

CURRENT PERMISSION REPORT

Table of Contents

1	Intro	oduction		3					
2	Curr	ent Permi	ssion Scan Settings	3					
	1.	Configur	e SQL Server	4					
	2.	Configure the Solution to Run a Scan							
		2.1.1	Configure the Primary Database						
		2.1.2	Add a Secondary Database	7					
	3.	Add a Da	ta Set for a File Server Permission Report	8					
	4.	Add a Da	ta Set for Exchange Online	13					
	5.	Add a Da	ta Set for Azure Active Directory	15					
	6.	Scan Per	missions Now						
	7. Modify a Data Set								
	8.	Remove	a Data Set	20					
3	File	rent Permission Report	21						
	9.	How to G	enerate the Current Permission Report						
		3.1.1	Row Filter	23					
		3.1.2	Sorting	23					
		3.1.3	Change Permissions	24					
		3.1.4	Permissions Report of User Only	26					
	10.	Account	Filter	26					
	11.	Effective	Permissions	27					
	12.	Explore 0	Group Membership	29					
	13.	Investiga	te Permissions						
	14.	Other Re	ports	31					
4	Sup	port							
5	Trac	lemarks		32					



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.

Component Management Grading Management Grading Management	Current Permission Scan	Settings									
) 192.168.20.192(SharePoint)	Primary Database		/	Secondary Database(s)						1	× tî
	Configure primary database to store	common information		Secondary database will store NTFS and Share permission for files and folders selected in the datasets						-	
🔤 192.168.20.193(File Server)					File Server(s) Sql server name Database				م		
I lepidesoftware.onmicrosoft.co	Database : CP_DB				P 8.20.193 DB1	94	,		,		
Delegation Control								CP193			
Message Delivery Settings	Stale Object Settings :	•	🖌 Apply	Find All SI	ares				0	1	X ti
UEBA	Data Set Name	Agent	Last :	Scan	Next Scan	Status	Scan Type		Component Type		
	SP-Online	Local		021 12:56:25 PM	Never	Success	Scan Once Only		SharePoint Online		
LDSP Web Console (beta)	SharePoint offine	Local		021 3:30:15 PM	Never	Success	Scan Once Only		SharePoint On Premise		
	One Drive	Local	6/9/2	021 2:33:00 PM	Never	Success	Scan Once Only		OneDrive for Business		
	FS 193Share	Local		2021 1:27:45 PM	Never	Success	Scan Once Only		File Server		
	Exchange-Online	Local		021 12:06:07 PM	Never	Success	Scan Once Only		Exchange Online		
	Exchange On-Premise Active Directory	Local		021 11:09:24 AM (2023 9:32:43 PM	Never 1/31/2023 9:31:38 PM	Success Success	Scan Once Only Scan Once Only; S		Exchange On Premise Active Directory		
5	, are breed, j	2000	1,00	2020 0102110111	101/2020 5101100111	outers	ban once only o		near conceany		
2											
	<										
	< .										,
	Data Set Information Data Set Name Description Component Type Folders Information Domain Controller Status	: FS193Share : File Server : \\192.168.20.1933 Scan all Fold Include Sensi : 192.168.20.191 : Success	rs and Files								~
< >>	<										>

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:

💥 Lej	pide Data Security Platform						-	8 ×
≡	Settings	🔅 Current Permission S	ican Settings					
0) 5) 4) 9)	LPDE1.local Harden Settings General Settings General Settings Degation Control Message Delivery Settings Default SQL Server Settings Default SQL Server Settings Gureat Settings Agent Settings	Primary Database Configure primary database to SQL Server : Database :	se(s) II store NTFS and Share po the datasets server name Datat					
\$		Stale Object Settings :	30 Days	• Apply	Find All Shares	•	/ x	ţţ
B		Data Set Name	Agent	Last S	Scan Ne	ext Scan	Status	
۰								
5								
۰								
4								
ହ		<	ш					>
	с ш >	[{]						>

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	
OWindows Authentication	
SQL Authentication	
User Name : sa	
Password :	
Test Connection	
Select Database : CP_DB	
Time-Out Settings	
Connection Time-Out : 300 🔶 Seconds	
Query Time-Out : 300 🗘 Seconds	
Apply Cancel	

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.

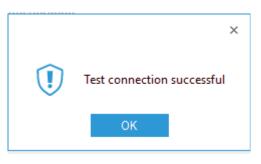


Figure 4: SQL Server Connection is Successful

NOTE:	You can click the	🛃 icon 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.

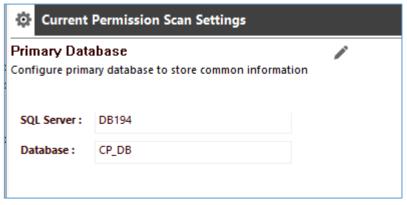


Figure 5: Selected SQL Server and its Database



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:

Configure SQL S	erver			
SQL Server :	DMD01			
	Authentication			
	Windows Authentic	ation		
	SQL Authentication			
	User Name :	sa		
	Password :	•••••		
			Test Connection	
elect Database:				~
Associated File S	Server			
Сог	nnection Time-Out: 300	\$\$ Second	s	
Que	ery Time-Out : 300	\$\$ Second	5	
	database for each file serve File_Server_Name]" in datab			
			Add F	rom AD
			Add Fr	rom OU
				Range

