Lepide

USE CASE GUIDE

HOW TO USE LEPIDE TO IDENTIFY USERS WITH ADMINISTRATIVE PRIVILEGES

Table of Contents

1. Introduction

Users who have administrative privileges are the most important users within your organization, but they also represent the biggest risk to your data security.

Administrative rights are essential to the efficient running of any IT system as they enable trusted users to perform essential tasks like installing software, adding new accounts, creating passwords and the many other system modifications needed to do their job.

The flip side of this, however, is that admin rights provide the user with the 'keys to the kingdom' and therefore present a huge risk to the security of an organization's data. An attacker who infiltrates a business with access to these rights could do significant harm.

For this reason, particularly in today's world of ever-increasing cyber risk, it is imperative to limit the number of user accounts with administrative privileges to the bare minimum.

2. 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 organizations to have visibility over the complete list of users who have administrative privileges in Active Directory. But as organizations grow, and Active Directory structures evolve, being able to see and understand the complete list of Active Directory users with administrative privileges can become a complex and time-consuming task.

3. The Users with Admin Privilege Report

The Lepide Data Security Platform overcomes this complexity and provides visibility in a clear and easy to understand way. By scanning Active Directory and running the Users with Admin Privilege Report you can quickly identify every user in Active Directory who has administrative privileges.

The scans can be run immediately and/or scheduled to run on a daily, weekly, or monthly basis therefore providing up-to-date visibility to mitigate the risk of privilege abuse.

All administrative privileges, whether assigned directly or indirectly, will be reported. Those privileges assigned indirectly will have been given via membership of the built-in administrative groups which are Enterprise Admins, Domain Admins, Schema Admins and Administrators.

Here is an example of the Users with Administrative Privilege Report:

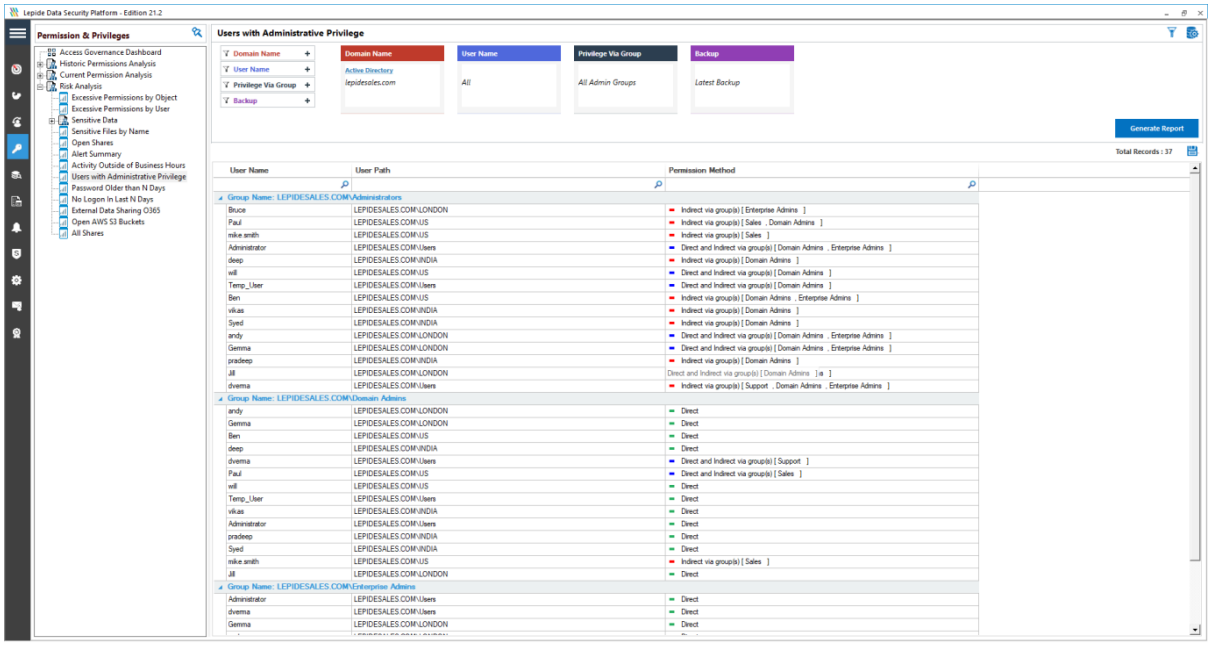


Figure 1: Users with Admin Privilege Report

The Permission Method column shows how the permission has been applied (direct, indirect or both). This column includes color coding so you can clearly see how permissions were given.

The color coding is follows:

- Green is direct permission
- Red is indirect permission
- Blue is both direct and indirect permission

For those users with indirect permissions, it is possible to drill down to see which groups they are a member of to give further clarity on how and why administrative permissions have been granted.

4. How to Configure Lepide to Identify Users with Admin Privileges

4.1. Prerequisites

To configure and run the Users with Administrative Privileges Report, you need to have added an Active Directory component. For details on how to do this please refer to the Active Directory Quick Guide.

4.2. Configure the Solution to Run a Scan

The Lepide Data Security Platform needs to be configured to run an Active Directory 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:

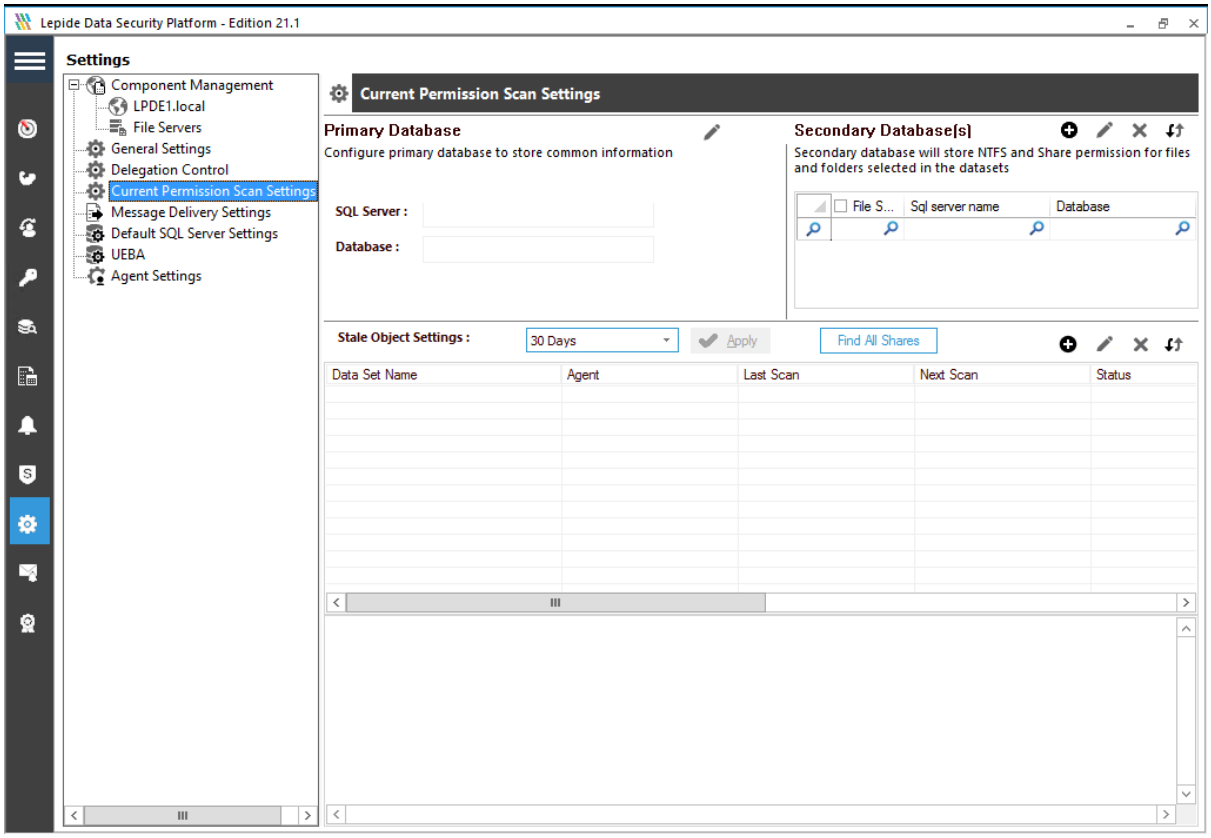


Figure 2: Current Permission Scan Settings

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:

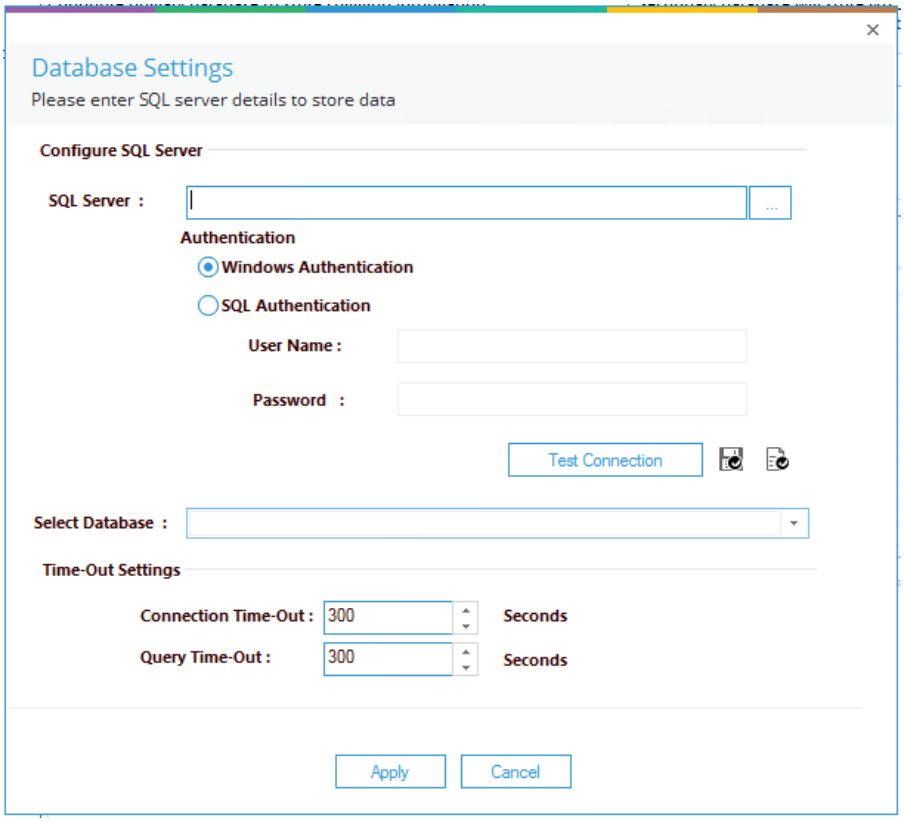


Figure 3: Database Settings

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 the **User Name** and **Password**

Click **Test Connection**

Select Database: Add a database name or select an existing, blank database from the drop-down list

