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 OneDrive. 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.
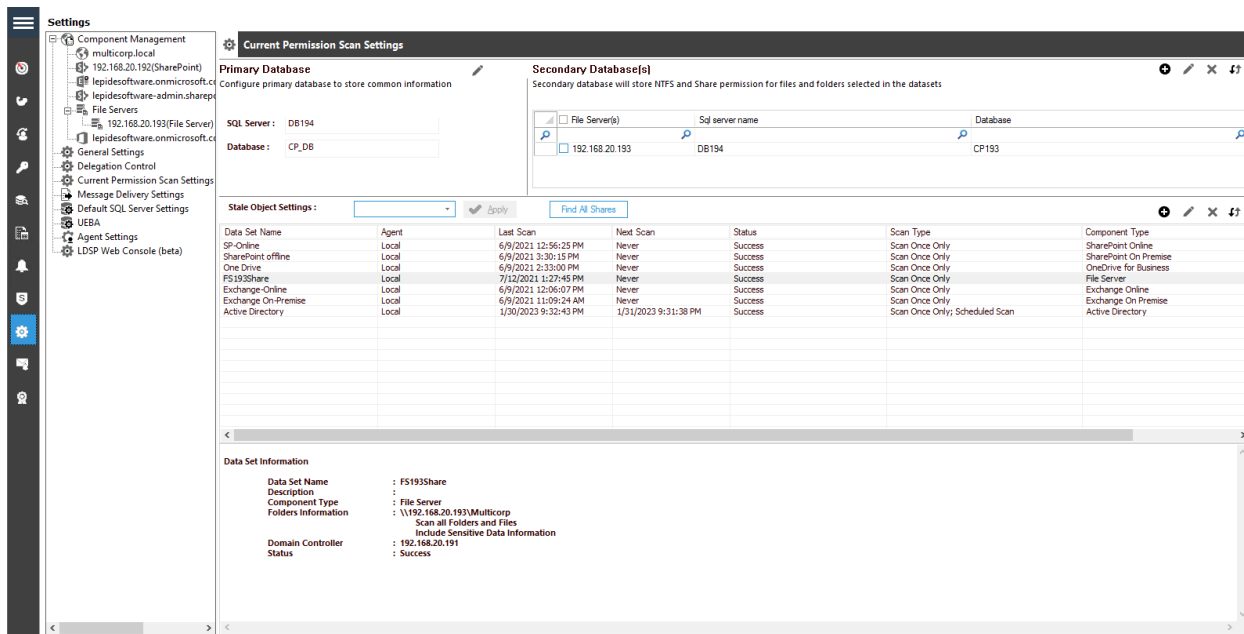

Figure 1: Current Permission Scan Settings

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

2.1 Configure SQL Server

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

2.2 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**

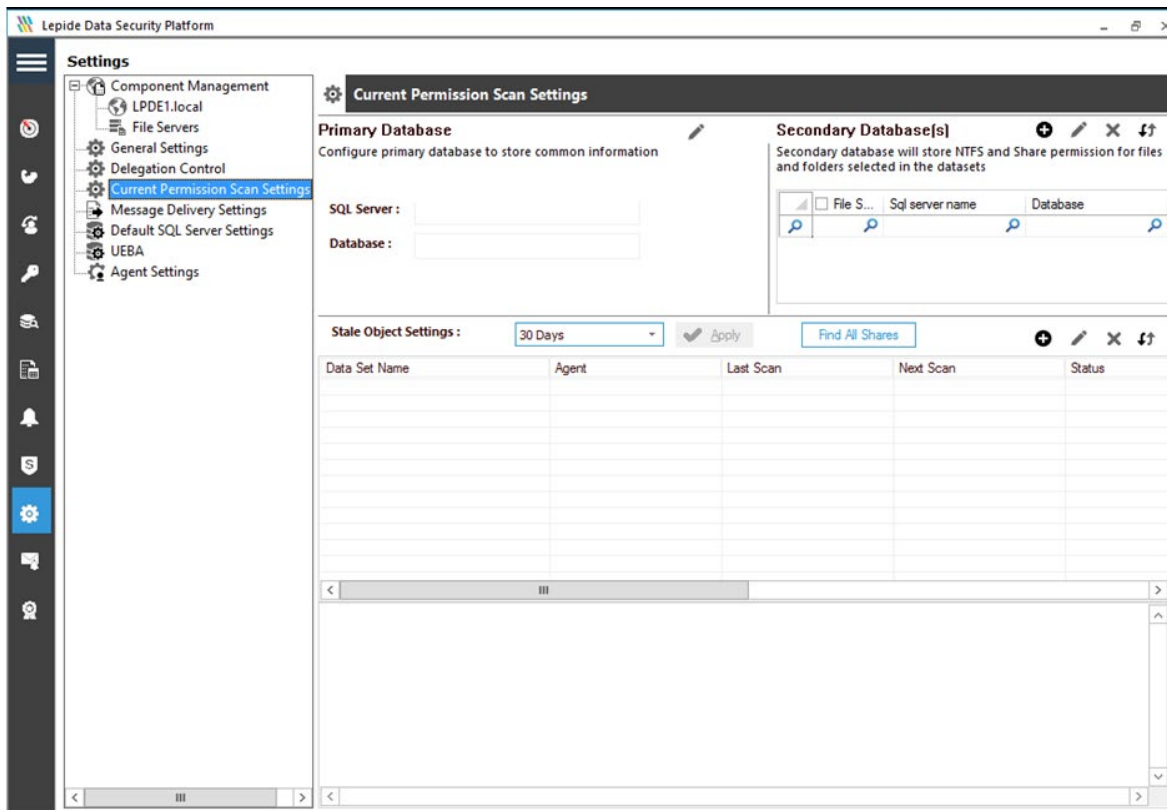The following screen will be displayed:

Figure 2: Current Permission Scan Settings

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

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.

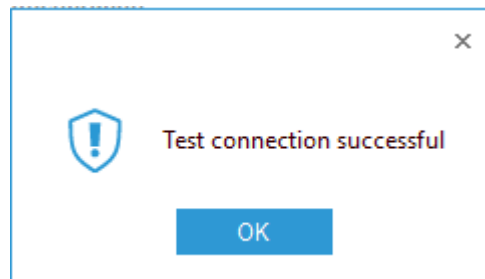**NOTE:** The software does not create this database until you add a Data Set and start its scanning.

Figure 4: SQL Server Connection is Successful

NOTE: You can click the [icon] 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.
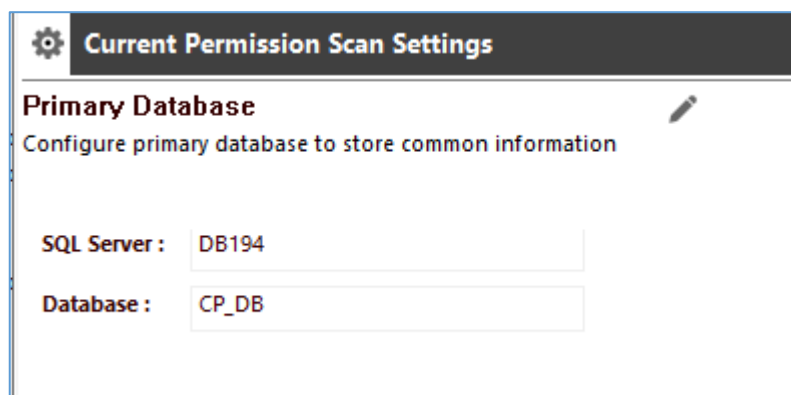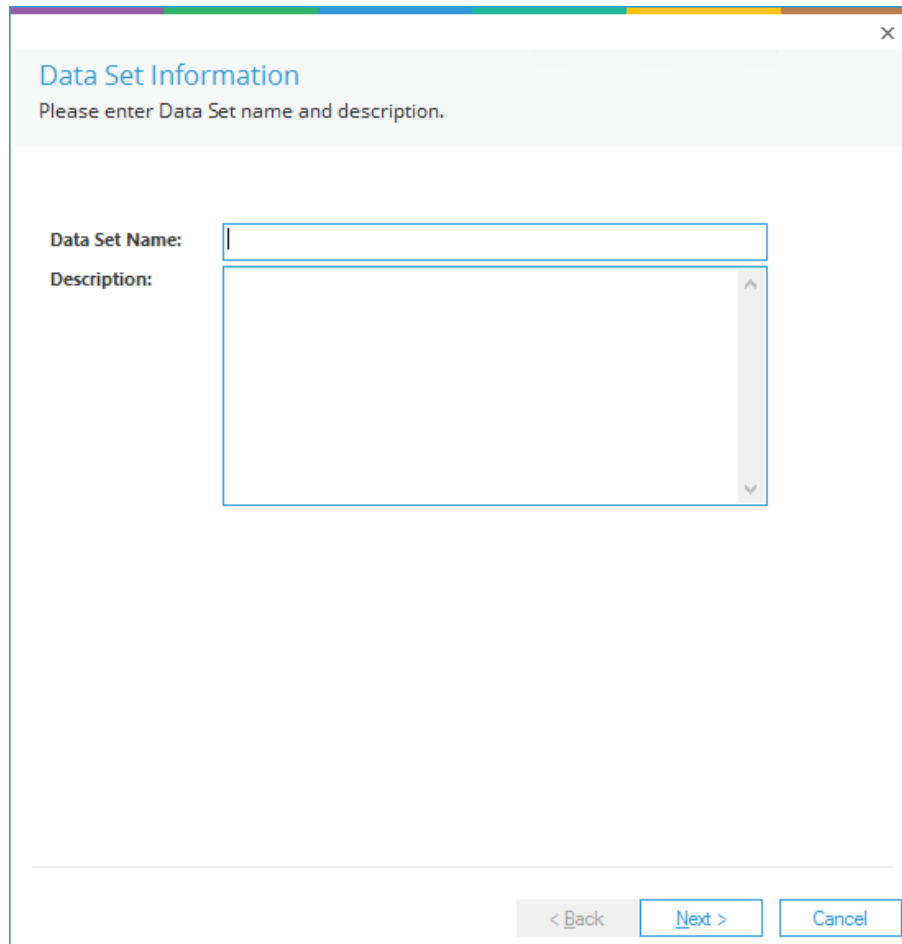

Figure 5: Selected SQL Server and its Database

3 Add a Data Set for File Server

Click the ⊕ icon to create a Data Set using the following wizard. The database you configured above is not created until you add a Data Set and start its scanning.