Figure 6: Database Settings for Secondary Database

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



			×
Database Se	attings		
	L server details to store d	data	
Configure SQL S	erver		
SQL Server :	DMD01		
	Authentication	/L/	
	OWindows Authentio	tication	
	SQL Authentication	n	
	User Name :	sa	
	Password :		
	Passworu :		
		Test Connection	
Select Database	Lepide-Permissions	•	
Associated File S	Server		
Co	nnection Time-Out : 300	Seconds	
Qu	ery Time-Out : 300	A Counda	
-		- Seconds	
	database for each file serv		
(Append _[File_Server_Name]" in datal	abase name)	
		Add From AD	
		Add From OU	
		Add IP Range	
	Аррі	uply Cancel	

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						
<u>م</u>	Q	Q	Q					
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



Component Management	🌣 Current Permi:	ssion Scan Settings							
DMD01(SQL)	Primary Database		1	Secondary Da	abase(s)				0 / ×
lepidesoftware.onmicrosoft.co lepidesoftware-admin.sharepe	Configure primary database t	o store common information		Secondary databa	se will store NTFS and	Share permission for files and fol-	lers selected in the datasets		
H File Servers								-	
LepideSoftware.onmicrosoft.c General Settings	SQL Server DMD01			Pile Serv	ir(s)	Sql server name		Database	
Current Permission Scan Settings	Database : CP DB			DCD01		DMD01		Lepide-Permissions	
Message Delivery Settings									
Default SQL Server Settings UEBA									
Agent Settings LDSP Web Console	Stale Object Settings :	90 Days *	🖋 Apply	Find All St	ares				0 / ×
Archive & Import	Data Set Name	 Agent 	Last Sci		Next Scan	Status	Scan Type	Component Type	
	Permission scanning Open Shares	Local	10/4/20	23 4:35:53 PM 23 4:34:53 PM	Never	Success	Scan Once Only Scan Once Only	File Server File Server	
	AD	Local	11/27/2	023 12:31:52 PM	Never	Success	Scan method not defined	Active Directory	
	Data Set Information								
	Data Set Name	: AD							
	Description	-							
	Component Type								
	Server Informatio Status	in : Ipde4.local : Success							
	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 ٠
- Click **Next** •

		×
Data Set Infor Please enter Data	rmation Set name and description.	
Data Set Name:	FS	
Description:	^	
	~	
	< <u>B</u> ack <u>N</u> ext > C	Cancel

Figure 10: Add a Data Set Name



- Choose File Server as the Component Name ٠
- Click on the (+) icon

Component Name:	File Server			-
				0 - >
Folder Name		Server Name	Apply To	



	Settings										
	Component Management Generation	Current Permissi	on Scan Settings								
0	DMD01(SQL)	Primary Database	/	s	econdary Database(s)						0 × × tr
	- El lepidesoftware.onmicrosoft.co	Configure primary database to st	ore common information	S	econdary database will store	NTFS and Share permission for fi	es and folders select	ed in the datasets			
۲				r						0	
G	LepideSoftware.onmicrosoft.c General Settings	SQL Server DMD01		-	File Server(s)	Sql server	name			Database O	م
	Current Permission Scan Settings	Database : CP DB			DCD01	DMD01				Lepide-Permissions	
۶	Message Delivery Settings										
8.	- 5 Default SQL Server Settings - 5 UEBA			L				×			
8	- G Agent Settings	Stale Object Settings :	90 Days 🔹 🖋	Apply		Server Information					O ≠ × 11
Ē.	- 御 LDSP Web Console - 御 Archive & Import	Data Set Name	< Agent	Last Scan		nt(s) and the server(s) to be so	anned			Component Type	
	-	Permission scanning Open Shares	Local	10/4/2023 10/4/2023					F	File Server File Server	
		AD	Local	11/27/202	Component Name:	File Server		*	ed 4	Active Directory	
5											
								0- ×			
۰					Folder Name	Server Name	Apply To	All Shares			
-									m CSV es from audited File Servers		
~								Export to 0			
Q											
											^
		Data Set Information									
		Data Set Name Description	AD								
		Component Type Server Information									
		Status	: Ipde4.local : Success			ſ	< Back Ner	t > Cancel			
						l	- Book Re				
											~
	< >	<									>



Choose All Shares. ٠



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

Comp Please	onent and Server Information	×
Flease		×
Comp	Select File Server(s) Please select file server(s) to scan all share.	*
Folde	Include Sensitive Data Information	×
	File Server(s) DCD01	
	OK	
	< <u>B</u> ack <u>N</u> ext >	Cancel

Figure 13: Select the File Server(s)



Settings									
Component Management	Current Permiss	tion Scan Settings							
 Tradeviocal DMD01(SQL) 	Primary Database								a 1
S Imideraftware annuissor	oft.cc Configure primary database to	/		econdary Database(s					0 / × 4
- E> lepidesoftware-admin.sh	areps	store common information	26	condary database will stor	e NTFS and Share permission for f	les and folders selected in	the datasets		
H H File Servers			-						
	ioft.c SQL Server DMD01			File Server(s)	Sql serve	rname		Database	
 General Settings 一位 Current Permission Scan Set 	Database : CP DB			DCD01	DMD01			Lepide-Permissions	
Message Delivery Settings	angs								
Default SQL Server Settings									
S UEBA							×		
- G Agent Settings	Stale Object Settings :	90 Days 👻 🖋	 Apply 		Server Information				0 / × 4
LDSP Web Console	Data Set Name	 Agent 	Last Scan	Please select compor	ient(s) and the server(s) to be so	anned		Component Type	
- Manuel Comport	Permission scanning	Local	10/4/2023					File Server File Server	
A	Open Shares AD	Local	11/27/2023	Component Name:	File Server		* ed	Active Directory	
8							0- ×		
•				Folder Name	Server Name	Apply To	All Shares		
				SSALLSS	DCD01	Scan Folders Only	Import from CSV		
							Scan Shares from audi	ited File Servers	
~							Export to CSV		
2									
	Data Set Information								
	Data Set Name Description	: AD							
	Component Type	: Active Directory							
	Server Information	: Ipde4.local : Success							
	Status	: Success				< Back Next >	Cancel		
c	• <								>

