Lepide

How to use Lepide to identify users with excessive privileges to sensitive data.

Use case guide.

Contents

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 second section 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.

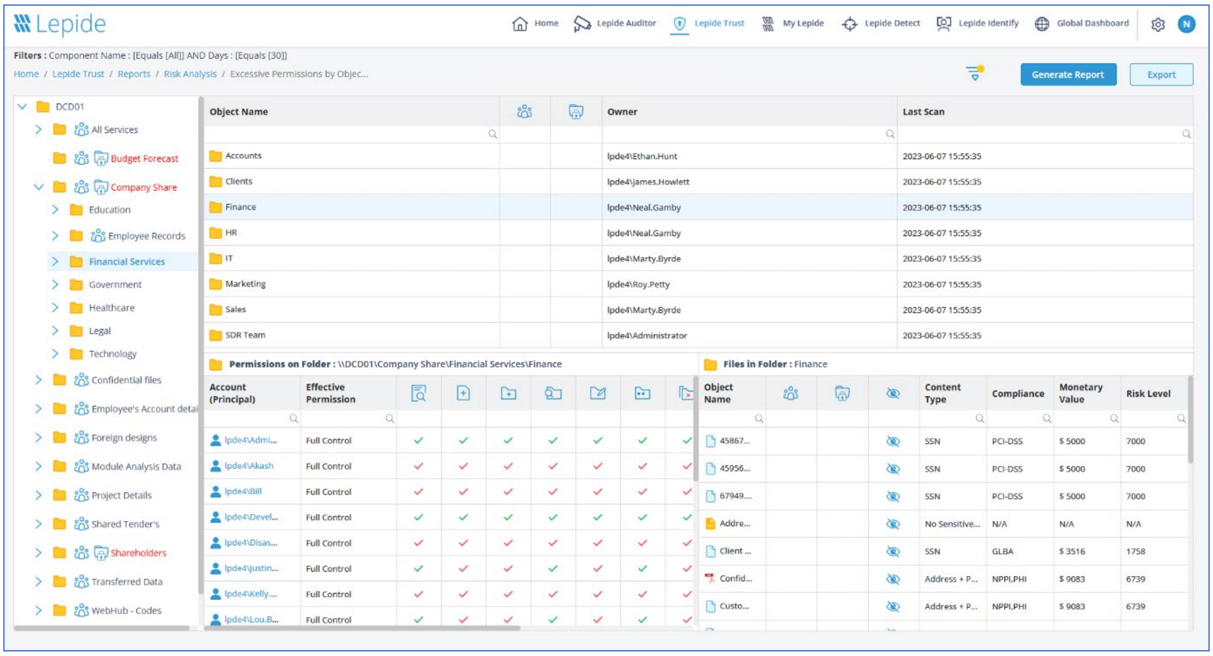
4. The Solution

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. They are shown below and explained in detail in Section 5.

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



Filters : Component Name : [Equals [All]] AND Days : [Equals [30]]

Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by Objec...

DCD01
All Services
Budget Forecast
Company Share
Education
Employee Records
Financial Services
Government
Healthcare
Legal
Technology
Confidential files
Employee's Account detai
Foreign designs
Module Analysis Data
Project Details
Shared Tender's
Shareholders
Transferred Data
WebHub - Codes

Object Name			Owner	Last Scan
Accounts			lpde4\Ethan.Hunt	2023-06-07 15:55:35
Clients			lpde4\James.Howlett	2023-06-07 15:55:35
Finance			lpde4\Neal.Gamby	2023-06-07 15:55:35
HR			lpde4\Neal.Gamby	2023-06-07 15:55:35
IT			lpde4\Marty.Byrde	2023-06-07 15:55:35
Marketing			lpde4\Roy.Petty	2023-06-07 15:55:35
Sales			lpde4\Marty.Byrde	2023-06-07 15:55:35
SDR Team			lpde4\Administrator	2023-06-07 15:55:35

Permissions on Folder : \\DCD01\Company Share\Financial Services\Finance

Account (Principal)	Effective Permission							
lpde4\Admi...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Akash	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Bill	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Devel...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Disas...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Justin...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Kelly....	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Lou.B...	Full Control	✓	✓	✓	✓	✓	✓	✓

