Lepide

USE CASE GUIDE

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

Table of 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.

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

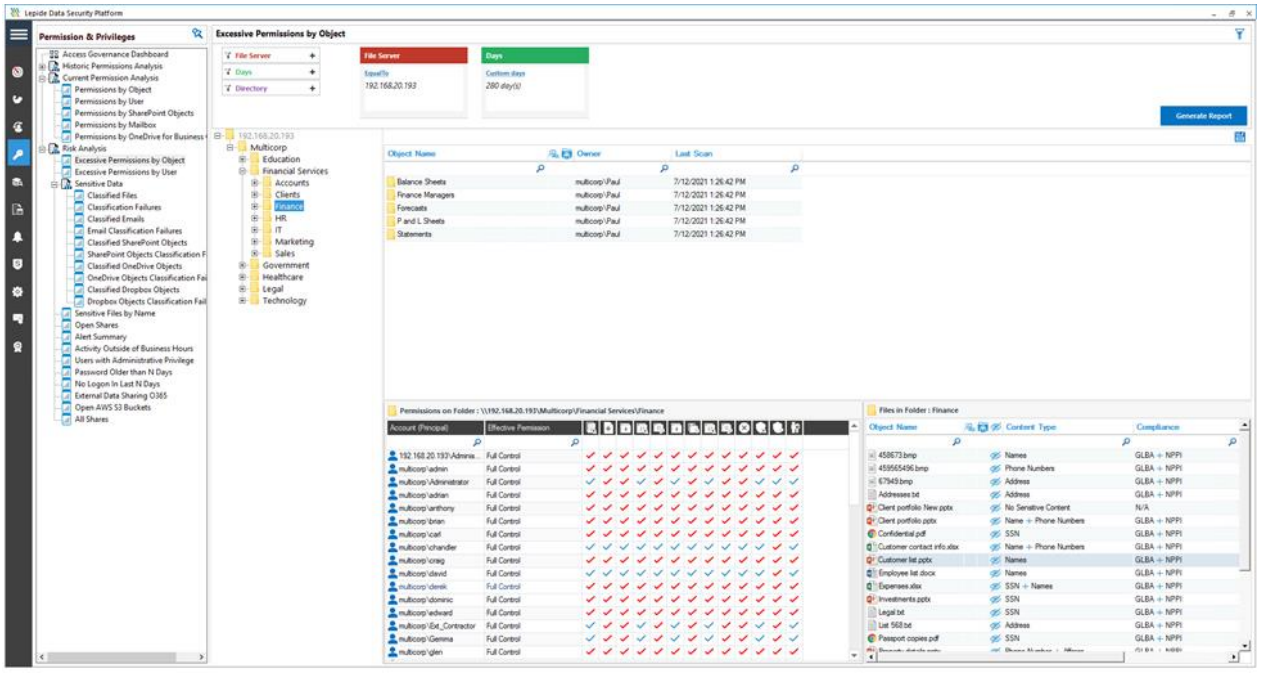

Figure 1: Excessive Permissions by Object Report

This report shows the following:

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:

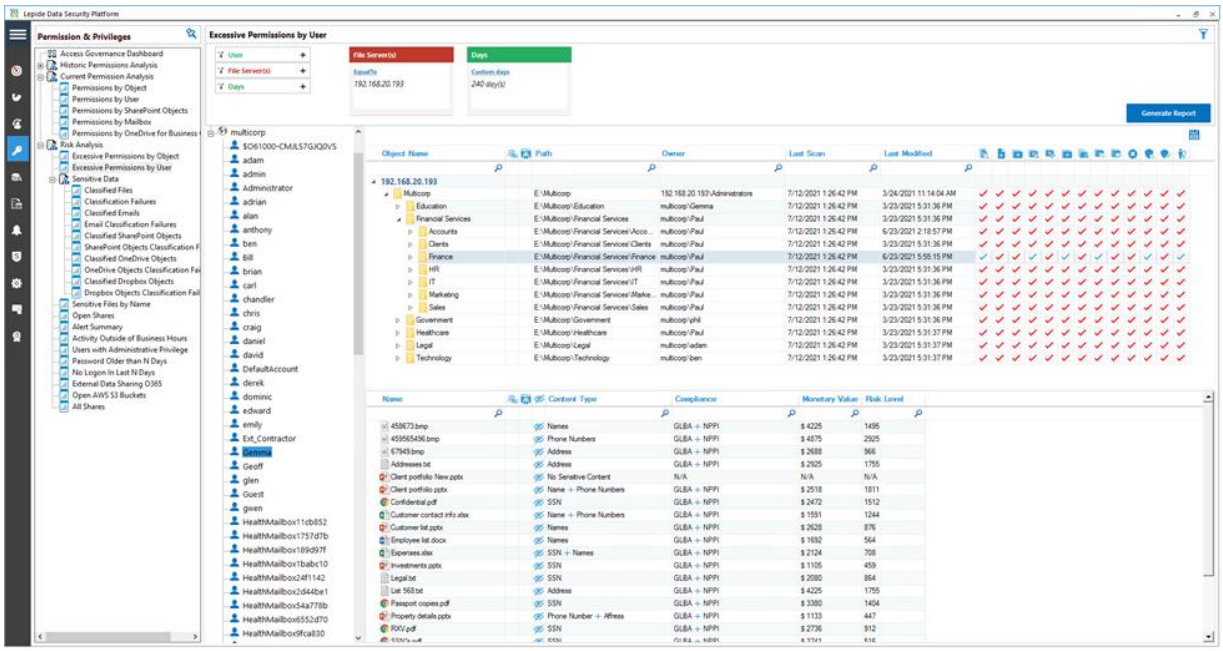

Figure 2: Excessive Permissions by User Report

This report shows the following:

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.

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
- To have enabled Data Discovery and Classification and run an initial scan.
- To have run an initial permissions scan

5.2. Running the Excessive Permissions by Object Report

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:

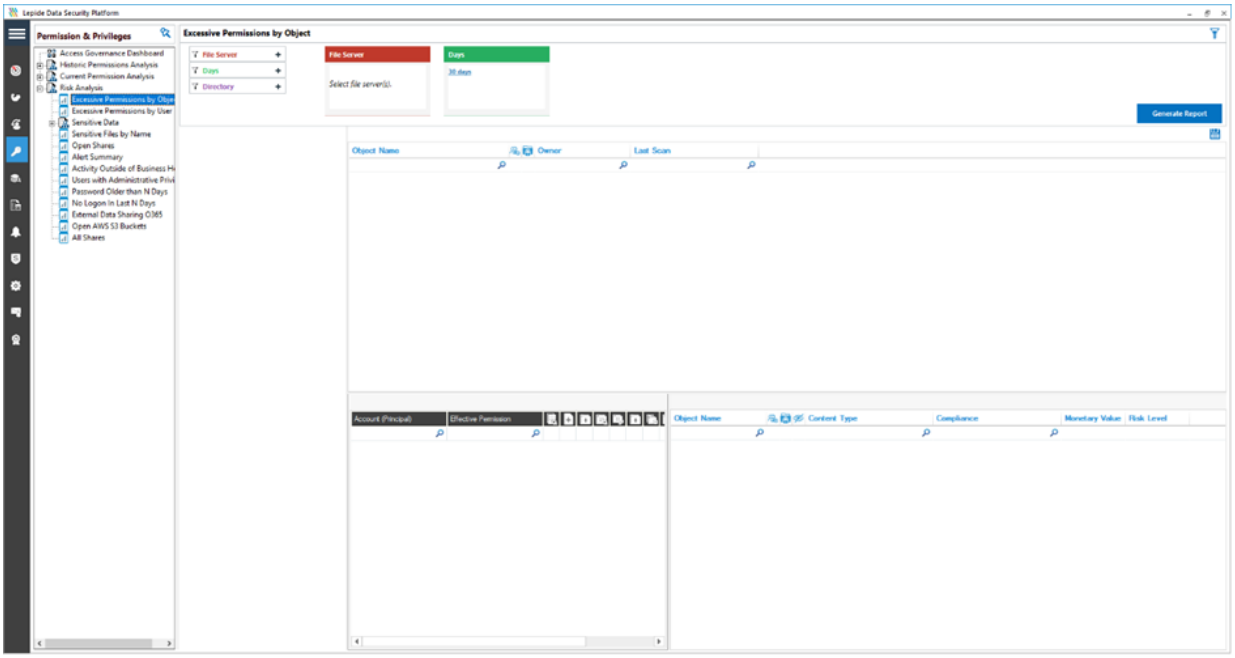

Figure 3: Permissions and Privileges

- 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 File Server click Select File Server(s):.

The following dialog box is displayed:

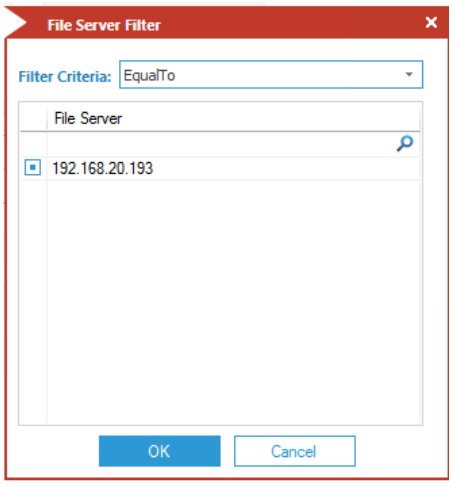

Figure 4: File Server Filter

- 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.