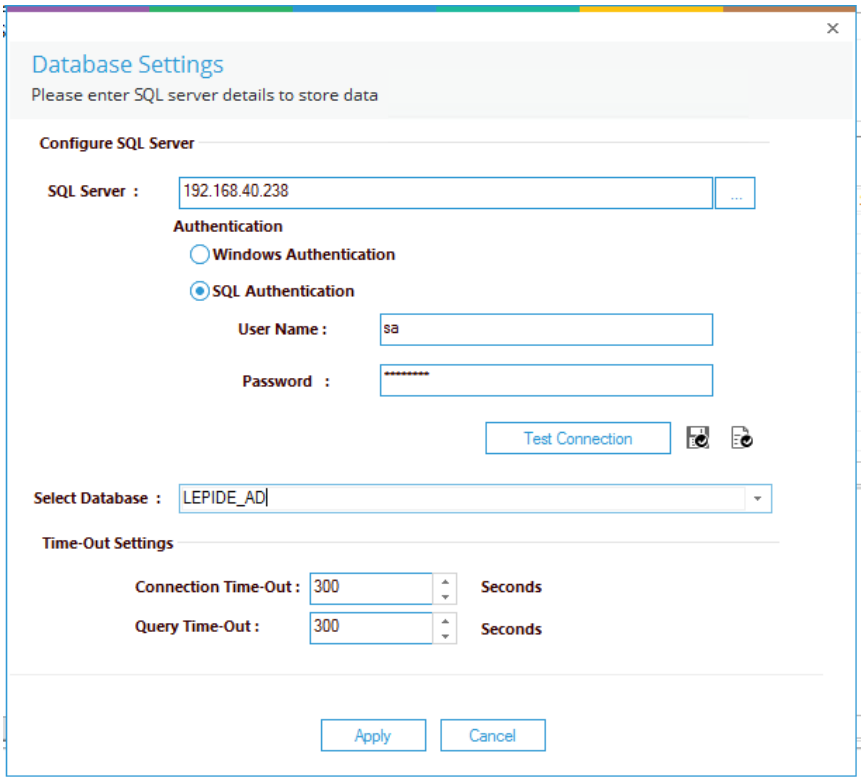


Figure 4: Database Settings

Click **Apply**

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

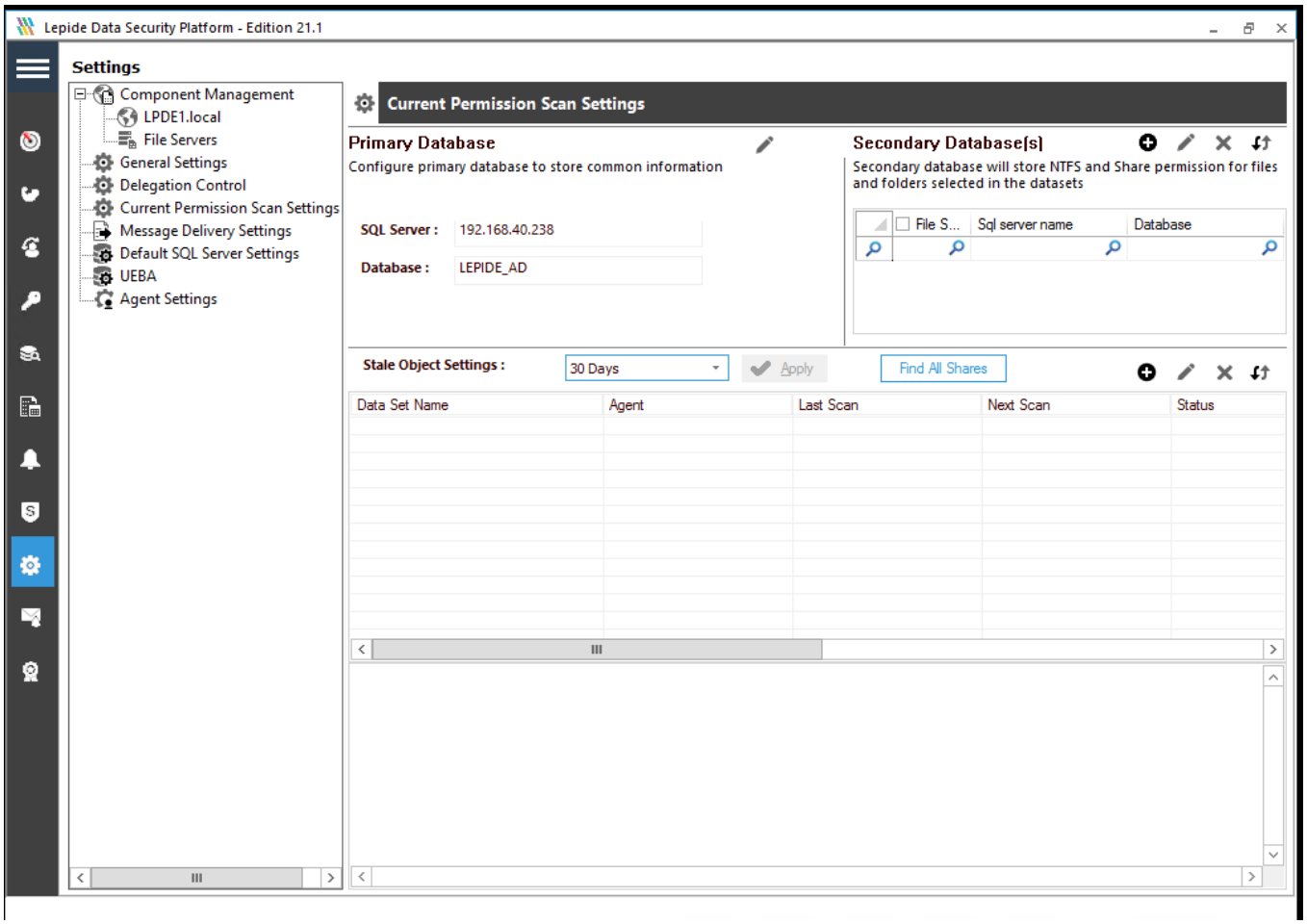


Figure 5: Primary Database Settings

Adding a Dataset

The middle section of the screen will show the data set information.

To add a data set, click the ⊕ button (from the middle section of the screen)

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

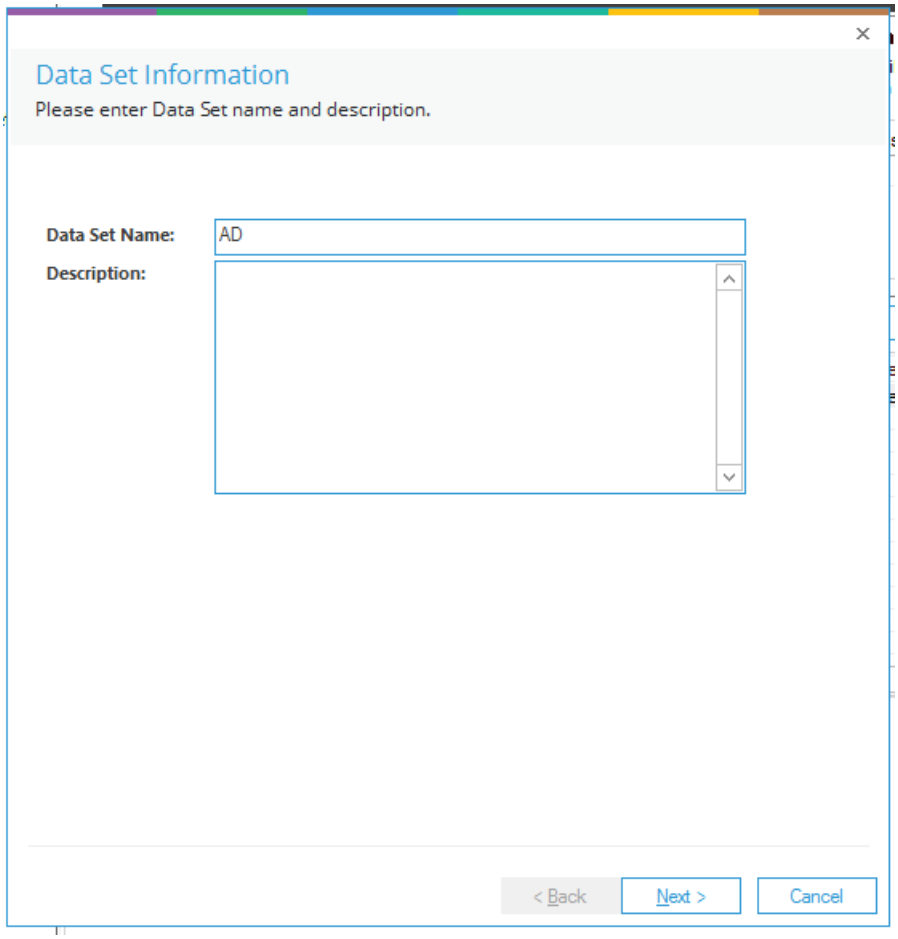


Figure 6:Data Set Information

Type in a **Data Set Name** and a **Description**

Click **Next**

From the Component Name drop down, select **Active Directory** (you may need to scroll up to see Active Directory in the list).

