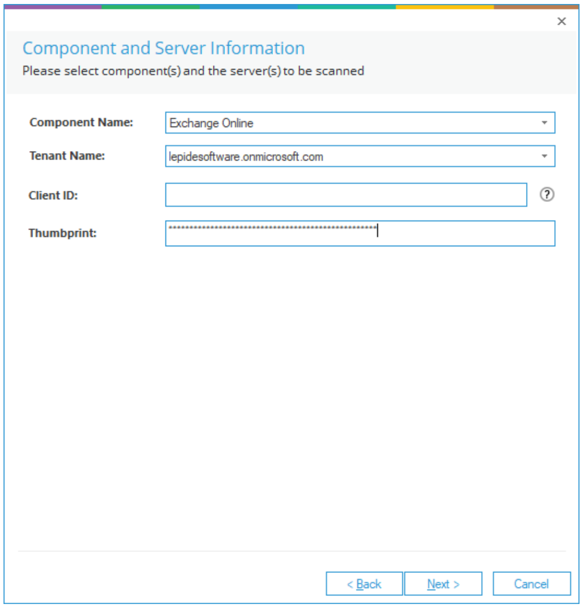


Data Set Information
Please enter Data Set name and description.

Data Set Name: ExchangeOnline
Description:

Figure 17: Add a Data Set Name

- Click **Next**
- Select **Exchange Online** and Add the Credentials as specified below:


Component and Server Information

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

Component Name: Exchange Online

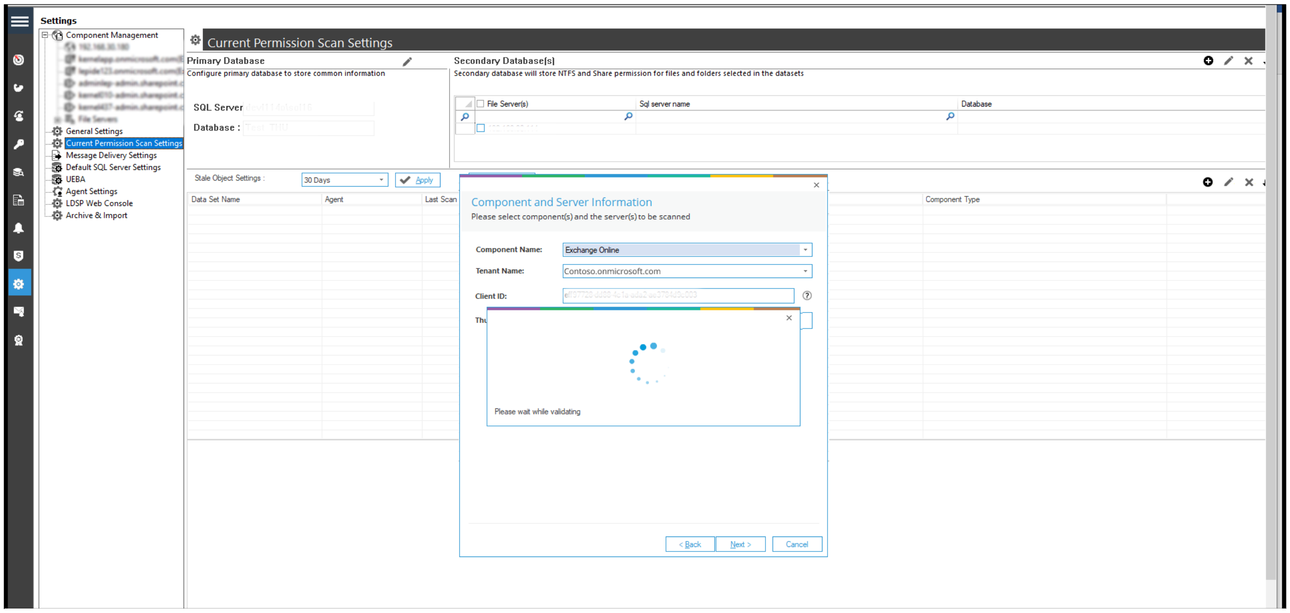
Tenant Name: lepidesoftware.onmicrosoft.com

Client ID:

Thumbprint: ••

Figure 18: Add Component and Server Information

- The Credentials will validate:


Settings
Component Management
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Current Permission Scan Settings
Primary Database
Configure primary database to store common information
SQL Server
Database :
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
Stale Object Settings :
30 Days
Apply
Data Set Name
Agent
Last Scan
Component Type

Component and Server Information

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

Component Name: Exchange Online

Tenant Name: Contoso.onmicrosoft.com

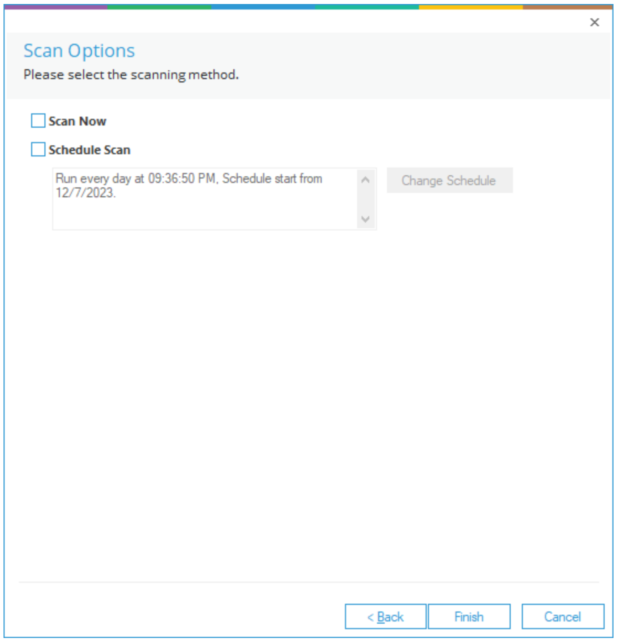
Client ID:

Please wait while validating

Figure 19: Validate Credentials

-

- Once the Credentials are Successfully verified, select the **Scan Now** option and click **Finish**.



Scan Options

Please select the scanning method.

☐ Scan Now

☐ Schedule Scan

Run every day at 09:36:50 PM, Schedule start from 12/7/2023.

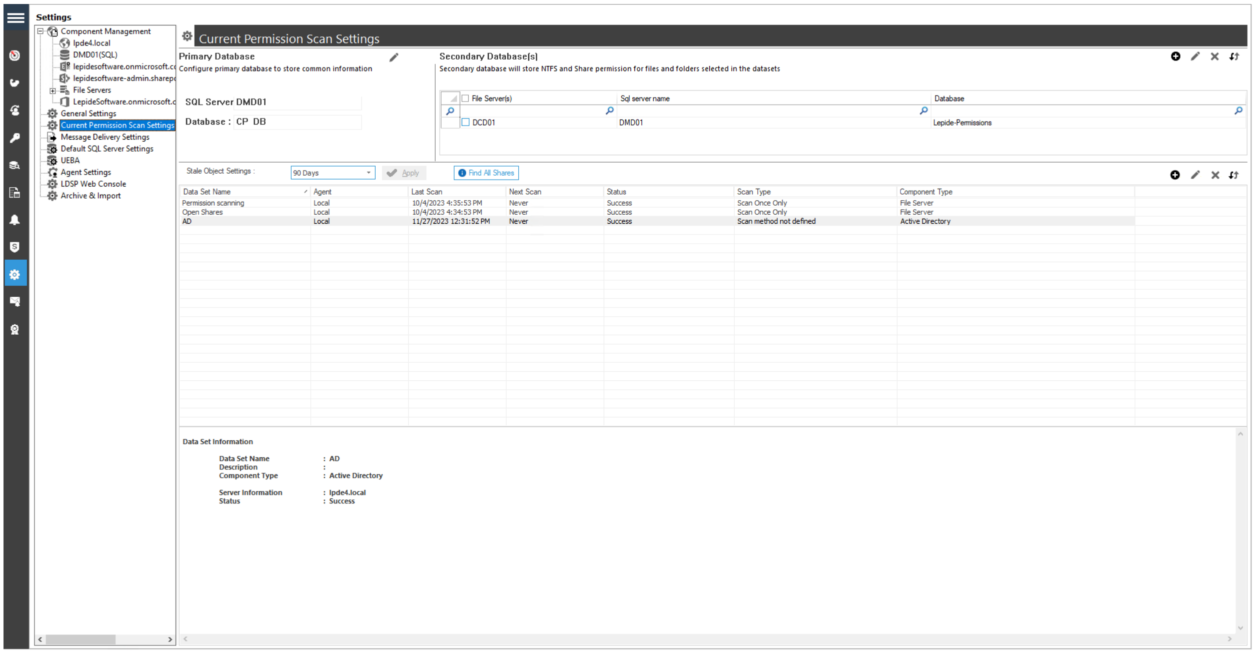
Figure 20: Scan Now

5. Add a Data Set for Azure Active Directory

NOTE: The data set for Azure Active Directory is added in the main console and the steps to do this are explained below. The output reports are only available in the Web Console.

