# Lepide USE CASE GUIDE

HOW TO USE LEPIDE TO IDENTIFY USERS WITH ADMINISTRATIVE PRIVILEGES

# Table of Contents

3
3
3
5
5
5
16
22
22
•••



## 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:

Description & Deballance 😵	Users with Administrative	Privilege			<b>Y</b>
Permission & Privileges		, interest			
B Access Governance Dashboard	Y Domain Name +	Domain Name User	Name Privilege Via Group	Backup	
Current Permissions Analysis	Y User Name +	Active Directory			
Risk Analysis	V Privilege Via Group +	lepidesales.com All	All Admin Groups	Latest Backup	
Excessive Permissions by Object	7 Autom				
Excessive Permissions by User	• backup •				
Sensitive Data					
Sensitive Files by Name					Generate Rep
					Total December 37
					Iotal Records : 37
Activity Outside of Business Hours	User Name	User Path		Permission Method	
Password Older than N Days		Q		0	Q
No Logon In Last N Days	▲ Group Name: LEPIDESALE	S.COM\Administrators			
	Bruce	LEPIDESALES.COM\LONDON		<ul> <li>Indirect via group(a) [Enterprise Admins ]</li> </ul>	
	Paul	LEPIDESALES.COM\US		<ul> <li>Indirect via group(s) [ Sales , Domain Admins ]</li> </ul>	
All Shares	mike smith	LEPIDESALES.COM\US		<ul> <li>Indirect via group(s) [ Sales ]</li> </ul>	
	Administrator	LEPIDESALES.COM\Users		<ul> <li>Direct and Indirect via group(s) [ Domain Admins _ Enterprise Admins ]</li> </ul>	
	deep	LEPIDESALES.COM\INDIA		<ul> <li>Indirect via group(s) [ Domain Admins ]</li> </ul>	
	will	LEPIDESALES.COM\US		<ul> <li>Direct and Indirect via group(s) [ Domain Admins ]</li> </ul>	
	Temp_User	LEPIDESALES.COM\Users		<ul> <li>Direct and Indirect via group(s) [Domain Admins ]</li> </ul>	
	Ben	LEPIDESALES.COM\US		<ul> <li>Indirect via group(s) [ Domain Admins , Enterprise Admins ]</li> </ul>	
	vikas	LEPIDESALES.COM\INDIA		<ul> <li>Indirect via group(s) [ Domain Admins ]</li> </ul>	
	Syed	LEPIDESALES.COM\INDIA		<ul> <li>Indirect via group(s) [ Domain Admins ]</li> </ul>	
	andy	LEPIDESALES.COM\LONDON		<ul> <li>Direct and Indirect via group(s) [Domain Admins . Enterprise Admins ]</li> </ul>	
	Germa	LEPIDESALES.COM\LONDON		<ul> <li>Direct and Indirect via group(s) [Domain Admins _ Enterprise Admins ]</li> </ul>	
	pradeep	LEPIDESALES.COM\INDIA		<ul> <li>Indirect via group(s) [ Domain Admins ]</li> </ul>	
	II.	LEPIDESALES.COM\LONDON		Direct and Indirect via group(s) [Domain Admins ] a ]	
	dvema	LEPIDESALES.COM\Users		<ul> <li>Indirect via group(s) [ Support , Domain Admins , Enterprise Admins ]</li> </ul>	
	▲ Group Name: LEPIDESALE	S.COM\Domain Admins			
	andy	LEPIDESALES.COM\LONDON		- Direct	
	Gemma	LEPIDESALES.COM\LONDON		- Direct	
	Ben	LEPIDESALES.COM\US		- Direct	
	deep	LEPIDESALES.COM\INDIA		= Direct	
	dvema	LEPIDESALES.COM\Users		<ul> <li>Direct and Indirect via group(s) [ Support ]</li> </ul>	
	Paul	LEPIDESALES.COM\US		<ul> <li>Direct and Indirect via group(s) [ Sales ]</li> </ul>	
	will	LEPIDESALES.COM\US		- Direct	
	Temp_User	LEPIDESALES.COM\Users		- Direct	
	vikas	LEPIDESALES.COM\INDIA		- Direct	
	Administrator	LEPIDESALES.COM\Users		- Direct	
	pradeep	LEPIDESALES.COM\INDIA		- Direct	
	Syed	LEPIDESALES.COM\INDIA		- Direct	
	mike.smith	LEPIDESALES.COM\US		<ul> <li>Indirect via group(s) [ Sales ]</li> </ul>	
	IL	LEPIDESALES.COM\LONDON		- Direct	
	▲ Group Name: LEPIDESALE	S.COM\Enterprise Admins			
	Administrator	LEPIDESALES.COM\Users		- Direct	
	dvema	LEPIDESALES.COM\Users		- Direct	
	Gemma	LEPIDESALES.COM\LONDON		- Direct	