Figure 6: Add Data Set

Follow the steps below.

1. Enter a name and description for the Data Set.

2. Click **Next**. The next step displays the options to add the shared folders, of which current permissions you want to monitor.
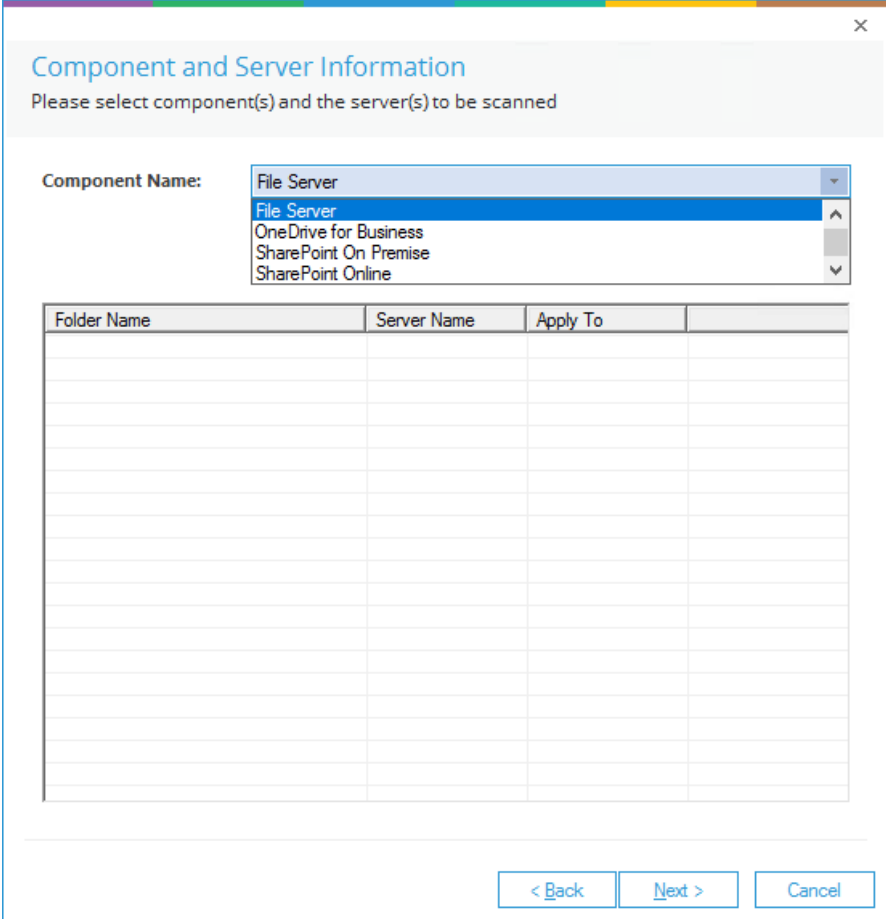
Figure 7: Component and Server Information

3. The default component is File Server, which is already selected in the drop-down menu.

4. You can perform the following steps to add folders.

   a. Click ⊕ icon to add the folders using the following dialog box:
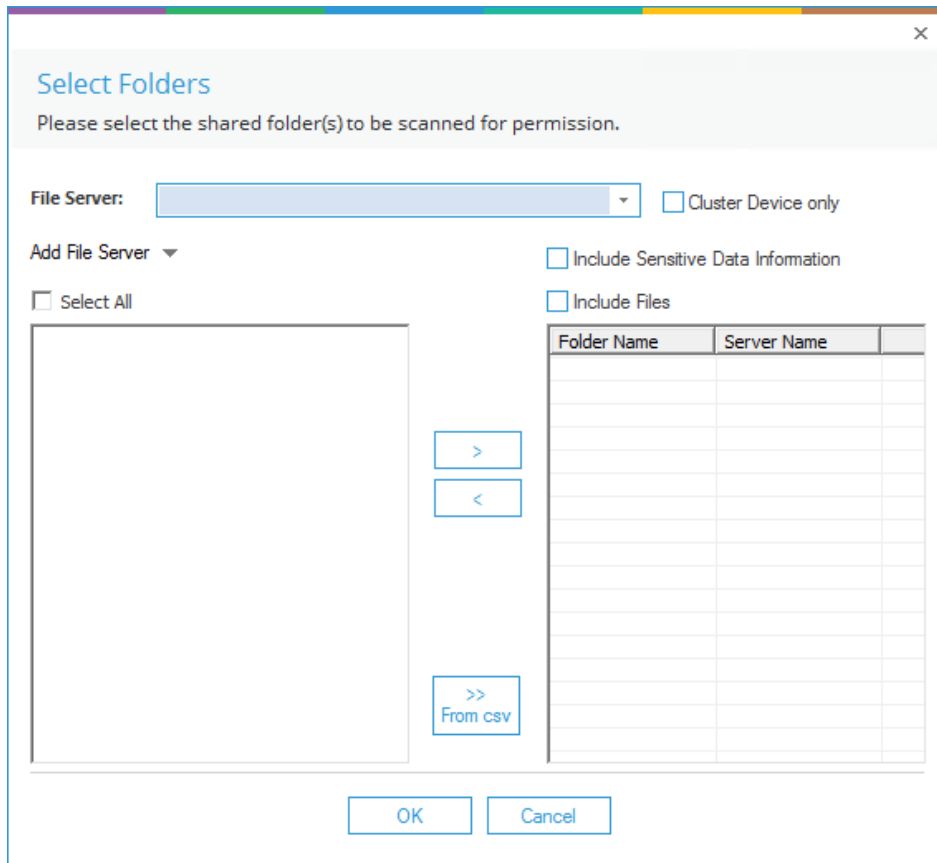
Figure 8: Select Folders

    b.   Select the File Server from the drop-down menu. It lists the folders in the left column **File Server folders**.

> **NOTE**:   Do not add the shared folders of the file servers of different domains in a Data Set. It is recommended to create a Data Set from the file server(s) of a single domain only.
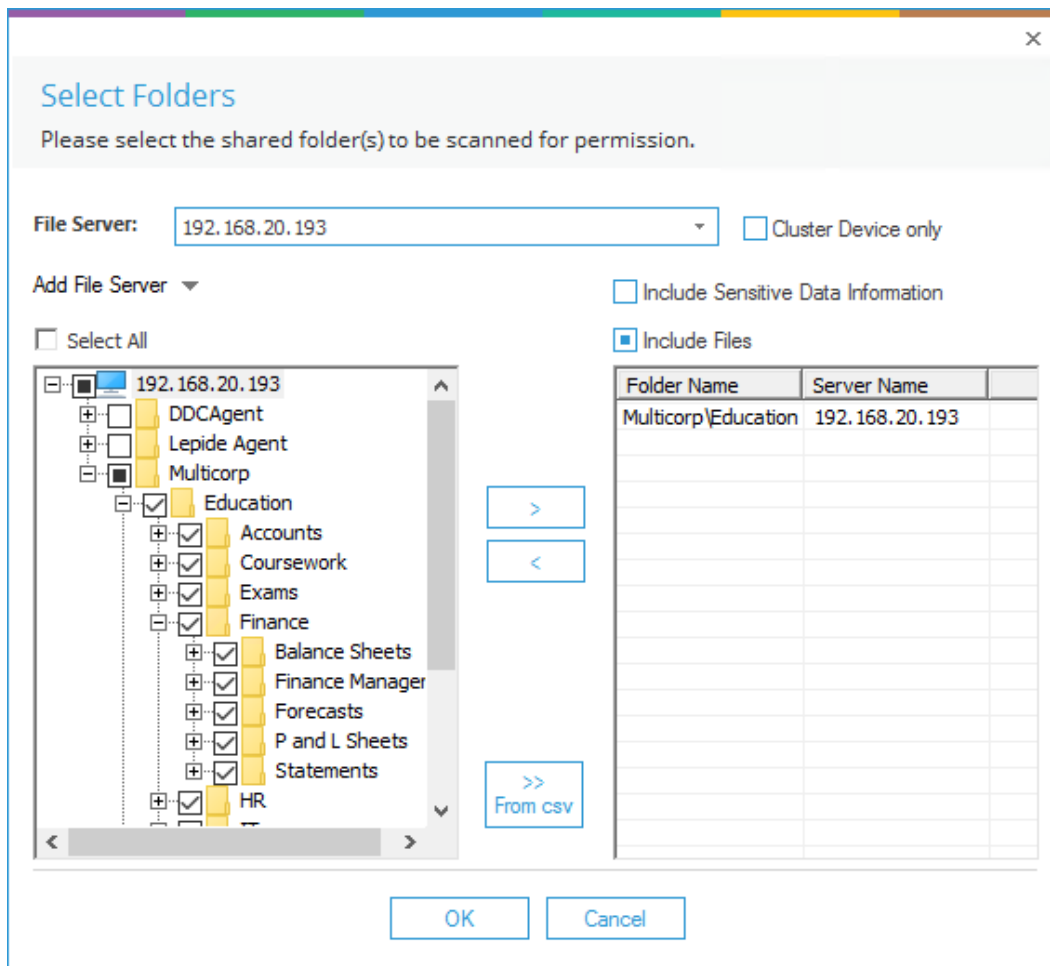
Figure 9: Select Folders

c.   You can expand the nodes to select the folders.