- From the Settings Screen

- Select the **Current Permission Scan Settings** option:


Settings
Component Management
lpde4.local
DMD01(SQL)
lepidesoftware.onmicrosoft.c
lepidesoftware-admin.sharep
File Servers
LepideSoftware.onmicrosoft.c
General Settings
Current Permission Scan Settings
Message Delivery Settings
Default SQL Server Settings
UEBA
Agent Settings
LDSP Web Console
Archive & Import
Current Permission Scan Settings
Apply
Find All Shares

Primary Database
Configure primary database to store common information

SQL Server DMD01
Database : CP DB

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
□ DCD01	DMD01	Lepide-Permissions

Stale Object Settings : 90 Days

Data Set Name	Agent	Last Scan	Next Scan	Status	Scan Type	Component Type
Permission scanning	Local	10/4/2023 4:35:53 PM	Never	Success	Scan Once Only	File Server
Open Shares	Local	10/4/2023 4:34:53 PM	Never	Success	Scan Once Only	File Server
AD	Local	11/27/2023 12:31:52 PM	Never	Success	Scan method not defined	Active Directory

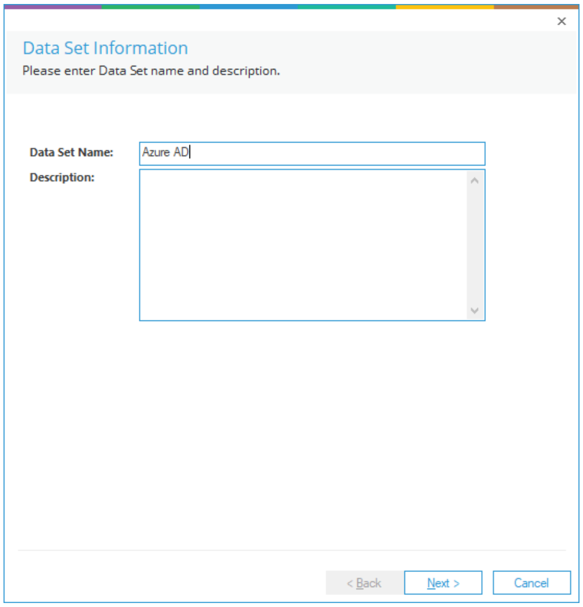
Data Set Information

Data Set Name : AD
Description :
Component Type : Active Directory

Server Information : lpde4.local
Status : Success

Figure 21: Current Permission Scan Settings

- Create a new **Data Set Profile** by clicking the (+) icon and give the Data Set a name

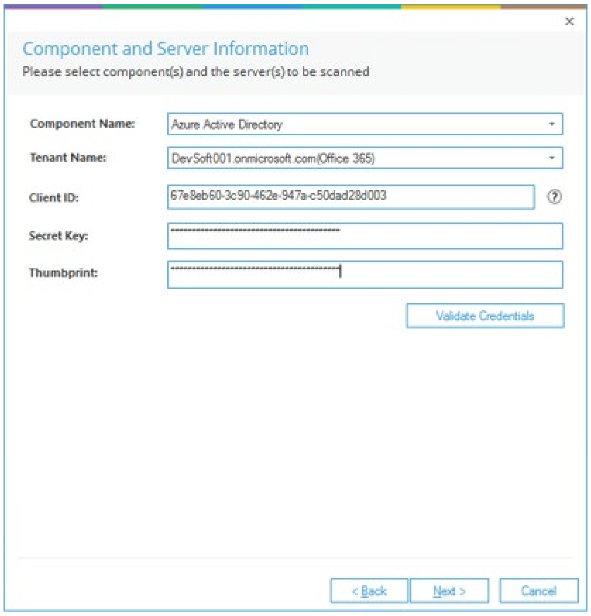


Data Set Information
Please enter Data Set name and description.

Data Set Name: Azure AD
Description:

Figure 22: Add a Data Set Name

- Click **Next**
- Select **Azure AD** and add the Credentials:



Component and Server Information

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

Component Name: Azure Active Directory

Tenant Name: DevSoft001.onmicrosoft.com(Office 365)

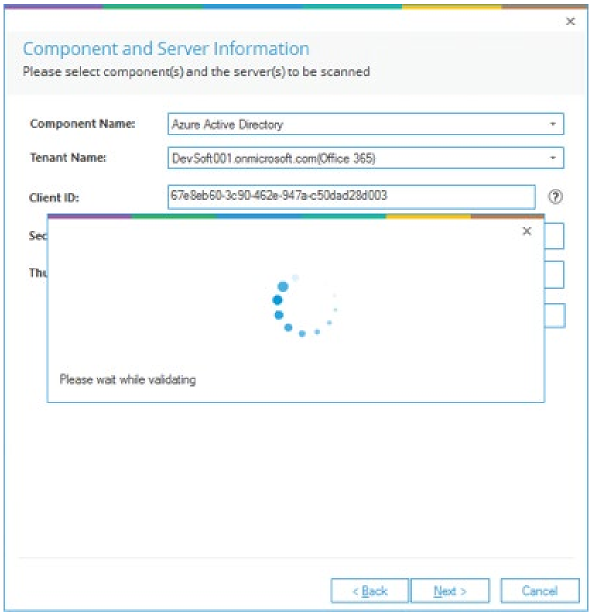
Client ID: 67e8eb60-3c90-462e-947a-c50dad28d003

Secret Key: **

Thumbprint: **

Figure 23: Add Component and Server Information

- Click **Validate Credentials** and the Credentials will validate:



Component and Server Information

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

Component Name: Azure Active Directory

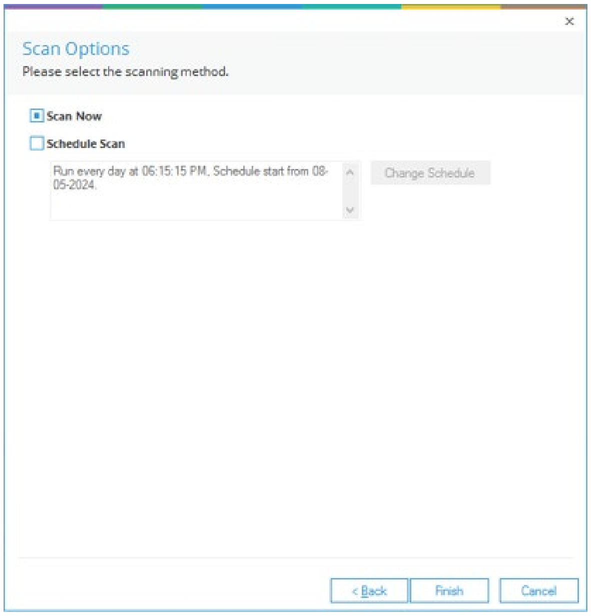
Tenant Name: DevSoft001.onmicrosoft.com(Office 365)

Client ID: 67e8eb60-3c90-462e-947a-c50dad28d003

Please wait while validating

Figure 24: Validate Credentials

- Once the Credentials are Successfully verified, select the **Scan Now** option and click **Finish**.



Scan Options

Please select the scanning method.

☑ Scan Now

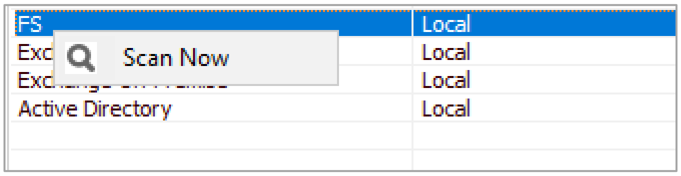
□ Schedule Scan

Run every day at 06:15:15 PM, Schedule start from 08-05-2024.

Figure 25: Scan Now

6. Scan Permissions Now

- To scan the permissions of the selected Data Set, right click on a data set and click **Scan Now**.

