

HOW TO USE LEPIDE TO IDENTIFY USERS WITH EXCESSIVE PRIVILEGES TO SENSITIVE DATA

Table of Contents

1.	Intro	oduction3
2.	Sens	sitive Data3
3.	Prin	ciple of Least Privilege (PoLP)
4.	The	Solution
5.	Exce	essive Permissions by Object Report6
	5.1.	Prerequisites
	5.2.	Running the Excessive Permissions by Object Report for File Server
		5.2.1. User Permissions
		5.2.2. Files Within the Selected Folder
	5.3.	The Excessive Permissions by Object Report for SharePoint Online
	5.4.	The Excessive Permissions by User Report14
6.	Supp	oort16
7.	Trad	lemarks16



1.Introduction

Data breaches are a serious threat to any organization and action needs to be taken to keep the risk of their occurrence to a minimum. The focus at Lepide is to provide visibility over what's happening with your data and through visibility you can take the necessary action to mitigate risk and stay compliant.

This guide is in two parts. The first explains the ways in which you can use Lepide Data Security Platform to provide visibility to reduce data breaches with sensitive data. The <u>second section</u> gives step-by-step instructions on how to configure the Excessive Permissions Reports to determine who has access to what data and whether that access is required.

2.Sensitive Data

The types of sensitive data which companies hold can include information such as social security numbers, credit card details, bank account information, and other account data that identifies customers or employees.

This information is necessary for employees to perform essential business functions but if there is uncontrolled access to this sensitive data it can lead to data breaches including fraud and identity theft, and to non-compliance.

When a user, either intentionally or accidentally, misuses legitimate privileges which they have been given it is known as privilege abuse. Despite these privileges being legitimately granted, users may access resources or perform actions that compromise data security.

Whether privilege abuse occurs through users purposefully mishandling data, or through employee carelessness, it is a security threat that must be taken seriously.

3. Principle of Least Privilege (PoLP)

The **Principle of Least Privilege** (PoLP) is an information security concept in which a user is given the minimum levels of access needed to perform their job functions. Applying this principle is a highly effective way to greatly reduce the chance of an attack within an organization.

To be able to do this, however, it is essential for an organization to have visibility over the complete list of users who have access to sensitive information. But as organizations grow, being able to see and understand who has access to sensitive data can become a complex and time-consuming task.

4.The Solution

The Lepide Data Security Platform provides a solution to this complexity with excessive permissions reports which provide visibility as to **who** has access and **what** type of sensitive data they have access to.

Once there is clarity as to exactly who requires access to do their job, it is a straightforward process to remove privileges for those who don't need them.

There are two reports within the Lepide Data Security Platform which can be used to see Excessive Permissions to sensitive data. They will both display the same data but in different ways depending on how you want to view the data. The reports are called Excessive Permissions by Object and Excessive Permissions by User.



Here is an example of the Excessive Permissions by Object Report:

Figure 1: Excessive Permissions by Object Report

This report shows the **object structure** for the selected file server, the users who have access to the selected object and the contents of the selected object. The elements of this window will be explained in more detail below.

The second report is the **Excessive Permissions by User Report**:



=	Permission & Privileges	Excessive Permissions by User									Ÿ
© •	B Access Governance Dashboard B Mathematical Analysis Current Permission Analysis Current Permission Sy Object Permissions by User Permissions by User Permissions by User	7 Component Name + 7 User + 7 Days +	Component Name EqualTo 192.168.20.193	Bays 30 days						G	ienerate Report
3	Permissions by Mailbox	n 9 multicoro	^								2
	🗄 🕼 Risk Analysis	\$061000-CMJLS7GJQ0VS	Object 1	lana	0 FR pat	Owner	Last Com	Last Maddind		-	
	Excessive Permissions by Object	adam	Object P	vanie C	/88 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Owner O	D Last Scan	D D D D D D D D D D D D D D D D D D D	0 0		
8.	E Sensitive Data	admin	▲ 192.168	.20.193							
~	Classified Files	Administrator	4 <mark>-</mark> Mu	iticorp	E:\Multicorp	192.168.20.193\Administrators	7/12/2021 1:26:42 P	M 3/24/2021 11:14:04 AM	~ ~ ~ ~ ~ ~	~ ~ ~ ~	~ ~ ~ ~ ~
Ш	Classified Emails	adrian	Þ	Education	E:\Multicorp\Education	multicorp \Gemma	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM	~ ~ ~ ~ ~ ~	~ ~ ~ ~	~ ~ ~ ~ ~
	Email Classification Failures	aian		Financial Services	E:\Multicorp\Financial Services	multicorp\Paul	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM	~ ~ ~ ~ ~ ~	~ ~ ~ ~	~ ~ ~ ~ ~
-	- Classified SharePoint Objects	anthony	p	Accounts	E:\Multicorp\Financial Services\Acco.	multicorp\Paul	7/12/2021 1:26:42 P	M 6/23/2021 2:18:57 PM		~~~~	~~~~
	- A SharePoint Objects Classification Failures	ben	p	Lients	E: Muticorp \Financial Services \Clients	multicorp (Paul	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM		~~~~	
6	- Classified OneDrive Objects		p	Hinance	E: Muticorp \Financial Services \Financial	e multicorp/Paul	7/12/2021 1:26:42 P	M 6/23/2021 5:55:15 PM			
	Classification Failures	brian	P	HR IT	E: Watcorp Vinancial Services (HH	muticorp viau	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM		× × × ×	
*	Dropbox Objects Classification Failures	carl		Makating	E: Widtcorp/Financial Services/Marke	matican Paul	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM			
-	Sensitive Files by Name			Sales	E-Multicom/Enancial Services/Sales	multicom\Paul	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM		2223	
~ 1		- chris	P P	Government	E:\Multicorp\Government	multicorp\phil	7/12/2021 1:26:42 P	M 3/23/2021 5:31:36 PM		0000	
~	- Alert Summary	craig		Heathcare	E:\Multicorp\Healthcare	multicorp\Paul	7/12/2021 1:26:42 P	M 3/23/2021 5:31:37 PM		2222	2222
×	- A Stale Data Report	daniel	P	Legal	E:\Multicorp\Legal	multicorp\adam	7/12/2021 1:26:42 P	M 3/23/2021 5:31:37 PM		~ ~ ~ ~ ~	
	Licers with Administrative Privilene	david	Þ	Technology	E:\Multicorp\Technology	multicorp\ben	7/12/2021 1:26:42 P	M 3/23/2021 5:31:37 PM		~ ~ ~ ~	~ ~ ~ ~ ~
	Password Older than N Days	DefaultAccount									
	- 🔄 No Logon In Last N Days	- derek	•)
	External Data Sharing 0365	dominic	Name		8 🙀 🕫 Content Type	Compliance	Monetary Value	e Risk Level			-
	All Shares	edward		م		P	P	<u>م م</u>			
		- emily	458673	3.bmp	🚿 Names	GLBA + NPPI	\$ 4225	1495			
		- Ext_Contractor	≥ 459565	5496.bmp	ge Phone Numbers	GLBA + NPPI	\$ 4875	2925			
		Gemma	E 67949.	bmp	🚿 Address	GLBA + NPPI	\$ 2688	966			
		Geoff	Addres	ses.bd	🚿 Address	GLBA + NPPI	\$ 2925	1755			
		glen	Client p	portfolio New.pptx	no Sensitive Content	N/A	N/A	N/A			
			Qt Client p	portfolio.pptx	Name + Phone Numbers	GLBA + NPPI	\$ 2518	1811			
		gwen	Confide	ential.pdf	SSN SSN	GLBA + NPPI	\$ 24/2	1512			
		HealthMailbox11cb852	Custom	ter contact info xisk	Name + Phone Numbers	GLBA + NPPI	\$ 1591	1244			
		HealthMailbox1757d7b	Custon	ter list ppox	Mames	GLBA + NPPI	\$ 2525	5/6			
		HealthMailbox189d97f	Employ The Employ	vee list.docx	CON 1 Marries	GLBA + NPPI	5 1632	209			
		HealthMailbox1babc10	C lovete	nente poty	Solv + Mariles	GLBA + NPPI	\$ 1105	459			
		HealthMailbox24f1142	E Lenal t	xt	SSN SSN	GLBA + NPPI	\$ 2080	864			_
		HealthMailbox2d44be1	List 56	8 bit	Address	GLBA + NPPI	\$ 4225	1755			
		HealthMailboy54a779b	Passo	ort copies.pdf	SSN SSN	GLBA + NPPI	\$ 3380	1404			
		HealthMailbox6552470	Propert	ty details.pptx	Phone Number + Affress	GLBA + NPPI	\$ 1133	447			
		Lealth talkau0532070	C RXV p	đ	🧭 SSN	GLBA + NPPI	\$ 2736	912			
			Y CONTA	ndf	CCM	CLEA _ NEEL	¢ 27/11	510			-