NOTE: The minimum permissions required by our solution are these:

List Folder/Read Data, Traverse Folder/Execute File and Read Permissions rights on the Shares which are to be scanned.

---

d.   Select a folder and click the [>] button to add it.

e.   Check **Include files** to monitor the permissions of sub-folders and files in the selected folder as well.

f.   To remove an added folder from the Data Set, select the folder in the right column and click the [<] button.

g.   Click **OK**.

It takes you back to the previous wizard, which shows the added folder. The current permissions of the added folders will be monitored.
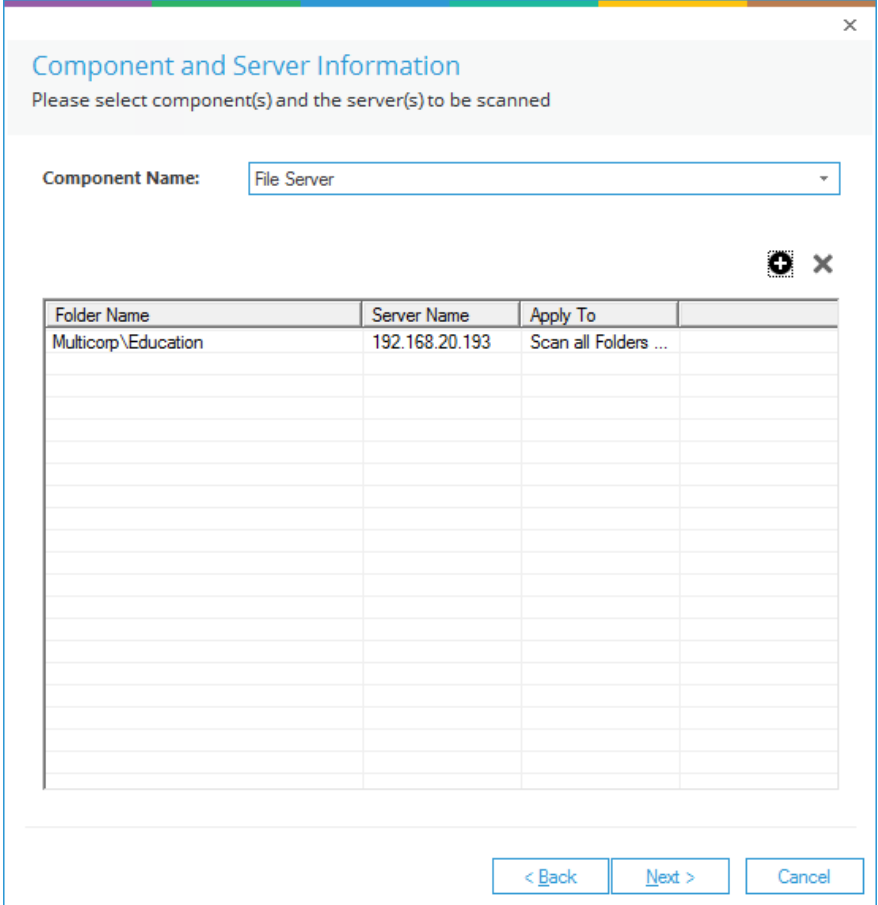

Figure 10: Folder Selected

Figure 11: Database Mapping

5. This shows the database mapping according to what you have previously selected.

6. Click **Next**

   The Permissions Scanning Options dialog box is displayed:

Figure 12: Permissions Scanning Options

7. It contains the following options.

   a. **Scan Permissions Now:** Select this option to scan the permissions now.

   b. **Schedule Permission Scan:** Select this option to schedule the scanning of permissions on different periodic intervals. Check **Schedule Permission Scan** box to activate this option and follow the steps below to set up a schedule:

   i. Click **Change Schedule** button to access the following dialog box.

Figure 13: Options to Schedule the Scan

It contains the following options.

- **Daily:** Select this option to scan the folders on a daily basis for updating the permissions. After selecting it, you have to select the start date and time, from which the scheduling will be created.

- **Weekly:** Select this option to scan the folders on a weekly basis. You have to select the start date from which the scheduling will be started. Select the days and time at which the scan will run.

- **Monthly:** Select this option to scan the folders on a monthly basis. You have to select the start date from which the scheduling will be started. Provide the time at which the scan will run. Select the months and their days when the scanning has to be scheduled.

ii. Select any of the above options and provide the required inputs.

iii. Click **OK** after you have defined the schedule. It takes you back to the previous wizard, which displays the scheduled days and timings for the scan.

Figure 14: Permission Scanning Options

c. **Login Credentials:** The Solution fetches the permissions from any Domain Controller, which hosts Active Directory.

The Solution will first use the login credentials which are provided while adding a File Server. If these credentials fail to authenticate the request, then the Solution uses the credentials provided here.

   i.   Enter the name of the domain controller.

   ii. Enter the login credentials of an administrative user manually.

   iii. The Solution collects the nested group membership and permissions using the provided credentials.

8. Click **Finish**

A new Data Set is created:
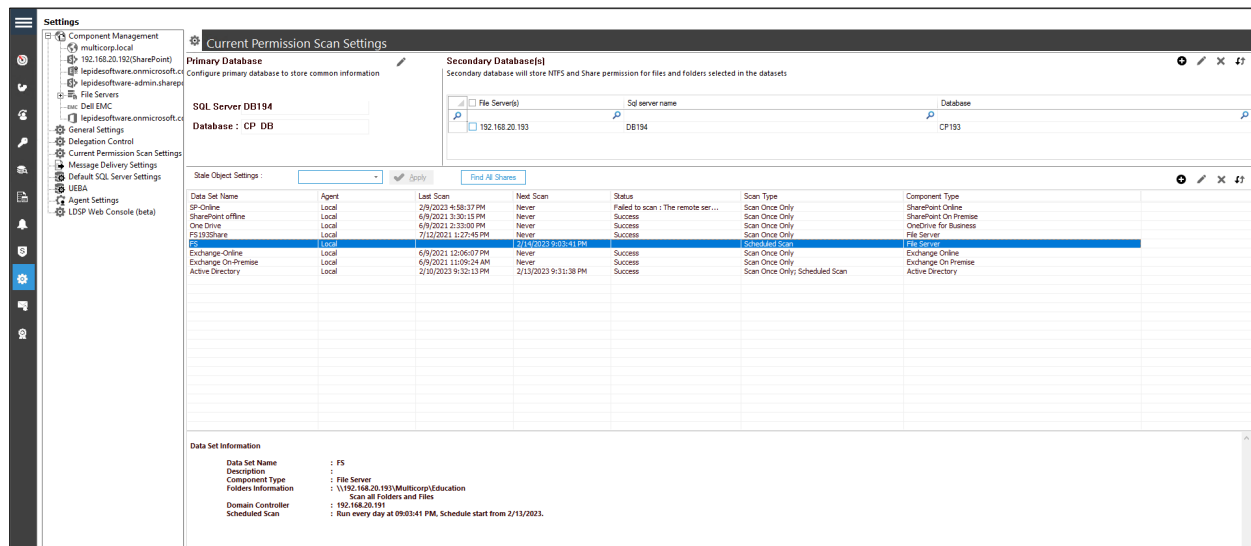
Figure 15: The Added Data Set

You can follow the above steps to create multiple Data Sets.

4 Add a Data Set for OneDrive

From version 21.1 onwards, the Lepide Data Security Platform is offering a capability to scan the permissions for OneDrive users as well. The component should be added for auditing in the solution to do a permission scan. Please follow the steps below to scan OneDrive for the permissions:

1.   Go to the **Settings** Page and click on **Current Permission Scan Settings**.

2.   Click on the ⊕ icon and create a new Dataset for OneDrive.
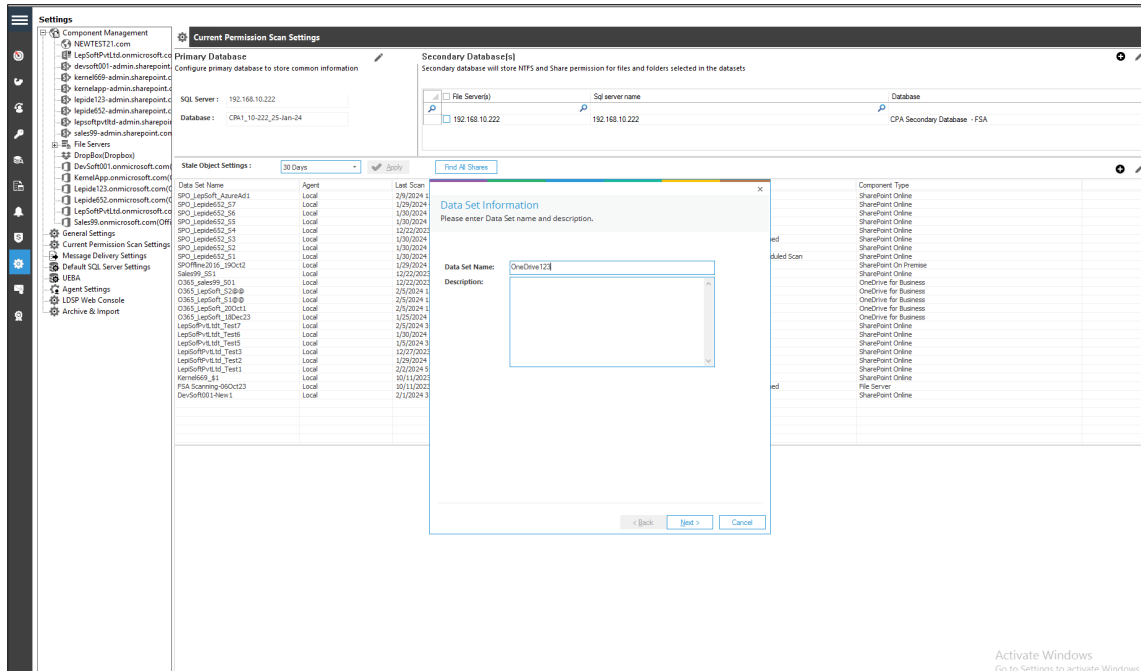
Figure 16: Add Data Set