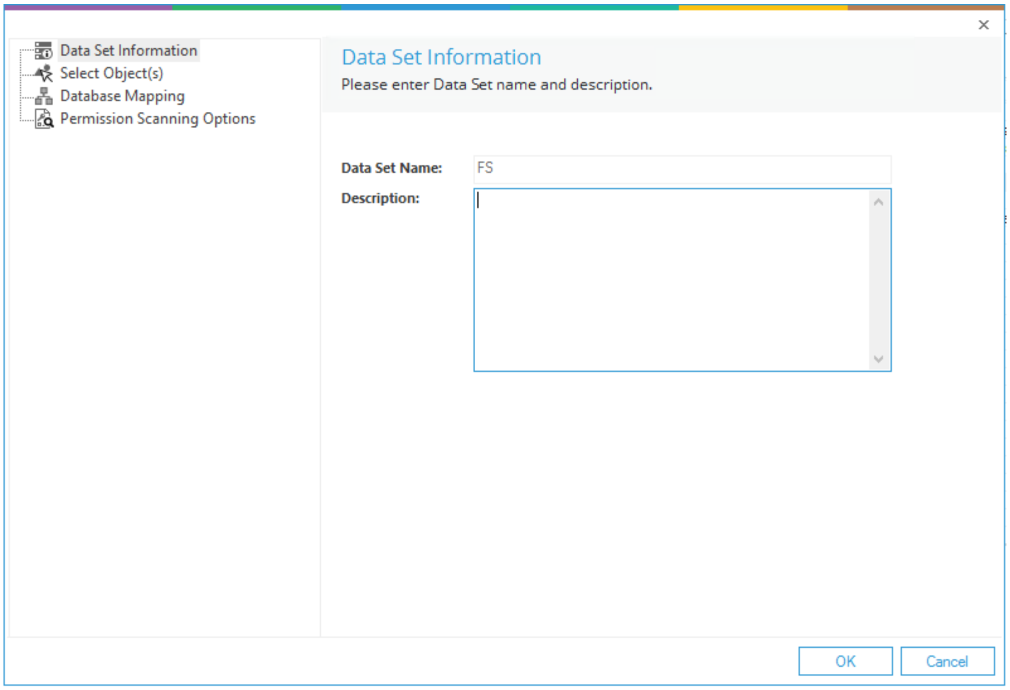


FS	Local
Exc	Local
Exc	Local
Active Directory	Local

Figure 26: Option to Scan Now

7. Modify a Data Set

- To modify a Data Set, select a Data Set in the list and click the ✎ icon. The following dialog box is displayed:



Data Set Information

Please enter Data Set name and description.

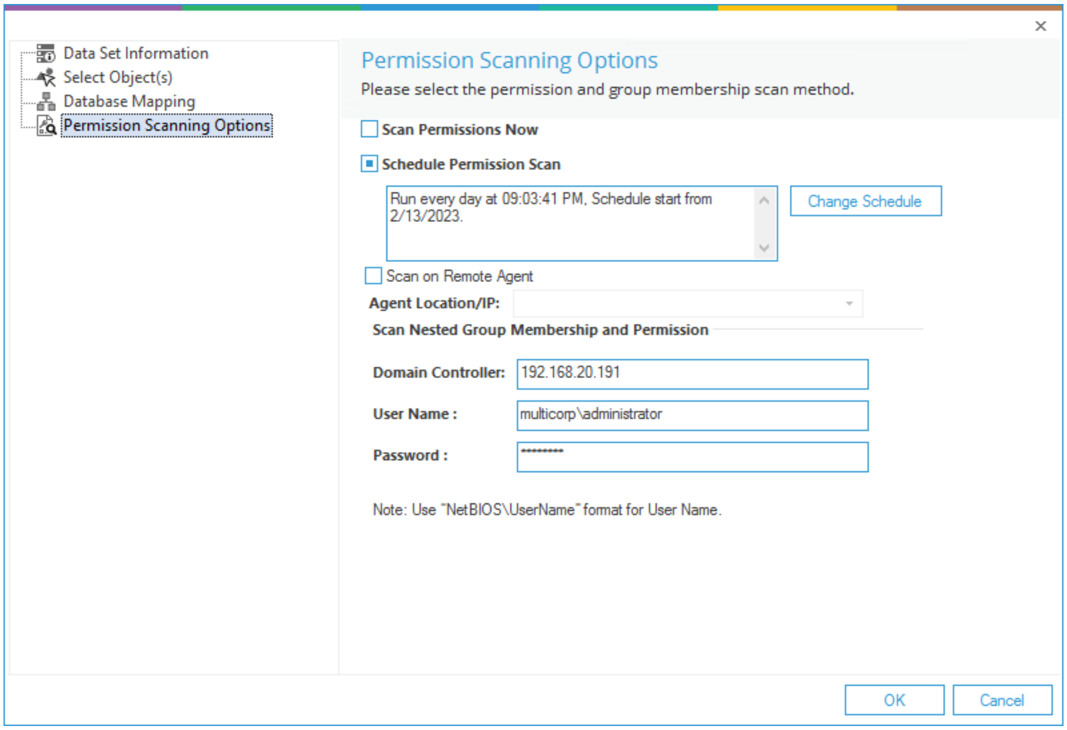
Data Set Name: FS

Description:

Figure 27: Modify Data Set

The options to modify a data set are the same as those available while adding the data set. The options are as follows:

1. **Data Set Information:** You can change the description of the Data Set; however, you cannot change its name
2. **Select Object(s):** Click this link in the left panel to access its settings. You can remove the listing of already added folder and add new folders
3. **Database Mapping:** Shows the database and server configuration
4. **Permission Scanning Options:** Click this link in the left panel to access its settings. You can change the update method and modify the scheduling of a permission scan



Permission Scanning Options

Please select the permission and group membership scan method.

☐ Scan Permissions Now

☑ Schedule Permission Scan

Run every day at 09:03:41 PM, Schedule start from 2/13/2023.

☐ Scan on Remote Agent

Agent Location/IP:

Scan Nested Group Membership and Permission

Domain Controller: 192.168.20.191

User Name : multicorp\administrator

Password : *********

Note: Use "NetBIOS\UserName" format for User Name.

Figure 28: Modify Permission Scanning Options

- Click **OK** at any option to save the changes in a Data Set

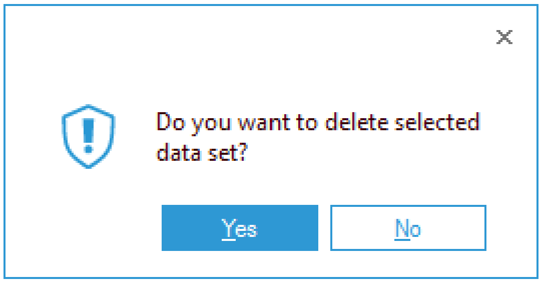
8. Remove a Data Set

If the Data Set is deleted, the software does not show the current permissions of the folders and its content added in the data set. The information contained about the Data Set and its scanning from the SQL Server Database is also removed.

NOTE: There is no way to retrieve a Data Set once removed.

Follow the steps below to remove a Data Set:

1. Select a Data Set from the list and click ✖ icon to remove the selected Data Set. The software displays the following warning message.



Do you want to delete selected data set?

Figure 29: Warning before deleting a Data Set

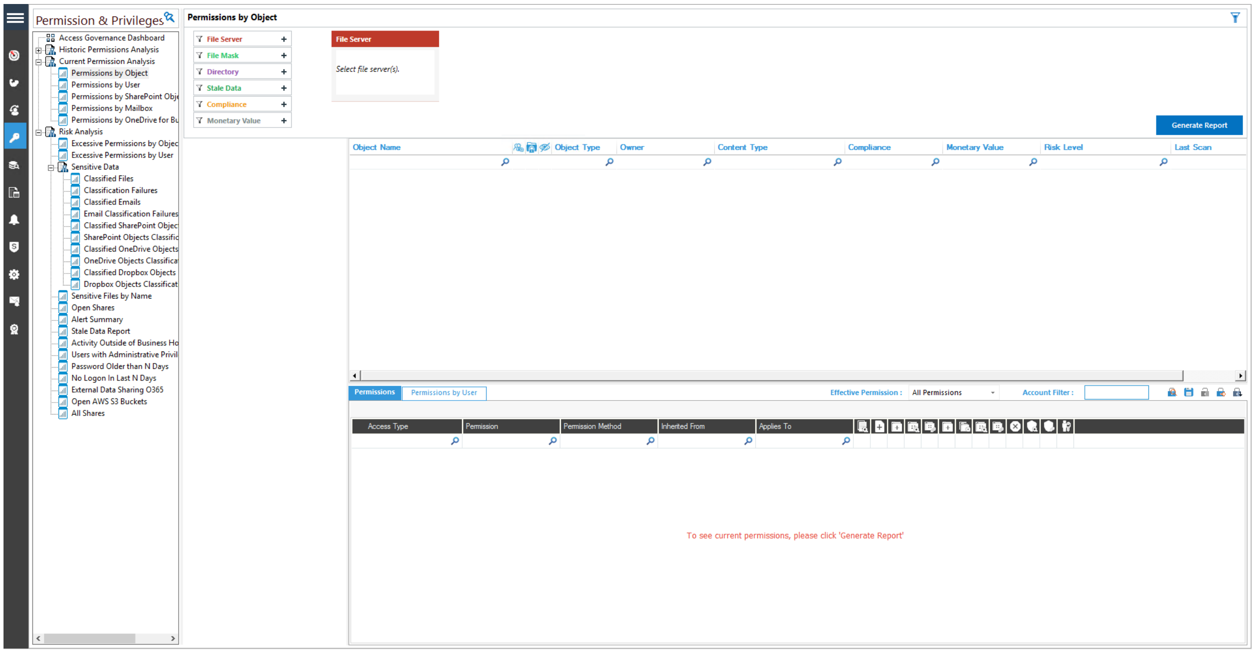
2. Click **Yes** to remove the selected Data Set