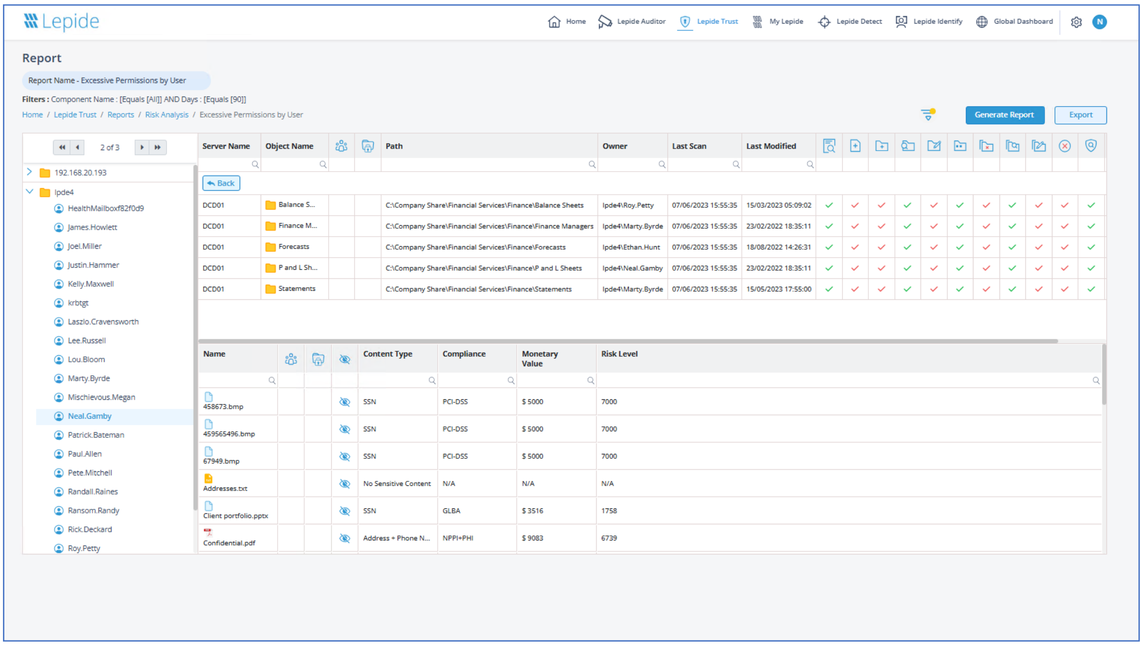
Files in Folder : Finance

Object Name				Content Type	Compliance	Monetary Value	Risk Level
45867...				SSN	PCI-DSS	$ 5000	7000
45956...				SSN	PCI-DSS	$ 5000	7000
67949....				SSN	PCI-DSS	$ 5000	7000
Addre...				No Sensitive...	N/A	N/A	N/A
Client ...				SSN	GLBA	$ 3516	1758
Confid...				Address + P...	NPPI,PHI	$ 9083	6739
Custo...				Address + P...	NPPI,PHI	$ 9083	6739

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:



Report

Report Name - Excessive Permissions by User

Filters : Component Name : [Equals [All]] AND Days : [Equals [90]]

Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by User

- 192.168.20.193
- lpde4
  - HealthMailboxf82f0d9
  - James.Howlett
  - Joel.Miller
  - Justin.Hammer
  - Kelly.Maxwell
  - krbtgt
  - Laszlo.Cravensworth
  - Lee.Russell
  - Lou.Bloom
  - Marty.Byrde
  - Mischievous.Megan
  - Neal.Gamby
  - Patrick.Bateman
  - Paul.Allen
  - Pete.Mitchell
  - Randall.Raines
  - Ransom.Randy
  - Rick.Deckard
  - Roy.Petty

Server Name	Object Name			Path	Owner	Last Scan	Last Modified											
DCD01	Balance S...			C:\Company Share\Financial Services\Finance\Balance Sheets	lpde4\Roy.Petty	07/06/2023 15:55:35	15/03/2023 05:09:02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Finance M...			C:\Company Share\Financial Services\Finance\Finance Managers	lpde4\Marty.Byrde	07/06/2023 15:55:35	23/02/2022 18:35:11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Forecasts			C:\Company Share\Financial Services\Finance\Forecasts	lpde4\Ethan.Hunt	07/06/2023 15:55:35	18/08/2022 14:26:31	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	P and L Sh...			C:\Company Share\Financial Services\Finance\P and L Sheets	lpde4\Neal.Gamby	07/06/2023 15:55:35	23/02/2022 18:35:11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Statements			C:\Company Share\Financial Services\Finance\Statements	lpde4\Marty.Byrde	07/06/2023 15:55:35	15/05/2023 17:55:00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name				Content Type	Compliance	Monetary Value	Risk Level
458673.bmp				SSN	PCI-DSS	$ 5000	7000
459565496.bmp				SSN	PCI-DSS	$ 5000	7000
67949.bmp				SSN	PCI-DSS	$ 5000	7000
Addresses.txt				No Sensitive Content	N/A	N/A	N/A
Client portfolio.pptx				SSN	GLBA	$ 3516	1758
Confidential.pdf				Address + Phone N...	NPPI+PHI	$ 9083	6739

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. The Excessive Permissions Reports

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

5.2 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:

- From the Web Console Home screen, choose **Lepide Trust**
- From the **Lepide Trust** Menu at the top of the screen, choose **Reports**

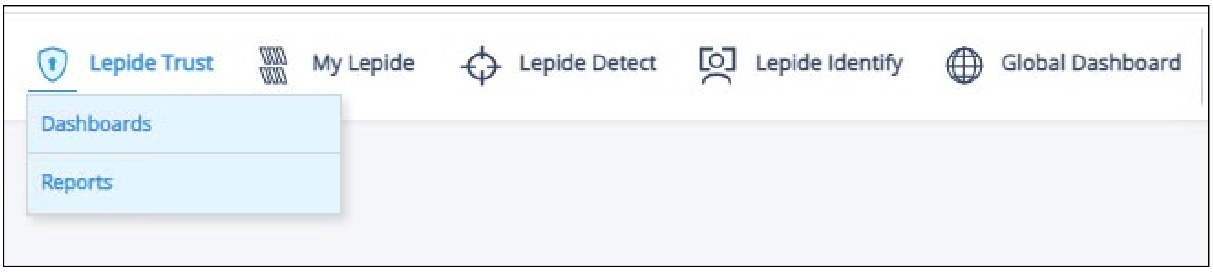


Figure 3: Lepide Trust Reports Menu

From the tree structure to the left side of the screen, expand Risk Analysis to see the Excessive Permissions by Object Report:

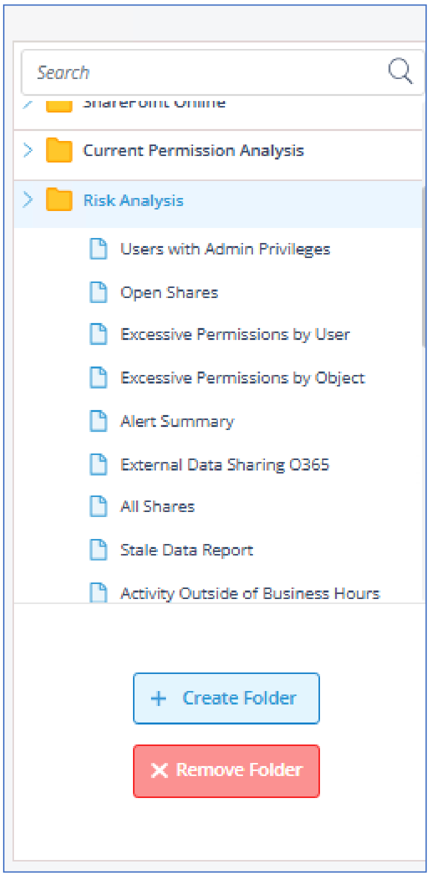
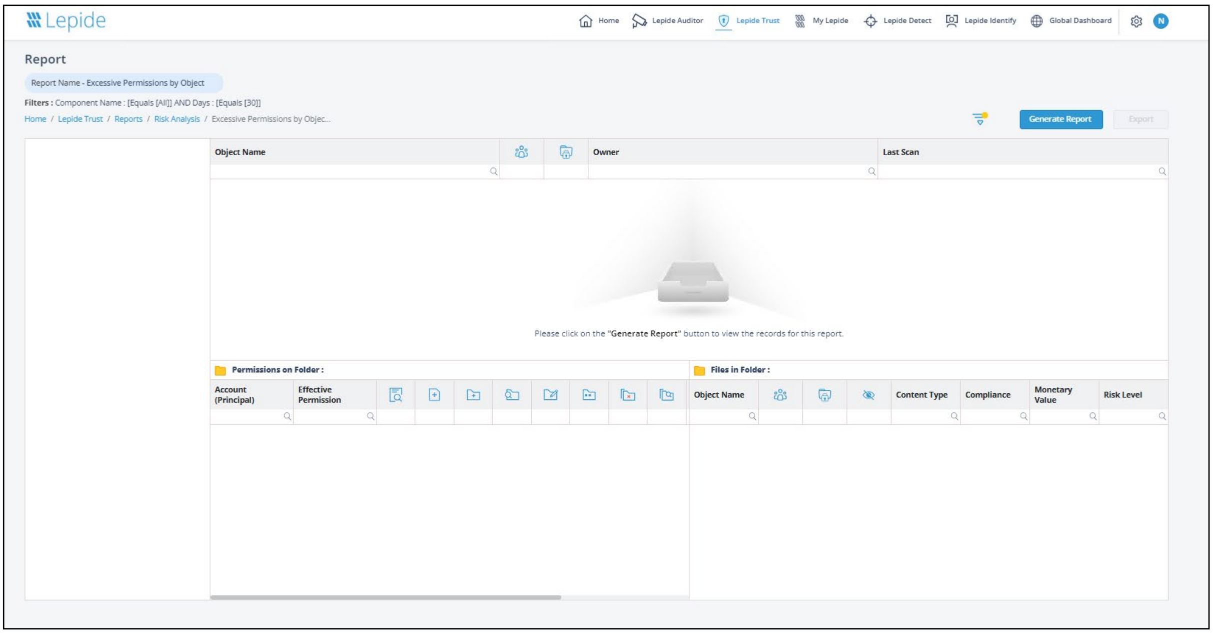

Search
SharePoint Online
Current Permission Analysis
Risk Analysis
Users with Admin Privileges
Open Shares
Excessive Permissions by User
Excessive Permissions by Object
Alert Summary
External Data Sharing O365
All Shares
Stale Data Report
Activity Outside of Business Hours
Create Folder
Remove Folder

Figure 4: Tree Structure showing Risk Analysis Reports

- Click on the Excessive Permissions by Object Report from the tree structure

The empty Excessive Permissions by Object Report is displayed:



Report

Report Name - Excessive Permissions by Object

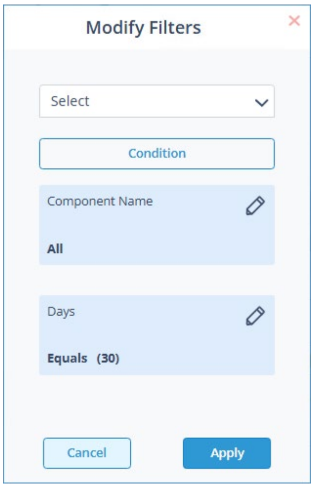
Filters : Component Name : [Equals [All]] AND Days : [Equals [30]]

Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by Objec...

Please click on the "**Generate Report**" button to view the records for this report.

Figure 5: Excessive Permissions by Object Report

- From the top of the screen, click the Filter icon
- The following dialog box is displayed:



Component Name

All

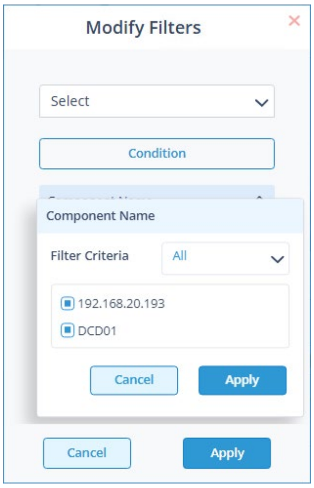
Days

Equals (30)

Figure 6: Modify Filters

- Here you can select **Component Name** and the number of **Days**

- Click the edit filter icon ✎ next to **Component Name** and then select the required File Server from the list



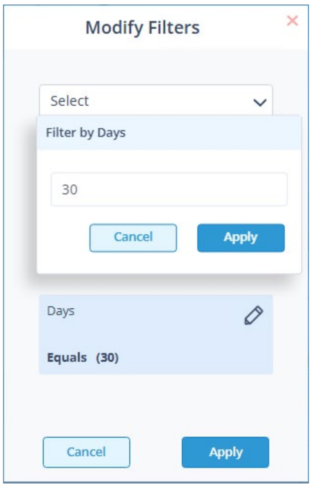
Filter Criteria: All

☒ 192.168.20.193

☒ DCD01

Figure 7: Component Name

- Click **Apply** when finished
- From the Modify Filters dialog box, click to edit the **Days** filter
- The Filter by Days dialog box is displayed:



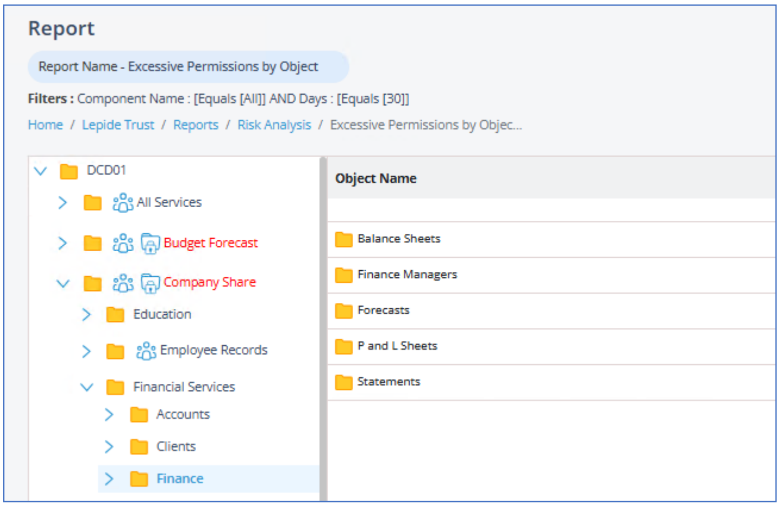
30

Equals (30)