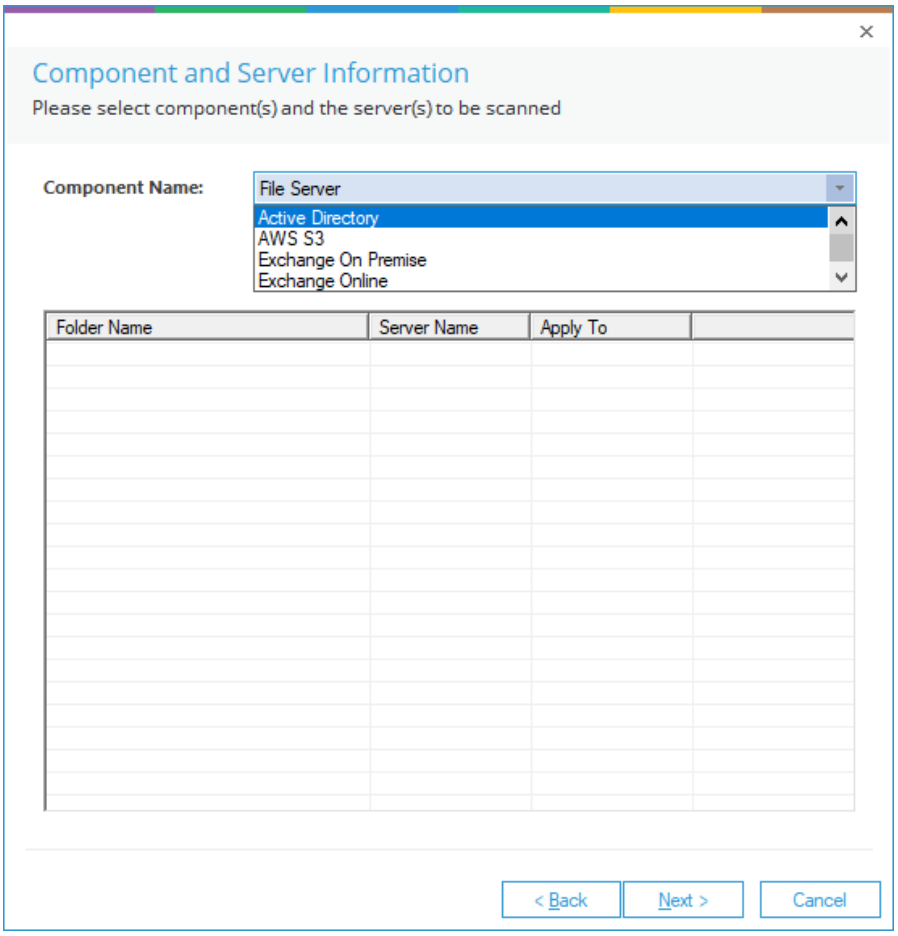


Figure 7: Component and Server Information

The Active Directory options will now be displayed in the dialog box:

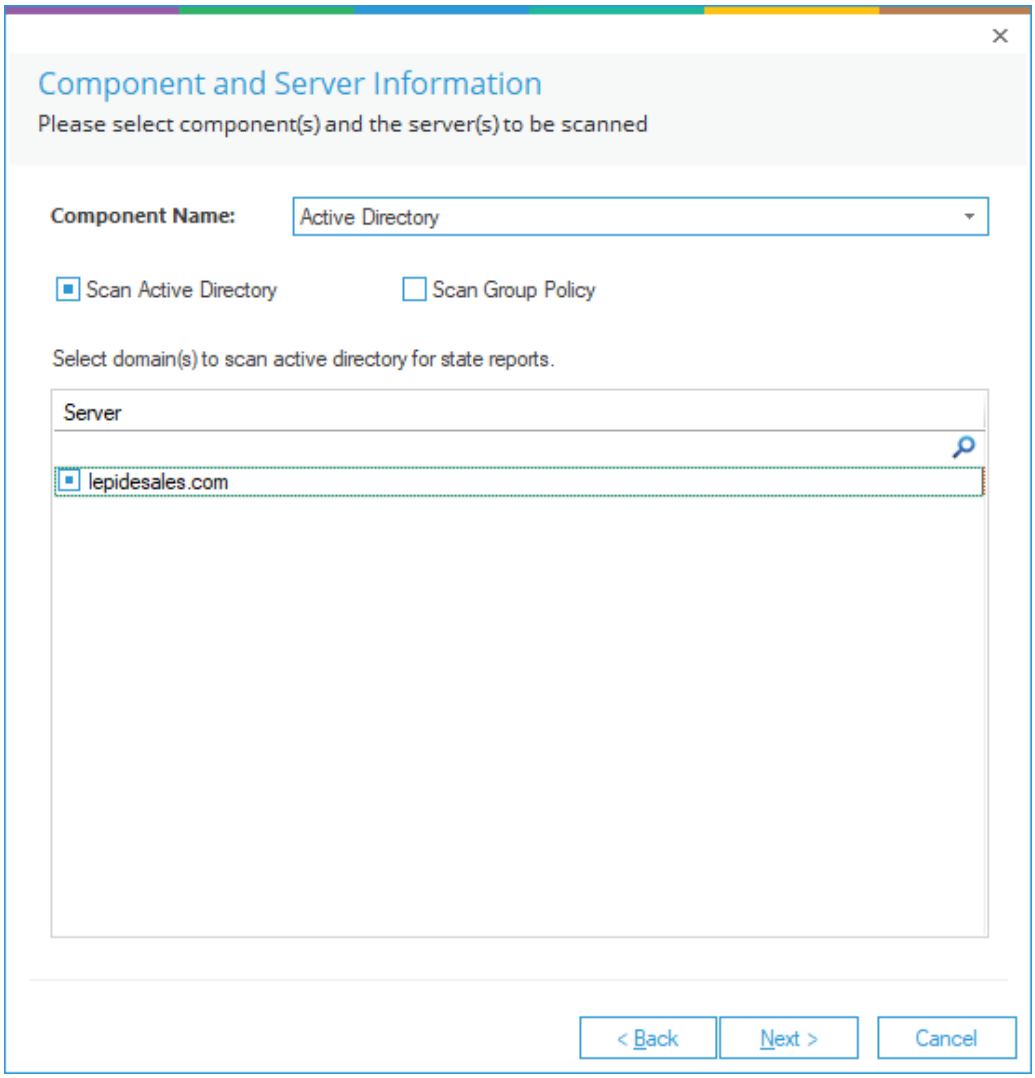


Figure 8: Active Directory Options

Check the **Scan Active Directory** box

Select the domain(s) to scan active directory for state reports

Click **Next**

The **Scan Options** dialog box will be displayed:

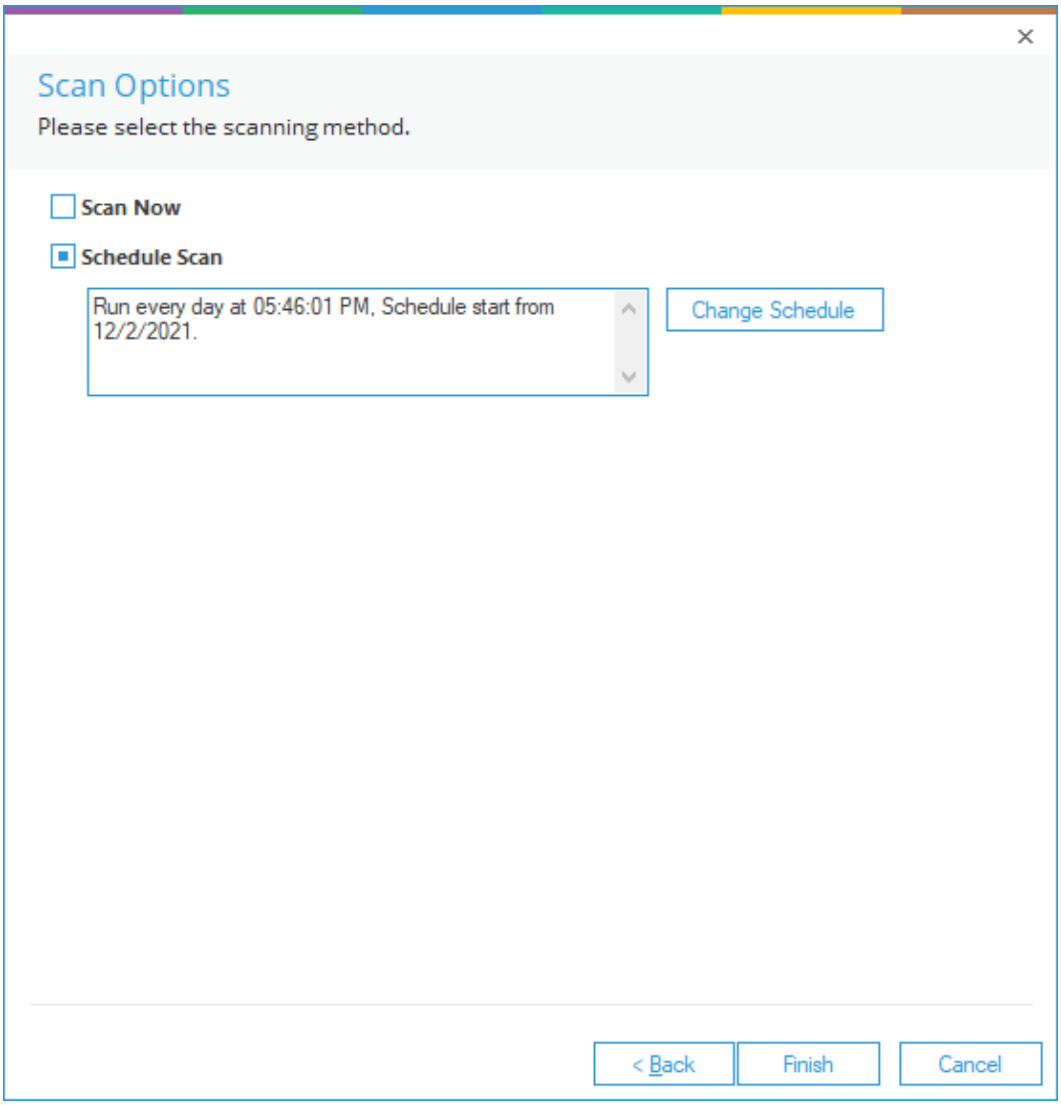


Figure 9: Scan Options

Select to **Scan Now** and/or **Schedule Scan**

Click the **Change Schedule** button to change the frequency and times of the schedule if required:

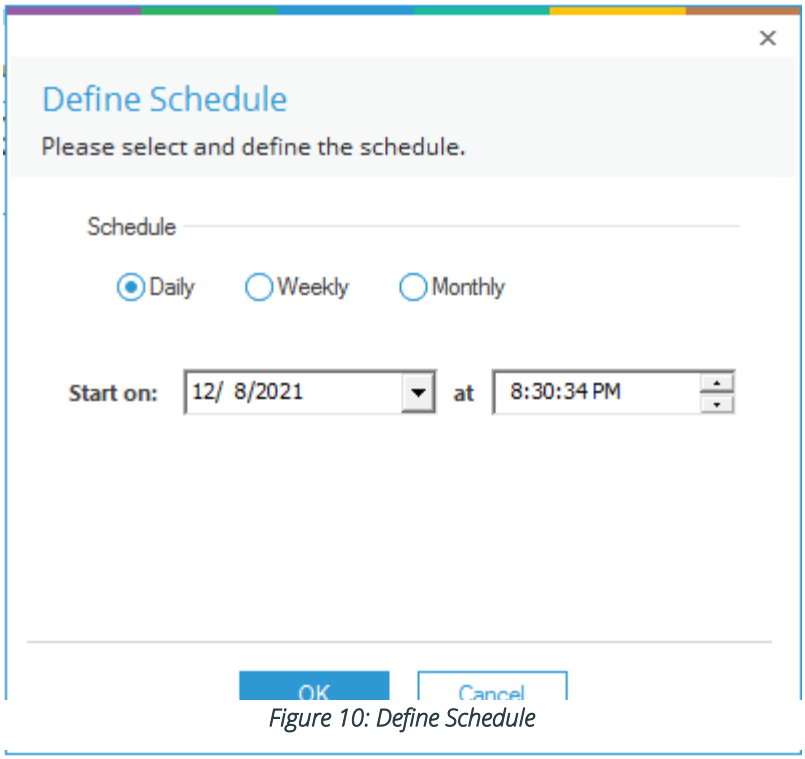


Figure 10: Define Schedule

Click **OK** once the schedule settings are updated.