3 File Server Current Permission Report

To open the File Server Current Permission Report:

- Click the Permissions & Privileges icon
- Expand Current Permissions Analysis
- Choose Permissions by Object

The Current Permissions by Object Report is displayed:



Select file server(s).

Effective Permission : All Permissions

Account Filter :

To see current permissions, please click 'Generate Report'

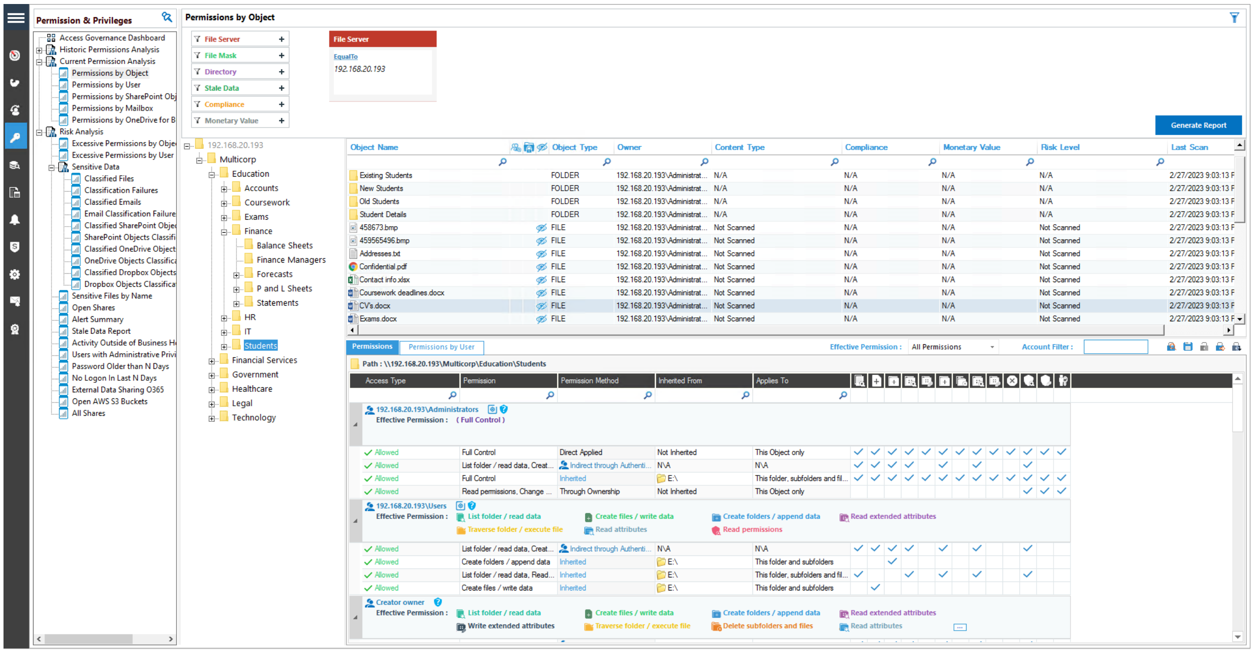
Figure 30: Current Permissions Report

You need to have configured **Current Permission Scan Settings** to be able to start analyzing the permissions. Please refer to Section 2 - Current Permission Scan Settings of this document for information on how to do this.

9. How to Generate the Current Permission Report

Follow the steps below to view the permission changes and compare the permissions of files and folders:

1. Select the File Server from the box at the top of the screen
2. Click **Generate Report** to run the Permission Analysis Report
3. Expand the file server node from the tree structure to the left-hand side to select the required folder
4. Select a folder and its contents will be displayed
5. Permission details for the selected folder of the left-hand pane, or for the selected file in the Object Section are displayed in the Permissions Section



File Server
EqualTo
192.168.20.193

Object Name	Object Type	Owner	Content Type	Compliance	Monetary Value	Risk Level	Last Scan
Existing Students	FOLDER	192.168.20.193\Administrat...	N/A	N/A	N/A	N/A	2/27/2023 9:03:13 F
New Students	FOLDER	192.168.20.193\Administrat...	N/A	N/A	N/A	N/A	2/27/2023 9:03:13 F
Old Students	FOLDER	192.168.20.193\Administrat...	N/A	N/A	N/A	N/A	2/27/2023 9:03:13 F
Student Details	FOLDER	192.168.20.193\Administrat...	N/A	N/A	N/A	N/A	2/27/2023 9:03:13 F
458673.bmp	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
459565496.bmp	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
Addresses.txt	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
Confidential.pdf	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
Contact info.xlsx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
Coursework deadlines.docx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
CV's.docx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F
Exams.docx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/27/2023 9:03:13 F

Effective Permission : All Permissions
Account Filter :

Path : \\192.168.20.193\Multicorp\Education\Students

Access Type	Permission	Permission Method	Inherited From	Applies To													
192.168.20.193\Administrators Effective Permission : (Full Control)																	
✓ Allowed	Full Control	Direct Applied	Not Inherited	This Object only	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓			✓		
✓ Allowed	Full Control	Inherited	E:\	This folder, subfolders and fil...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	Read permissions, Change ...	Through Ownership	Not Inherited	This Object only											✓	✓	✓
192.168.20.193\Users Effective Permission : List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions																	
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓			✓		
✓ Allowed	Create folders / append data	Inherited	E:\	This folder and subfolders			✓										
✓ Allowed	List folder / read data, Read...	Inherited	E:\	This folder, subfolders and fil...	✓			✓		✓		✓			✓		
✓ Allowed	Create files / write data	Inherited	E:\	This folder and subfolders		✓											
Creator owner Effective Permission : List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Write extended attributes, Traverse folder / execute file, Delete subfolders and files, Read attributes ...																	

Figure 31: Current Permissions Report

6. You can use the top filter section to apply one or more filters
7. You can view the analysis report in the **Permissions** tab with or without applying filters
8. The **Object Section** and **Reports Section** contain the following icons:

a. this shows that the permission is assigned to everyone

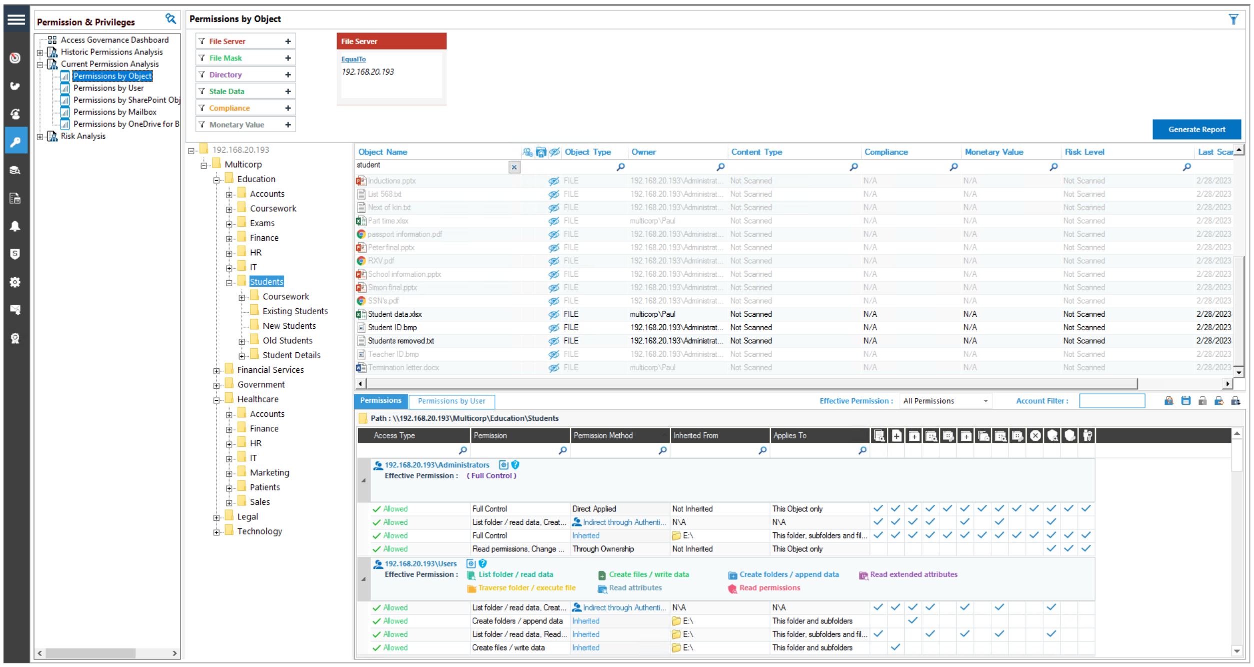
b. this indicates that object is not inheriting permissions from its parent