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

Figure 14: Export to CSV

- 🚻 Save As \times ← → ~ ↑
 Image: A provide the second sec ✓ ^で Search Documents Q Organize 🔻 New folder == -? Date modified Туре Size Name 🗸 🖈 Quick access 📃 Desktop No items match your search. * 👆 Downloads 🖈 🗄 Documents 🖈 Pictures - Finance > 📥 OneDrive > 🜰 OneDrive 🛩 💻 This PC > 🧊 3D Objects > 📃 Desktop > 🔮 Documents File name: Save as type: CSV Files (*.csv) Cancel Save ∧ Hide Folders
- Specify the path where you want to export to and then click **Save**

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 Gi Ipde4.local	Current Permiss	sion Scan Settings						
8	DMD01(SQL)	Primary Database	/	Secondary Da	tahaan(a)				O ≠ × 41
•	- If lepidesoftware.onmicrosoft.c	Primary Database				d Share permission for files and foli			U / X +7
	> lepidesoftware-admin.sharep	Configure primary database to	store common information	Secondary databa	ise will store wirs and	a share permission for files and for	iers selected in the datasets		
6	E - The File Servers								
	LepideSoftware.onmicrosoft.c	SQL Server DMD01		🖃 🗌 File Serv	er(s)	Sql server name		Database	
3	- Ceneral Settings			Q		P		P	م
	- Ourrent Permission Scan Settings	Database : CP DB		DCD01		DMD01		Lepide-Permissions	
1	- Message Delivery Settings	1							
	- 👼 Default SQL Server Settings								
84	- 🐻 UEBA								
~	Agent Settings	Stale Object Settings :	90 Days 🔹 🖋	Apply Brind All S	hares				O ∕ × #
B	- DSP Web Console	Data Set Name	< Agent	Last Scan	Next Scan	Status	Scan Type	Component Type	
E.	Archive & Import	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	
5									
Ø									
-									
-									
~									
ହ									
									^
		Data Set Information							
		Data Set Name	: AD						
		Description Component Type	: Active Directory						
		Server Information Status	: Ipde4.local : 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 Info		
Please enter Data	Set name and description.	
Data Set Name:	ExchangeOnline	
Description:	^	
	~ ·	
	< Back Next > Ca	ancel

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 compon	ent(s) and the server(s) to be scan	ned		
Component Name:	5 L 0 L			-
component Name:	Exchange Online			Ŧ
Tenant Name:	lepidesoftware.onmicrosoft.com			-
	replaced tware of intereast.com			
Client ID:				(?)
chention				\odot
Thumbprint:	*****			
		< Back	Next >	Cancel

Figure 18: Add Component and Server Information

• The Credentials will validate:

	Settings								
	E- Component Management	🔅 Current Permi	ssion Scan Setting	s					
8		Primary Database			Secondan	/ Database[s]			0 / × .
	Inpide123.onmicrosoft.com/8	Configure primary database	to store common information				NTFS and Share permission for files and folders selected in the datasets		
6	 D adminlep-admin.sharepoint.c 	compare primary autoose.			secondary of				
	- D kernel010-admin.sharepoint.c								
G	- D kendi(37-admin.sharepoint.c	SQL Server			I Fle	Server(s)	Sql server name	Database	
	 B_h File Servers 	Database : Test TH			<u>م</u>		ų	لر	
	- 🥸 General Settings	Database .							
۶	Current Permission Scan Settings Message Delivery Settings								
	Befault SQL Server Settings								
₿4	- B UEBA	Stale Object Settings :	30 Days *	Apply	_				0 / X -
_	Agent Settings						×		U / A .
E	- 🔅 LDSP Web Console	Data Set Name	Agent	Last Sca	Comp	ponent and	Server Information	Component Type	
	Archive & Import				Please	select compone	ent(s) and the server(s) to be scanned		
							Exchange Online *		
5					Comp	onent Name:	Exchange Online *		
					Tenan	t Name:	Contoso.onmicrosoft.com *		
۰.					-				
					Client	ID:	eff97728-dd88-4c1a-ada2-ae3784d9c003		
N									
					Thu		×		
2					-				
^							•••.		
					-		•		
					-				
					•	lease wait while v	alidating		
					-				
					-				
							< <u>Back</u> <u>N</u> ext > Cancel		

