



USE CASE GUIDE

# HOW TO REPORT ON STALE DATA USING LEPIDE

# Table of Contents

1	Introduction.....	3
2	Why is there a Need to Monitor Stale Data?.....	3
3	How to Configure Lepide to Run the Stale Data Report .....	3
3.1	Prerequisites .....	3
3.2	Configure the Solution to Run a Scan.....	3
3.3	Run the Stale Data Report.....	17
3.4	Saving the Report.....	20
4	Support .....	21
5	Trademarks.....	21

# 1 Introduction

Understanding and securing your organization's unstructured data can become difficult and overwhelming without an appropriate data centric and audit protection strategy in place. One of the first challenges many organizations face is understanding how much of their unstructured data is still being accessed and if it is safe to archive this data without disrupting business continuity.

The Lepide Data Security Platform Stale Data Report gives you an overview as to how much data within your organization is deemed as stale which is based upon a variable timeframe you can specify within the Lepide Platform.

## 2 Why is there a Need to Monitor Stale Data?

Holding a large amount of stale data increases security risk and increases costs.

Cybercriminals are always on the lookout for stale data as soon as they land on a network. This stale data could include sensitive information about former or current employees, customers and so on and so needs to be managed appropriately. To reduce this risk, it's important to identify stale data and determine what can be moved, archived, or deleted. Once stale data has been identified, it is important to establish a consistent policy to manage it moving forward.

Another example of the need to manage stale data is as part of a migration process, Migration projects require a clear and accurate understanding of the type of data held—the size, relevance, sensitivity, and risk profile. Stale data can be expensive to store and manage and so only essential data should be migrated and anything else moved, archived, or deleted.

## 3 How to Configure Lepide to Run the Stale Data Report

### 3.1 Prerequisites

To configure and run the Stale Data Report, you need to have added a File Server component. For details on how to do this please refer to the [File Server Quick Start Guide](#).

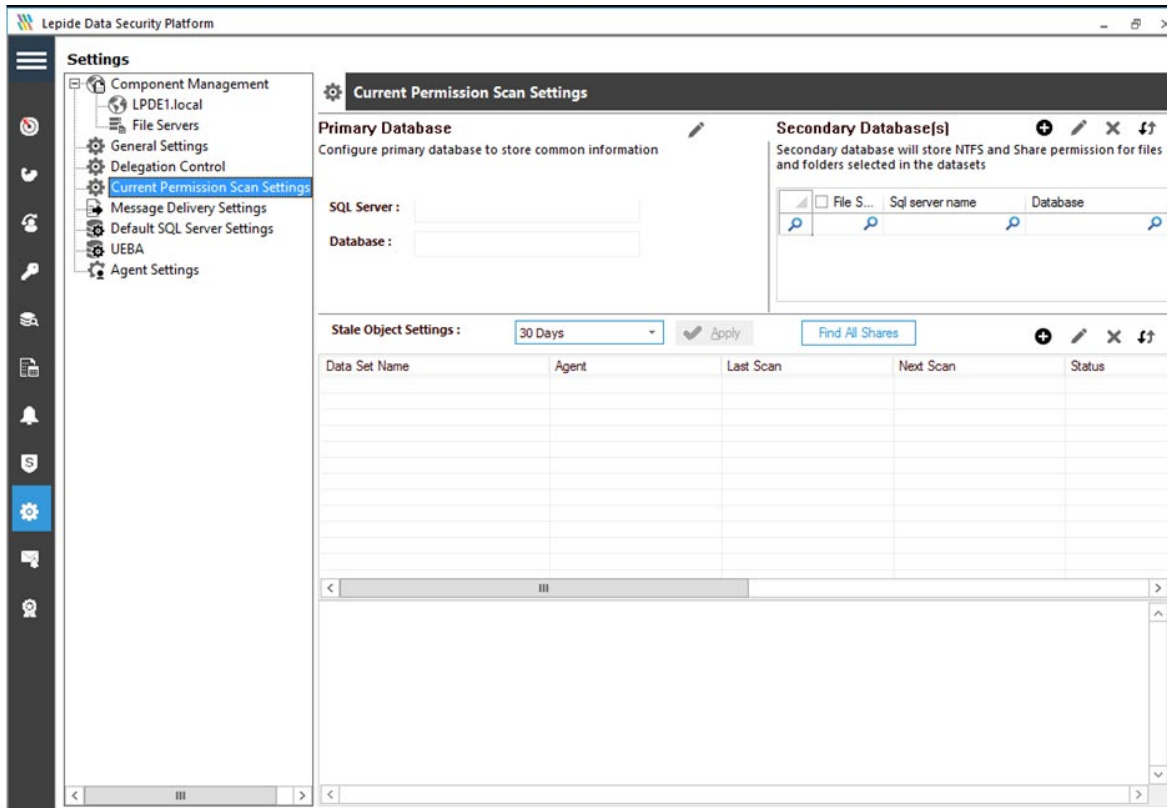
### 3.2 Configure the Solution to Run a Scan