c. this shows that the selected object has not been accessed for the last 30 days

d. this shows that the object, which is accessing the selected object, is a group.

3.1.1 Row Filter

9. The top row of both the **Objects Section** and the **Reports Section** is the filter row. In any cell, you can type a word to filter their content. In the example below, ‘Student’ has been typed under Object Name and all objects starting with ‘Student’ are highlighted:



File Server
EqualTo
192.168.20.193

Object Name	Object Type	Owner	Content Type	Compliance	Monetary Value	Risk Level	Last Scar
student							
Inductions.pptx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
List 568.txt	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Next of kin.txt	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Part time.xlsx	FILE	multicorp\Paul	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
passport information.pdf	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Peter final.pptx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
RXV.pdf	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
School information.pptx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Simon final.pptx	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
SSN's.pdf	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Student data.xlsx	FILE	multicorp\Paul	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Student ID.bmp	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Students removed.txt	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Teacher ID.bmp	FILE	192.168.20.193\Administrat...	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
Termination letter.docx	FILE	multicorp\Paul	Not Scanned	N/A	N/A	Not Scanned	2/28/2023

Path : \\192.168.20.193\Multicorp\Education\Students

Access Type	Permission	Permission Method	Inherited From	Applies To													
192.168.20.193\Administrators Effective Permission : (Full Control)																	
✓ Allowed	Full Control	Direct Applied	Not Inherited	This Object only	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓			✓		
✓ Allowed	Full Control	Inherited	E:\	This folder, subfolders and fil...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	Read permissions, Change ...	Through Ownership	Not Inherited	This Object only											✓	✓	✓
192.168.20.193\Users Effective Permission : List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions																	
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓			✓		
✓ Allowed	Create folders / append data	Inherited	E:\	This folder and subfolders			✓										
✓ Allowed	List folder / read data, Read...	Inherited	E:\	This folder, subfolders and fil...	✓			✓		✓		✓			✓		
✓ Allowed	Create files / write data	Inherited	E:\	This folder and subfolders		✓											

Figure 32: Row Filter Applied

You can apply multiple filters in both **Object Section** and **Reports Section**. Click the ✖ icon to remove the filter.

3.1.2 Sorting

You can click any column header in the **Object Section** or **Reports Section** to sort the content in the ascending or descending order.

3.1.3 Change Permissions

In the **Object Section**, you can right click on any folder to access the following context menu:

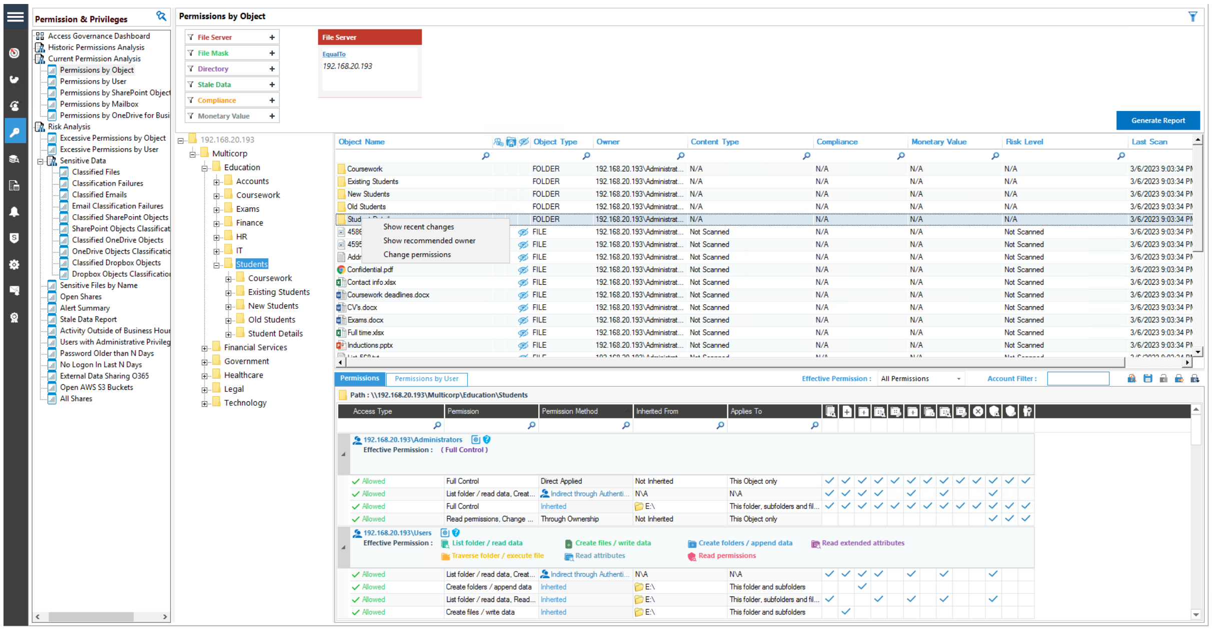
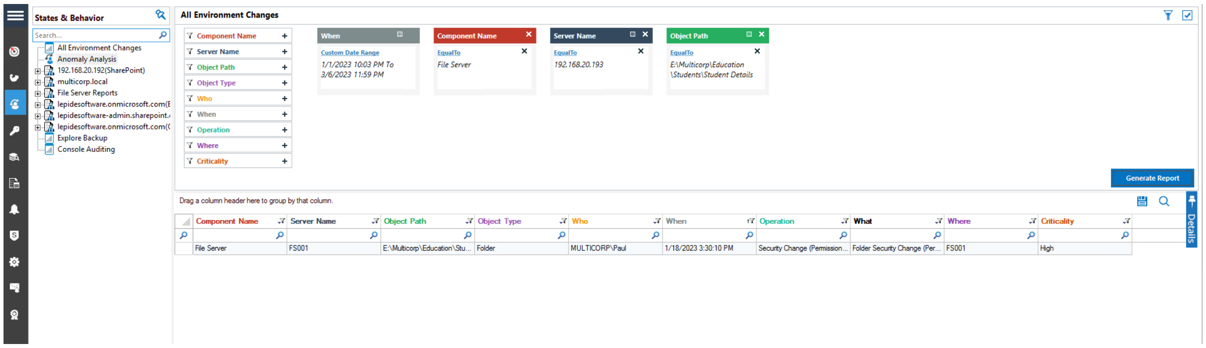


Figure 33: Displaying the Context Menu

It contains the following options.

a. **Show Recent Changes:** Select this option to show recent changes to the selected folder:



When: Custom Date Range 1/1/2023 10:03 PM To 3/6/2023 11:59 PM

Component Name: EqualTo File Server

Server Name: EqualTo 192.168.20.193

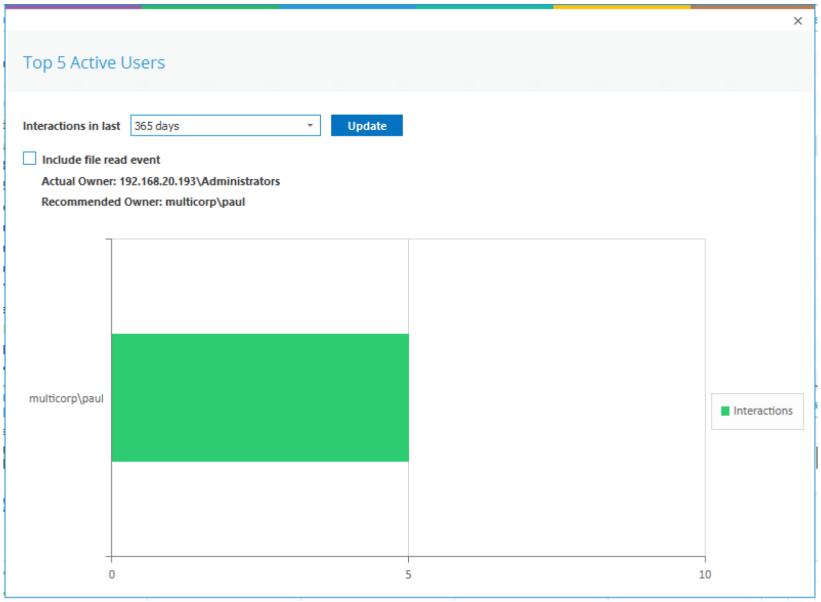
Object Path: EqualTo E:\Multicorp\Education \Students\Student Details

Component Name	Server Name	Object Path	Object Type	Who	When	Operation	What	Where	Criticality
File Server	FS001	E:\Multicorp\Education\Stu...	Folder	MULTICORP\Paul	1/18/2023 3:30:10 PM	Security Change (Permission...	Folder Security Change (Per...	FS001	High

Figure 34: Recent Changes

The **All Environment Changes Report** is displayed. The filters can be changed as required

b. **Show Recommended Owner:** Select this option to display a graph showing the user who has made the most changes on the folder and are therefore suggested as the recommended owner



Top 5 Active Users

Interactions in last 365 days

Update

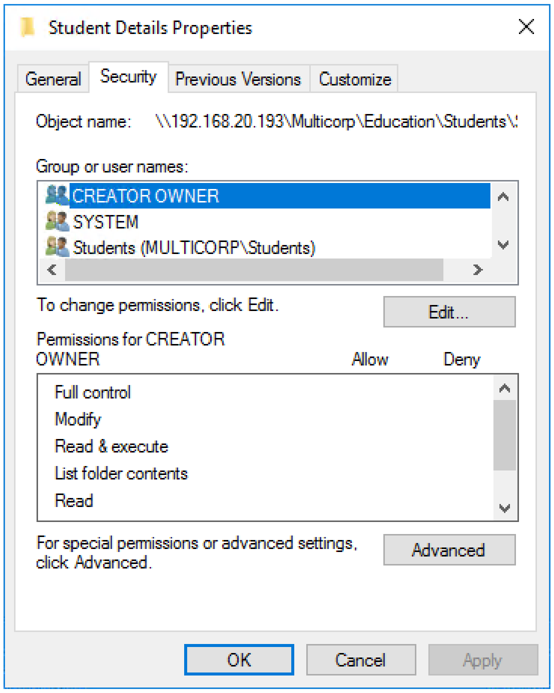
□ Include file read event

Actual Owner: 192.168.20.193\Administrators

Recommended Owner: multicorp\paul

Figure 35: Recommended Owner

c. **Change Permissions:** Select this option to display the Folder Properties dialog box and make changes to the folder permissions:



Student Details Properties

Object name: \\192.168.20.193\Multicorp\Education\Students\!

Group or user names:

CREATOR OWNER
SYSTEM
Students (MULTICORP\Students)

To change permissions, click Edit.

Permissions for CREATOR OWNER	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		

For special permissions or advanced settings, click Advanced.

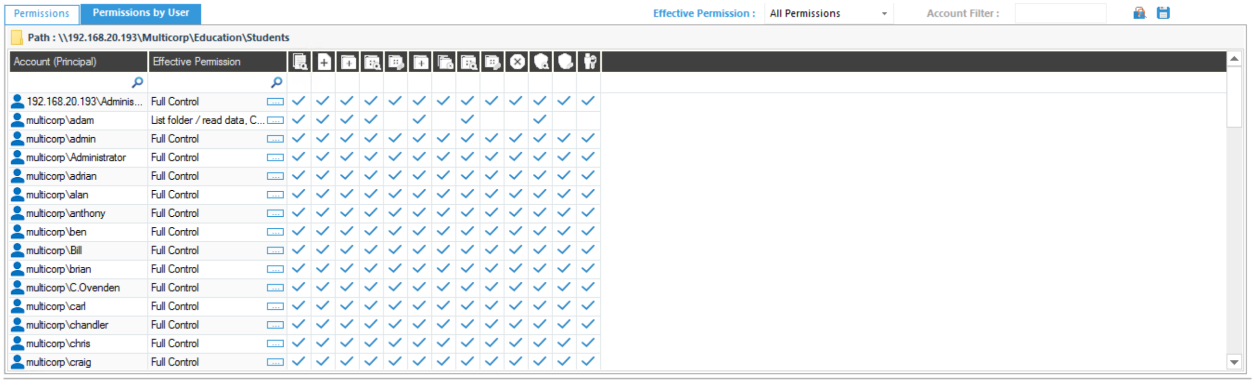
Figure 36: Folder Properties

3.1.4 Permissions Report of User Only

There are two tabs in the Reports section.

a. **Permissions:** This displays the current permissions of the selected object

b. **Permissions by User:** This displays the Current Permissions sorted by the users. Here, only the permissions of the users are displayed.



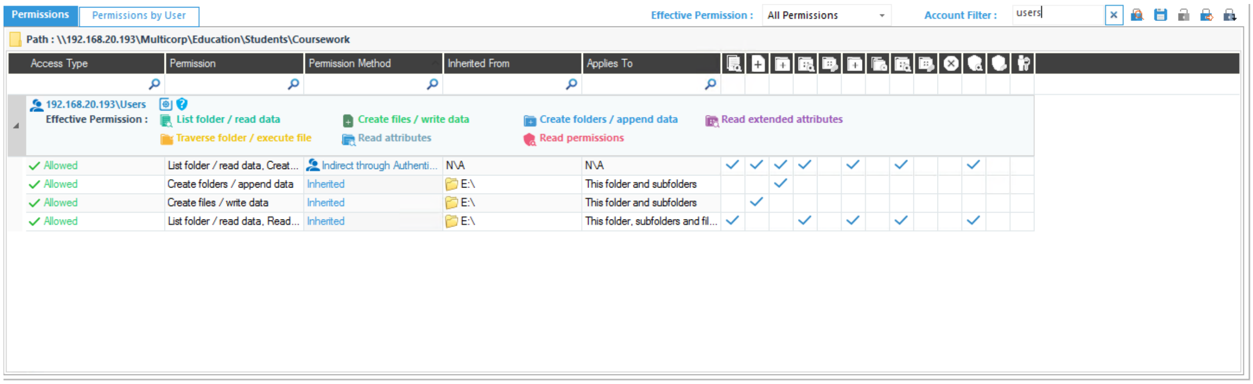
Path : \\192.168.20.193\Multicorp\Education\Students

Account (Principal)	Effective Permission													
192.168.20.193\Adminis...	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\adam	List folder / read data, C...	✓	✓	✓	✓		✓		✓			✓		
multicorp\admin	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\Administrator	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\adrian	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\alan	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\anthony	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\ben	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\Bill	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\brian	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\C.Ovenden	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\carl	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\chandler	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\chris	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
multicorp\craig	Full Control	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figure 37: Permissions by User Report of a Shared Folder

10. Account Filter

From the permissions report, you can type the name of the User Account in **Account Filter** text box to filter the report of the current tab as per the user account.



Path : \\192.168.20.193\Multicorp\Education\Students\Coursework

192.168.20.193\Users
Effective Permission : List folder / read data, Create files / write data, Create folders / append data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions

Access Type	Permission	Permission Method	Inherited From	Applies To													
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓			✓		
✓ Allowed	Create folders / append data	Inherited	E:\	This folder and subfolders			✓										
✓ Allowed	Create files / write data	Inherited	E:\	This folder and subfolders		✓											
✓ Allowed	List folder / read data, Read...	Inherited	E:\	This folder, subfolders and fil...	✓			✓		✓		✓			✓		

Figure 38: Account Filter for Users

You can click ☒ icon, which is next to the textbox, to remove the account filter.