Figure 2: Excessive Permissions by User Report

This report shows a **list of users** for the selected file server, a tree structure listing objects, the files contained within the object and the permissions which the selected user has for the files. The elements of this window will be explained in more detail below.

Once a report has been generated, it can be scheduled to run on a regular basis, saved and exported.



5. Excessive Permissions by Object Report

As described previously, there are two reports which show excessive permissions to sensitive data. In this document, we will focus on the **Excessive Permissions by Object Report** but both reports work in a similar way.

The Excessive Permissions by Object Report can be run for file servers or for SharePoint online.

5.1. Prerequisites

Before running either of the Excessive Permissions Reports, you will need the following:

- To have configured <u>Windows File Server</u> to enable auditing for file server reports
- To have configured SharePoint<u>Online</u> to enable auditing for SharePoint Online reports
- To have enabled <u>Data Discovery and Classification</u> and run an initial scan for file server reports
- To have run an <u>initial permissions scan</u>

5.2. Running the Excessive Permissions by Object Report for File Server

Once the prerequisites are met and a scan has run, the **Excessive Permissions by Object Report** can be generated as follows:

• Click the **Permissions and Privileges** icon and the following screen will be displayed:





Figure 3: Permissions and Privileges

- Expand Risk Analysis (from the tree structure to the left side of the screen)
- Click on Excessive Permissions by Object
- From the top of the screen, under the Component Name filter, click Component Name

The following dialog box is displayed:

Component Name Filter	×	2
Component : File Server Filter Criteria: EqualTo	• •	
File Server		
 192.168.20.193 	Q	
OK Cancel		

Figure 4: Component Name Filter

- Here you can select File Server or SharePoint Online from the list
- For this example, select File Server and then select the required File Server from the list

- Click **OK** and you will return to the Excessive Permissions by Object screen
- From the top of the screen, under **Days** click to select the number of days to report on.

Days Filter	r	×
Filter Criteria:	30 days 👻	
	30 days 60 days 180 days Custom days OK Cancel	

Figure 5: Days Filter

- Click **OK**
- Click Generate Report

The report will run showing the objects in a tree structure:

Component Name	+	Component Name
7 Days 7 Directory	++	EqualTo 192.168.20.193
192.168.20.193 → Multicorp ⊕ Educatio ⊕ Financial ⊕ Gient ⊕ Gient ⊕ Financial ⊕ Gient ⊕ Financial ⊕ Financial ⊕ Financial ⊕ Financial ⊕ Financial ⊕ Governm	n Services Ints s ce eting nent	Object Name Balance Sheets Finance Manager Forecasts P and L Sheets Statements

Figure 6: Object List

To see a list of users and permissions, click on the required folder from the tree structure:

=	Permission & Privileges 😵	Excessive Permissions by Object										Y
© • •	Bacess Governance Dishboard Bit District Permission Analysis Current Permission Analysis Permissions by Object Permissions by UsarePoint Objects Permissions by ManPoint Objects Permissions by OneDrive for Business Objects	Y Component Name + Y Days + Y Directory + B- 192.168.20.193	Component Name Equatio 192.168.20.193	Days 30 days							Generate Repor	rt 🗒
✓ Sa Ba Ba<	E Lug, Risk Analysis Excessive Permissions by Object Excessive Permissions by User Construct Part Construct Part Construc	Multicorp Multicorp Financial Services Financial Services Gents Gents Gents HR Gent T Marketing Gents Sales	Object Name Balance Sheets Finance Managers Finecasts P and L Sheets Statements	ه الم ح	Owner multicorp\Paul multicorp\Paul multicorp\Paul multicorp\Paul	٩	Last Scan 7/12/2021 1: 7/12/2021 1: 7/12/2021 1: 7/12/2021 1: 7/12/2021 1:	26:42 PM 26:42 PM 26:42 PM 26:42 PM 26:42 PM 26:42 PM	۶ ۲	2		
8 4 2 2	Classified OncDrive Objects Classified TonDrive Object Statistication Failures Classified Tonpolox Object Statisfication Failures Classified Tonpolox Object Statisfication Failures Open Object Object Statisfication Failures Open Antivity Outside of Business Hours Open Antivity Outside of Business Hours Open Antivity Object Statisfication Failures Open ANV S3 Buckets Open ANV S3 Buckets	B→ Government B→ Gevernment B→ Legal B→ Legal B→ Technology	Permissions on Folder : Account (Phropa) 9 193 193 01 193 (Marine) 9 multicory Vatinistrator 9 mul	VI92.168.20.193/Multicorp Effective Remsson Ril Cortrol Ril Cortrol	VFinancial Servi Image: Ima	Cest/Finance				Files In Folder : Finance CReject Name 4 5955556 bmp 4 5955556 bmp 4 6595536 bmp 4 6595536 bmp 4 659535 bmp 4 659555 bmp 4 6595555 bmp 4 65955555 bmp 4 65955555555555555555555555555555555555	A Content Type Content Type Content Type Content of Addees Content	e P s orite e Ni. i

Figure 7: Excessive Permissions by Object Report for File Server

The example above shows the **Finance** folder has been selected. Users within the **Finance** folder are then listed to the lower left of the screen and to the right are the files contained within the **Finance** folder.

5.2.1. User Permissions

This section of the window shows the username, the permission which that user has and then the individual permissions for that user.

Pause on a tick or on an icon at the top of the columns to display a tool tip to explain the permission:

Permissions on Folder : \	\\192.168.20.193\Multicorp\Fi	inanc	ial Se	rvice	s\Fin	ance									
Account (Principal)	Effective Permission		+	+	16	Đ,	Ŧ	٦.	16	E,	⊗	R	0	i ?	
Q	Q														
2 192.168.20.193\Adminis	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 	
admin 💄	Full Control	~	\checkmark	~	\checkmark	~	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	~	 Image: A set of the set of the	
2 multicorp \Administrator	Full Control	\checkmark	~	~	\checkmark	~	\checkmark	~	\checkmark	~	~	\checkmark	\checkmark	\checkmark	
adrian 💄	Full Control	~	~	\checkmark	~	~	~	~	\checkmark	~	~	~	~	 Image: A second s	
anthony anthony	Full Control	~	~	\checkmark	~	~	~	~	\checkmark	~	~	~	\checkmark	 Image: A second s	
amulticorp\brian	Full Control	~	~	~	~	~	~	~	\checkmark	~	~	~	~	 Image: A second s	
amulticorp\carl	Full Control	~	~	~	\checkmark	~	~	\checkmark	\checkmark	~	~	\checkmark	~	 Image: A second s	
2 multicorp\chandler	Full Control	\checkmark	~	\checkmark											
amulticorp\craig	Full Control	~	\checkmark	\checkmark	\checkmark	~	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	~	 Image: A set of the set of the	
amulticorp\david	Full Control	\checkmark	~	\checkmark											
amulticorp\derek	Full Control	~	~	\checkmark	~	~	\checkmark	~	\checkmark	~	~	~	~	 Image: A second s	
amulticorp\dominic	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp \edward	Full Control	~	~	~	\checkmark	~	~	\checkmark	\checkmark	~	~	\checkmark	~	 Image: A set of the set of the	
multicorp\Ext_Contractor	Full Control	\checkmark	\checkmark	\checkmark	\checkmark	~	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	~	\checkmark	
amulticorp \Gemma	Full Control	\checkmark	~	~	\checkmark	~	\checkmark	\checkmark	\checkmark	~	~	\checkmark	~	\checkmark	
amulticorp \glen	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	~	Ŧ