Click **Finish**

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

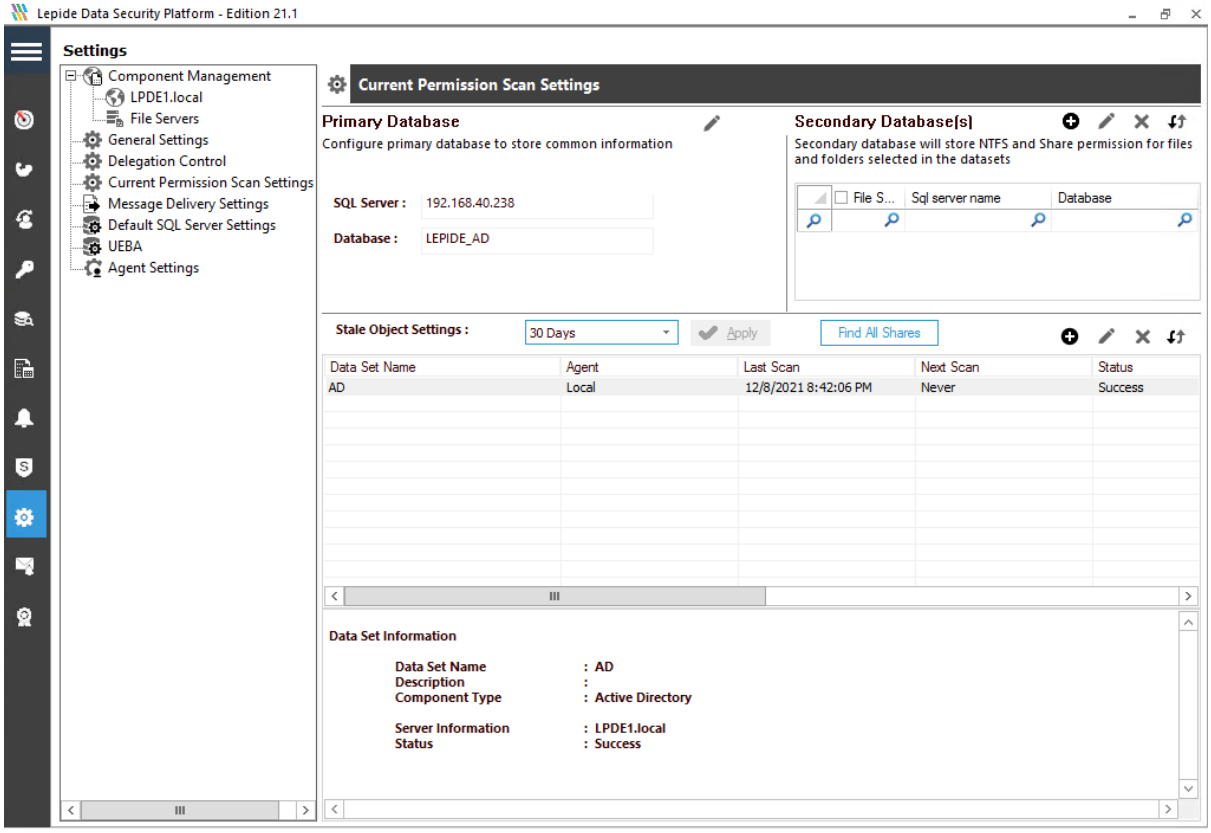


Figure 11: Data Set Settings

4.3. Run the Users with Admin Privileges Report

Once a scan has run, you can generate the Users with Admin Privileges Report:

To view the Users with Admin Privileges Report:

Click the Permissions and Privileges icon:

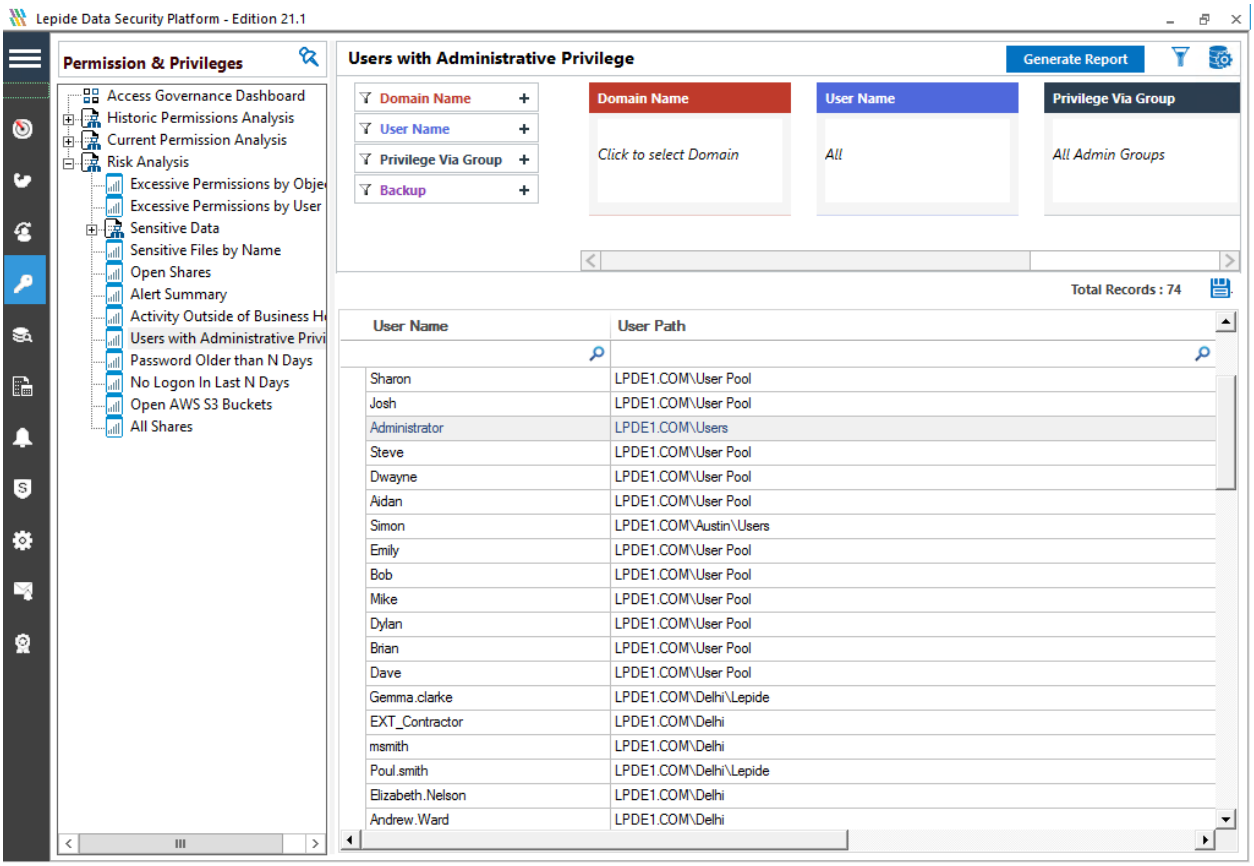


Figure 12: Permissions & Privileges

- Expand **Risk Analysis**
- Click on **Users with Administrative Privilege**
- From the top of the screen, under **Domain Name** click on **Click to select Domain**.

