

How to identify open shares.

Use case guide.

Contents

1. Introduction..... 2

2. What is an Open Share?..... 2

3. The Effect of Open Shares on Data Security 3

4. Access Governance 3

5. The Lepide Solution 4

 5.1 Running a Scan..... 4

 5.2 Running the Report..... 7

6. Support..... 11

7. Trademarks 11

1. Introduction

The misuse of user privileges is one of the main sources of a data breach within an organization and so appropriate action must be taken to keep the risk of these threats to a minimum. One such threat is being unaware of the files and folders that users have access to via open shares.

Organizations allow open shares on their systems to make it easy for end-users to have easy access to a given resource. However, if these open shares are not managed correctly, they can create security risks with potentially catastrophic consequences.

The focus at Lepide is to provide visibility over what's happening with your network and through visibility you can take the necessary steps to mitigate risk and stay compliant. Once you have visibility over open shares within your network it is a straightforward process to take action to manage the access to them.

2. What is an Open Share?

An open share is a resource where access is unrestricted to most end users and is achieved using Open Access Groups. These types of groups can include:

Everyone – all users and accounts that have authenticated to the system.

Authenticated Users – everyone except build-in, non-password protected groups.

Anonymous Logon – a built-in group that enables users to access resources from an anonymous account.

Domain Users – a default group within Active Directory to which users accounts are automatically added.

3. The Effect of Open Shares on Data Security

Open shares are especially problematic when dealing with resources that contain sensitive data, such as Personally Identifiable Information (PII), Protected Health Information (PHI) and Payment Card Information (PCI), as it makes it a lot easier for hackers to gain access to this data.

There are times when it is necessary to have resources that are accessible to all users on a network for example calendars, press releases, job descriptions and marketing materials and so on, but it only takes one employee who has been wrongly granted write-access to a resource to result in a serious security incident.

A lot of malware and viruses are designed to spread using open shares. A hacker may obtain a legitimate set of credentials and if they have been granted full write-access to the resource in question, they could use those credentials to infect the resource with malware.

4. Access Governance

Access Governance is the process of monitoring and controlling who within an organization has access rights and ensuring that users only have access to those functions that are essential to do their job. The need for access governance has become more evident as organizations seek to remain compliant and to manage risk with a more strategic approach.

Within the process of monitoring all network user privileges, it is essential that open shares are reported on regularly as if they are not managed correctly, they can become a significant threat to network security within an organization. Without Access Governance processes in place, access to files and folders via an open share could be used by an attacker to gain access to the network and cause a data breach.

However, while the constant monitoring of open shares is achievable, it can be complex and time consuming without the right solution in place.


5. The Lepide Solution

The Lepide Data Security Platform provides a complete solution that scans and reports on all open shares within an organization.

By first running a scan and then running the All Shares Report, it is possible to identify all open shares and then to take action to manage how they are being used.

5.1 Running a Scan

The **Find All Shares** scan needs to be run before the report can be generated and the steps to do this are from the Legacy Console and are as follows:

- From the Legacy Console main screen, click on the **Settings** icon 
- From the tree structure on the left-hand side, click on **Current Permission Scan Settings**

The following screen will be displayed:

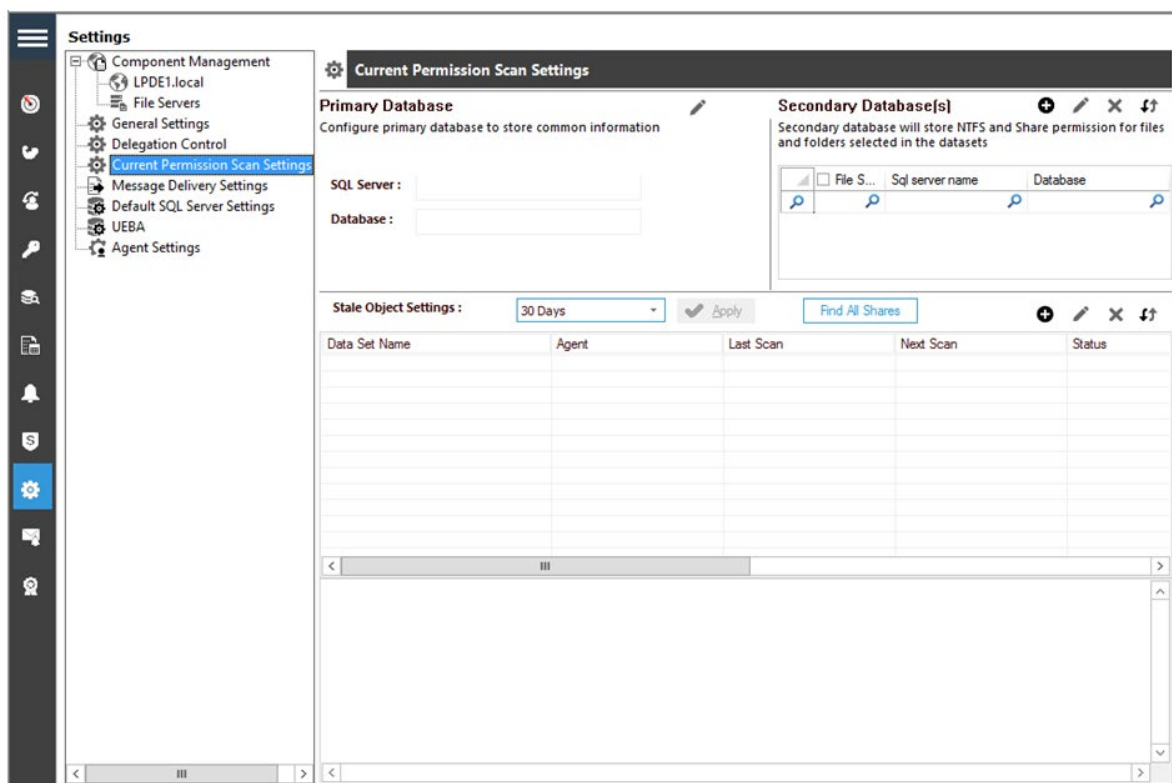
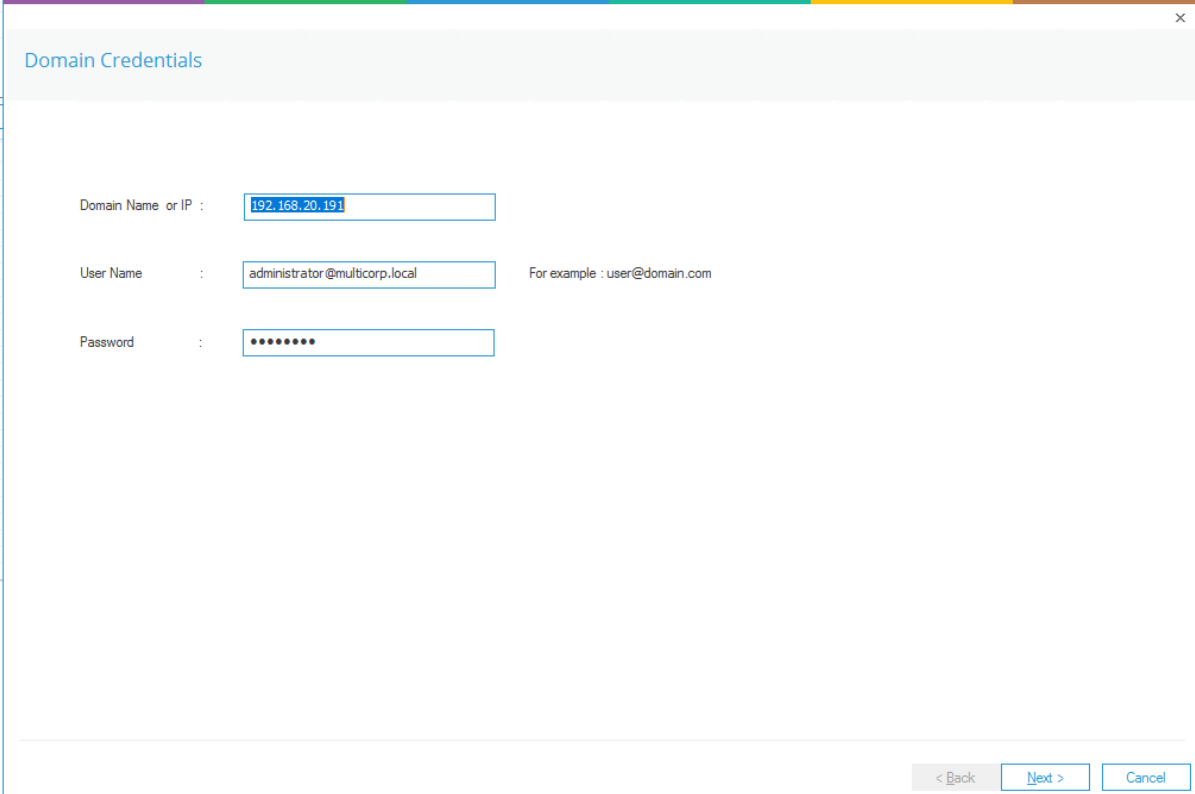


Figure 1: Current Permission Scan Settings

Find All Shares

- Click the Find All Shares button and a wizard will start. The Domain Credentials dialog box will be displayed:



Domain Credentials

Domain Name or IP : 192.168.20.191

User Name : administrator@multicorp.local For example : user@domain.com

Password :

< Back Next > Cancel

Figure 2: Domain Credentials

- Add the Domain Credentials and click **Next** to continue

The Map the Computer IP address dialog box is displayed:

Please review and map the Computer IP address

Computer Name	IP Address
DCBDC001	192.168.20.195
DCD002	192.168.20.191
EXD001	192.168.20.196
FS001	192.168.20.193
LEPIDE-SERVER2	192.168.20.197
SPD001	192.168.20.192

NOTE : IP address field is editable. LepideDSP will not monitor the Computer until mapped to its correct IP Address.