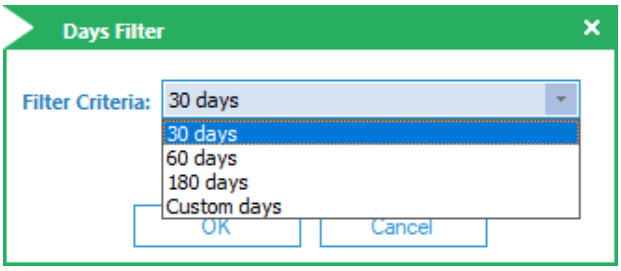

Figure 5: Days Filter

- Click **OK**
- Click **Generate Report**

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

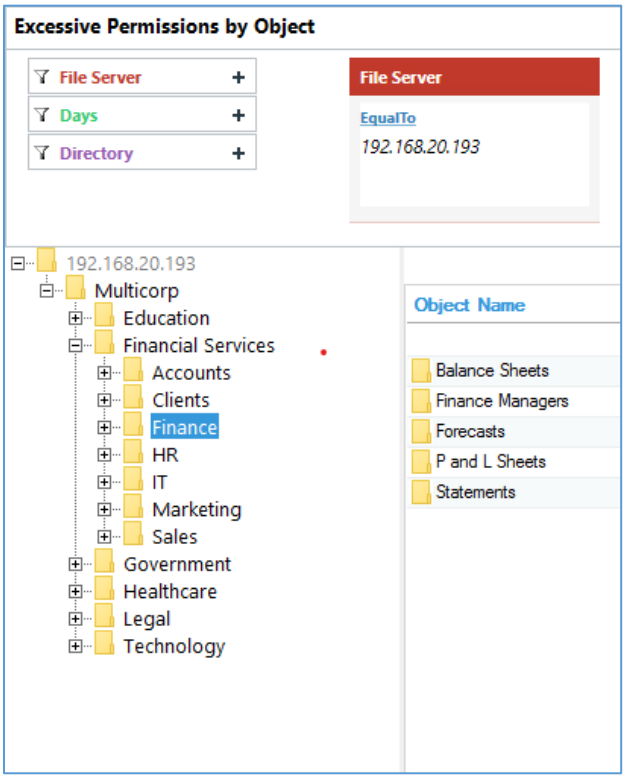

Figure 6: Object List

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

