%Lepide

CONFIGURATION GUIDE

THE PRINCIPLE OF LEAST PRIVILEGE FOR ACTIVE DIRECTORY

Table of Contents

1.	Introduction	3
2.	Least Privilege Model for Active Directory, Group Policy and Exchange On-Premises	3
	2.1. What's Available with the Least Privilege Model?	3
	2.2. What's Not Available with the Least Privilege Model?	3
	2.3. Minimum Rights Required	4
	2.4. Setting up the Account Privileges	4
3.	Support	19
4.	Trademarks	19

1. Introduction

The purpose of this document is to detail the minimum rights and privileges required for configuring the Lepide Active Directory component for auditing and the steps which are needed to complete the configuration for a successful setup.

2. Least Privilege Model for Active Directory, Group Policy and Exchange On-Premises

2.1. What's Available with the Least Privilege Model?

- a. All AD/GPO/Exchange Modification reports, i.e. States and Changes.
- b. Real time alerts and Schedules.
- c. Full reporting under Web Console.
- d. AD and GPO Backups.
- e. AD and GPO State Reports.
- f. Lepide Active Directory Cleaner.
- g. Lepide User Password Expiration Reminder.
- h. All AD/GPO Risk Analysis Reports.
- i. Agent-Less Auditing

2.2. What's Not Available with the Least Privilege Model?

- a. AD and GPO Restore.
- b. Non-Owner Mailbox Auditing under Exchange.
- c. Health Monitoring.
- d. Automatic Enabling of the Native Auditing from the DCs. (This is a one time process and can be done manually)
- e. Automatic Event Log Management of the DCs.
- f. Data Discovery and Classification of Exchange Mailboxes.



g. Agent Based Auditing.

2.3. Minimum Rights Required

- a. A Domain User Account.
- b. This account should have **Db_owner/Db_creator** rights over the SQL databases. An SQL account with the mentioned privileges can also be used.
- c. This account should be a member of the **Event Log Readers** group inside AD.
- d. This account should be a member of the **Administrators** Group on the Lepide Server.
- e. This account should be a member of **Organization Management** group inside AD for Exchange Auditing.

2.4. Setting up the Account Privileges

1. Create a user account in Active Directory and add it under the **Event Log Readers** group.

Remote	control	Remote	Desktop Se	ervices Profile	CC	+Me
General	Address	Account Profile Telephones (Organi	zatio
Member Of		Dial-in	al-in Environment		Sessions	
Member o	of:					
Name		Active Direct	ory Domain	Services Folder		
Domain	Users	LPDE1.local	/Users			
Event L	og Readers	LPDE1.local	/Builtin			

Figure 1: Add User Account in Active Directory

- 2. Add this user account under the **Local Admin Group** on the Lepide Server. To do this, follow the steps below:
 - i. In the **Run** window, type **mmc** and press **Enter**.

The following screen will be displayed:

E		Console1 - [Console Root]
<u> File</u> Action <u>V</u> iew Fav <u>o</u> rites <u>W</u> ind	ow <u>H</u> elp	
🗢 🏟 📰 🔒 🛛 🗊		
Console Root	Name	
		There are no items to show in this view.
	1	



ii. From the File Menu, choose **Add/Remove Snap-IN**.

		_				
-	File	Action	View	Favorites	Window	Help
		New				Ctrl+N
r		Open				Ctrl+O
		Save				Ctrl+S
		Save As				
		Add/Rem	ove Sna	p-in		Ctrl+M
		Options				
	1 C:\Windows\system32\secpol					
	2 C:\Windows\system32\eventwvr					
		3 C:\Wind	lows\sy	stem32\serv	rices	
		4 C:\Wind	lows\sy	stem32\dsa		
		Exit				

Figure 3: File Menu

The following dialog box is displayed:



iap-in	Vendor	^		Console Root	Edit Extensions
Failover Cluster Man	Microsoft Cor				
Folder	Microsoft Cor				Remove
Group Policy Manag	Microsoft Cor				
Group Policy Manag	Microsoft Cor				Move Lin
Group Policy Object	Microsoft Cor				
Group Policy Starter	Microsoft Cor				Move <u>D</u> own
Internet Informatio	Microsoft Cor	≡	<u>A</u> dd >		h
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor				
Docal Backup	Microsoft Cor				
Local Users and Gro	Microsoft Cor				
NAP Client Configur	Microsoft Cor	~]		Advanced

Figure 4: Add or Remove Snap-ins

i. Choose Local Users and Groups

ii. Click Add

The following dialog box is displayed:

Choose Target Machine	x
Select the computer you want this snap-in to manage. This snap-in will always manage: Local computer: [the computer on which this console is running]	
Another computer: Allow the selected computer to be changed when launching from the commonly applies if you save the console.	Browse hand line. This
< <u>B</u> ack Finish	Cancel

Figure 5: Choose Target Machine

- iii. Select Local computer
- iv. Click Finish
- v. Click **OK**

1. When the **Choose Target Machine** wizard is closed, the **Local Users and Group** node is added to the console:



Figure 6: Microsoft Management Console

- 2. Select **Administrator** from the middle pane and double click.
- 3. The Administrators Properties dialog box is displayed:



Administrators Properties ? X					\times
General					
Administrators					
Description:	Administrator the compute	rs have complet r/domain	te and unrestricte	ed access	s to
Members:					
Administrator & LPDE1\Dom LPDE1\Svol LPDE1\Svol	r ain Admins ∟epide (Svo-Le	apide@LPDE1.I	local)		
Add	Remove	Changes to are not effe user logs or	a user's group r ctive until the ne n.	members xt time th	hip .e
	ОК	Cancel	Apply	Hel	p

Figure 7: Administrators Properties

- 4. From the Administrators Properties window, add the newly created user with default access rights.
- 5. Log in to the Lepide Server using the newly created user credentials.
- 6. Open **ADSIEdit** and provide access rights to the newly created user using the different naming context of Active Directory.
- 7. To do this, follow these steps:
 - i. From the **Run** window, type **ADSIEDIT**.**msc** and press **Enter**:
 - ii. Right click on the ADSI Edit node and Select **Connect to....**



		ADSI Edit
File Actio	on View Help	
📝 ADSI Ed	Connect to View	Welcome to ADSI Ec
	Refresh Help	Active Directory Services Interf Editor (ADSI Edit) is a low-leve editor for Active Directory Don Services / Active Directory Lightweight Directory Services



iii. From the Connection Settings dialog box, select **Default naming context** and click **OK**

Connection Settings
Name: Default naming context
Path: LDAP://H-EX13.www.ldp13.com/Default naming context
Connection Point O Select or type a <u>D</u> istinguished Name or Naming Context:
✓
Select a well known Naming Context:
Default naming context 🗸 🗸
Computer
O Select or type a domain or <u>server</u> : (Server Domain [:port])
×
• Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced OK Cancel

Figure 9: Connection Settings

- iv. The **Default Naming context** node will be added to the console.
- v. Expand **Default naming context** node and right click on the domain name node as shown below:

2						
File Action View Help						
🗢 🄿 📶 💥 🗐 🖬 🗟 🖬						
📝 ADSI Edit	📝 ADSI Edit					
Default naming context [H-EX13.v	www.lo	dp13.com]				
DC=www,DC=Idp13,DC=com						
		New	•			
		View	•			
		Rename				
		Refresh				
		Export List				
		Properties				
		Help				



vi. From the Properties window, add the newly created user with default access rights:



DC=LPDE1,DC=local Properties		? ×		
Attribute Editor Security				
Group or user names:				
Administrators (LPDE1\Administrators) Pre-Windows 2000 Compatible Access (LPDE1\Pre-Windows 20 Incoming Forest Taust Builders (LPDE1)(propring Forest Taust Builders (LP				
Incoming Forest Must Builders (LPDE Micoming Forest Must Bu				
Svc Lepide (Svc-Lepide@LPDE1.loca	al)	~		
	Add	Remove		
Permissions for Suc Lonido	Allow	Denv		
Permissions for SVC Lepide	Allow	Deny		
Full control				
Full control Read				
Full control Read Write				
Full control Read Write Create all child objects				
Full control Read Write Create all child objects Delete all child objects				
Full control Read Write Create all child objects Delete all child objects For special permissions or advanced setting Advanced.	gs, dick	Advanced		
Full control Read Write Create all child objects Delete all child objects For special permissions or advanced setting Advanced.	gs, click	Advanced		
Full control Read Write Create all child objects Delete all child objects For special permissions or advanced setting Advanced.	gs, click	Advanced		

Figure 11: Properties

vii. Repeat the steps above to add another naming context.

Please do not give any permissions to **RootDSE**, as the rights will not be accepted.