Figure 19: Validate Credentials



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

X Scan Options Please select the scanning method. Schedule Scan Run every day at 09:36:50 PM, Schedule start from 12/7/2023. Change Schedule (Back Finish Cancel					
Please select the scanning method. Schedule Scan Run every day at 09:36:50 PM, Schedule start from 12/7/2023. Change Schedule					×
Please select the scanning method. Schedule Scan Run every day at 09:36:50 PM, Schedule start from 12/7/2023. Change Schedule	Scan Options				
Scan Now Schedule Scan Pur every day at 09:36:50 PM, Schedule start from 12/7/2023. Change Schedule					
Schedule Scan Pun every day at 09:36:50 PM, Schedule start from 12/7/2023.					
Run every day at 09:36:50 PM, Schedule start from 12/7/2023.	Scan Now				
12/7/2023.	Schedule Scan				
12/7/2023.			Chara	Calcadala	
Rnish Cancel	12/7/2023.		Chan	ge Schedule	
< Back Finish Cancel		~			
< Back Finish Cancel					
< <u>Back</u> Finish Cancel					
< <u>Back</u> Finish Cancel					
< <u>Back</u> Finish Cancel					
< <u>Back</u> Finish Cancel					
< Back Finish Cancel					
< Back Finish Cancel					
< Back Finish Cancel					
< Back Finish Cancel					
< <u>Back</u> Fnish Cancel					
< <u>Back</u> Fnish Cancel					
< <u>B</u> ack Fnish Cancel					
< <u>B</u> ack Fnish Cancel					
< <u>B</u> ack Fnish Cancel					
< <u>Back</u> Fnish Cancel					
< <u>D</u> ack Finish Cancel			l-	Detab	
		< <u>B</u> i	BCK	FILISH	ncei