3. In the next window, select the component name as OneDrive for Business:
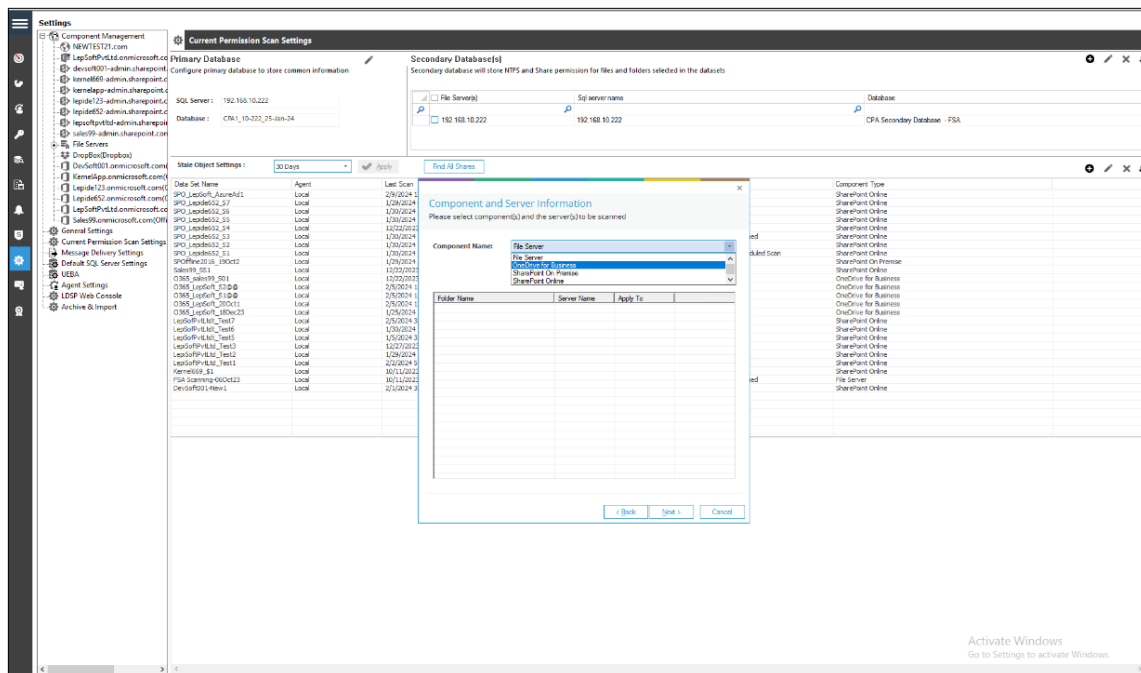
Figure 17: Component and Server Information

4. Now from the Component and Server Information dialog box, enter the following details:

    •   Tenant URL

    •   The Username and Password (User must be Global admin)

    •   Now click to refresh the User account URL list
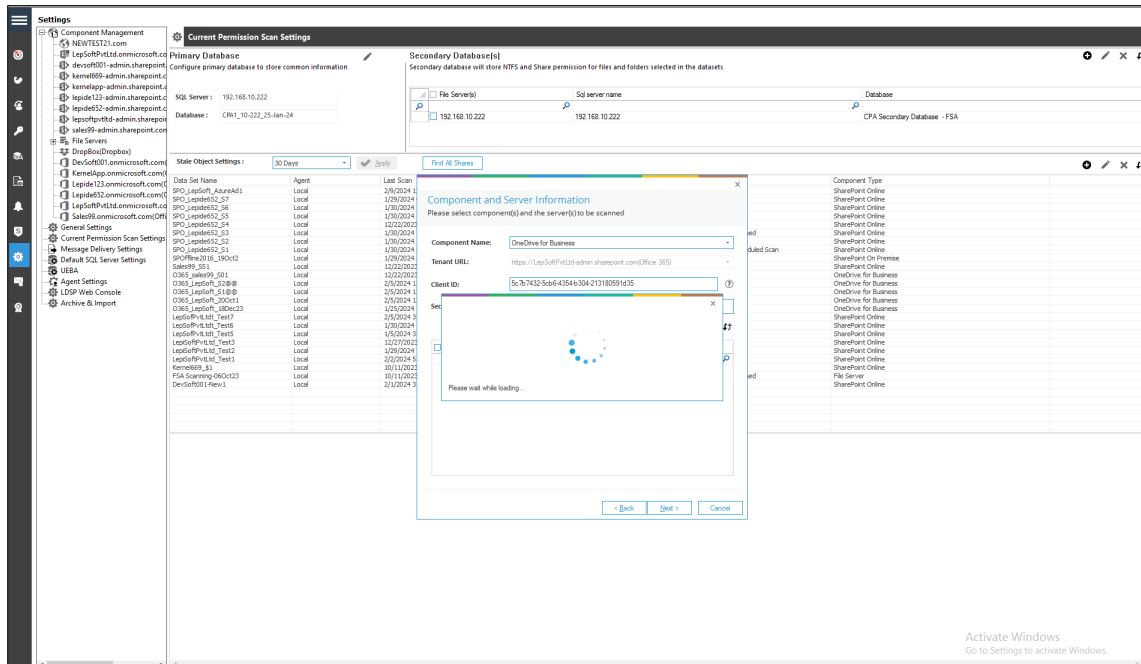
Figure 18: Add Details and Refresh