Figure 8: User Permissions

Permissions on Folder : \\192.168.20.193\Multicorp\Financial Services\Finance															
Account (Principal)	Effective Permission	R	+	+	Ĩ.	Ð,	$\left[+ \right]$	Ē.	6	E,	×	R	0	1 2	
م	Q														
2 192.168.20.193\Adminis	Full Control	~	~	~	~	~	~	~	\checkmark	~	~	~	~	 Image: A set of the set of the	
admin 🚬 🙎	Full Control	~	~	~	~	\checkmark	~	Del	ete sı	ubfold	ers ar	nd file:	s 🗸	 Image: A set of the set of the	
amulticorp \Administrator	Full Control	\checkmark	~	~	\checkmark	~	\checkmark	÷	•	•	•	v	\mathbf{V}	\checkmark	
adrian \adrian	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
anthony \anthony	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp\brian	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp \carl	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp\chandler	Full Control	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	~	\checkmark	
amulticorp\craig	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp\david	Full Control	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	\checkmark	~	\checkmark	
amulticorp \derek	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp/dominic	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	
amulticorp \edward	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A second s	
amulticorp \Ext_Contractor	Full Control	\checkmark	~	~	\checkmark	~	\checkmark	~	\checkmark	~	~	\checkmark	~	\checkmark	
amulticorp\Gemma	Full Control	\checkmark	~	~	\checkmark	~	\checkmark	~	\checkmark	~	~	\checkmark	~	\checkmark	
nulticorp \glen	Full Control	~	~	~	~	~	~	~	~	~	~	~	~	 Image: A set of the set of the	

Figure 9: User Permissions with Tool Tip

The red ticks show that the user has a permission but **has not** used it in the time period specified in the Days filter.

The blue ticks show that a user has a permission and **has** used it within the time period specified in the Days filter.

Therefore, this example shows that many of the users have permissions that they do not need. This scenario should be avoided as permissions should only be given when a user needs them to do their job. Eliminating unnecessary permissions will mitigate security risks as less users will have access to sensitive data.



Files in Folder : Finance							
Object Name	& 🗟 🕫	Content Type		Compliance		Monetary Value	Risk Level
م			Q		Q		
458673.bmp	ø	Names		GLBA + NPPI		\$ 4225	1495
459565496.bmp	ø	Phone Numbers		GLBA + NPPI		\$ 4875	2925
67949.bmp	ø	Address		GLBA + NPPI		\$ 2688	966
Addresses.txt	ø	Address		GLBA + NPPI		\$ 2925	1755
👔 Client portfolio New.pptx	ø	No Sensitive Content		N/A		N/A	N/A
👔 Client portfolio.pptx	ø	Name + Phone Numbers		GLBA + NPPI		\$ 2518	1811
Confidential.pdf	ø	SSN		GLBA + NPPI		\$ 2472	1512
Customer contact info xlsx	ø	Name + Phone Numbers		GLBA + NPPI		\$ 1591	1244
Customer list.pptx	ø	Names		GLBA + NPPI		\$ 2628	876
Employee list.docx	ø	Names		GLBA + NPPI		\$ 1692	564
Expenses xlsx	ø	SSN + Names		GLBA + NPPI		\$ 2124	708
investments.pptx	ø	SSN		GLBA + NPPI		\$ 1105	459
Legal.txt	ø	SSN		GLBA + NPPI		\$ 2080	864
List 568.txt	ø	Address		GLBA + NPPI		\$ 4225	1755
Passport copies.pdf	ø	SSN		GLBA + NPPI		\$ 3380	1404
Property details.pptx	ø	Phone Number + Affress		GLBA + NPPI		\$ 1133	447
- DAL 10	-1	0.011		01.04 - 10001		* 0700	040

5.2.2. Files Within the Selected Folder

Figure 10: Files in Folder

This section of the screen shows details about the files which are contained within the selected folder. The information here includes the filename, the content type, any compliance regulations the file is needed for, the monetary value and risk level. These can all be configured in the Data Discovery and Classification configuration section.