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 <u>Active Directory Quick Guide</u>.

### 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:

🚻 Lep	pide Data Security Platform - Edition 21.1						-	8 ×
	Settings							
	Component Management	Current Permission Scan S	ettings					
8	File Servers General Settings	Primary Database	ommon information		Secondary Data	base(s)	permission	K ↓Ĵ
<b>ن</b>	Delegation Control     Current Permission Scan Settings				and folders selecte	d in the datasets		
C	Message Delivery Settings Default SQL Server Settings UEBA	SQL Server : Database :			▶ File S	Sql server name Da	:abase	٩
^	Agent Settings							
<b>S</b> A		Stale Object Settings : 30 1	Days 🔹 🖌	Apply	Find All Share	s e		tt X
Ē		Data Set Name	Agent	Last S	can	Next Scan	Status	
5								
۲								
M								
0		<	Ш					>
×								~
	< III >	<						>

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:

							×
Database Set	tings						
Please enter SQL s	erver details to s	tore data					
Configure SQL Ser	ver						
SQL Server :	1						
	Authentication				I		
	Windows Au	thentication					
	<b>SQL</b> Authent	ication					
	User Nam	ie :					
	Password	d :					
				Test Connection			
Select Database :						*	
Time-Out Settings							
Conn	ection Time-Out :	300	÷ :	Seconds			
Query	/ Time-Out :	300	÷ :	Seconds			
		Apply	Ca	ancel			

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



		×
Database Set Please enter SQL	ttings server details to store data	
Configure SQL Se	rver	
SQL Server :	192.168.40.238	
	Authentication OWindows Authentication	
	SQL Authentication User Name : Sa	
	Password :	
	Test Connection	
Select Database :	LEPIDE_AD +	
Time-Out Setting	5	
Con	nection Time-Out : 300 📮 Seconds	
Que	ry Time-Out : 300 🐥 Seconds	
	Apply Cancel	

Figure 4: Database Settings

#### Click Apply

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



🚻 Lep	oide Data Security Platform - Edition 21.1										- 6	J X
	Settings											
	Component Management	🔅 Current P	ermission Scan Se	ttings								
8	File Servers	Primary Datab	lase		-		Secondary Data	base(s)	0	<b>A</b> <sup>2</sup>	×	ţţ
	Delegation Control	Configure primary	y database to store co	ommon information			Secondary database and folders selected	will store NTFS ar in the datasets	nd Share p	ermissio	n for	files
	Current Permission Scan Settings	SQL Server :	192.168.40.238				File S 9	oql server name	Data	base		
4	Default SQL Server Settings	Database :	LEPIDE_AD				Q Q		Q			Q
1	Agent Settings		-									
<b>2</b> 4		Stale Object Set	ttings : 30 D	ays -	🖌 🗛	oply	Find All Share	S	0	<b>A</b> <sup>2</sup>	×	t).
		Data Set Name		Agent		Last Sc	can	Next Scan		Status		
S												
•												
		<	1	1								>
ହ												
		<									;	~

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:



				×	
Data Set Infor	rmation				
Please enter Data	Set name and description.				
Data Set Name:	AD				
Description:			^		
			~		
	< <u>B</u>	ack	<u>N</u> ext >	Cancel	

#### 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).



					~
omponent and	Server Info	ormation			
ease select compone	ent(s) and the s	erver(s) to be sca	anned		
Component Name:	File Server				-
	Active Directo AWS S3	ry			^
	Exchange On	Premise			~
	Exchange On	ine			•
Folder Name		Server Name	Apply To		
		Γ	< Back	Next >	Cancel

Figure 7: Component and Server Information

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



				×
Component and S	Server Information			
Please select componer	nt(s) and the server(s) to be so	canned		
Component Name	Active Directory			Ŧ
component numer	Active Directory			
Scan Active Directory	Scan Group Poli	су		
Select domain(s) to scan a	ctive directory for state reports.			
Server				
				٩
lepidesales.com				
		< <u>B</u> ack	<u>N</u> ext >	Cancel

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:

						×
Scan Options						
Please select the scanni	ng method.					
Scan Now						
Schedule Scan					_	
Run every day at 05:4 12/2/2021	6:01 PM, Schedule start from	$\sim$	Char	ige Schedule		
		~				
		< D-	- la	Dinish	Cree	
		< <u>B</u> a	ICK	Finish	Cano	ei

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:

Define Schedule Please select and define the schedule.	×
Schedule     Daily     Weekly     Monthly	
Start on: 12/ 8/2021 • at 8:30:34 PM •	
0K Cancel	

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

#### Click **Finish**

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



🚻 Lep	ide Data Security Platform - Edition 21.1									- 1	8 ×
	Settings										
	Component Management	🔅 Current	Permission Sc	an Settings							
8	File Servers	Primary Dat	abase		/	Secondary Da	atabase(s)	0	/	×	ţĵ
	General Settings	Configure prim	ary database to si	tore common informat	ion	Secondary datab and folders selec	ase will store NTFS a ted in the datasets	nd Share p	ermissi	on foi	r files
•	Current Permission Scan Settings	FOL Convert	102 168 40 228			File S	Sol server name	Data	oase		
3	Default SQL Server Settings	SQL Server :	192,166,40,236			<u>م</u> م	)	P			Q
		Database :	LEPIDE_AD								
	s <u>s</u> rigen seconds										
<b>S</b> A		Stale Object S	Settings :	30 Days	• Apply	Find All Sh	ares	0	<i><i><i>n</i><sup>2</sup></i></i>	×	14
R		Data Set Name		Agent	Last	t Scan	Next Scan	•	Statu	5	
		AD		Local	12/8	8/2021 8:42:06 PM	Never		Succe	SS	
+											
S											
101											
2											
\$		<		Ш							>
×		Data Set Infor	mation								^
		Dat	a Set Name	: AD							
		Cor	nponent Type	: Active Di	ectory						
		Ser Sta	ver Information tus	: LPDE1.lo : Success	al						
	< III >	<									>