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 Get Ipde4.local	Current Permis	sion Scan Settings						
8	DMD01(SQL)	Primary Database	/	Secondary Da	tabase(s)				0 ∕ × 47
	- El lepidesoftware.onmicrosoft.co	Configure primary database to	store common information			d Share permission for files and folder:	selected in the datasets		
6									
		SOL Server DMD81		File Serv	er(s)	Sql server name		Database	
6	- General Settings			P		Q		م	م
	- Current Permission Scan Settings	Database : CP DB		DCD01		DMD01		Lepide-Permissions	
1	 Message Delivery Settings 								
	- 🔂 Default SQL Server Settings - 🔂 UEBA								
84	- C Agent Settings	Stale Object Settings :	90 Days 🔹 🖋	Apply Brind All S	hares				0 ≠ × ⊅
	- DSP Web Console	D							0 /
E	- 🕼 Archive & Import	Data Set Name Permission scanning	 Agent Local 	Last Scan 10/4/2023 4:35:53 PM	Next Scan Never	Status Success	Scan Type Scan Once Only	Component Type 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	
-									
5									
٥									
*									
-									
•									
<u>Q</u>									
-									
									A
		Data Set Information							
		Data Set Name Description	: AD						
		Component Type	: Active Directory						
		Server Information	: Ipde4.local						
		Status	: Success						
	< >	1							~
	```								

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 Info	rmation	
Please enter Data	Set name and description.	
Data Set Name:	Azure AD	
Description:	^	
	~	
	< <u>B</u> ack <u>N</u> ext > Ca	ncel

Figure 22: Add a Data Set Name



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

Component Name:	Azure Active Direc	tory		
Tenant Name:	DevSoft001.onmic	rosoft.com(Office 365)		•
Client ID:	67e8eb60-3c90-46	52e-947a-c50dad28d003		0
Secret Key:				
Thumbprint:	******			
			Validate Crede	antials

Figure 23: Add Component and Server Information

• Click Validate Credentials and the Credentials will validate:

Component Name:	Azure Active Directory	
Tenant Name:	Dev Soft001.onmicrosoft.com(Office 365)	
Client ID:	67e8eb60-3c90-462e-947a-c50dad28d003	0
Sec		×
Thu		F
	*****	_
2010/08/10		
Please wait while v	validating	

Figure 24: Validate Credentials

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

Scan Options				
lease select the scanning m	ethod.			
Scan Now				
Schedule Scan				
Run every day at 06:15:15 8 05-2024.	PM, Schedule start from 08-	^	Change Schedule	
		~		

#### 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 Q Scan Now	Local
Exd	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 Info Please enter Dat	ormation ta Set name and description.		
E	Data Set Name: Description:	FS	×	
1			OK Car	ncel

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



				×
電の Data Set Information 一義 Select Object(s) 一番 Database Mapping	Permission Scanning Please select the permissio	g Options n and group membership scan	method.	
Permission Scanning Options	Scan Permissions Now			
	Schedule Permission Scan			
	Run every day at 09:03:41 2/13/2023.	PM, Schedule start from	Change Schedule	
	Scan on Remote Agent			
	Agent Location/IP:		Ŧ	
	Scan Nested Group Membe	rship and Permission		
	Domain Controller: 192.16	8.20.191		
	User Name : multico	orp \administrator		
	Password :	,		
	Note: Use "NetBIOS\UserNan	ne" format for User Name.		
			OK Cancel	

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.



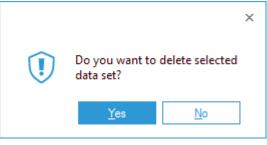


Figure 29: Warning before deleting a Data Set

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:

	Permission &	Privileges 🛠	Permissions by Obje	ect									Ÿ	ř
	Access Govern	ance Dashboard	Y File Server	+	File Server									
8	Current Permis	sion Analysis	T File Mask	+										
	- Permission	s by Object s by User s by SharePoint Obje	V Directory	+	Select file server(s).									
۳	- Permission	s by User	Y Stale Data	+										
æ	Permission	s by SharePoint Obje s by Mailbox	T Compliance	+										
*	Permission	s by OneDrive for Bu	V Monetary Value	+									Generate Report	
P	🖻 🗽 Risk Analysis													
		ermissions by Objec ermissions by User			Object Name		🗃 % Object Type 🛛 Ow	mer	Content Type	Compliance	Monetary Value	Risk Level	Last Scan	
84	🗄 🕅 Sensitive Di	ata				Q	٩		Q	P	P	P	P	
-	- 🛛 Classifie	ed Files												
Ē.	- Classifie	cation Failures ed Emails Tassification Failures												
	Email C	lassification Failures												
*	- 🔄 Classifie	ed SharePoint Objec sint Objects Classific												
5														
	- 🔄 OneDriv	ed OneDrive Objects ve Objects Classifica ed Dropbox Objects x Objects Classificat												
۵	- 🔄 Classifie	ed Dropbox Objects												
_	Sensitive Fi	les by Name												
4	- 🕢 Open Share - 🕢 Alert Summ	5												
Q	- Alert Sumn - Alert Sumn Stale Data F	nary												
*		tside of Business Ho												
	Users with a	Administrative Privil												
		Older than N Days			•									ы
	- External Da	ta Sharing O365			Permissions Permissio	ns by User				Effective Permission : A	Il Permissions -	Account Filter :		<u>.</u>
	- Open AWS	ta Sharing O365 S3 Buckets												
	- II Shares				Access Type	Permission	Permission Method	Inherted Fro	m Applies To			8 8 8 9		
						P	Q	P	Q	ρ 				71
								То	see current permissions, please o	lick 'Generate Report'				
		,			L									_

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

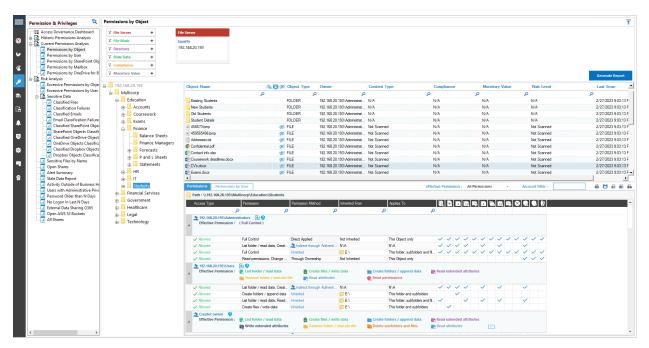


Figure 31: Current Permissions Report

- 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:





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

rivileges 🕅 🕅	Permissions by Object								Ŧ