11. Effective Permissions

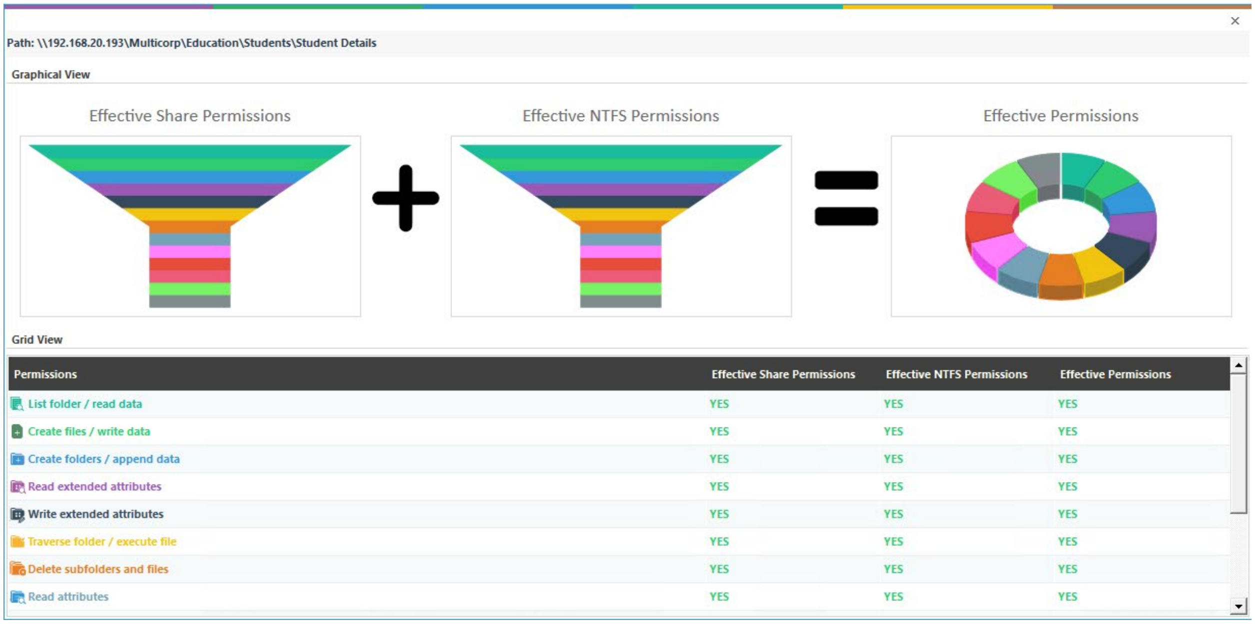
Effective Permissions are the final resultant permissions on an object, which are calculated after analyzing the NTFS and Share Permissions on it. Here, the drop-down menu lists all permissions for a file or folder. You can check any of these permissions to view the account, which have the selected permission on an object. The following table lists the different permissions and their icons that represent them in the Current Permissions Report.

Permission	Icon in Header Row	Icon in Report	Color in Permission Calculation
Full Control			
List folder / read data	📄	📄	🟩
Create files / write data	✎	✎	🟩
Create folders / append data	⊞	⊞	🟦
Read extended attributes	▣	▣	🟪
Write extended attributes	✎	✎	⬛
Traverse folder / execute	⊞	⊞	🟨
Delete subfolders and files	✕	✕	🟧
Read attributes	▣	▣	🟦
Write attributes	✎	✎	🟪
Delete	⊗	✕	🟥
Read permissions	🔑	🔑	🟥
Change permissions	🔑	🔑	🟩

Permission	Icon in Header Row	Icon in Report	Color in Permission Calculation
Take ownership	🗎	🔒	⬛
None			

Figure 39: List of the Effective Permissions

The ? icon appears with the object in the **Current Permission Report**. Click it to view the source, from where the effective permission comes to the selected object. Effective Share Permissions are those, which are applied in the **Sharing** tab of the shared folder, whereas the NTFS Permissions are those, which are applied in the Access Control Lists of the shared folder.



Path: \\192.168.20.193\Multicorp\Education\Students\Student Details

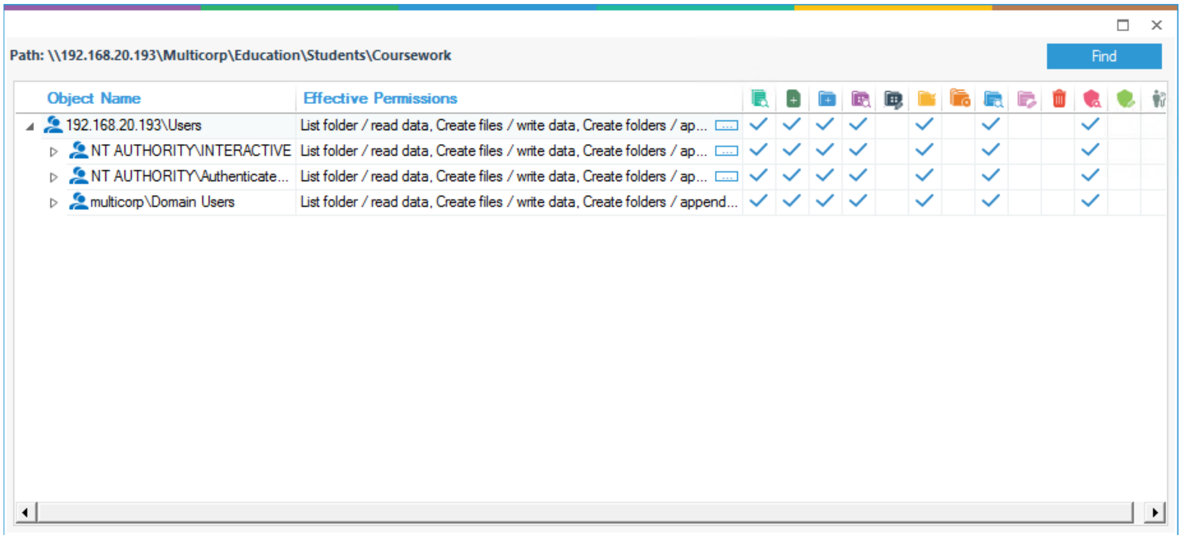
Permissions	Effective Share Permissions	Effective NTFS Permissions	Effective Permissions
List folder / read data	YES	YES	YES
Create files / write data	YES	YES	YES
Create folders / append data	YES	YES	YES
Read extended attributes	YES	YES	YES
Write extended attributes	YES	YES	YES
Traverse folder / execute file	YES	YES	YES
Delete subfolders and files	YES	YES	YES
Read attributes	YES	YES	YES

Figure 40: Effective Permissions

Each permission has a different color. Figure 39 lists the name and color of permissions. Here, you can analyze the permission flow for an object. You can scroll down the Effective Permissions screen to see the detailed report.

12. Explore Group Membership

If you have selected **Scan Nested Group Membership and Permission**, then the ⊞ icon appears with the Groups listed in the Permissions Report. Click this icon to view the group memberships in the following dialog box.



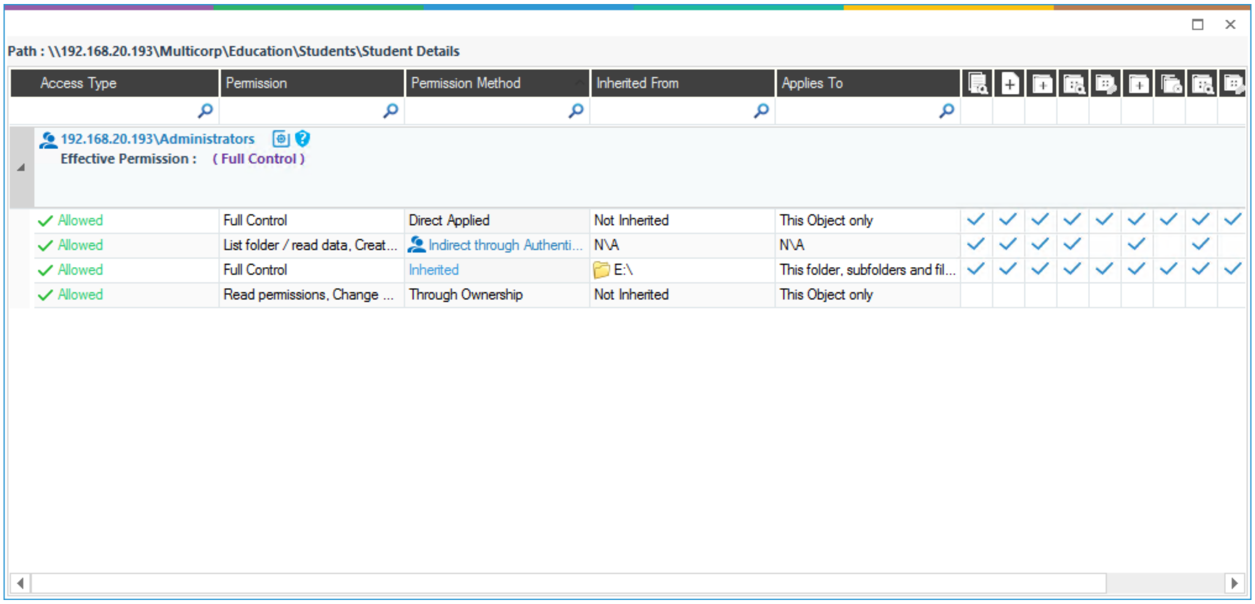
Path: \\192.168.20.193\Multicorp\Education\Students\Coursework