The Lepide Data Security Platform needs to be configured to run a File Server scan before the report can be run and the steps to do this are as follows:

- Click on the **Settings** icon 

- Click on **Current Permission Scan Settings**

The following screen will be displayed:



*Figure 1: Current Permission Scan Settings*

The **Primary Database** needs to be configured to store the information retrieved from the scans:


- Click on the  icon next to Primary Database
- The **Database Settings** dialog box is displayed:

Figure 2: Database Settings

Configure the database settings as follows:

- **SQL Server:** Type in a SQL server name or click  to select the name and path
- Choose **SQL Authentication** and add a **User Name** and **Password**
- Click **Test Connection**
- **Select Database:** Add a database name or select an existing, blank database from the drop-down list

The screenshot shows a 'Database Settings' dialog box with the following fields and options:

- SQL Server :** DB194
- Authentication:**  Windows Authentication,  SQL Authentication
- User Name :** sa
- Password :** [masked]
- Select Database :** CP\_DB
- Time-Out Settings:**
  - Connection Time-Out :** 300 Seconds
  - Query Time-Out :** 300 Seconds

Buttons: Test Connection, Apply, Cancel

Figure 3: Database Settings

- Click **Apply**

The Primary Database information will now be displayed in the top part of the screen:

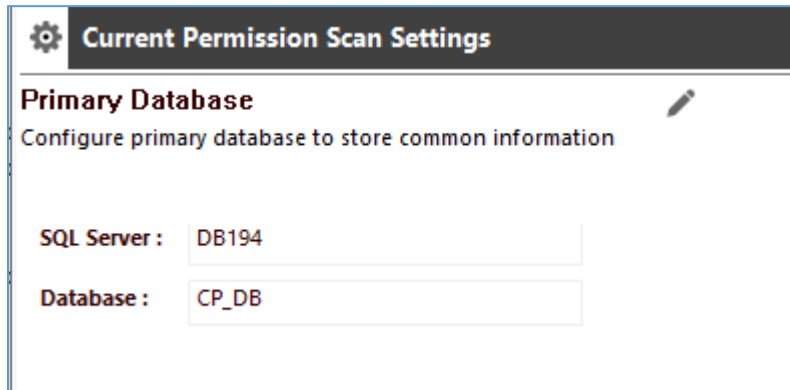


Figure 4: Primary Database Settings

### Adding a Dataset

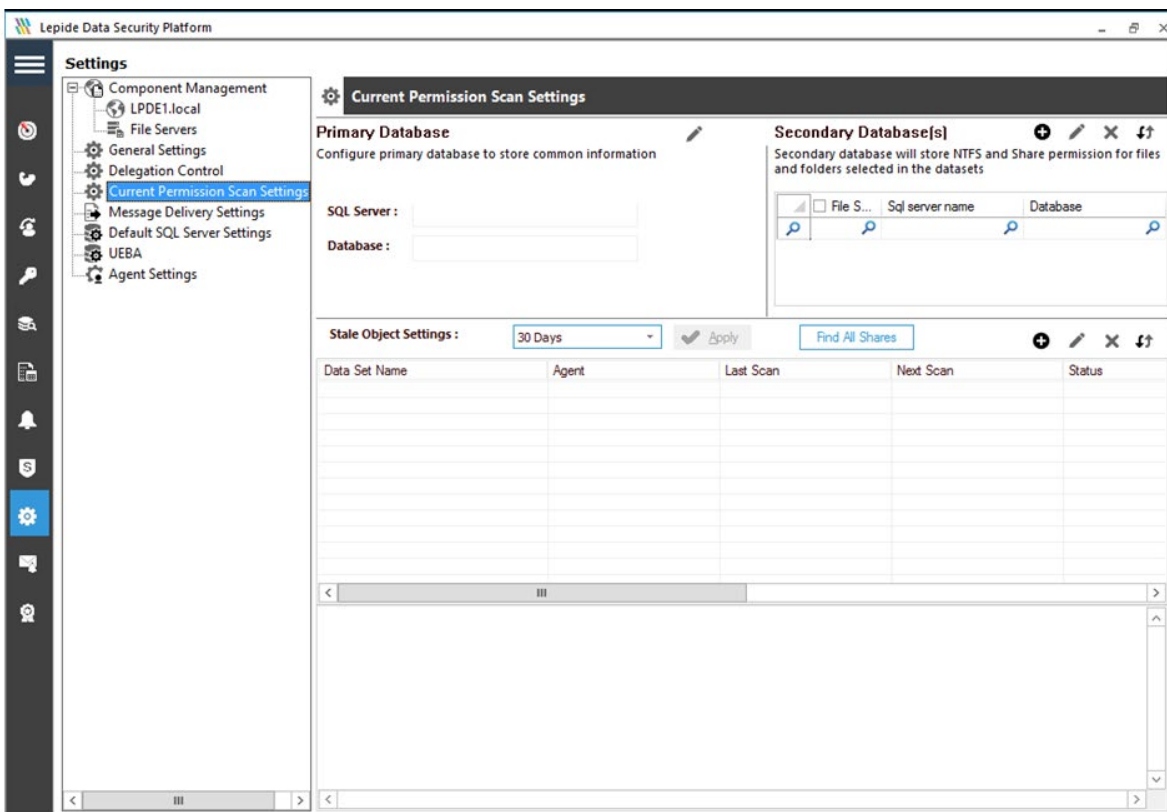

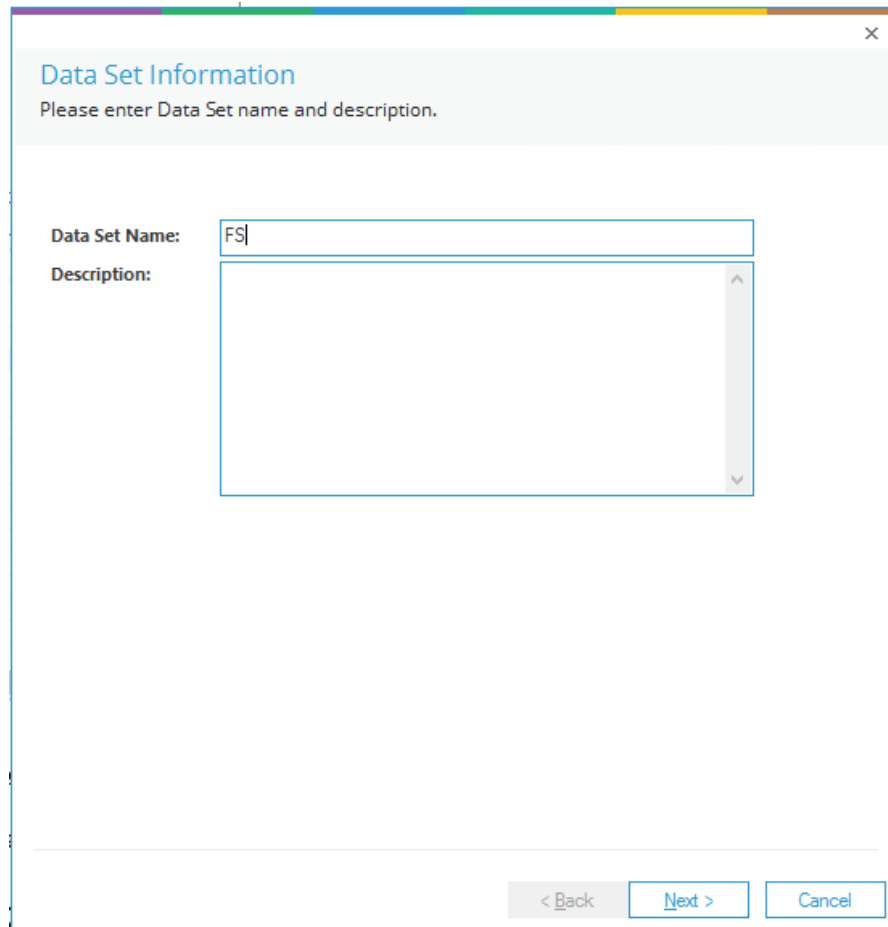


Figure 5: Current Permission Scan Settings

To add a data set

- From the Current Permission Scan Settings screen, click the  button (from the middle section of the screen)