Figure 8: Days Filter

- Specify the number of days as required and click **Apply** when finished
- Click **Apply** to return to the report
- Click **Generate Report**

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



Report

Report Name - Excessive Permissions by Object

Filters : Component Name : [Equals [All]] AND Days : [Equals [30]]

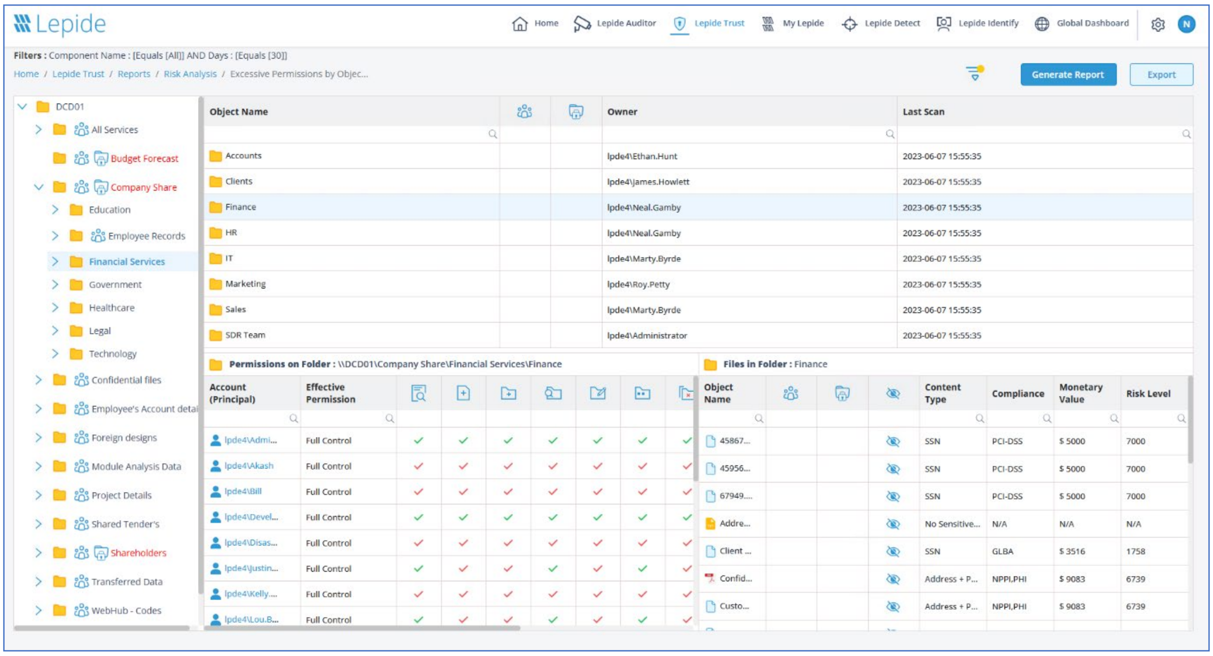
Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by Objec...

- DCD01
  - All Services
  - Budget Forecast
  - Company Share
    - Education
    - Employee Records
    - Financial Services
      - Accounts
      - Clients
      - Finance

Object Name
Balance Sheets
Finance Managers
Forecasts
P and L Sheets
Statements

Figure 9: Object List

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



Filters : Component Name : [Equals [All]] AND Days : [Equals [30]]

Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by Objec...

- DCD01
  - All Services
  - Budget Forecast
  - Company Share
    - Education
    - Employee Records
    - Financial Services
    - Government
    - Healthcare
    - Legal
    - Technology
  - Confidential files
  - Employee's Account detai
  - Foreign designs
  - Module Analysis Data
  - Project Details
  - Shared Tender's
  - Shareholders
  - Transferred Data
  - WebHub - Codes

Object Name			Owner	Last Scan
Accounts			lpde4\Ethan.Hunt	2023-06-07 15:55:35
Clients			lpde4\James.Howlett	2023-06-07 15:55:35
Finance			lpde4\Neal.Gamby	2023-06-07 15:55:35
HR			lpde4\Neal.Gamby	2023-06-07 15:55:35
IT			lpde4\Marty.Byrde	2023-06-07 15:55:35
Marketing			lpde4\Roy.Petty	2023-06-07 15:55:35
Sales			lpde4\Marty.Byrde	2023-06-07 15:55:35
SDR Team			lpde4\Administrator	2023-06-07 15:55:35

Permissions on Folder : \\DCD01\Company Share\Financial Services\Finance

Account (Principal)	Effective Permission							
lpde4\Admi...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Akash	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Bill	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Devel...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Disas...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Justin...	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Kelly....	Full Control	✓	✓	✓	✓	✓	✓	✓
lpde4\Lou.B...	Full Control	✓	✓	✓	✓	✓	✓	✓