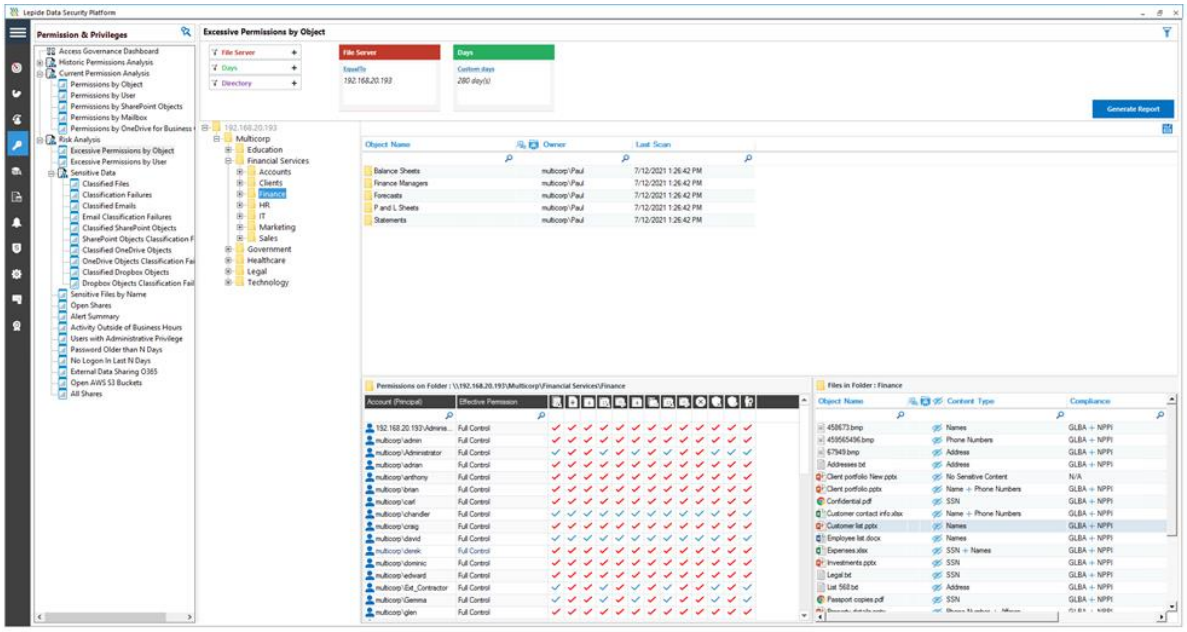

Figure 7: Excessive Permissions by Object Report

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

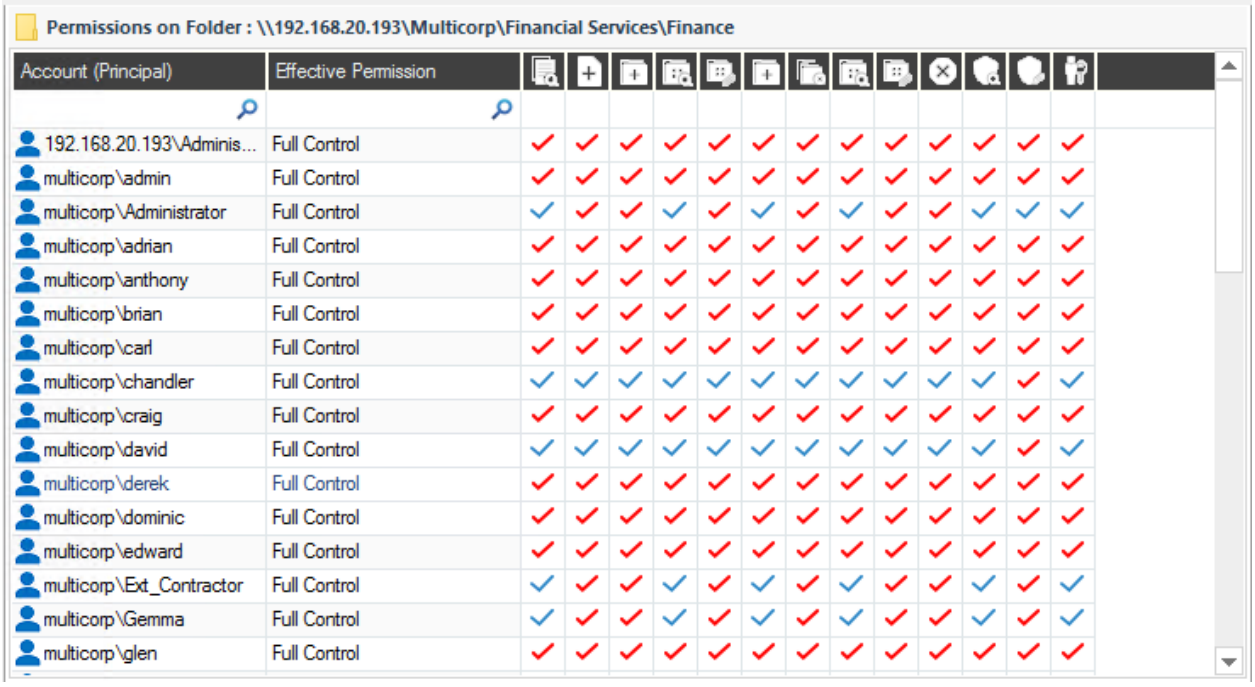

Figure 8: User Permissions

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:

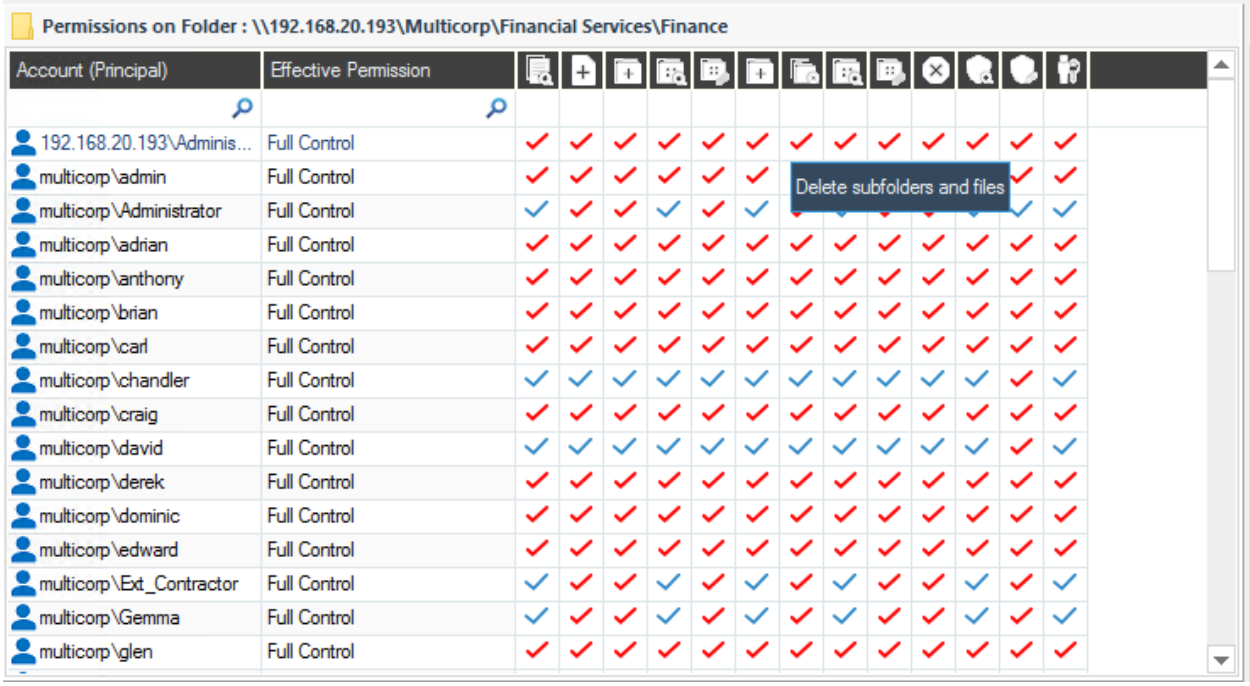

Figure 9: User Permissions with Tool Tip

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.

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 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 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 file server and number of days.

Click **Generate** to run the report:

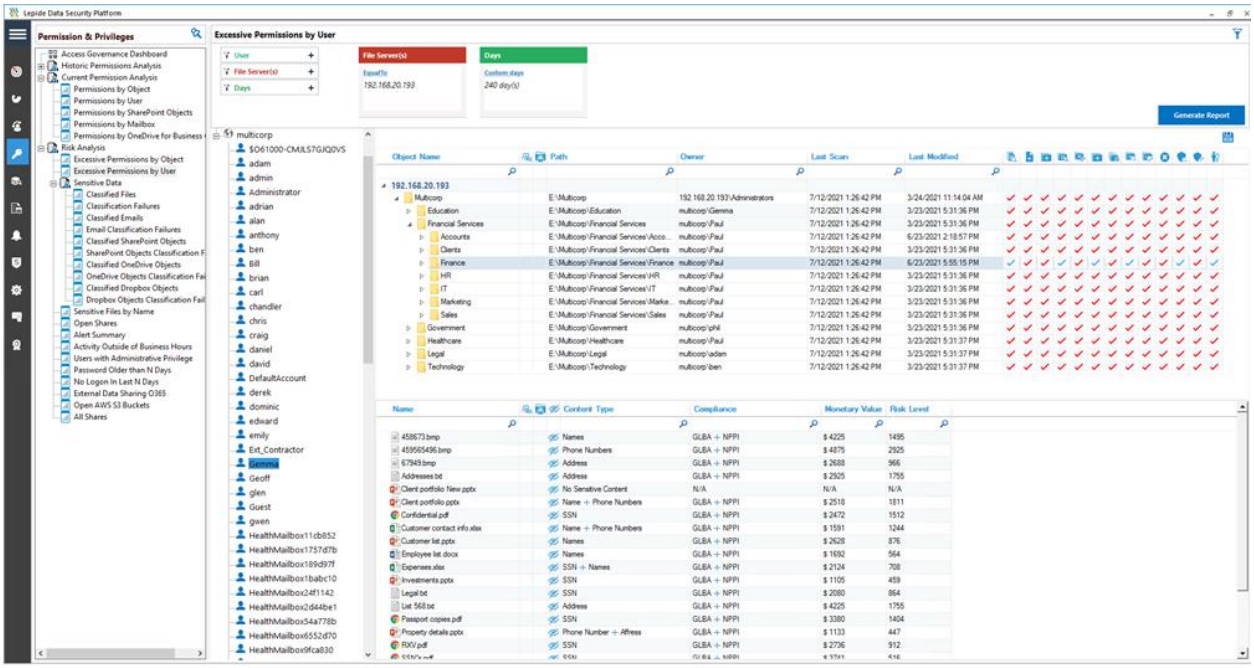

Figure 11: Excessive Permissions by User Report

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 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/.

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 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.