The **Data Set Information** dialog box is displayed:



The screenshot shows a dialog box titled "Data Set Information" with a close button (X) in the top right corner. Below the title, it says "Please enter Data Set name and description." There are two input fields: "Data Set Name:" with the text "FS" entered, and "Description:" with an empty text area. At the bottom right, there are three buttons: "< Back" (disabled), "Next >" (active), and "Cancel".

*Figure 6:Data Set Information*

- Type in a **Data Set Name** and a **Description**
- Click **Next**

The Component and Server Information dialog box will be displayed:



Component and Server Information

Please select component(s) and the server(s) to be scanned

Component Name: File Server

Folder Name	Server Name	Apply To

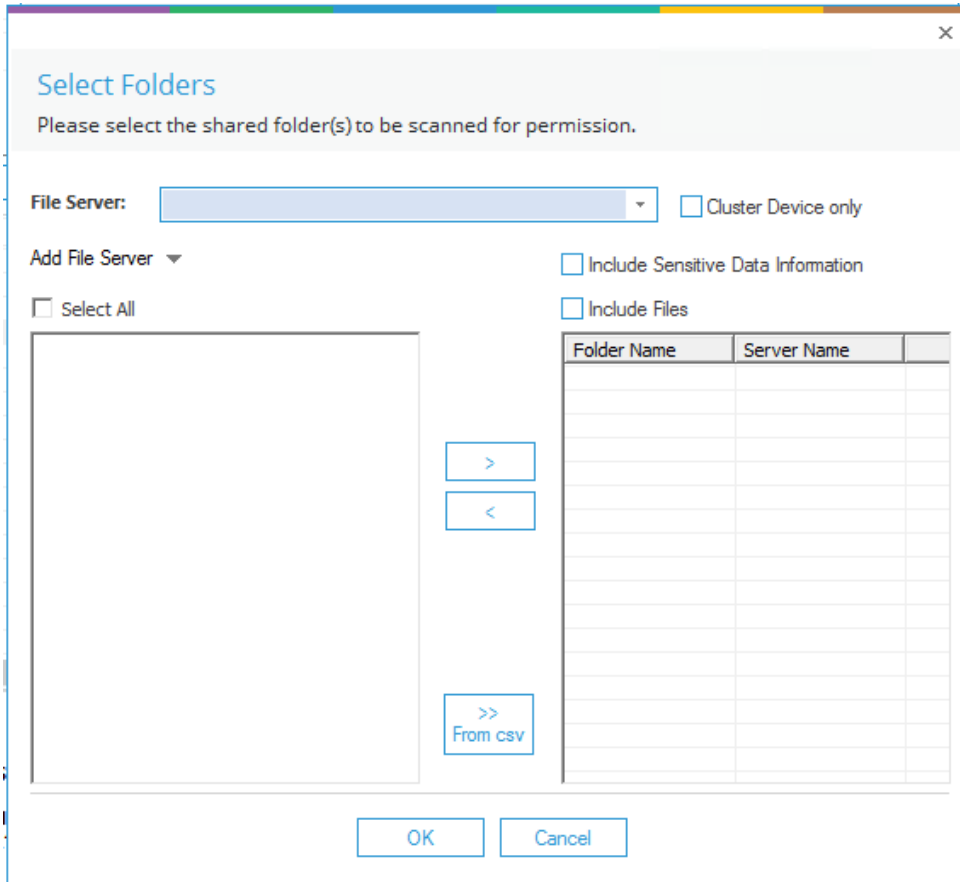
< Back   Next >   Cancel

Figure 7: Component and Server Information

- From the Component Name drop down, select **File Server**

- Click the **+** icon to select a folder

The Select Folders dialog box is displayed:



*Figure 8: Select Folders*

- Select the **File Server Name** from the drop-down menu

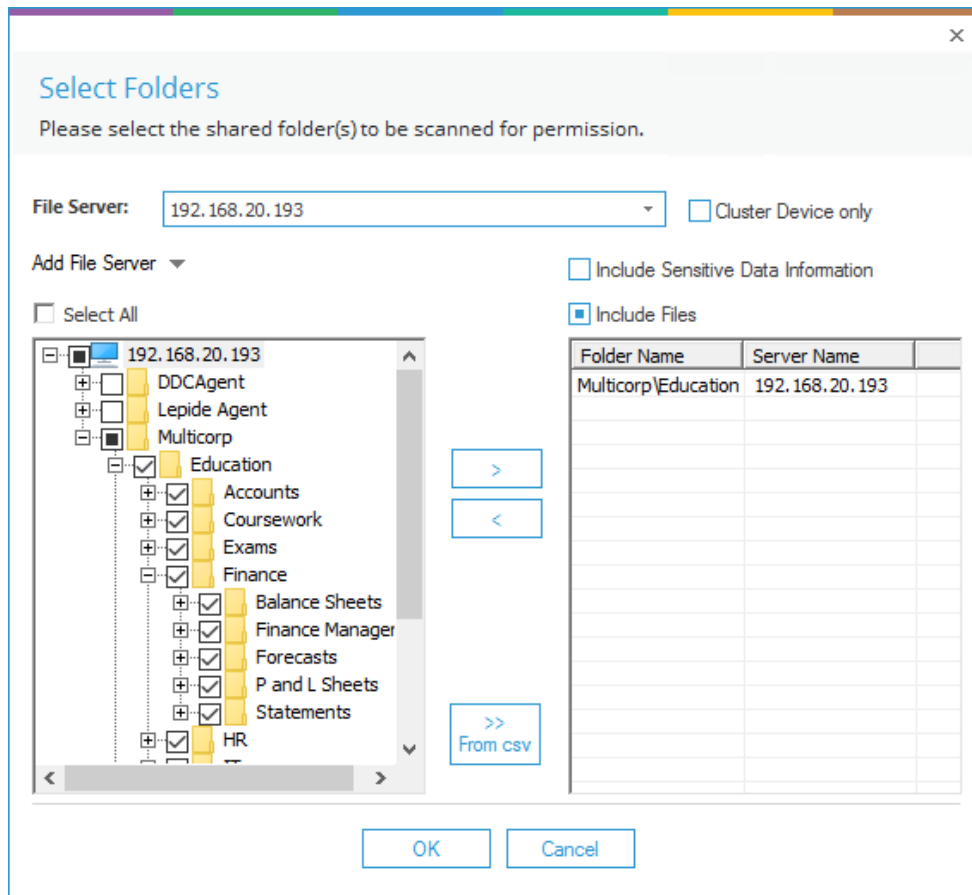




Figure 9: Select Folders

- The folders are listed in the left hand column
- You can expand the nodes to see more folders
- Select a folder and click the  button to add it to the list on the right
- Check **Include files** to monitor the permissions of sub-folders and files in the selected folder as well
- To remove an added folder from the Data Set, select the folder in the right column and click the  button.
- Click **OK**

- You are taken back to the previous wizard, which shows the added folder. The current permissions of the added folders will be monitored

Folder Name	Server Name	Apply To
Multicorp\Education	192.168.20.193	Scan all Folders ...

*Figure 10: Folder Selected*

- Click **Next**
- The Database Mapping dialog box is displayed:

File server	SQL server	Database name
192.168.20.193		

Figure 11: Database Mapping

- Click **Next**
- The Database Settings dialog box is displayed

*Figure 12: Database Settings*

- Here you can specify a Secondary Database if required. If you want to use a Secondary Database, type the Secondary Database name into the **Select Database** box
- If you want to use only a Primary Database, type the Primary Database Name into the Select Database Box.
- Click **OK**  
The Permission Scanning Options dialog box is displayed:

**Permission Scanning Options**

Please select the permission and group membership scan method.

**Scan Permissions Now**

**Schedule Permission Scan**

Run every day at 06:55:57 PM, Schedule start from 1/31/2023. Change Schedule

**Scan on Remote Agent**

**Agent Location/IP:**

**Scan Nested Group Membership and Permission**

**Domain Controller:**

**User Name :**

**Password :**

Note: Use "NetBIOS\UserName" format for User Name.