ernance Dashboard	▼ File Server +	File Server							
missions Analysis	Y File Mask +	EqualTo							
mission Analysis	7 Directory +	192.168.20.193							
ions by User	7 Stale Data +								
ions by SharePoint Obj									
ions by Mailbox									
ions by OneDrive for B is	√ Monetary Value +								Generate Report
	⊞- 192.168.20.193	Object Name	Als 😭 🕫 Object Type	Owner	Content Type	Compliance	Monetary Value	Risk Level	Last Scar
	Multicorp	student	×	ر م	D	Q	Q	Q	Q
	😑 📙 Education	inductions.pptx	💋 FILE	192.168.20.193\Administrat.	. Not Scanned	N/A		Not Scanned	
	Accounts	List 568.bd	💋 FILE	192.168.20.193\Administrat.	Not Scanned	N/A	N/A	Not Scanned	
	- Coursework	Next of kin.bt	95 FILE	192.168.20.193\Administrat.	Not Scanned		N/A	Not Scanned	
	Exams	Part time xlex	ø File	multicorp\Paul	Not Scanned	N/A	N/A	Not Scanned	
	E Finance	passport information.pdf	💋 FILE	192.168.20.193\Administrat.	Not Scanned		N/A	Not Scanned	
	HR	Reter final pptx	💋 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	
	е 🔤 п	RXV.pdf	ø FILE	192.168.20.193\Administrat.				Not Scanned	
	Students	School information.ppbx	💋 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	
	Coursework	Simon final ppb:	💋 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	
		SSN's.pdf	💋 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	
	- Existing Students		🚿 FILE	multicorp\Paul	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
		Student ID.bmp	95 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	2/28/2023
	Old Students	Students removed txt	🚿 FILE	192.168.20.193\Administrat.		N/A	N/A	Not Scanned	2/28/2023
	🔬 📙 Student Details	Teacher ID.bmp	ø File	192.168.20.193\Administrat.			N/A	Not Scanned	
	Financial Services	Termination letter.docx	ø File	multicorp/Paul	Not Scanned	N/A	N/A	Not Scanned	2/28/2023
	🐵 🔜 Government	4							•
	😑 📙 Healthcare	Permissions Permissions by User				Effective Permission : All Perm	issions - Accor	int Filter :	🗌 🔒 🗎 👜 📾
	Accounts	Path : \\192.168.20.193\Multicorp	\Education\Students						
	E- Finance	Access Type Per	nission Permission M	ethod Inherted From	Applies To				
	HR HR						3906894		
		٩	ρ	Q	Q	Q			
	B- Marketing	192.168.20.193\Administrator Effective Permission : (Full)							
	- Patients	4	control y						
	B- Sales								
	E Legal		Control Direct Applied		This Object on		/ / / / / / / /		
	Technology		older / read data, Creat 🤽 Indirect th		N'A			✓	
	reamonogy		Control Inherited	📁 E:\	This folder, sub		/ / / / / / / /		
			d permissions, Change Through Own	ership Not Inherited	This Object on	ly l		$\checkmark$ $\checkmark$ $\checkmark$	
		2 192.168.20.193\Users () () Effective Permission : () Lis	t folder / read data 🛛 🚦 C	reate files / write data rad attributes	Create folders / appen Read permissions	d data 🛛 🗽 Read extended at	ttributes		
		Allowed List	older / read data, Creat 🤰 Indirect th	puch Authenti NVA	NVA.	~ ~ ~ ~ ~		~	
			te folders / append data inherited	E\	This folder and			-	
			older / read data. Read Inherited	E L		ofolders and fil 🗸		~	

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:

Permission & Privileges 🛛 🛠	Permissions by Object								
Access Governance Dashboard	T File Server +	File Server							
Historic Permissions Analysis	7 File Mask +	EqualTo							
Current Permission Analysis	7 Directory +	192,168,20,193							
Permissions by Object     Permissions by User									
Permissions by User	√ Stale Data +								
Permissions by Mailbox	T Compliance +								
Permissions by OneDrive for Busi	7 Monetary Value +								
Risk Analysis									Generate Repor
Excessive Permissions by Object	192.168.20.193	Object Name	Sa 🛐 Ø Object Type	Owner	Content Type	Compliance	Monetary Value	Risk Level	Last Scan
Excessive Permissions by User	H- Multicorp		p p	2		Q	Q	Q	Q
🕀 🙀 Sensitive Data	Education	Coursework	FOLDER	192 168 20 193\Administrat		N/A	N/A	N/A	3/6/2023 9.03:34
Classified Files	Accounts	Existing Students	FOLDER	192.168.20.193 Administrat		N/A	N/A	N/A	3/6/2023 9:03:34
Classified Emails		New Students	FOLDER	192.168.20.193\Administrat		N/A	N/A	N/A	3/6/2023 9:03:34
Email Classification Failures		Old Students	FOLDER	192.168.20.193 Administrat		N/A	N/A	N/A	3/6/2023 9:03:34
Classified SharePoint Objects	Exams	Stud 201	FOLDER	192 168 20 193 Administrat		N/A	N/A	N/A	3/6/2023 9:03:34
SharePoint Objects Classificat	E Finance	4585 Show recent changes	S FILE	192.168.20.193\Administrat		N/A N/A	N/A	Not Scanned	3/6/2023 9:03:34
Classified OneDrive Objects	⊞- <mark>_</mark> HR	4595 Show recommended owner	Ø FILE	192.168.20.193 Administrat		N/A	N/A	Not Scanned	3/6/2023 9:03:34
- OneDrive Objects Classificatic	e	Addr Change permissions	S FILE	192 168 20 193 Administrat		N/A	N/A	Not Scanned	3/6/2023 9:03:34
	E Students	Confidential off	S FILE	192.168.20.193 Administrat		N/A	N/A	Not Scanned	3/6/2023 9:03:34
Dropbox Objects Classification	Coursework	Contact info xisx	S FILE	192.168.20.193 Administrat		N/A N/A	N/A	Not Scanned	3/6/2023 9:03:34
- Sensitive Files by Name	Existing Students	Context Info Xesx	S FILE	192.168.20.193 Administrat		N/A	N/A	Not Scanned	3/6/2023 9:03:34
Open Shares     Alert Summary	New Students	Counterwork deadures dock	Ø FILE	192.168.20.193 Administrat		N/A N/A	N/A	Not Scanned	3/6/2023 9:03:34
- Alert Summary - Stale Data Report	Old Students	Exems.docx	S FILE	192.168.20.193 \Administrat		N/A N/A	N/A	Not Scanned	3/6/2023 9:03:34
Activity Outside of Business Hour		Full time dax	ILE I FILE	192.168.20.193 Administrat		N/A N/A	N/A	Not Scanned	3/6/2023 9:03:34