Object Name	Effective Permissions														
192.168.20.193\Users	List folder / read data, Create files / write data, Create folders / ap...	…	✓	✓	✓	✓		✓		✓			✓		
NT AUTHORITY\INTERACTIVE	List folder / read data, Create files / write data, Create folders / ap...	…	✓	✓	✓	✓		✓		✓			✓		
NT AUTHORITY\Authenticate...	List folder / read data, Create files / write data, Create folders / ap...	…	✓	✓	✓	✓		✓		✓			✓		
multicorp\Domain Users	List folder / read data, Create files / write data, Create folders / append...		✓	✓	✓	✓		✓		✓			✓		

Figure 41: Displaying Group Memberships

You need to modify the Data Set and apply **Scan Nested Group Membership and Permission** Settings and then scan the permissions to access this group membership dialog box. Refer to Section 2.3.3 Modify Data Set to know the steps.

The … icon appears in Permission Report or in **Explore Group Membership** for the groups. You can click it to view the permissions of a group.



Path : \\192.168.20.193\Multicorp\Education\Students\Student Details

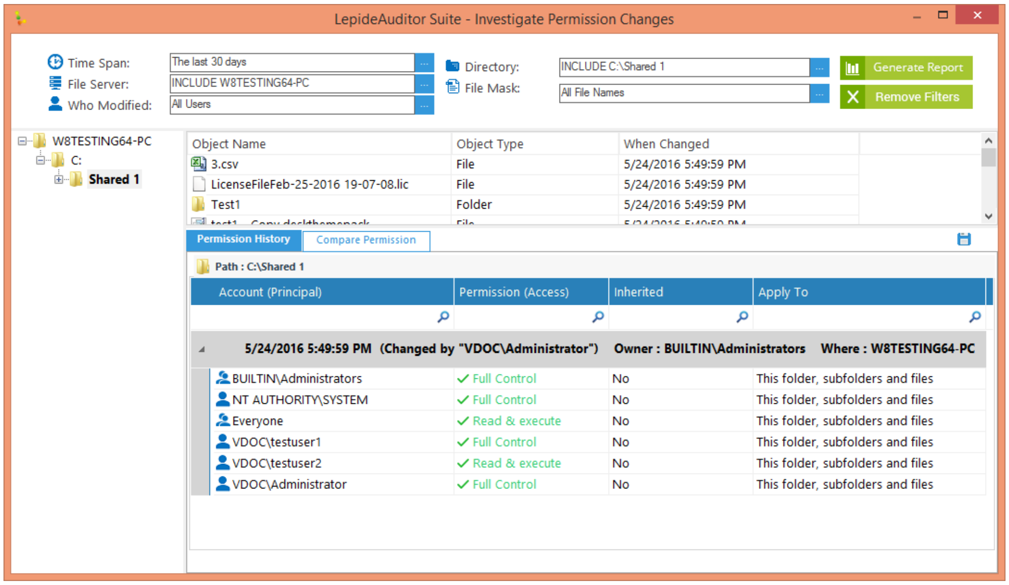
192.168.20.193\Administrators
Effective Permission : (Full Control)

Access Type	Permission	Permission Method	Inherited From	Applies To									
✓ Allowed	Full Control	Direct Applied	Not Inherited	This Object only	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	List folder / read data, Creat...	Indirect through Authenti...	N\A	N\A	✓	✓	✓	✓		✓		✓	
✓ Allowed	Full Control	Inherited	E:\	This folder, subfolders and fil...	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓ Allowed	Read permissions, Change ...	Through Ownership	Not Inherited	This Object only									

Figure 42 Explore Group Permissions

13. Investigate Permissions

Click the icon to investigate the changes in the permissions of the selected object. It displays **Historical Permission Analysis** for the selected object to let the Administrator investigate how the permissions are changed.



LepideAuditor Suite - Investigate Permission Changes

Time Span: The last 30 days
File Server: INCLUDE W8TESTING64-PC
Who Modified: All Users
Directory: INCLUDE C:\Shared 1
File Mask: All File Names

Object Name	Object Type	When Changed
3.csv	File	5/24/2016 5:49:59 PM
LicenseFileFeb-25-2016 19-07-08.lic	File	5/24/2016 5:49:59 PM
Test1	Folder	5/24/2016 5:49:59 PM

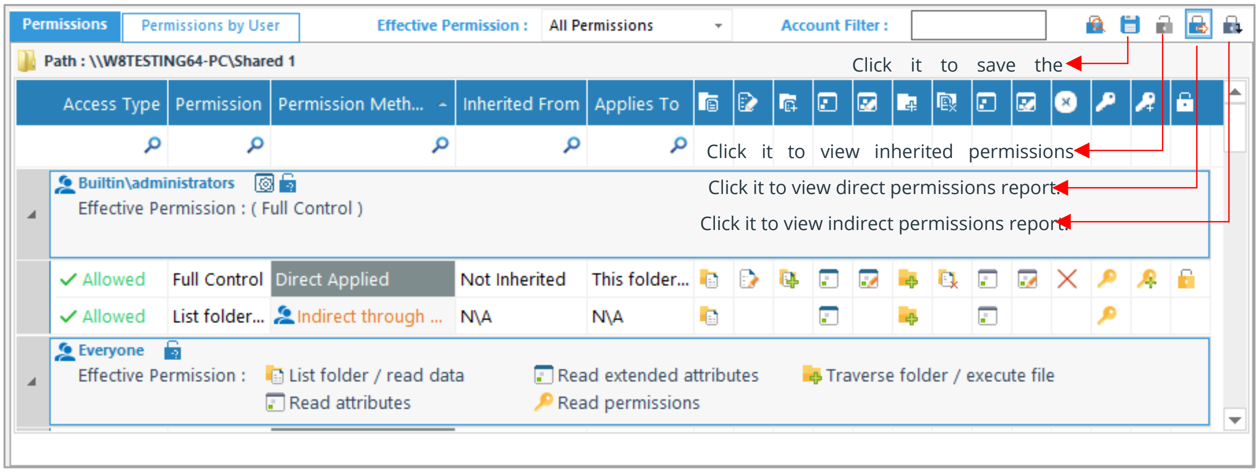
Path : C:\Shared 1

5/24/2016 5:49:59 PM (Changed by "VDOC\Administrator") Owner : BUILTIN\Administrators Where : W8TESTING64-PC

Account (Principal)	Permission (Access)	Inherited	Apply To
BUILTIN\Administrators	✓ Full Control	No	This folder, subfolders and files
NT AUTHORITY\SYSTEM	✓ Full Control	No	This folder, subfolders and files
Everyone	✓ Read & execute	No	This folder, subfolders and files
VDOC\testuser1	✓ Full Control	No	This folder, subfolders and files
VDOC\testuser2	✓ Read & execute	No	This folder, subfolders and files
VDOC\Administrator	✓ Full Control	No	This folder, subfolders and files

Figure 43: Investigate Permission

14. Other Reports



Effective Permission : All Permissions

Account Filter :

Path : \\W8TESTING64-PC\Shared 1

Access Type	Permission	Permission Meth...	Inherited From	Applies To
Builtin\administrators Effective Permission : (Full Control)				
✓ Allowed	Full Control	Direct Applied	Not Inherited	This folder...
✓ Allowed	List folder...	Indirect through ...	N\A	N\A
Everyone Effective Permission : List folder / read data, Read extended attributes, Traverse folder / execute file, Read attributes, Read permissions				

Click it to save the

Click it to view inherited permissions

Click it to view direct permissions report.

Click it to view indirect permissions report.

Figure 44: Direct Permissions Report of "Shared 1" folder

There are different icons on the top right corner as displayed in the image.

1. Click 🔒 icon to sort the report as per the inherited permissions.
2. Click 🔒 icon to sort the report as per the direct permissions.
3. Click 🔒 icon to sort the report as per the indirect permissions.
4. Click 💾 icon to save the report.

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.