< Back Finish Cancel

Figure 13: Permission Scanning Options

- Select to **Scan Permissions Now** and/or **Schedule Permission Scan**
- Click the **Change Schedule** button to change the frequency and times of the schedule if required:

Figure 14: Define Schedule

- Click **OK** once the schedule settings are updated and you will return to the Permission Scanning Options dialog box
- From the Permission Scanning Options dialog box:
  - Check the **Scan on Remote Agent** box if you want to run a permissions scan from a remote machine. Then add the details of this remote agent.
  - Specify the **Domain Controller** – this can be the IP address or name of any domain controller
  - Add the **User Name** and **Password**. This user must have at least the rights listed below to the folders:
    - List Folder/Read Data
    - Traverse Folder/Execute File
    - Read Permissions
- Click **Finish**



The Data Set information is now displayed in the middle part of the screen:

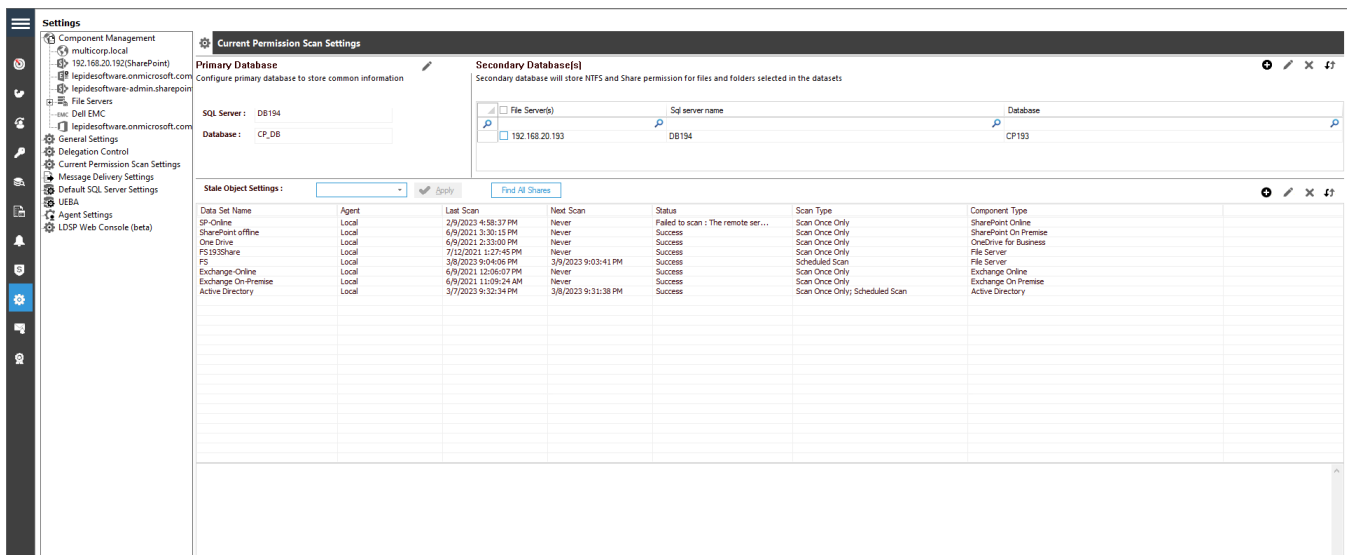


Figure 15: Data Set Settings

### 3.3 Run the Stale Data Report

Once a scan has run, you can generate the Stale Data Report:

To view the Stale Data Report:

- Click the Permissions and Privileges  icon:
- Expand **Risk Analysis**
- Click on **Stale Data Report**

The Stale Data Report screen is displayed:

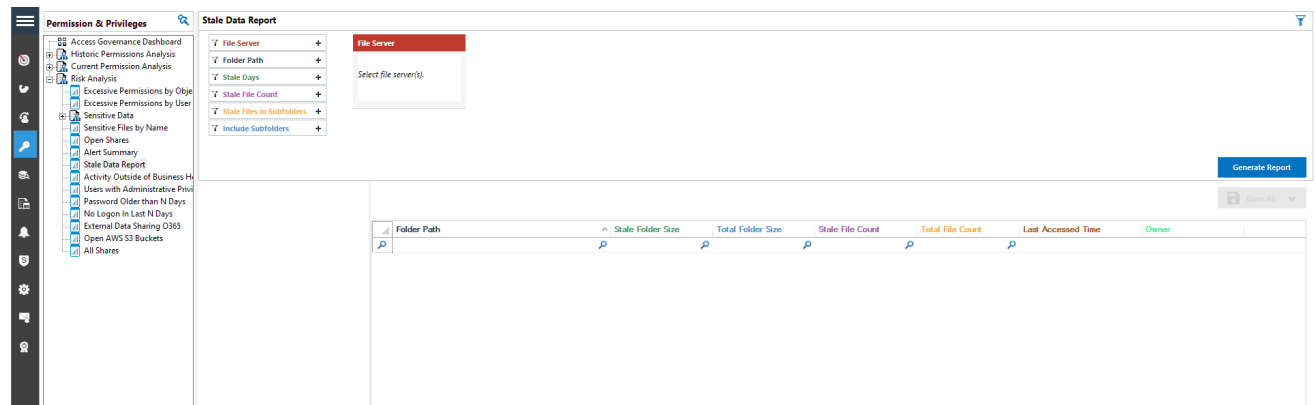


Figure 16: Stale Data Report

- Select the **File Server**
- Use the **Stale Days** filter to specify the number of days which you want to define as stale data. The default is 30 days but you can choose 30, 90, 180, 360 or Custom number of days:

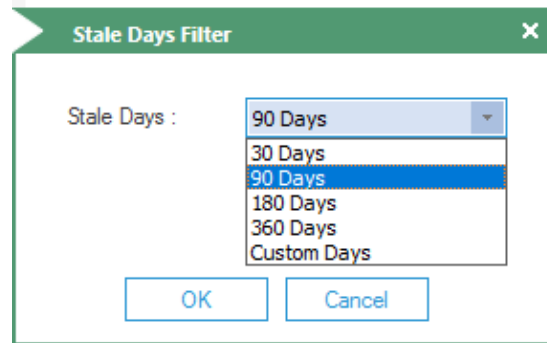


Figure 17: Custom Days Filter

- Click **Generate Report**
- Expand the File Server from the tree structure on the left-hand side:

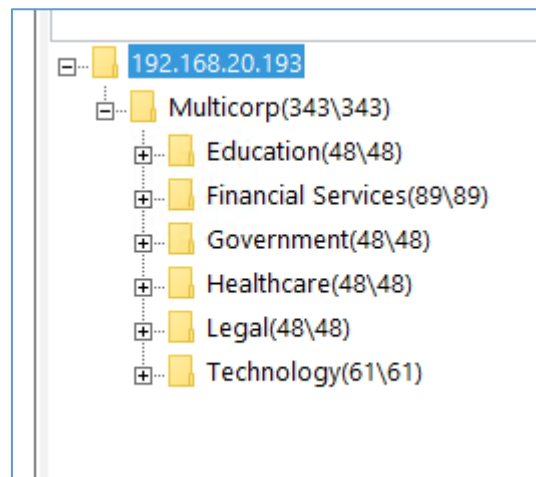


Figure 18: Choose Folder

- Click on the Folder you want to view data for (eg Financial Services)
- All stale data for that folder will be displayed:

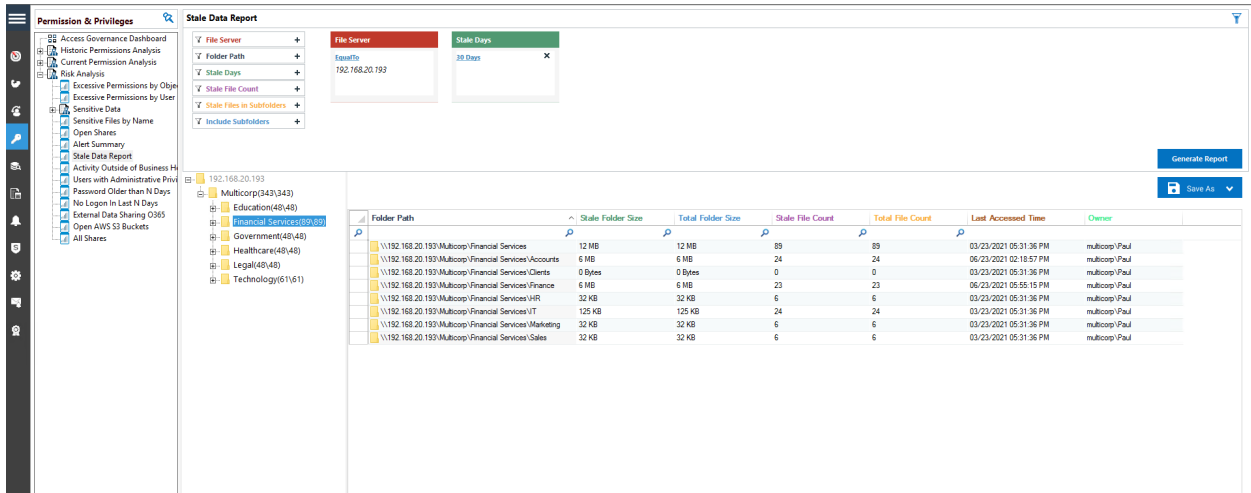


Figure 19: Stale Data Report

- The report can be sorted, filtered, and saved.

**Other Filter Options:**

- **Folder Path Filter:** this filter allows you to enter a UNC path

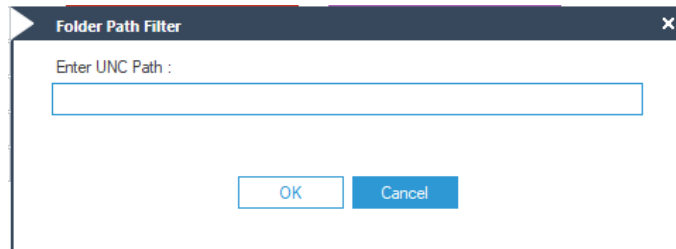


Figure 20: Folder Path Filter

- **Stale File Count:** this filter allows you to specify the number of stale files that a folder contains. Choose from **Equal to**, **Greater than** or **Less than** and enter a number in the Value box. Only folders containing the specified number of files will be shown in the report.

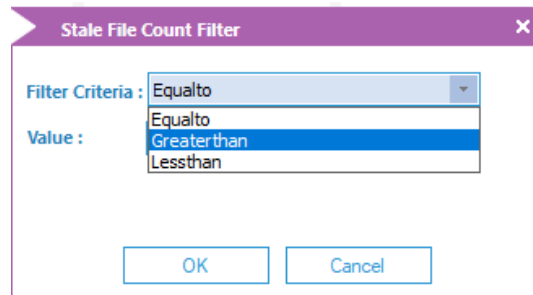


Figure 21: Stale File Count Filter

- **Stale Files in Subfolders:** this filter allows you to specify the number of stale files that a subfolder contains. Choose from **Equal to**, **Greater than or Less than** and enter a number in the Value box. Only subfolders containing the specified number of files will be shown in the report
- **Include Subfolders:** this filter is on by default but you can choose **Exclude Subfolders** if you want to exclude subfolders from the report

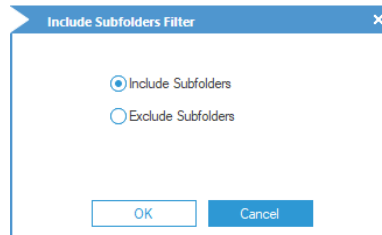


Figure 22: Include Subfolders Filter

## 3.4 Saving the Report

The report can be saved by clicking the **Save As** button to the top right of the screen:

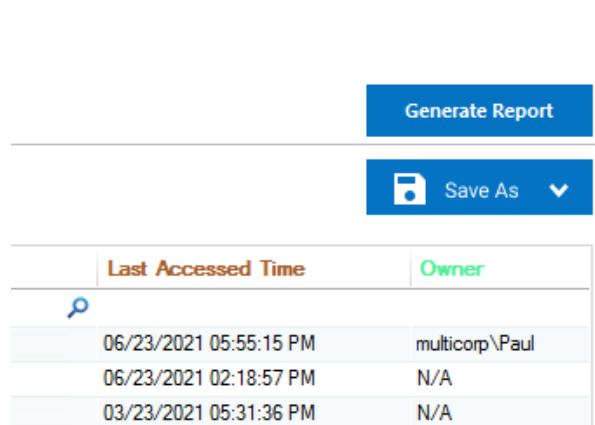


Figure 23: Save As

## 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 <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](mailto:sales@Lepide.com)

[support@Lepide.com](mailto: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.