This Report can then be scheduled, saved or exported.



5.3. The Excessive Permissions by Object Report for SharePoint Online

The steps for running this report are very similar to those described previously for running the report for file servers except that you need to select SharePoint Online from the Component Name filter:

Componer	nt Name Filter	×
Component : Filter Criteria:	SharePoint Online File Server SharePoint Online	•
Sharepoin	t Online	_
lepidesoftv	vare-admin.sharepoint.com	, C
	OK Cancel	

Figure 11: Component Name Filter

- Select the Tenant Name and click **OK** and you will return to the Excessive Permissions by Object screen
- From the top of the screen, under **Days** click to select the number of days to report on.

Days Filter	r		×
Filter Criteria:	30 days	•	
	30 days 60 days 180 days Custom days OK Cancel		

Figure 12: Days Filter

- Click **OK**
- Click Generate Report

The report will run showing the objects in a tree structure:



Lepide Data Security Platform - Edition 23.0.1							- 8 ×
Permission & Privileges 🕅 🛠	Excessive Permissions by Object						Ÿ
Access Governance Dashboard Access Governance Dashboard Access Governance Dashboard Covernitions Analysis Covernition Structure Covernition Structure Covernition Structure Covernition Structure	7 Component Name + 7 Days + 7 Directory +	Component Name EqualTo adminlep- admin.sharepoint.com	Days 30 days				Converte Proved
G Sensitive Data							Generate Report
Classified Files	B adminiep-admin.sharepoint.com						間
Classification Failures	B-O ShashiT1 16Sep22	Object Name		1200	Owner	Last Scan	Last Scan
Email Classification Failures	🕀 👀 ShashiT219Sep22			Q		۹ ۹	<u>م</u> ز
Classified SharePoint Objects	🗄 🛅 Documents	Balance Sheet			FS22112126\Administr	ators 02/28/2023 14:57:38	
SharePoint Objects Classification Failure	🕀 🌇 Form Templates	Finance Manager			FS22112126\Administr	ators 02/28/2023 14:57:38	
Classified OneDrive Objects	e-uu List11	Forecast			FS22112126\Administr	ators 02/28/2023 14:57:38	
Classified Dropher Objects	Reat Lib1	P and L Sheet			FS22112126\Administr	ators 02/28/2023 14:57:38	
Drophox Objects	E Foll1	Statement			LDSP5\NetApp_Admin	02/28/2023 14:57:38	
Sensitive Files by Name	B Root_Lib2	Credit Statement			LDSP5\Sonu	02/28/2023 14:57:38	
S Open Shares	B Site Assets	Loan Upadtes			LDSP5\Sonu	02/28/2023 14:57:38	
- Alert Summary	🕀 🌇 Site Pages	Accounts			LDSP5\Sonu	02/28/2023 14:57:38	
Stale Data Report	B Stide Library	Permissions on Object : h	attps://adminlep.sharepoint.c	om/sites/ShashiTeam	2_21Sep22/List_New1	Files in Object : https://adminlep.sharepoint.org	om/sites/ShashiTeam2_21Sep22/List_N
Users with Administrative Privilege	B SubSite2	Account (Principal)	Effective Permission			Object Name	A Torrent Type Complia
- Password Older than N Days	🖻 🕥 ShashiTeam2_21Sep22					1	Q Q
- No Logon in Last N Days	Documents	David	Limited Access		1 1 1	001Patterns List with Description and Links xl	Aadhar Card + A ALL_Patt
External Data Sharing O365	Form Templates	Michael	Limited Access	11 .	/ /	Aussie Patterns xisx	Italian Driving Lic ALL_Pati
- Open AWS S3 Buckets		Larry	Contribute, Read	111	~	DDC_US Id Resource Directory.pdf	Aadhar Card + A ALL_Patt
All Shares	Site Pages	Vince	Limited Access, Read	1110	/ / /	DSSpolicyclassifier.pdf	Australia Driver's ALL_Patt
	E Style Library	Richard	Limited Access, Read	////	1 1 1	France-TIN.pdf	Australia Driver's ALL_Pati
	Test Doc1					French National ID New.txt	Aadhar Card + B ALL_Patt
	E Test_Doc2					Indian IFSC Code Regex.txt	No Sensitive Con N/A
						Indonesia Driver License REGEX.txt	No Sensitive Con N/A
						Wew_Renamed_Files (1).csv	🚿 Date mmddyyyy f ALL_Pati
						New_Renamed_Files (1).mht	💋 Date mmddyyyy f ALL_Patt
						New_Renamed_Files (1).pdf	💋 Date mmddyyyy f ALL_Patt
						New_Renamed_Files (1).bt	🚿 IPv4 + Italian Dri ALL_Pati
						New_Renamed_Files (2).csv	💋 Date mmddyyyy f ALL_Pati
						New_Renamed_Files (2).mht	💋 Date mmddyyyy f ALL_Patt
						New_Renamed_Files (2).pdf	🚿 Australia Driver's ALL_Patt
< >						Haw Danamad Elas (2) and	Amontina Matiana Al I Date