Files in Folder : Finance

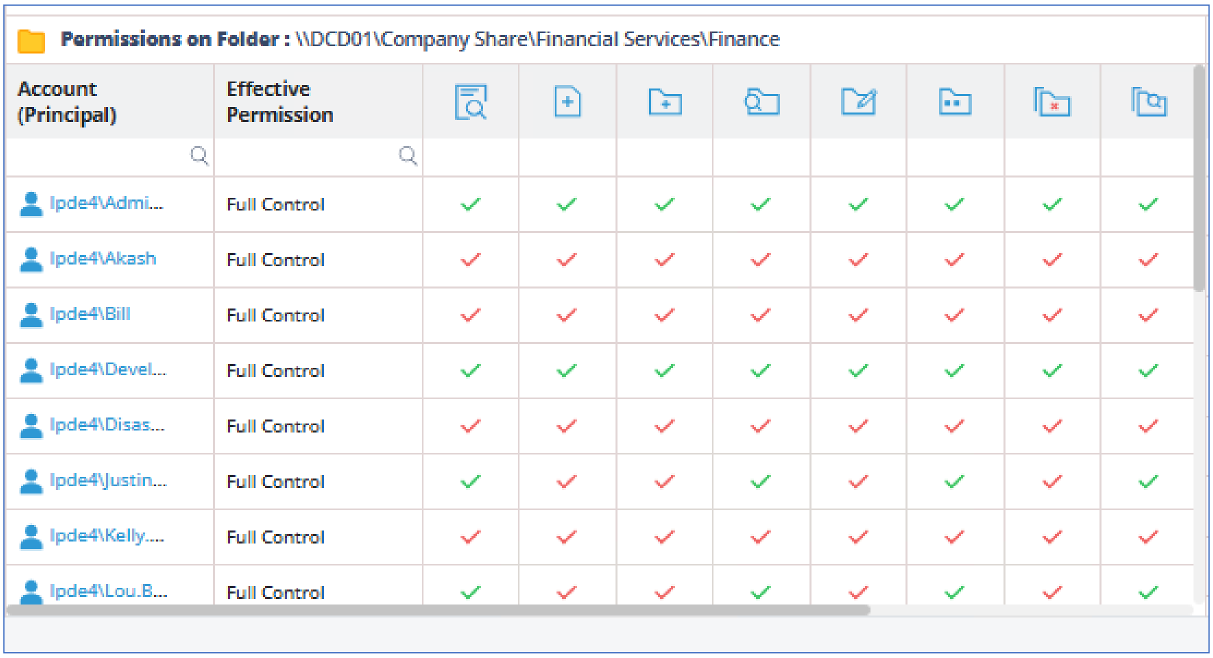
Object Name				Content Type	Compliance	Monetary Value	Risk Level
45867...				SSN	PCI-DSS	$ 5000	7000
45956...				SSN	PCI-DSS	$ 5000	7000
67949....				SSN	PCI-DSS	$ 5000	7000
Addre...				No Sensitive...	N/A	N/A	N/A
Client ...				SSN	GLBA	$ 3516	1758
Confid...				Address + P...	NPPI,PHI	$ 9083	6739
Custo...				Address + P...	NPPI,PHI	$ 9083	6739

Figure 10: Excessive Permissions by Object Report

The example above shows the **Finance** folder has been selected. Users within the **Finance** folder are then listed along with their permissions 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:



Permissions on Folder : \\DCD01\Company Share\Financial Services\Finance

Account (Principal)	Effective Permission								
lpde4\Admi...	Full Control	✅	✅	✅	✅	✅	✅	✅	✅
lpde4\Akash	Full Control	✓	✓	✓	✓	✓	✓	✓	✓
lpde4\Bill	Full Control	✓	✓	✓	✓	✓	✓	✓	✓
lpde4\Devel...	Full Control	✅	✅	✅	✅	✅	✅	✅	✅
lpde4\Disas...	Full Control	✓	✓	✓	✓	✓	✓	✓	✓
lpde4\Justin...	Full Control	✅	✓	✓	✅	✓	✅	✓	✅
lpde4\Kelly....	Full Control	✓	✓	✓	✓	✓	✓	✓	✓
lpde4\Lou.B...	Full Control	✅	✓	✓	✅	✓	✅	✓	✅

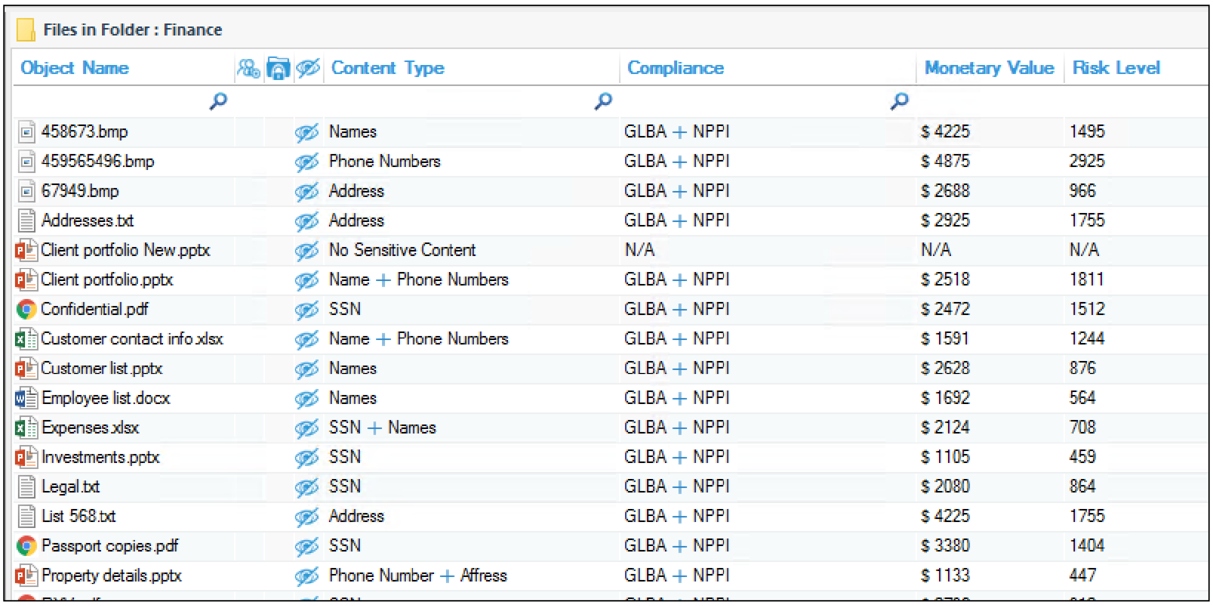
Figure 11: User Permissions

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 green 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.