Schedule

☒ Every Monday at 19:38:01

< Back Finish Cancel

Figure 3: Review and Map the Computer IP Address

- All Computer names will be selected. De-select any that you do not want to be included in the scan
- You can also schedule the scan to happen weekly by choosing a day and time for the scan in the Schedule section of the dialog box
- Click **Finish**

5.2 Running the Report

Once a scan has run, the **All Shares Report** can be generated from the Lepide Web Console 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 4: Lepide Trust Reports Menu

From the tree structure to the left side of the screen, expand Risk Analysis to see the All Shares Report:

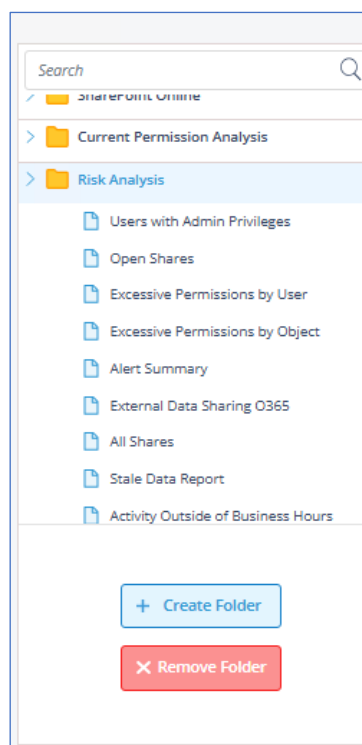


Figure 5: Tree Structure showing Risk Analysis Reports

- Click on the **All Shares** Report from the tree structure

The empty All Shares report is displayed:

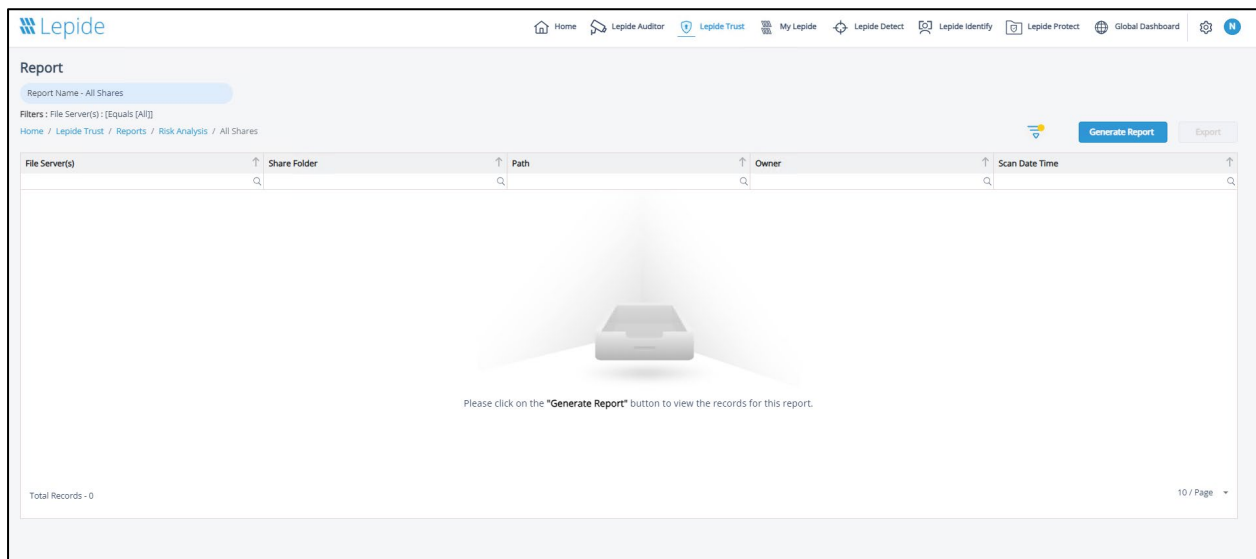


Figure 6: All Shares Report with no data

We need to show only Open Shares in the report which is as follows:

- To select the Share Type, click the Filter icon  and the following dialog box is displayed:

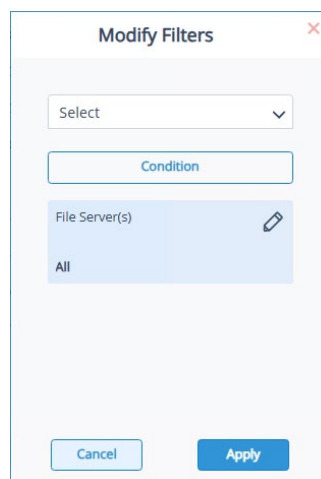


Figure 7: Modify Filters

- From the drop-down menu choose **Share Type**:

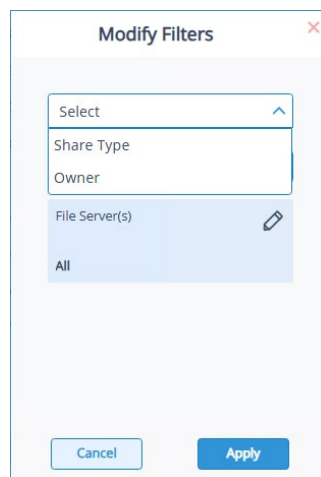


Figure 8: Share Type Filter

The Share Type filter will be displayed:

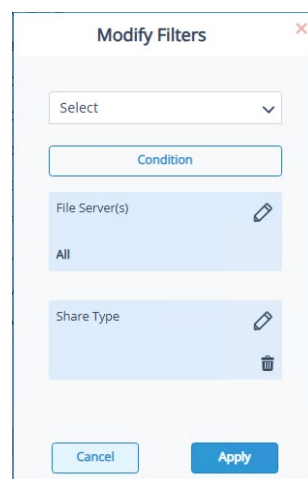



Figure 9: Share Type Filter

- Click the Edit filter icon  to edit the Share Type
- Choose **Show Open Shares Only**

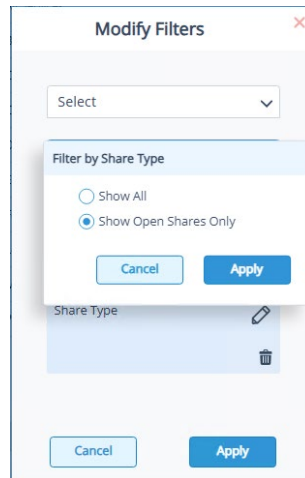


Figure 10: Filter by Share Type

- Click **Apply** to close the Filter by Share Type dialog box
- Click **Apply** to close the Modify Filters dialog box
- Click **Generate Report**

The **All Shares Report** filtered by Open Shares is displayed:


<div>  Home Lepide Auditor Lepide Trust My Lepide Lepide Detect Lepide Identify Lepide Protect Global Dashboard </div>					
<div> Report <div>Report Name - All Shares</div> <div> Filters : File Server(s) : [Equals [All]] AND Share Type : [Equals [Show Open Shares Only]] </div> <div> Home / Lepide Trust / Reports / Risk Analysis / All Shares </div> <div> <div>Generate Report</div> <div>Export</div> </div> </div>					
File Server(s)	Share Folder	Path	Owner	Scan Date Time	
192.168.1.10	All Services	C:\All Services	LPDE4\Kelly.Macwell	2023-10-03 16:59:02	
192.168.1.10	Budget Forecast	C:\Budget Forecast	LPDE4\Roy.Petty	2023-10-03 16:59:02	
192.168.1.10	Company Share	C:\Company Share	LPDE4\Administrator	2023-10-03 16:59:02	
192.168.1.10	Confidential Files	C:\Confidential Files	LPDE4\Roy.Petty	2023-10-03 16:59:02	
192.168.1.10	DDC Agent	C:\DDC Agent	LPDE4\Neal.Gamby	2023-10-03 16:59:02	
192.168.1.10	Employee's Account details	C:\Employee's Account details	LPDE4\Marty.Byrde	2023-10-03 16:59:02	
192.168.1.10	Foreign designs	C:\Foreign designs	LPDE4\Marty.Byrde	2023-10-03 16:59:02	
192.168.1.10	Lepide Agent	C:\Lepide Agent	LPDE4\Neal.Gamby	2023-10-03 16:59:02	
192.168.1.10	Module Analysis Data	C:\Module Analysis Data	LPDE4\Ethan.Hunt	2023-10-03 16:59:02	
192.168.1.10	Project Details	C:\Project Details	LPDE4\Ethan.Hunt	2023-10-03 16:59:02	
<div> Total Records - 16 <div> First Previous 1 / 2 Next Last </div> <div>10 / Page</div> </div>					

Figure 11: All Shares Report

6. 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

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 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.