Figure 13: Excessive Permissions by Object Report for SharePoint Online

5.4. The Excessive Permissions by User Report

This is the second of the two Excessive Permissions Reports. It is showing the same data but based around an individual user rather than an object.

Follow the steps given previously but choose **Excessive Permissions by User**.

As before, select the required component and number of days.

Click **Generate** to run the report:



≡	Permission & Privilege 🤽	Excessive Permissions by User									¥
	Access Governance Dashboard	Access Governance Dashboard 7 Component Name + Component Name Days		Days							
5	Historic Permissions Analysis	Z liser +	ferral la	Custom days							
•	Current Permission Analysis		192 169 20 192	240 dou(c)							
6.0	Permissions by Object	Y Days +	132.100.20.133	240 009(3)							
•	Permissions by User										
æ	Permissions by Mailhoy									Generate Rep	port
	Permissions by OneDrive for B	- 9 multicorp	^								123
	🗄 🔝 Risk Analysis	\$061000-CMJLS7GJQ0VS									
<u> </u>	Excessive Permissions by Obje	- 🐣 adam	Object Name	AB_ 1	Path	Owner	Last Scan	Last Modified		E O C V V	
	- Excessive Permissions by User	💄 admin		Q	م		Q	Q	Q		
er.	E Sensitive Data	Administrator	4 192.168.20.193								
E.	Classification Failures	adrian	A Muticorp		E:\Multicorp	192.168.20.193\Administrators	2/15/2023 9:03:40 PM	3/24/2021 11:14:04 AM		~ ~ ~ ~ ~ ~	
80	Classified Emails	e alan	Education		E:\Multicorp\Education	multicorp \Gemma	2/15/2023 9:03:40 PM	3/23/2021 5:31:36 PM		~~~~	
•	Email Classification Failure		A Financial Servi	ces	E:\Multicorp\Financial Services	multicorp\Paul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM		~~~~	
*	- Classified SharePoint Object	Alexs	Accounts		E:\Multicorp\Financial Services\Acco	multicorp\Paul	7/12/2021 1:26:42 PM	6/23/2021 2:18:57 PM		~~~~	
-		anthony	Clients		E:\Muticorp\Financial Services\Clients	multicorp \Paul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM		~~~~	
8	- Classified OneDrive Object	ben	Enance		E:\Multicorp\Financial Services\Finance	multicorp \Paul	7/12/2021 1:26:42 PM	6/23/2021 5:55:15 PM			
	OneDrive Objects Classificat	Bill	D HR		E: Muticorp \Hnancial Services \HH	muticorp yPaul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM			
•	Classified Dropbox Objects	Lorian			E: Multicorp \Financial Services \1	muticorp Paul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM			
_	Sensitive Files by Name	- C.Ovenden	D Markeong		E: Muticorp Vinancial Services Marke	muticorp (Paul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM			
1	Open Shares	carl	D Sales		E: Muticorp (Hnancial Services (Sales	multicorp (Paul	7/12/2021 1:26:42 PM	3/23/2021 5:31:36 PM			
	- Alert Summary	- 🚨 chandler	D Government		E: Watcorp Government	muticorp (pril	7/12/2021 1:20:42 PM	3/23/2021 5:31:36 PM			