5.2.2 Files within the Selected Folder



Files in Folder : Finance

Object Name	Content Type	Compliance	Monetary Value	Risk Level
458673.bmp	Names	GLBA + NPPI	$ 4225	1495
459565496.bmp	Phone Numbers	GLBA + NPPI	$ 4875	2925
67949.bmp	Address	GLBA + NPPI	$ 2688	966
Addresses.txt	Address	GLBA + NPPI	$ 2925	1755
Client portfolio New.pptx	No Sensitive Content	N/A	N/A	N/A
Client portfolio.pptx	Name + Phone Numbers	GLBA + NPPI	$ 2518	1811
Confidential.pdf	SSN	GLBA + NPPI	$ 2472	1512
Customer contact info.xlsx	Name + Phone Numbers	GLBA + NPPI	$ 1591	1244
Customer list.pptx	Names	GLBA + NPPI	$ 2628	876
Employee list.docx	Names	GLBA + NPPI	$ 1692	564
Expenses.xlsx	SSN + Names	GLBA + NPPI	$ 2124	708
Investments.pptx	SSN	GLBA + NPPI	$ 1105	459
Legal.txt	SSN	GLBA + NPPI	$ 2080	864
List 568.txt	Address	GLBA + NPPI	$ 4225	1755
Passport copies.pdf	SSN	GLBA + NPPI	$ 3380	1404
Property details.pptx	Phone Number + Affress	GLBA + NPPI	$ 1133	447

Figure 12: 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.

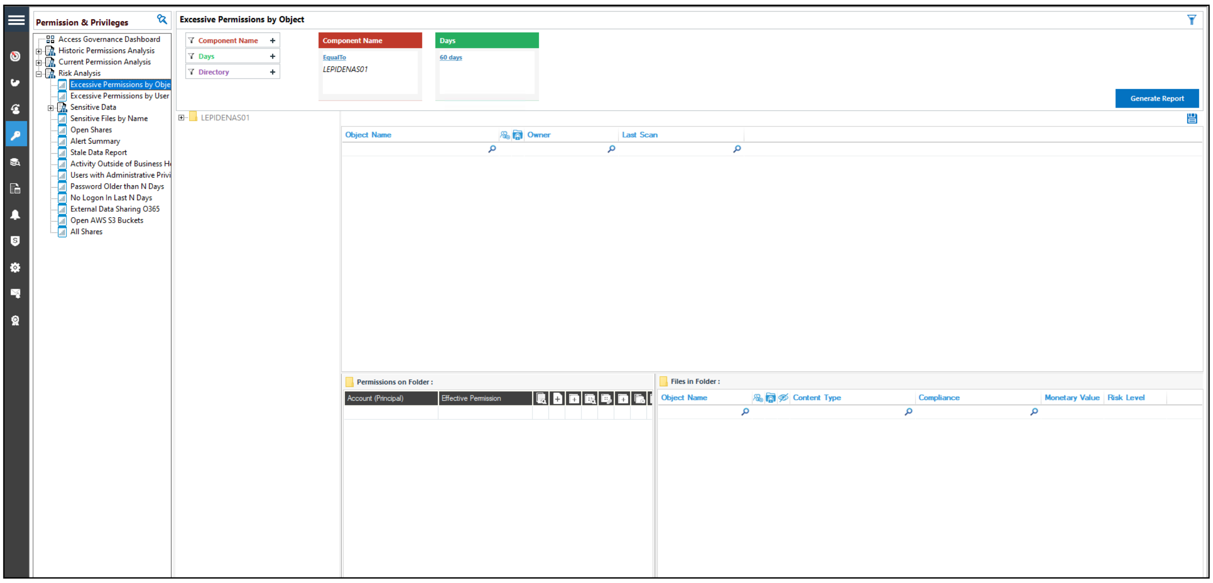
This Report can then be scheduled, saved or exported.

5.3 Excessive Permissions by Object Report for SharePoint Online

Running the Excessive Permissions Reports for SharePoint Online needs to be done using the Lepide Data Security Platform Legacy Console and the steps for running it are as follows:

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

From the icons to the left-hand side of the screen, click the **Permissions and Privileges** icon and the following screen will be displayed:



Component Name: EqualTo LEPIDENAS01

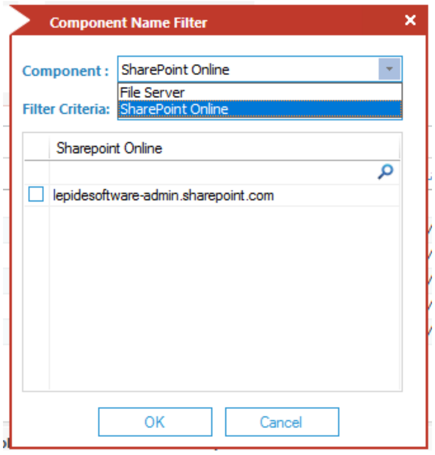
Days: 60 days

Figure 13: 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**



Component : SharePoint Online

Filter Criteria:

☐ lepidesoftware-admin.sharepoint.com

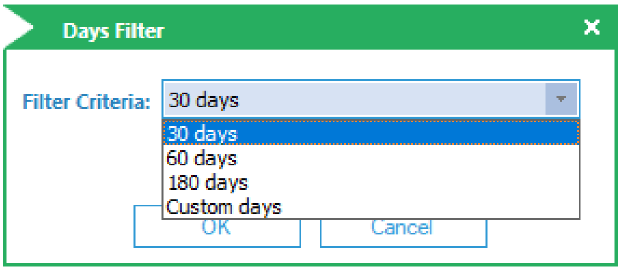
Figure 14: Component Name Filter

Select **SharePoint Online** from the Component drop down menu

Select the **Tenant Name** from the list and click **OK.**

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



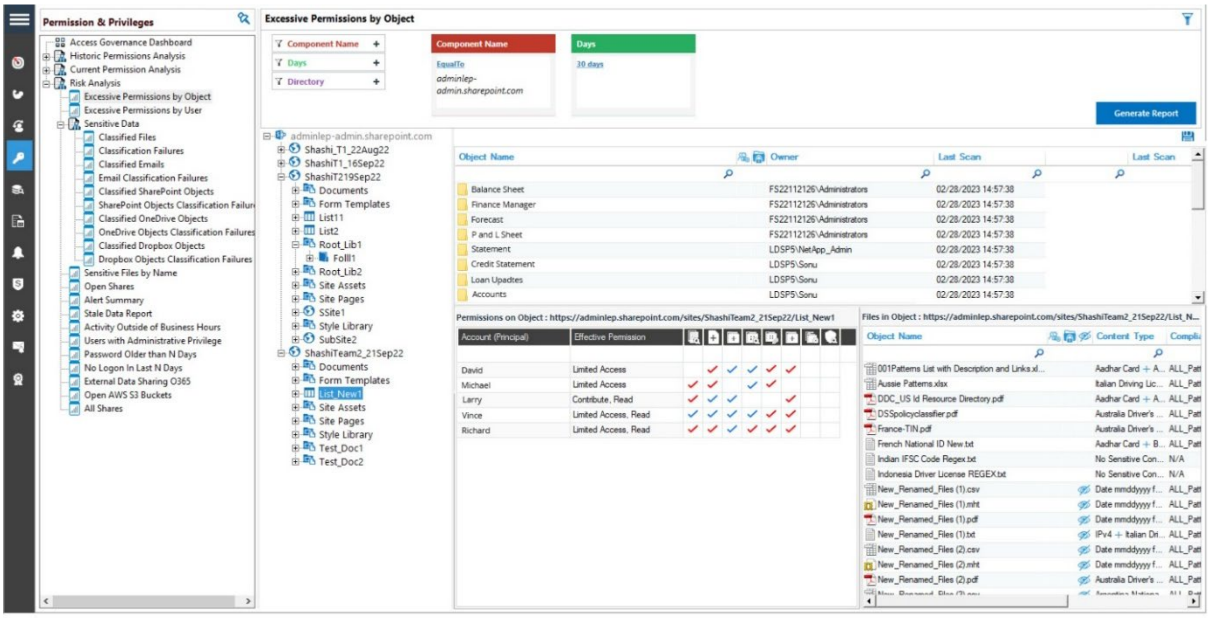
Filter Criteria: 30 days

Figure 15: Days Filter

Click **OK**

Click **Generate Report**

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


Permission & Privileges
Access Governance Dashboard
Historic Permissions Analysis
Current Permission Analysis
Risk Analysis
Excessive Permissions by Object
Excessive Permissions by User
Sensitive Data
Classified Files
Classification Failures
Classified Emails
Email Classification Failures
Classified SharePoint Objects
SharePoint Objects Classification Failur
Classified OneDrive Objects
OneDrive Objects Classification Failures
Classified Dropbox Objects
Dropbox Objects Classification Failures
Sensitive Files by Name
Open Shares
Alert Summary
Stale Data Report
Activity Outside of Business Hours
Users with Administrative Privilege
Password Older than N Days
No Logon In Last N Days
External Data Sharing O365
Open AWS S3 Buckets
All Shares
Excessive Permissions by Object
Component Name
Days
Directory
adminlep-admin.sharepoint.com
Shashi_T1_22Aug22
ShashiT1_16Sep22
ShashiT219Sep22
Documents
Form Templates
List11
List2
Root_Lib1
Folll1
Root_Lib2
Site Assets
Site Pages
SSite1
Style Library
SubSite2
ShashiTeam2_21Sep22
Documents
Form Templates
List_New1
Site Assets
Site Pages
Style Library
Test_Doc1
Test_Doc2
Generate Report

Component Name: EqualTo adminlep-admin.sharepoint.com

Days: 30 days

Object Name	Owner	Last Scan	Last Scan
Balance Sheet	FS22112126\Administrators	02/28/2023 14:57:38	
Finance Manager	FS22112126\Administrators	02/28/2023 14:57:38	
Forecast	FS22112126\Administrators	02/28/2023 14:57:38	
P and L Sheet	FS22112126\Administrators	02/28/2023 14:57:38	
Statement	LDSP5\NetApp_Admin	02/28/2023 14:57:38	
Credit Statement	LDSP5\Sonu	02/28/2023 14:57:38	
Loan Upadtes	LDSP5\Sonu	02/28/2023 14:57:38	
Accounts	LDSP5\Sonu	02/28/2023 14:57:38	

Permissions on Object : https://adminlep.sharepoint.com/sites/ShashiTeam2_21Sep22/List_New1

Account (Principal)	Effective Permission								
David	Limited Access		✓	✓	✓	✓	✓		
Michael	Limited Access	✓	✓		✓	✓			
Larry	Contribute, Read	✓	✓	✓			✓		
Vince	Limited Access, Read	✓	✓	✓	✓	✓	✓		
Richard	Limited Access, Read	✓	✓	✓	✓	✓	✓		

Files in Object : https://adminlep.sharepoint.com/sites/ShashiTeam2_21Sep22/List_N...

Object Name	Content Type	Complia
001Patterns List with Description and Links.xl...	Aadhar Card + A...	ALL_Patt
Aussie Patterns.xlsx	Italian Driving Lic...	ALL_Patt
DDC_US Id Resource Directory.pdf	Aadhar Card + A...	ALL_Patt
DSSpolicyclassifier.pdf	Australia Driver's ...	ALL_Patt
France-TIN.pdf	Australia Driver's ...	ALL_Patt
French National ID New.txt	Aadhar Card + B...	ALL_Patt
Indian IFSC Code Regex.txt	No Sensitive Con...	N/A
Indonesia Driver License REGEX.txt	No Sensitive Con...	N/A
New_Renamed_Files (1).csv	Date mmddyyyy f...	ALL_Patt
New_Renamed_Files (1).mht	Date mmddyyyy f...	ALL_Patt
New_Renamed_Files (1).pdf	Date mmddyyyy f...	ALL_Patt
New_Renamed_Files (1).txt	IPv4 + Italian Dri...	ALL_Patt
New_Renamed_Files (2).csv	Date mmddyyyy f...	ALL_Patt
New_Renamed_Files (2).mht	Date mmddyyyy f...	ALL_Patt
New_Renamed_Files (2).pdf	Australia Driver's ...	ALL_Patt