The following dialog box is displayed:

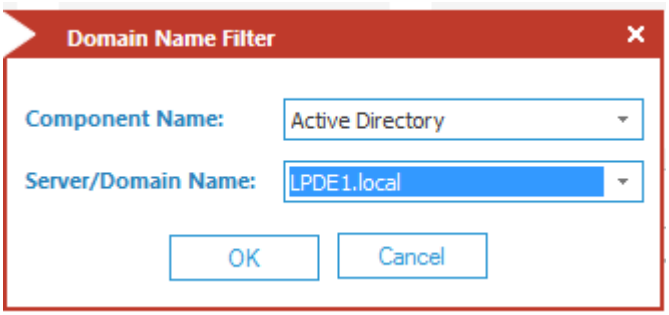


Figure 13: Domain Name Filter

- Select **Active Directory** from the Component Name drop down list
- Select the **Server/Domain Name**
- Click **OK**
- Click **Generate Report**

The report will run showing all Admin users grouped by the different Admin types:

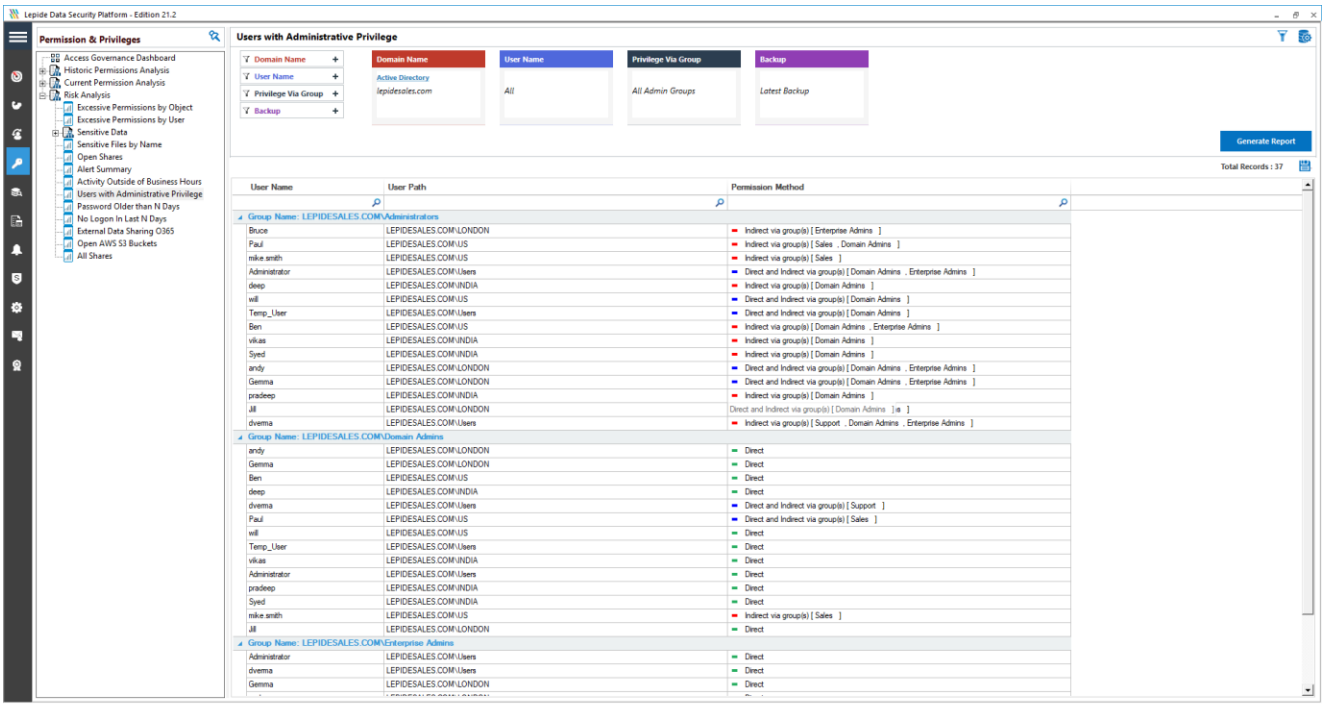


Figure 14: Users with Administrative Privilege Report

The report consists of three columns: User Name, User Path and Permission Method.

The **Permission Method** column includes color coding to show how the users' permissions are derived:

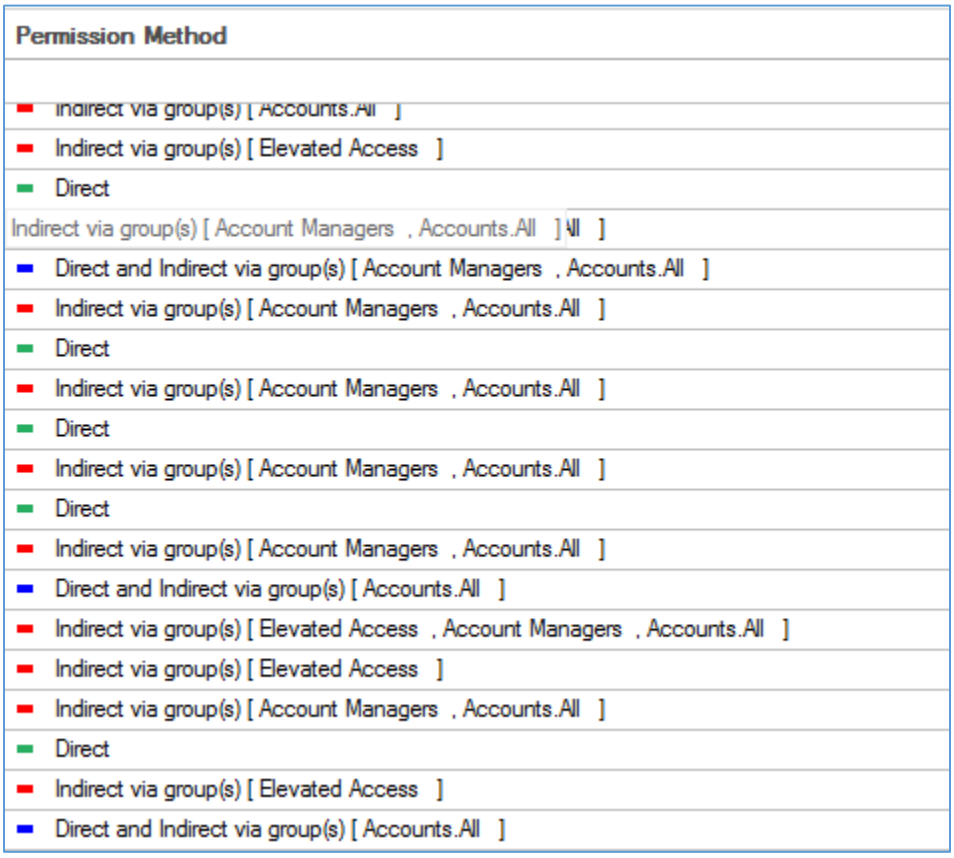


Figure 15: Permission Method Column

Green: Direct permission

Red: Indirect permissions

Blue: Direct and Indirect permissions

Where privileges have been given via a group, you can click in the **Permission Method** column for the user permissions you want to check, and a dialog box will be displayed:

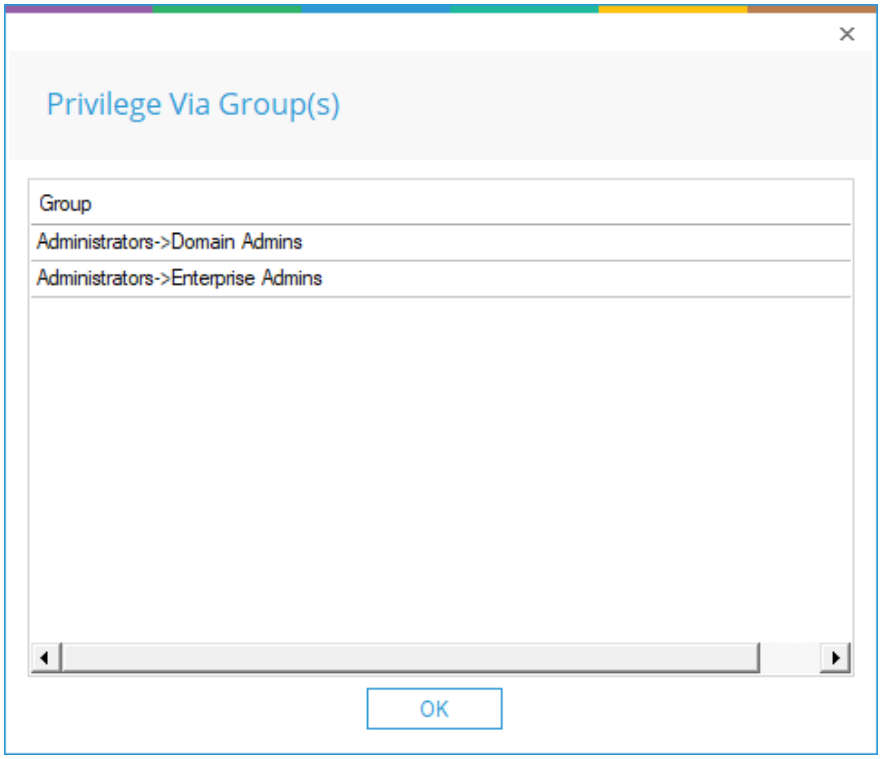
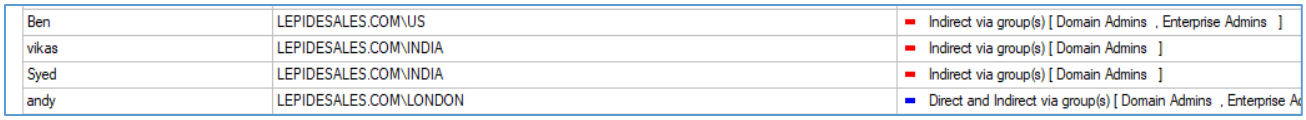


Figure 16: Privilege Via Groups

Example Report



Ben	LEPIDESALES.COM\US	Indirect via group(s) [Domain Admins , Enterprise Admins]
vikas	LEPIDESALES.COM\INDIA	Indirect via group(s) [Domain Admins]
Syed	LEPIDESALES.COM\INDIA	Indirect via group(s) [Domain Admins]
andy	LEPIDESALES.COM\LONDON	Direct and Indirect via group(s) [Domain Admins , Enterprise A

Figure 17: Report Example

For example, in the above section of a report, we can see that Ben has Indirect privileges via the Domain Admins and Enterprise Admins group. Clicking on that entry in the report will show the following:

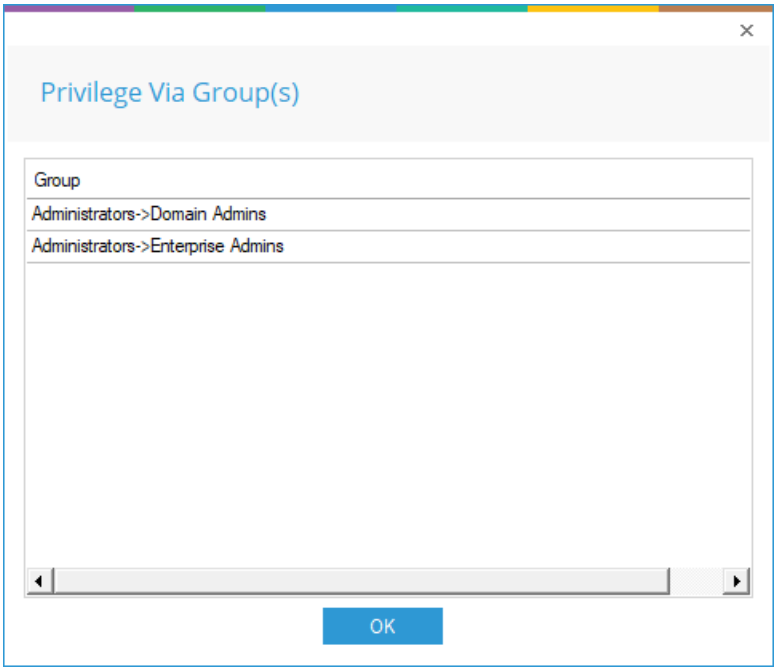


Figure 18: Privilege Groups for a Particular User

5. 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/.

6. 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.