ଛ		- 2 chris	p neatricare		E: Wutcorp (neathcare	muticorp (raul	7/12/2021 1:20:42 PM	3/23/2021 5:31:37 PM			
	- Activity Outside of Business He	🛁 craig	Technology		E. Midlicorp (Degel	maticop lagan	7/12/2021 1/20/42 PM	2/22/2021 5:31:37 PM			
	Users with Administrative Privi	daniel	P Gornougy		E. Matcolp (Technology	indecolp ben	1/12/2021 1.20/42 FM	3/23/2021 3.31.37 FM		~ ~ ~ ~ ~	
	No Logon In Last N Days	Adavid									
	External Data Sharing 0365	- A DefaultAccount	Name		Content Tune	Compliance	Monstery Volum Dick Lovel				•
		💄 derek		0	Bi by conservation	0	0 0	0			
	- All Shares	A dominic	3 459672 https	~	Names	CI PA + NPPI	\$ 4225	1495			- 1
		. edward	459565496 hmp		Choce Numbers	GLDA + NPPI	¢ 4975	2925			
		e omiki	 67949 bmp 		Address	GLBA + NPPI	\$ 2688	966			
		• End Contraction	Addresses by		Address	GLBA + NPPI	\$ 2925	1755			
		Excontractor	Client potfolio New pot	ĸ	So Senaitive Content	N/A	N/A	N/A			
		Gemma	Cient potfolio potx		Some + Phone Numbers	GLBA + NPPI	\$ 2518	1811			
		Geott	Confidential pdf		SSN SSN	GLBA + NPPI	\$ 2472	1512			
		glen	Customer contact info	iex	S Name + Phone Numbers	GLBA + NPPI	\$ 1591	1244			
		Guest	Customer list potx		🧭 Names	GLBA + NPPI	\$ 2628	876			
		gwen	Employee list.docx		Names	GLBA + NPPI	\$ 1692	564			
		- HealthMailbox11cb852	Expenses xisx		SSN + Names	GLBA + NPPI	\$ 2124	708			
		- 🚨 HealthMailbox1757d7b	Investments.pptx		🚿 SSN	GLBA + NPPI	\$ 1105	459			
		LealthMailbox189d97f	Egal.bt		🚿 SSN	GLBA + NPPI	\$ 2080	864			
		HealthMailbox1babc10	List 568.txt		🚿 Address	GLBA + NPPI	\$ 4225	1755			
		HealthMailbox24f1142	Passport copies.pdf		🚿 SSN	GLBA + NPPI	\$ 3380	1404			
		HealthMailbox2d44be1	Property details.pptx		Phone Number + Affress	GLBA + NPPI	\$ 1133	447			
		HealthMailbox54a778b	RXV.pdf		🚿 SSN	GLBA + NPPI	\$ 2736	912			
	,		Y (1000 🐴 Y		≪ CCM	CI BA I MPDI	e 37/11	516			

Figure 14: Excessive Permissions by User Report

This example has the user named Gemma selected. It shows the objects, folder contents and permissions for Gemma. Clicking on a different username will show information related to that user.

The report can be scheduled, saved or exported.



6.Support

If you are facing any issues whilst installing, configuring or using the solution, you can connect with our team using the below contact information.

Product Experts

USA/Canada: +1(0)-800-814-0578 UK/Europe: +44 (0) -208-099-5403 Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578 UK/Europe: +44 (0) -208-099-5403 Rest of the World: +91(0)-991-085-4291

Alternatively, visit <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/.

7.Trademarks

Lepide Data Security Platform, Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform for 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.