5. Select the URL from the list and click **Next**:
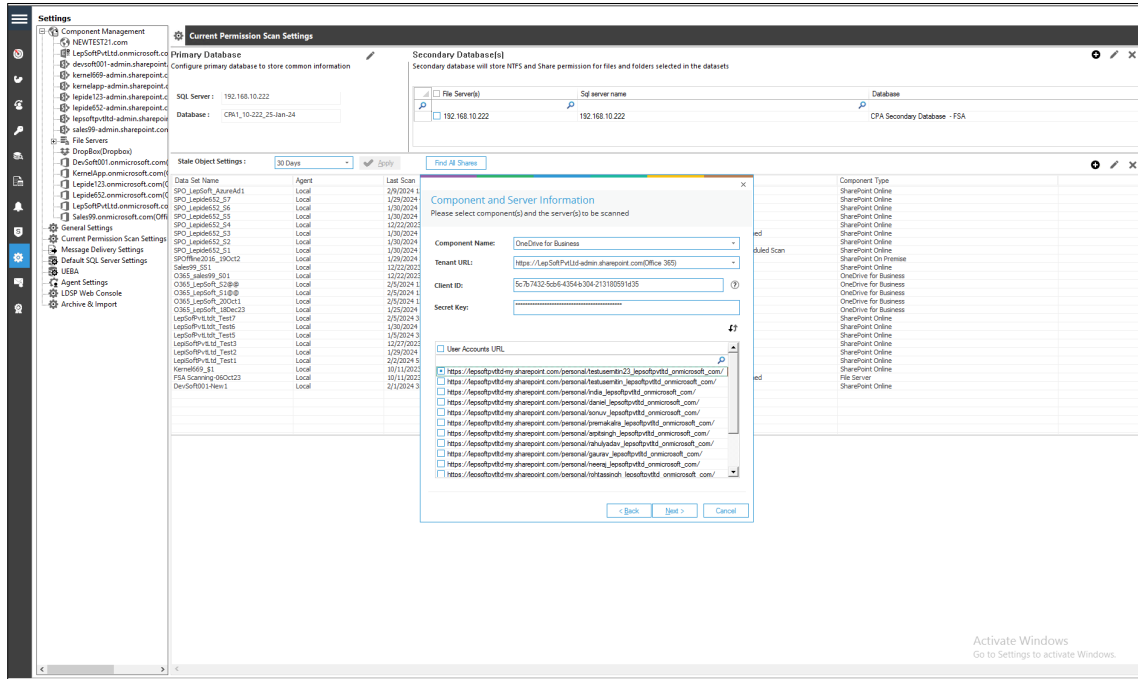
Figure 19: Select URL

6. Select the **Scan Now** option or **Schedule Scan** as per your requirements

7. Click **Finish**
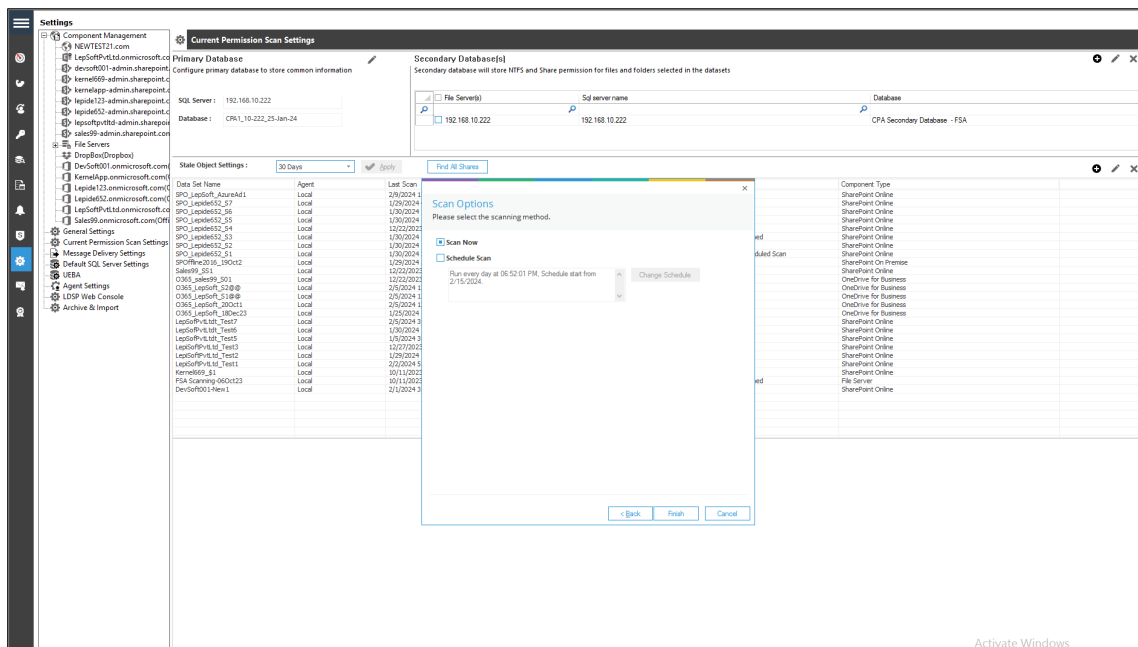
Figure 20: Scan Options

8. The Data Set should be visible on the Current Permission Scan Settings Page:
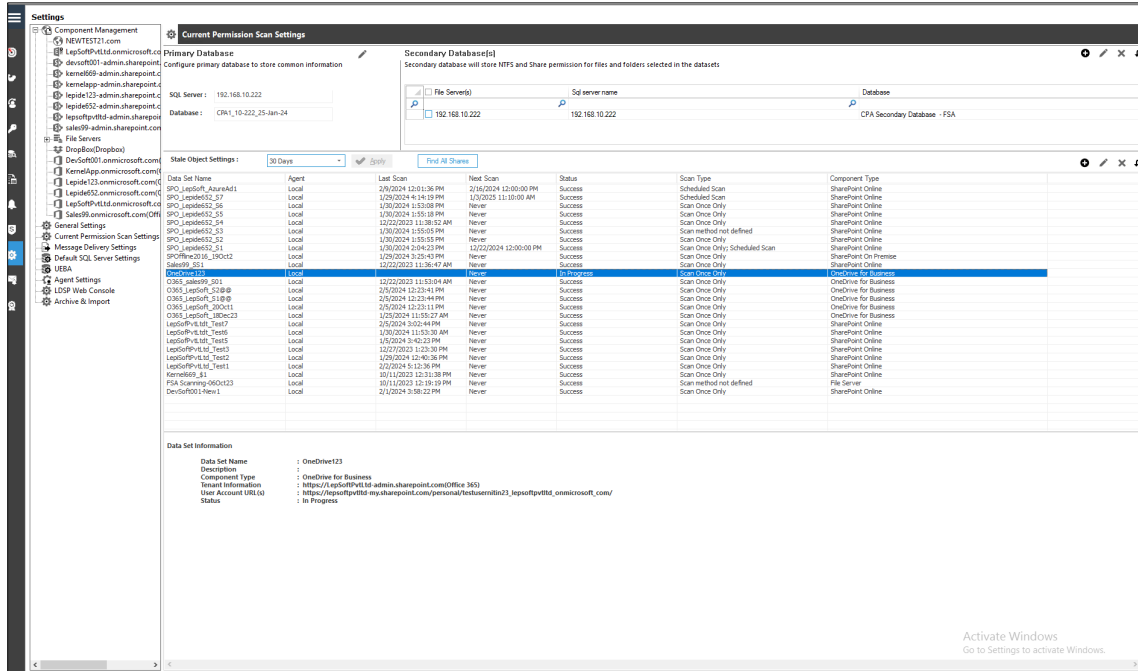
Figure 21: Current Permission Scan Settings

5 Scan Permissions Now

- To scan the permissions of the selected Data Set, right click on a data set and click **Scan Now**.
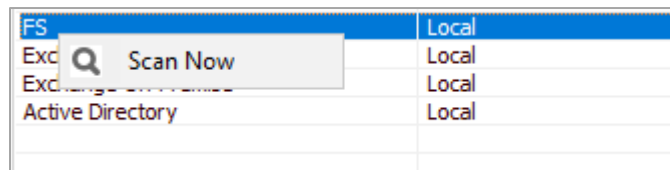
Figure 22: Option to Scan Now

6 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:
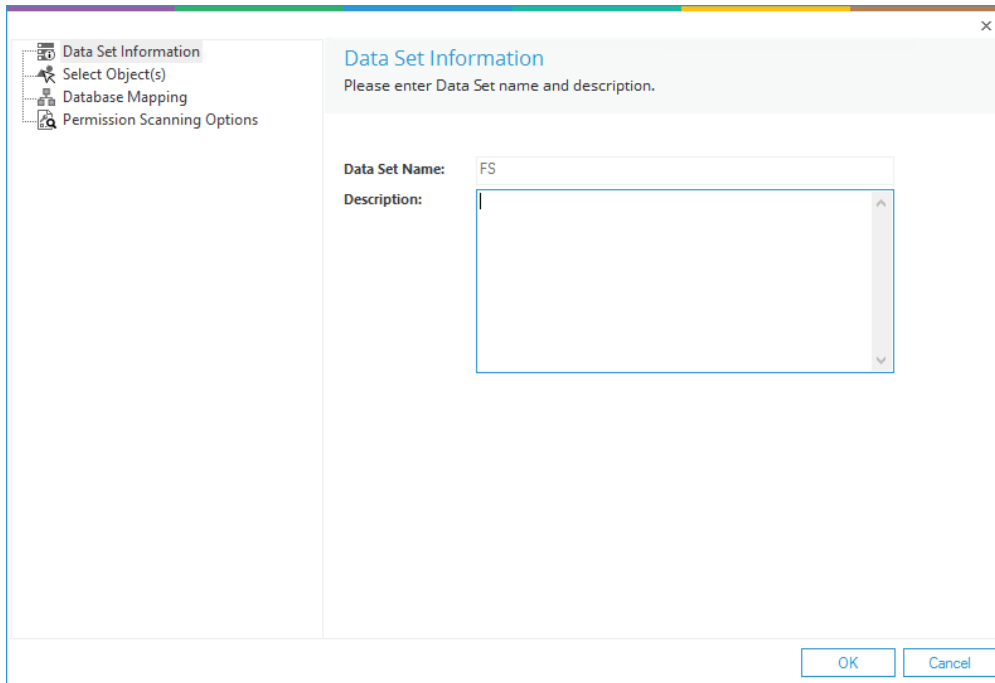
Figure 23: Modify Data Set

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
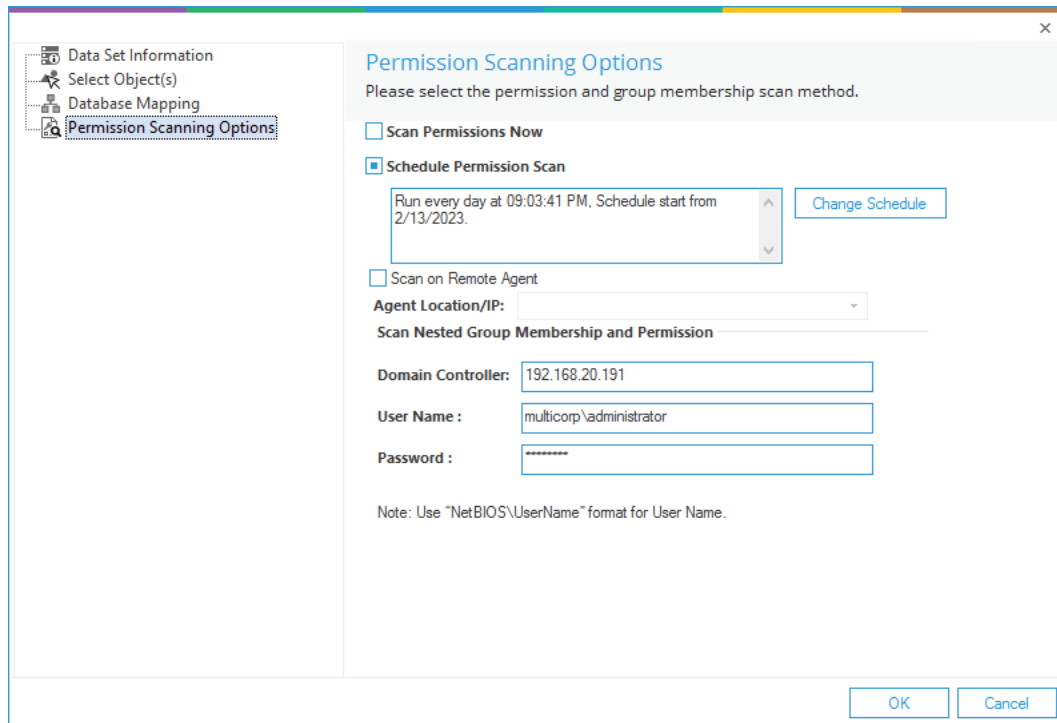
Figure 24: Modify Permission Scanning Options