Figure 16: Excessive Permissions by Object Report for SharePoint Online

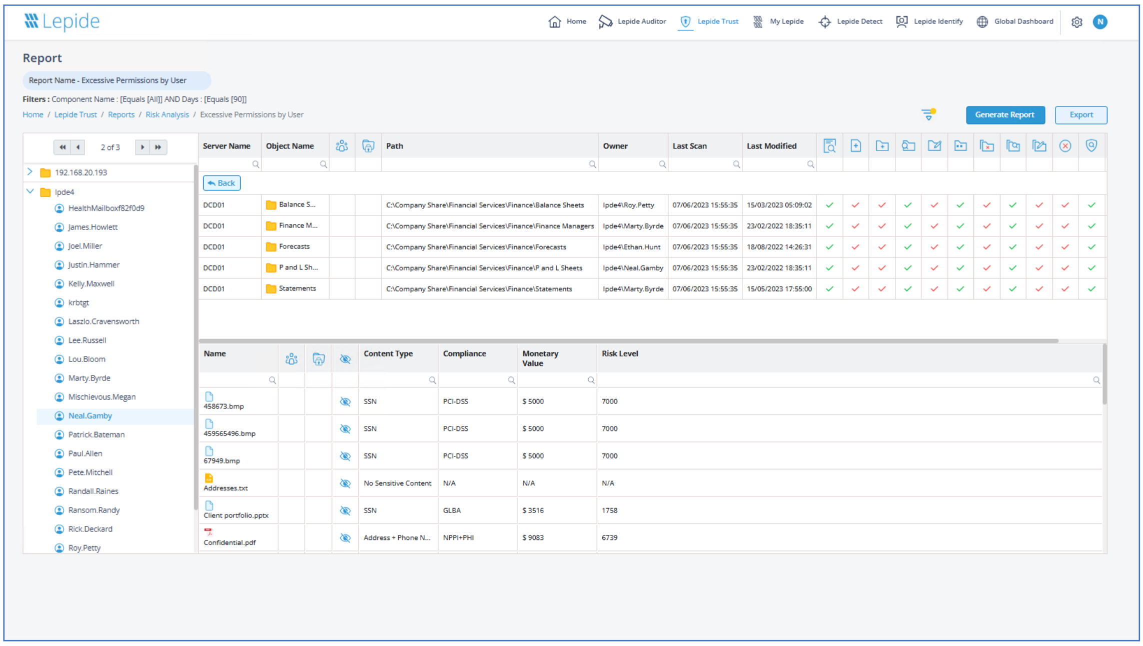
5.4 The Excessive Permissions by User Report

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 Report** to run the report:



Report

Report Name - Excessive Permissions by User

Filters : Component Name : [Equals [All]] AND Days : [Equals [90]]

Home / Lepide Trust / Reports / Risk Analysis / Excessive Permissions by User

- 192.168.20.193
- lpde4
  - HealthMailboxf82f0d9
  - James.Howlett
  - Joel.Miller
  - Justin.Hammer
  - Kelly.Maxwell
  - krbtgt
  - Laszlo.Cravensworth
  - Lee.Russell
  - Lou.Bloom
  - Marty.Byrde
  - Mischievous.Megan
  - Neal.Gamby
  - Patrick.Bateman
  - Paul.Allen
  - Pete.Mitchell
  - Randall.Raines
  - Ransom.Randy
  - Rick.Deckard
  - Roy.Petty

Server Name	Object Name			Path	Owner	Last Scan	Last Modified											
DCD01	Balance S...			C:\Company Share\Financial Services\Finance\Balance Sheets	lpde4\Roy.Petty	07/06/2023 15:55:35	15/03/2023 05:09:02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Finance M...			C:\Company Share\Financial Services\Finance\Finance Managers	lpde4\Marty.Byrde	07/06/2023 15:55:35	23/02/2022 18:35:11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Forecasts			C:\Company Share\Financial Services\Finance\Forecasts	lpde4\Ethan.Hunt	07/06/2023 15:55:35	18/08/2022 14:26:31	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	P and L Sh...			C:\Company Share\Financial Services\Finance\P and L Sheets	lpde4\Neal.Gamby	07/06/2023 15:55:35	23/02/2022 18:35:11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DCD01	Statements			C:\Company Share\Financial Services\Finance\Statements	lpde4\Marty.Byrde	07/06/2023 15:55:35	15/05/2023 17:55:00	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Name				Content Type	Compliance	Monetary Value	Risk Level
458673.bmp				SSN	PCI-DSS	$ 5000	7000
459565496.bmp				SSN	PCI-DSS	$ 5000	7000
67949.bmp				SSN	PCI-DSS	$ 5000	7000
Addresses.txt				No Sensitive Content	N/A	N/A	N/A
Client portfolio.pptx				SSN	GLBA	$ 3516	1758
Confidential.pdf				Address + Phone N...	NPPI+PHI	$ 9083	6739

Figure 17: Excessive Permissions by User Report

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

The report can be scheduled, saved or exported.

Support

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

Product Experts

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

Rest of the World: +91 (0) -991-004-9028

Technical Gurus

USA/Canada: +1(0)-800-814-0578

UK/Europe: +44 (0) -208-099-5403

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

Alternatively, visit https://www.lepide.com/contactus.html to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit https://www.lepide.com/data-security-platform/.

Trademarks

Lepide Data Security Platform, Lepide Data Security Platform, Lepide Data Security Platform App, Lepide Data Security Platform App Server, Lepide Data Security Platform (Web Console), Lepide Data Security Platform Logon/Logoff Audit Module, Lepide Data Security Platform for Active Directory, Lepide Data Security Platform for Group Policy Object, Lepide Data Security Platform for Exchange Server, Lepide Data Security Platform for SQL Server, Lepide Data Security Platform SharePoint, Lepide Object Restore Wizard, Lepide Active Directory Cleaner, Lepide User Password Expiration Reminder, and LiveFeed are registered trademarks of Lepide Software Pvt Ltd.

All other brand names, product names, logos, registered marks, service marks and trademarks (except above of Lepide Software Pvt. Ltd.) appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only.