Users with Administrative Privileg	E Student Details	Q ² Inductions pptx	S FILE	192.168.20.193 \Administrat		N/A	N/A	Not Scanned	3/6/2023 9:03:34
Password Older than N Days	Financial Services	Inductions ppox	90 FILE	102.166.20.103 Vidministrat		N/A	N/A N/A	Not Scanned	3/6/2023 3:03:34
- No Logon In Last N Days	Government	4							
- Z External Data Sharing 0365	Healthcare	Permissions Permissions by User				Effective Permission :	All Permissions -	Account Filter :	A 🗎 A 🗟
Open AWS S3 Buckets     All Shares	🕮 🔚 Legal	Path : \\192.168.20.193\Multicorp\Educa	tion\Students						
- All Shares	— Technology	Access Type Permission	Permission Meti	od Inherted From	Apples To	RDDI			
		٩	٩	Q	Q	P			
		Effective Permission : (Full Contro							
		Effective Permission : (Full Control	0						
		Allowed Full Control	Direct Applied	Not Inherited	This Object only	~ ~ ~ ~ ~	/ / / / / / / /	/ / / /	
		✓ Allowed List folder /	ead data, Creat 🙎 Indirect throu	gh Authenti NVA	N'A	~ ~ ~ ~		~	
		✓ Allowed Full Control	Inherted	📁 E:\	This folder, subfolders	and fil 🗸 🗸 🗸 🤸	/ / / / / / / /	1 1 1 1	
		Allowed Read permis	sions, Change Through Owner	hip Not Inherited	This Object only			~ ~ ~	
		👲 192.168.20.193\Users 🛛 🔞							
		Effective Permission : 💽 List folde	r / read data 🛛 📑 Crea	te files / write data	💼 Create folders / append data	Read extended a	ttributes		
		Traverse 1	older / execute file 👘 📑 Rea	d attributes	Read permissions				
		Allowed List folder /	ead data. Creat 急 Indirect throu	oh Authenti NVA	NA	~ ~ ~ ~ ~		~	
			s / append data inherited	E/	This folder and subfold				
			ead data. Read Inherted	E E	This folder, subfolders			~	
		✓ Allowed Create files		E E	This folder and subfold				
< >									

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:

	States & Behavior 🛛 🕅 🛠	All Environm	ent Changes																- ¥ (	~
	Search 🔎	T Compone	nt Name	+	When	8	omponent N	_{lame} ×	Serv	er Name	= ×	Object Path	8	×						
8	All Environment Changes	7 Server Na	me	+	Custom Date Rang	28 6	quallo	×	Equa	Το	×	EqualTo	×	<						
	<ul> <li>Anomaly Analysis</li> <li>192.168.20.192(SharePoint)</li> </ul>	7 Object Par	th	+	1/1/2023 10:03 I 3/6/2023 11:59 I		ile Server		192.	168.20.193		E:\Multicorp\Education \Students\Student Detu								
۳	multicorp.local	7 Object Typ	pe .	+	5/0/2025 11:591							15tudents 15tudent Det	0113							
æ	File Server Reports     Iepidesoftware.onmicrosoft.com(E	7 Who		+																
•	🗄 🕅 lepidesoftware-admin.sharepoint.	Y When		+																
۶	Image:	7 Operation		+																
		7 Where		+																
8		7 Criticality		+																
B																		Gen	erate Report	
		Drag a column h	eader here to gro	oup by that co	lumn.													8	<u>a</u>	Ŧ
		Compone	nt Name	7 Server	Name J	V Object Path	4	bject Type	4	Who	د	When	r7	Operation 🗸	7 What	X Where	J Criticality	7		R
S		P		P	۶		Q		P		۶		٩	۶		D	<u>م</u>	P		ii:
		File Server		FS001		E:\Multicorp\Educa	tion\Stu F	older		MULTICORPVE	laul	1/18/2023 3:30:10 PM	1	Security Change (Permission.	Folder Security Change (Per.	FS001	High			
۵																				
-																				
Q																				

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	e Users			
Interactions in la		Update		
Recommende	ed Owner: multicorp\paul			
multicorp\paul				Interactions
-	0	5	10	

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	$\times$
General Security Previous Versions Customize	
Object name: \\192.168.20.193\Multicorp\Education\Student	ts\!
Group or user names:	
SCREATOR OWNER	^
SYSTEM	
Students (MULTICORP\Students)	×
To change permissions, click Edit. Edit	
Permissions for CREATOR OWNER Allow Deny	
Full control	^
Modify	
Read & execute	
List folder contents	
Read	~
For special permissions or advanced settings, Advanced click Advanced.	
OK Cancel Appl	у

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.

Permissions Permission	s by User															Effective Permission : All Permissions - Account Filter :	
Path : \\192.168.20.193\I	Multicorp\Education\Stud	lents															
Account (Principal)	Effective Permission			÷	Ĩ.	10	В,	+	۴.	Ē.	D,	$\otimes$	R	0	19		ľ
Q		ρ															
192.168.20.193\Adminis	Full Control		$\checkmark$														
ulticorp \adam	List folder / read data, C		$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		$\checkmark$		$\checkmark$			$\checkmark$				
ulticorp\admin	Full Control		$\checkmark$														
amulticorp \Administrator	Full Control		$\checkmark$														
adrian	Full Control		$\checkmark$														
ulticorp\alan	Full Control		$\checkmark$														
anthony multicorp \anthony	Full Control		$\checkmark$														
ulticorp\ben	Full Control		$\checkmark$														
multicorp \Bill	Full Control		$\checkmark$														
ulticorp \brian	Full Control		$\checkmark$														
multicorp\C.Ovenden	Full Control		$\checkmark$														
ulticorp \carl	Full Control		$\checkmark$	~	$\checkmark$	$\checkmark$											
multicorp\chandler	Full Control		$\checkmark$														
multicorp\chris	Full Control		~	$\checkmark$													
multicorp\craig	Full Control		$\checkmark$														

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.

erm'	issions Permissions by	User			Effective Pern	nission	11	All Per	missions		-	Accoun	t Filter :	users	× 🙆	i i	6
Pa	th : \\192.168.20.193\Multi	icorp\Education\Students\C	oursework														
A	ccess Type	Permission	Permission Method	Inherited From	Applies To		+	Ĩ+	R P	<b>F</b>		D, 😣		<b>1</b> 2			
	Q	م	م م		<u>م</u>												
4	Effective Permission :	َّا <b>؟</b> List folder / read data Traverse folder / execute :	E Create files / writ		reate folders / append data	Read	exte	nded	attribute	s							