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

7 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.
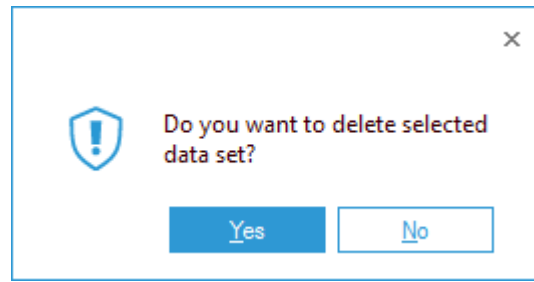
Figure 25: Warning before deleting a Data Set

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

8 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:
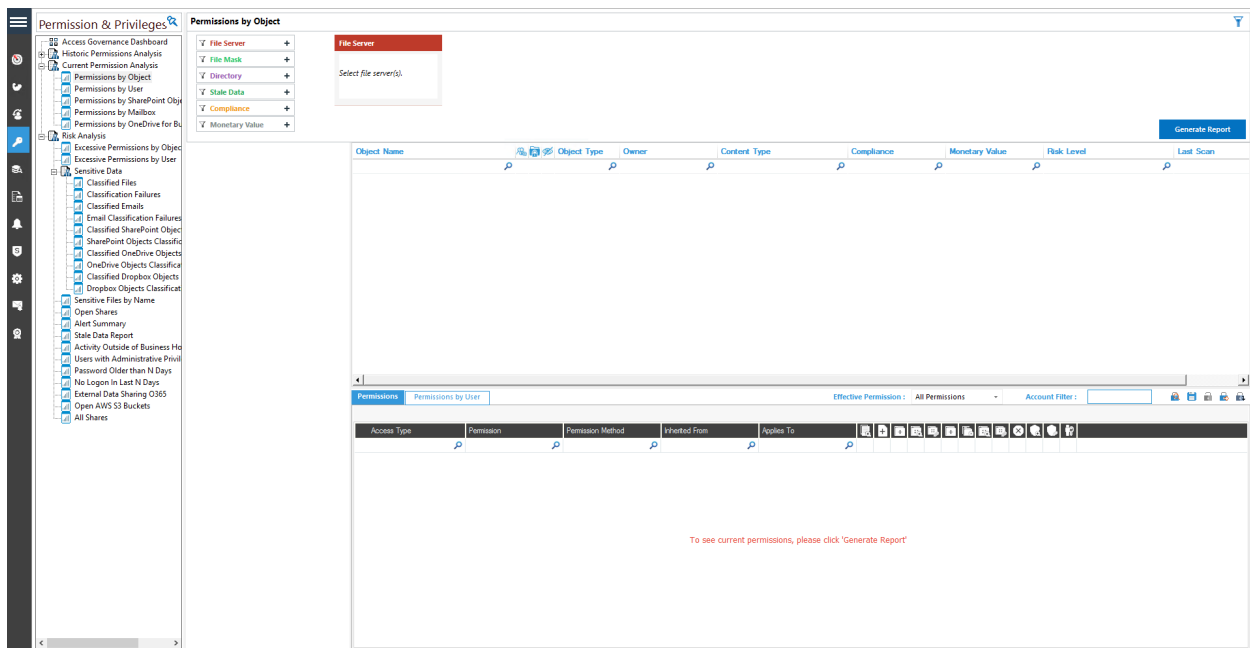
Figure 26: File Server Current Permissions Report

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.

8.1 Steps 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

Figure 27: 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. ![icon] this shows that the permission is assigned to everyone

b. ![icon] this indicates that object is not inheriting permissions from its parent

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

d. ![icon] this shows that the object, which is accessing the selected object, is a group.

8.1.1 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:
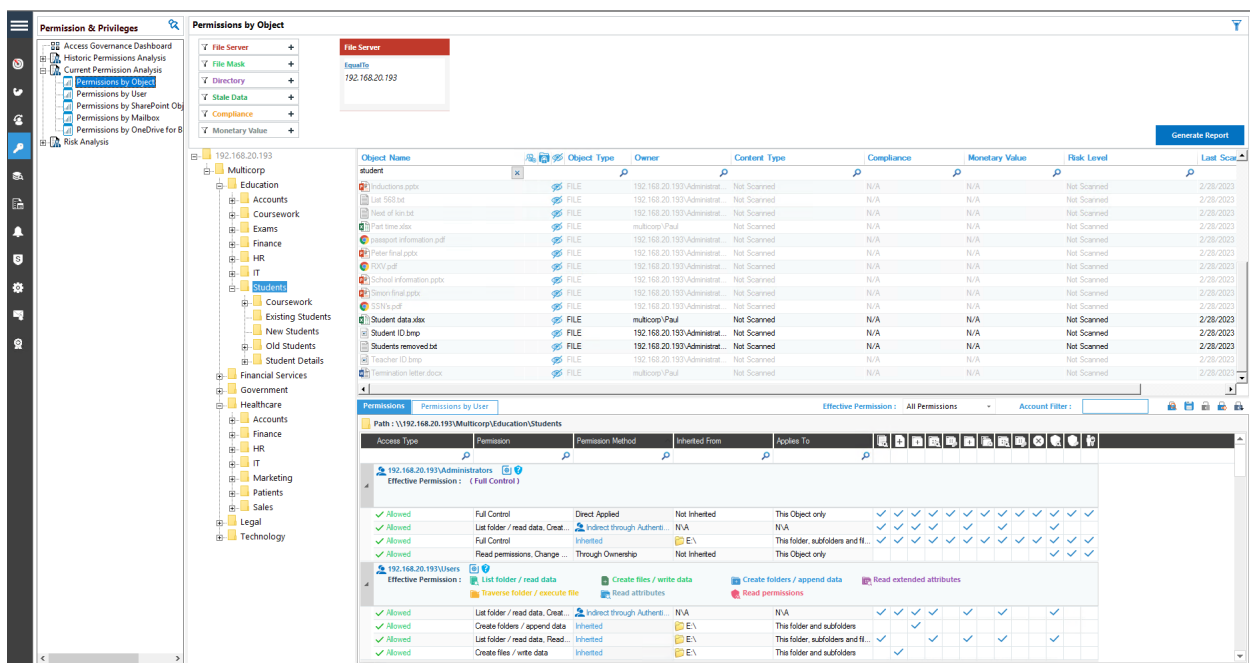
Figure 28: Row Filter Applied

You can apply multiple filters in both **Object Section** and **Reports Section**. Click the ![x icon] icon to remove the filter.

8.1.2 Sorting

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

8.1.3 Change Permissions

In the **Object Section**, you can right click on any folder to access the following context menu:
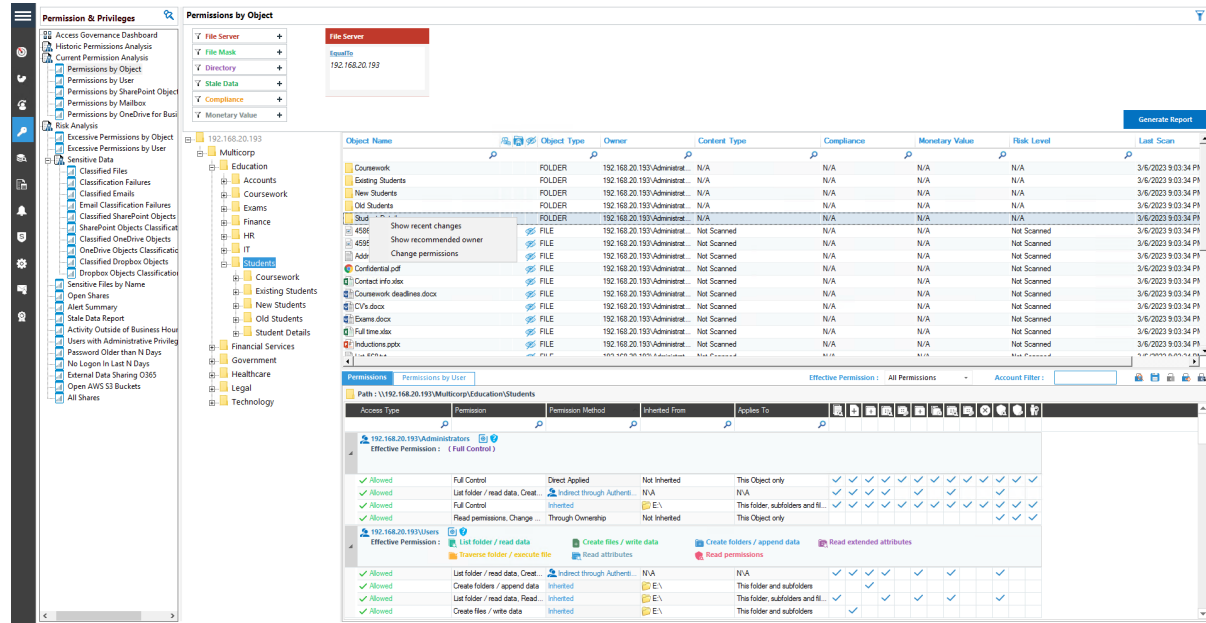
Figure 29: Displaying the Context Menu

It contains the following options.