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

🐰 Lepide Data Security Platform - Edition 21.1 📃 🖉 🗙								
	Permission & Privileges 🛛 🕅	Users with Administrative Privile	ge		Generate Report	Ø		
	Access Governance Dashboard	Y   Domain Name	omain Name	User Name	Privilege Via Group			
© •	Tristone Permissions Analysis     Risk Analysis     Excessive Permissions by Objee     Excessive Permissions by User     Sonetive Data	Y     User Name     +       Y     Privilege Via Group     +       Y     Backup     +	ick to select Domain	All	All Admin Groups			
*	Sensitive Files by Name					>		
۶	Open Shares				Total Records : 74			
	Activity Outside of Business H	User Name	User Path					
~	Password Older than N Days	Q				2		
Ē.		Sharon	LPDE1.COM\User Pool					
	Open AWS S3 Buckets	Josh	LPDE1.COM\User Pool			_ 11		
<b>A</b>	All Shares	Administrator	LPDE1.COM\Users			_		
_		Steve	LPDE1.COM\User Pool			- 11		
S		Dwayne	LPDE1.COM\User Pool					
		Aidan	LPDE1.COM\User Pool			_		
0		Simon	LPDE1.COM\Austin\Users			_		
		Emily	LPDET.COM\User Pool			- 11		
$\sim$		BoD	LPDET.COM/User Pool			—		
		Dutan	LPDE1.COM/User Pool			— 11		
Θ		Brian	LPDE1.COM/User Pool			- 11		
		Dave	LPDE1.COM\User Pool			- 11		
		Germa clarke	LPDE1.COM\Delbi\Lenide			- 11		
		EXT Contractor	LPDE1.COM\Delhi			- 11		
		msmith	LPDE1 COM\Delhi			- 11		
		Poul.smith	LPDE1.COM\Delhi\Lepide					
		Elizabeth.Nelson	LPDE1.COM\Delhi					
		Andrew.Ward	LPDE1.COM\Delhi			-		
	< III >							

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:

Domain Name Filter		×
Component Name:	Active Directory	-
Server/Domain Name:	LPDE 1.local	-
ОК	Cancel	

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:

🚻 Le	{ Lepide Data Security Platform - Edition 21.2 _ − Ø ×										
=	Permission & Privileges	2	Users with Administrative P	rivilege							Y 🐻
0	BE Access Governance Dashboard     Bar Historic Permissions Analysis     Grave Current Permission Analysis     Grave Rask Analysis     Grave Rask Analysis     Grave Rask Analysis		Y     Domain Name     +       Y     User Name     +       Y     Privilege Via Group     +       Y     Backup     +	Domain Name Active Directory lepidesoles.com	User Name All	Privilege Via Group All Admin Groups		Backup Latest Backup			
6	Excessive Permissions by User     Excessive Data     Gamma Sensitive Files by Name									Generate Re	eport
۶	Open Shares									Total Records : 3	s7 💾
-			User Name	User Path			Perm	ission Method			-
8	Users with Administrative Privilege			Q		\$	>		Q		
EA.	No Logon In Last N Days		▲ Group Name: LEPIDESALES.0	COMVAdministrators							
68	External Data Sharing O365		Bruce	LEPIDESALES.COM\LONDON			- k	idirect via group(s) [Enterprise Admins ]			
•			Paul	LEPIDESALES.COM\US			- k	idirect via group(s) [ Sales , Domain Admins ]			
•	All Shares		mike.smith	LEPIDESALES.COM\US			- k	idirect via group(s) [ Sales ]			
			Administrator	LEPIDESALES.COM\Users			- 0	irect and Indirect via group(s) [ Domain Admins , Enterprise Admins ]			
•			deep	LEPIDESALES.COM/INDIA			- k	idirect via group(s) [ Domain Admins ]			
*			will	LEPIDESALES.COM\US			- 0	irect and Indirect via group(s) [ Domain Admins ]			
*			Temp_User	LEPIDESALES.COM\Users			- 0	irect and Indirect via group(s) [ Domain Admins ]			
-			Ben	LEPIDESALES.COM\US			- k	idirect via group(s) [ Domain Admins . Enterprise Admins ]			
•			vikas	LEPIDESALES.COM/INDIA			- k	idirect via group(s) [ Domain Admins ]			
~			Syed	LEPIDESALES.COM/INDIA			- k	idirect via group(s) [Domain Admins ]			
8			andy	LEPIDESALES.COM\LONDON			- 0	irect and Indirect via group(s) [ Domain Admins , Enterprise Admins ]			
			Gemma	LEPIDESALES.COM\LONDON			- 0	irect and Indirect via group(s) [ Domain Admins , Enterprise Admins ]			
			pradeep	LEPIDESALES.COM/INDIA			- 1	idirect via group(s) [ Domain Admins ]			
			38	LEPIDESALES.COM\LONDON			Direct	and Indirect via group(s) [ Domain Admins ] is ]			
dverma LEPIDESALES.COM/Users - Indirect via group(s) [Support . Domain			idirect via group(s) [ Support , Domain Admins , Enterprise Admins ]								
			▲ Group Name: LEPIDESALES.0	COM\Domain Admins							
			andy	LEPIDESALES.COM\LONDON			- 0	liect			
			Gemma	LEPIDESALES.COM/LONDON			- 0	Wect			
			Ben	LEPIDESALES.COM/US			- 0	wect			
			oeep	LEPIDESALES.COM/INDIA			- 0	weet			
			uventia Revi	LEPIDESALES.COM/Users			- 0	mech and indirect via group(a) [ Support ]			
			rau	LEPIDESALES.COM/US				rect and indirect via group(s) [ Sales ]			
			Terro Liter	LEPIDESALES COMULIAR				eeu			
			vikas	LEPIDESALES COMUNDIA				inet.			
			Administrator	LEPIDESALES COMULTARY				inst.			
			pradeep	LEPIDESALES COM/INDIA			- 0	iect			
			Sved	LEPIDESALES COM/INDIA			- 0	ired			
			mike.smith	LEPIDESALES.COM\US			- 1	direct via group(s) [ Sales ]			
		JAI LEPIDESALES COMILONDON - Direct									
		▲ Group Name: LEPIDESALES.COMVEnterprise Admins									
Administrator LEPIDESALES.COM\Users				- 0	irect						
			dverma	LEPIDESALES.COM\Users			- 0	lirect			
			Gemma	LEPIDESALES.COM\LONDON			- 0	irect			
											•