	Allowed	List folder / read data, Creat	2 Indirect through Authenti	N\A	N∖A	$\checkmark$	~	~	~	~	$\checkmark$		~				
~	Allowed	Create folders / append data	Inherited	📁 E:\	This folder and subfolders			$\checkmark$									
~	<ul> <li>Allowed</li> </ul>	Create files / write data	Inherited	📁 E:\	This folder and subfolders		$\checkmark$										
~	<ul> <li>Allowed</li> </ul>	List folder / read data, Read	Inherited	📁 E:\	This folder, subfolders and fil	. 🗸			~	$\checkmark$	$\checkmark$		$\checkmark$				

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	lcon in Header Row	lcon in Report	Color in Permission Calculation
Full Control			
List folder / read data	B		
Create files / write data			
Create folders / append data	R	<mark>€</mark> ∔	
Read extended attributes			
Write extended attributes			
Traverse folder / execute	<u>"</u>	÷	
Delete subfolders and files	<u>r</u>	E,	
Read attributes			
Write attributes		<b>n</b> /	
Delete	×	×	
Read permissions	۶	<u></u>	
Change permissions	2	<u>,</u> ,	



Permission		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.

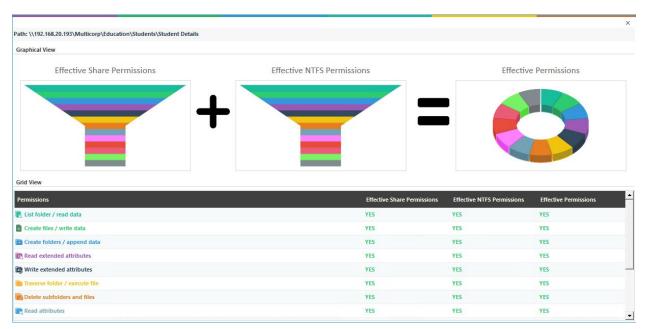


Figure 40: Effective Permissions

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.

Object Name	Effective Permissions			+				6		Û 💼	۲	
2 192.168.20.193\Users	List folder / read data, Create files / write data, Create folders / ap					-	~		~	~		Ť
NT AUTHORITY\INTERACTIVE	List folder / read data, Create files / write data, Create folders / ap	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		$\checkmark$		$\checkmark$	~		
NT AUTHORITY\Authenticate	List folder / read data, Create files / write data, Create folders / ap	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$		$\checkmark$		$\checkmark$	~		
Amulticorp \Domain Users	List folder / read data, Create files / write data, Create folders / append	$\checkmark$	. 1									
			~	~	~		~		~	~		
			~	~	~		~		~	~		

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 <u>Section 2.3.3 Modify Data Set</u> 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.



				Applies To	410.	+	+	6	۳,	+	L0	ġ.
	P	<u>م</u>	م	Q								
	Administrators 💿 🝞 sion : (Full Control)											
✓ Allowed	Full Control	Direct Applied	Not Inherited	This Object only	~	~	~	~	~	~	~ •	/
✓ Allowed	List folder / read data, Cre	at 🙎 Indirect through Authenti	N\A	N\A	~	$\checkmark$	~	~		~	-	/
✓ Allowed	Full Control	Inherited	📁 E:\	This folder, subfolders and fil	~	$\checkmark$	~	$\checkmark$	~	~	~ .	/
✓ Allowed	Read permissions, Change	e Through Ownership	Not Inherited	This Object only								

#### Figure 42 Explore Group Permissions

# 13. Investigate Permissions

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

Who Modified: Al Users WRESTING64-PC  WRESTING64-PC  Shared 1	W8TESTING64-PC ect Name 3.csv icenseFileFeb-25-2016 19-07-08.lic	Directory: File Mask: Object Type File	INCLUDE C			Generate Rej	_
Who Modified: Al Users WBTESTING64-PC 	ect Name B.csv .icenseFileFeb-25-2016 19-07-08.lic	Object Type File	All File Nam			🗙 Remove Filt	ers
	3.csv .icenseFileFeb-25-2016 19-07-08.lic	File		When Changed			
B	icenseFileFeb-25-2016 19-07-08.lic						
↓ 1 				5/24/2016 5:49:59 PM			
		File		5/24/2016 5:49:59 PM			
	Test1	Folder		5/24/2016 5:49:59 PM			
Per	oct1 Conviderlithemenade	rile.		E /04 /0016 E-40-E0 DN4			
	mission History Compare Permission						E
	Path : C:\Shared 1						
	Account (Principal)	Permission (Acce	ss)	Inherited	Apply To		
		Q	Q	م			
	5/24/2016 5:49:59 PM (Change	d by "VDOC\Adminis	trator")	Owner : BUILTIN\Admin	istrators	Where : W8TESTING	64-F
	SUILTIN\Administrators	✓ Full Control	ľ	No	This folder,	subfolders and files	
	SYSTEM	✓ Full Control	1	No	This folder,	subfolders and files	
	🙎 Everyone	✓ Read & execut	e I	No	This folder,	subfolders and files	
	L VDOC\testuser1	✓ Full Control	1	No	This folder,	subfolders and files	
	L VDOC\testuser2	✓ Read & execut	e I	No	This folder,	subfolders and files	
	L VDOC\Administrator	✓ Full Control	1	No	This folder,	subfolders and files	

Figure 43: Investigate Permission

## 14. Other Reports

Peri	Permissions by User Effective Permission: All Permissions - Account Filter:																		
<b>)</b>	Path : \\W8TESTI	NG64-PC\Share	ed 1							Click	it	to	sav	e tł	ne 🗲				
	Access Type	Permission	Permission Meth 🔺	Inherited From	Applies To	ē	D	Ē.			류	R			×	۶	8	£	
	Q	م	Q	Q	م	Clie	ck it	to	viev	v in	herit	ed	pern	nissio	ons	-			
	Label Section (Administrators)       Image: Section (Administrators)       Image: Section (Administrators)         Click it to view direct permissions report       Click it to view indirect permissions report         Click it to view indirect permissions report       Click it to view indirect permissions report																		
	✓ Allowed	Full Control	Direct Applied	Not Inherited	This folder		٥	Q.			÷	E),			$\times$	۶	æ	6	
	✓ Allowed	List folder	옱 Indirect through	N\A	N\A						÷					۶			
	Effective Permission :       List folder / read data         Read attributes       Praverse folder / execute file         Praverse folder / execute file													↓					

#### 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  $\overrightarrow{\mathbf{m}}$  icon to sort the report as per the inherited permissions.
- 2. Click  $\blacksquare$  icon to sort the report as per the direct permissions.
- 3. Click  $\blacksquare$  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 <u>https://www.lepide.com/contactus.html</u> 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.