a. **Show Recent Changes:** Select this option to show recent changes to the selected folder:
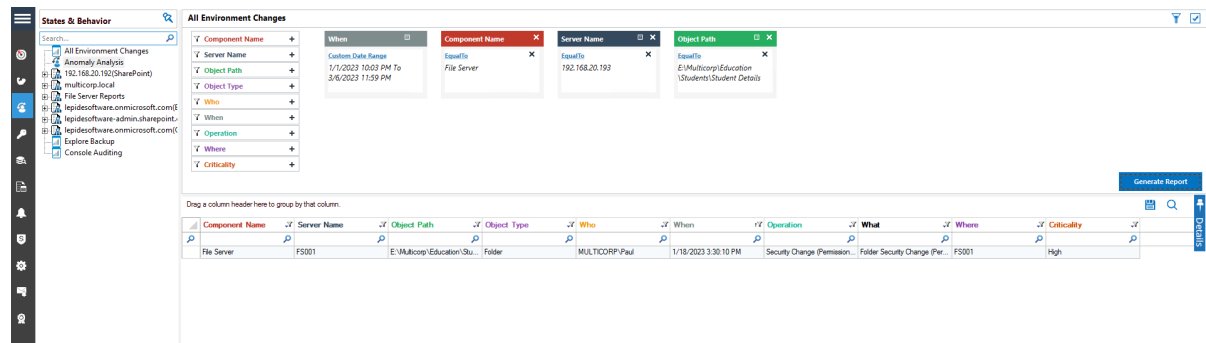
Figure 30: Recent Changes

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
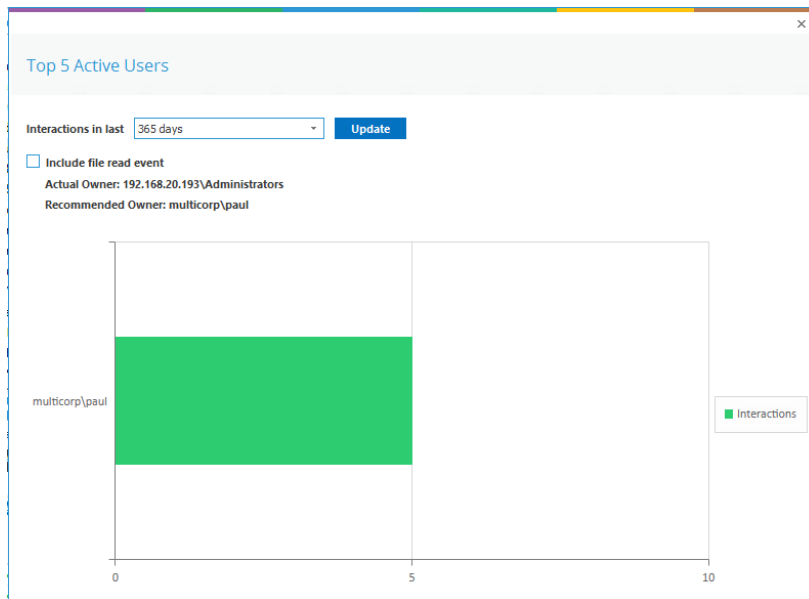
Figure 31: Recommended Owner

c. **Change Permissions:** Select this option to display the Folder Properties dialog box and make changes to the folder permissions:
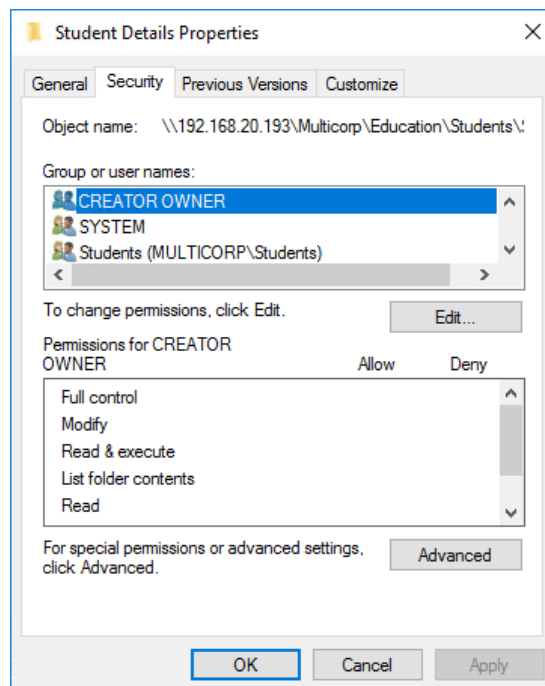
Figure 32: Folder Properties

8.1.4 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.

Figure 33: Permissions by User Report of a Shared Folder

8.2 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.

Figure 34: Account Filter for Users

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

8.3 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			(teal)
Create files / write data			(green)
Create folders / append data			(blue)
Read extended attributes			(purple)
Write extended attributes			(dark navy)
Traverse folder / execute			(yellow)
Delete subfolders and files			(orange)
Read attributes			(slate blue)
Write attributes			(pink)
Delete			(red)
Read permissions			(rose)
Change permissions			(light green)

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

Figure 35: 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.

Figure 36: Effective Permissions

Each permission has a different color. Figure 28 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.

8.4 Explore Group Membership

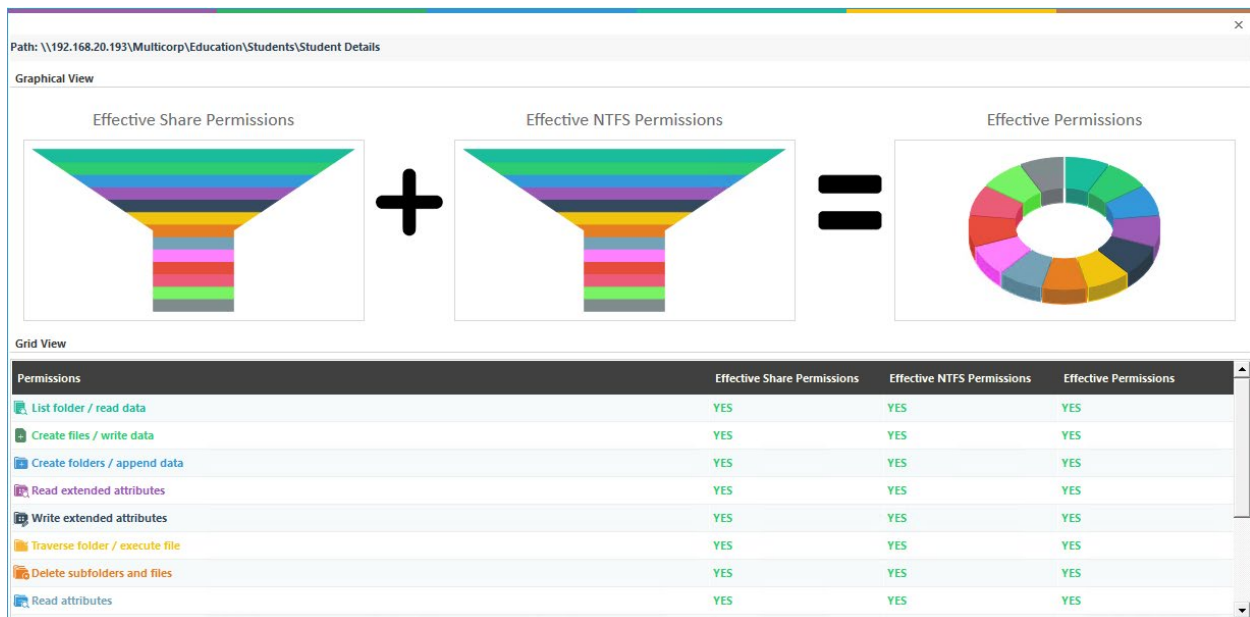If you have selected **Scan Nested Group Membership and Permission**, then the ⚙ icon appears with the Groups listed in the Permissions Report. Click this icon to view the group memberships in the following dialog box.

Figure 37: Displaying Group Memberships
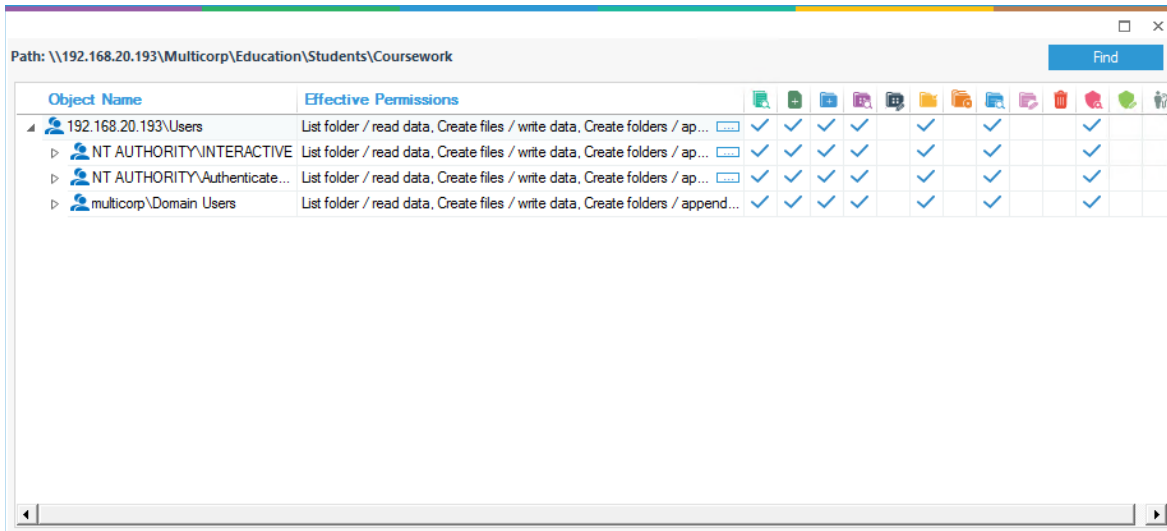
You need to modify the Data Set and apply **Scan Nested Group Membership and Permission** Settings and then scan the permissions to access this group membership dialog box. Refer to Section 2.3.3 Modify Data Set to know the steps.