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:

Permission Method					
<ul> <li>Indirect via group(s) [ Accounts.Aii ]</li> </ul>					
<ul> <li>Indirect via group(s) [ Elevated Access ]</li> </ul>					
- Direct					
Indirect via group(s) [ Account Managers , Accounts.All ] 🛚					
<ul> <li>Direct and Indirect via group(s) [Account Managers , Accounts.All ]</li> </ul>					
<ul> <li>Indirect via group(s) [ Account Managers , Accounts.All ]</li> </ul>					
- Direct					
<ul> <li>Indirect via group(s) [ Account Managers , Accounts.All ]</li> </ul>					
= Direct					
<ul> <li>Indirect via group(s) [ Account Managers , Accounts.All ]</li> </ul>					
- Direct					
<ul> <li>Indirect via group(s) [ Account Managers , Accounts.All ]</li> </ul>					
<ul> <li>Direct and Indirect via group(s) [ Accounts.All ]</li> </ul>					
<ul> <li>Indirect via group(s) [ Elevated Access , Account Managers , Accounts.All ]</li> </ul>					
<ul> <li>Indirect via group(s) [ Elevated Access ]</li> </ul>					
<ul> <li>Indirect via group(s) [ Account Managers , Accounts.All ]</li> </ul>					
- Direct					
<ul> <li>Indirect via group(s) [ Elevated Access ]</li> </ul>					
<ul> <li>Direct and Indirect via group(s) [ Accounts.All ]</li> </ul>					

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:



			>
Privilege Via Group(s)	1		
Group			
Administrators->Domain Admins			
Administrators->Enterprise Admins			
•			•
		_	
	ОК		

Figure 16: Privilege Via Groups

### **Example Report**

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

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:

		/		
Group				
Administrators->Do	omain Admins			
Administrators->Er	terprise Admins			

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	Technical Gurus
USA/Canada: +1(0)-800-814-0578	USA/Canada: +1(0)-800-814-0578
UK/Europe: +44 (0) -208-099-5403	UK/Europe: +44 (0) -208-099-5403
Rest of the World: +91 (0) -991-004-9028	Rest of the World: +91(0)-991-085-4291

Alternatively, visit <u>https://www.lepide.com/contactus.html</u> 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 <u>https://www.lepide.com/data-security-platform/</u>.

## 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.