Connection Settings X				
Name: Default naming context				
Path: LDAP://H-EX13.www.ldp13.com/Default naming context				
Connection Point O Select or type a <u>D</u> istinguished Name or Naming Context:				
✓				
Select a well known Naming Context:				
Default naming context				
Comp RootDSE Se Schema				
✓				
Default (Domain or server that you logged in to) Use SSL-based Encryption				
Ad <u>v</u> anced OK Cancel				

Figure 12: Connection Settings

1. From the Properties dialog box, select **Organization Management**:



DC=LPDE1,DC=local Properties	?	x		
Attribute Editor Security				
Group or user names:				
& NETWORK SERVICE		^		
Corganization Management (LPDE1\Organization Management)				
😣 Delegated Setup (LPDE1\Delegated Setup)				
Exchange Servers (LPDE1\Exchange Servers)				
Exchange Trusted Subsystem (LPDE1\Exchange Trusted S	& Exchange Trusted Subsystem (LPDE1\Exchange Trusted Subs			
Kchange Windows Permissions (LPDE1\Exchange Window	ws			
A <u>d</u> d <u>R</u>	emove	е		
Permissions for Organization Management Allow	Deny			
Full control	\Box			
Read				
Write				
Create all child objects				
Delete all child objects		$\overline{}$		
For special permissions or advanced settings, click Ad <u>v</u> anced Advanced.				
OK Cancel Apply	He	elp		

Figure 13: Properties

- 2. Give **Full Control** access rights to this account on the installation folder (C:\Program Files (x86)\LepideAuditor Suite).
- 3. Configure the Lepide service with the newly created user.
- 4. In SQL, create a login by adding the newly created user and selecting **DB Creator** as the role.
- 5. For Active Directory Cleaner, select Delegation Control for this user account:

1		
1	File Action View Help	
	🗢 🔿 🙍 🖬 📋 🖾 🕰 🕞 🖉 📷 🗏 📚 箇	7 🖻 🐍
	Active Directory Users and Computers [DCD01.LPDE1.local] Saved Queries Image: Saved Queries <th>Name Builtin Computers Computers ForeignSecurityf Managed Service Computer Pool Computer Pool</th>	Name Builtin Computers Computers ForeignSecurityf Managed Service Computer Pool

Figure 15: Delegate Control

The Delegation of Control Wizard will start:



Figure 14: Delegation of Control Wizard

6. Click Next

Delegation of Control Wizard X				
Users or Groups Select one or more users or groups to whom you want to delegate control.				
Selected users and groups:				
Add Remove				
< Back Next > Cancel Help				

Figure 16: Add User

7. Click **Add** to add a user

Delegation of Control Wizard
Users or Groups Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
Sam (Sam@LPDE1.Jocal)
Add Remove
<back next=""> Cancel Help</back>

Figure 17: Added User

Delegation of Control Wizard	x		
Tasks to Delegate You can select common tasks or customize your own.	P		
O Delegate the following common tasks:			
□ Create, delete, and manage user accounts ^ □ Reset user passwords and force password change at next logon □ □ Read all user information □ □ Modify the membership of a group □ □ Join a computer to the domain □ □ Manage Group Policy links □ □ Generate Resultant Set of Policy (Planning) ✓			
Oreate a custom task to delegate			
< Back Next > Cancel He	lp		

Figure 18: Tasks to Delegate

- 8. Select Create a custom task to delegate
- 9. Select User Objects and Computer Objects from the list

Delegation of Control Wizard
Active Directory Object Type Indicate the scope of the task you want to delegate.
Delegate control of:
O This folder, existing objects in this folder, and creation of new objects in this folder
Only the following objects in the folder:
 transportStack objects Trusted Domain objects ✓ User objects x25Stack objects x25X400Link objects x400Link objects Create selected objects in this folder Delete selected objects in this folder
< Back Next > Cancel Help

Figure 19: Active Directory Object Type

10. Click Next

Delegation of Control Wizard	x
Permissions Select the permissions you want to delegate.	R
Show these permissions: General Property-specific Creation/deletion of specific child objects Permissions:	
 Full Control Read Write Create All Child Objects Delete All Child Objects Read All Properties 	< III >
< Back Next > Cancel	Help

Figure 20: Permissions

11. Select the **Permissions** to delegate

12. Click Next

The last step of the Wizard will appear with a summary of delegation of control you have set up:



De	elegation of Control Wizard
	Completing the Delegation of Control Wizard You have successfully completed the Delegation of Control wizard. You chose to delegate control of objects in the following Active Directory folder: LPDE1.Jocal/ The groups, users, or computers to which you have given control are: Sam (Sam@LPDE1.Jocal) They have the following permissions: Vouces this wizard, click Finish.
	< Back Finish Cancel Help

Figure 21: Summary of Delegation of Control

13. Click Finish

NOTE: A new account must be created for using AD Cleaner and then the Lepide server should be logged on with the same account.

3. 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 <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 https://www.lepide.com/data-security-platform/.

4. 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.