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.
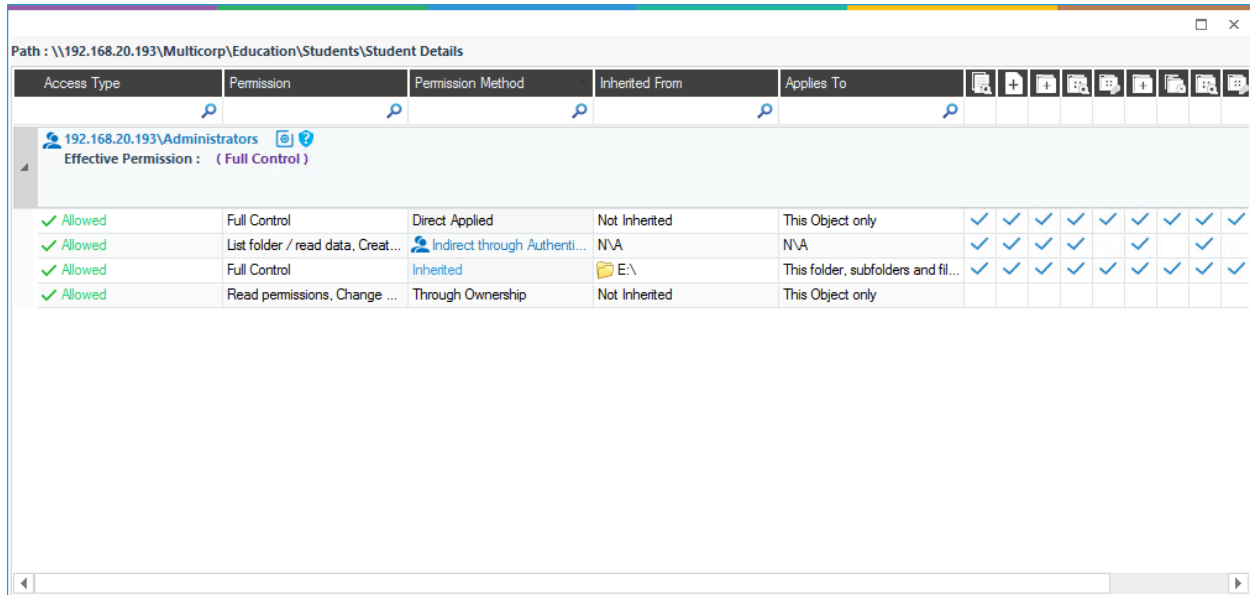
Figure 38 Explore Group Permissions

8.5 Investigate Permissions

Click the ![icon] 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.
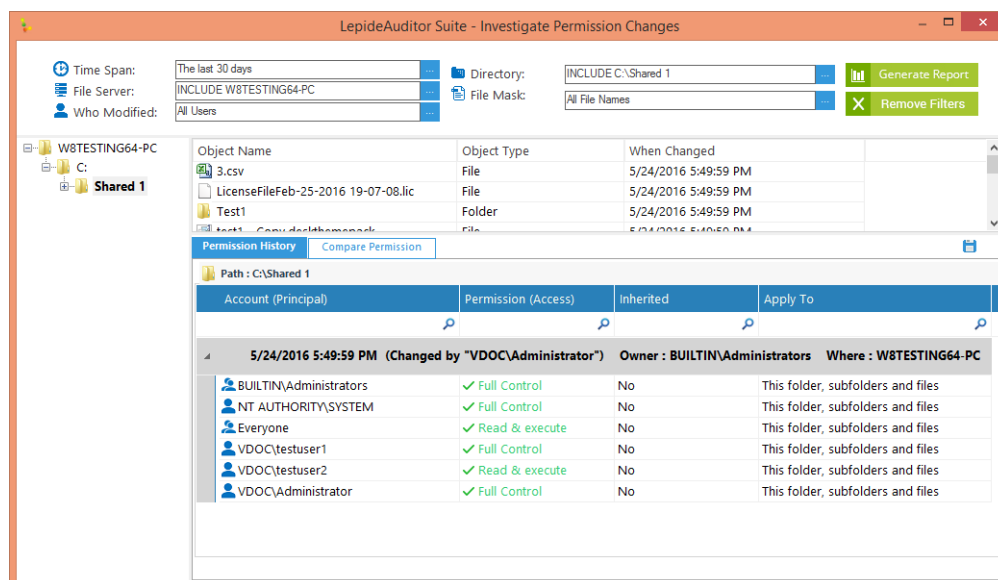

Figure 39: Investigate Permission

8.6 Other Reports
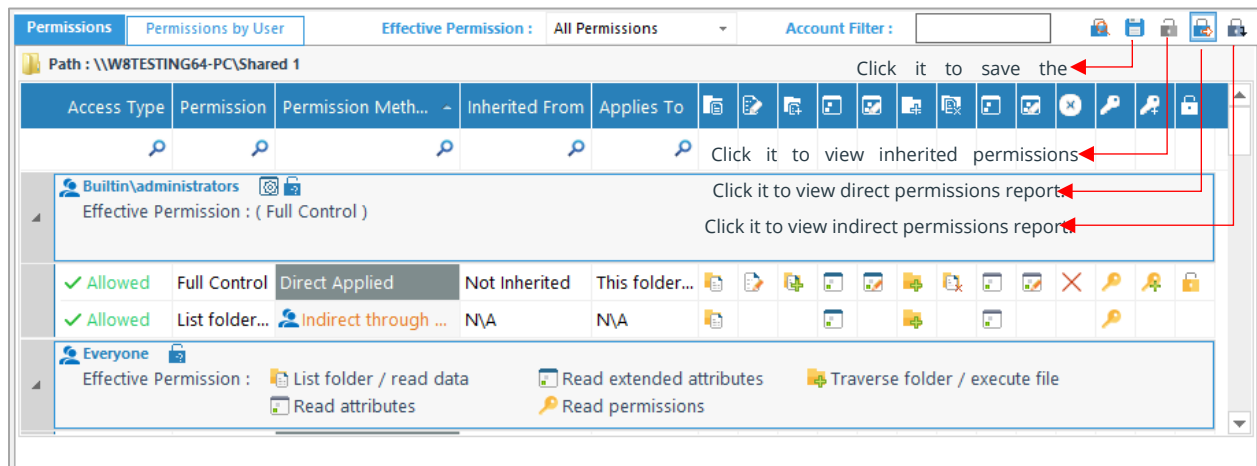
Figure 40: Direct Permissions Report of "Shared 1" folder

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.

9 OneDrive Current Permission Report

The report will be visible under the **Permissions & Privileges** screen. The report name is **Permissions by OneDrive for Business Objects**:

Figure 41: Permissions by One Drive for Business Objects Report

10 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

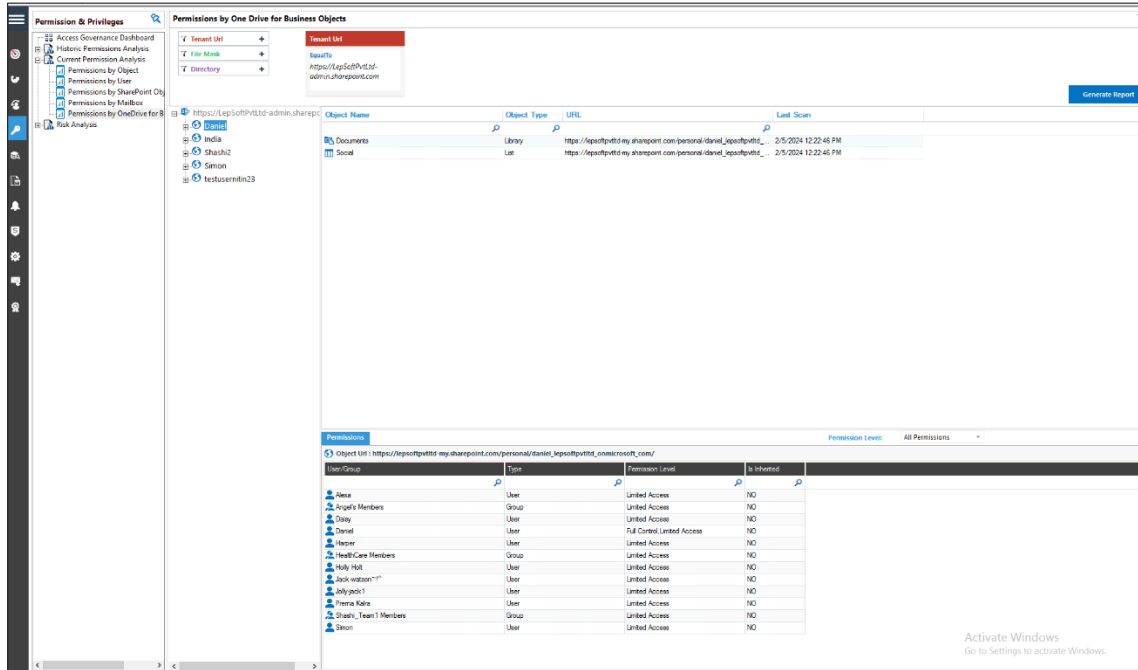Rest of the World: +91(0)-991-085-4291

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/.

11 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.