%Lepide

CONFIGURATION GUIDE

PRINCIPLE OF LEAST PRIVILEGE MODEL

Table of Contents

1	Intro	oduction	4
2	Activ	e Directory, Group Policy and Exchange On-Premises	4
	2.1	What's Available with the Least Privilege Model?	4
	2.2	What's Not Available with the Least Privilege Model?	4
	2.3	Minimum Rights Required	5
	2.4	Setting up the Account Privileges	5
3	Wine	dows File Server Auditing	20
	3.1	What's Available?	20
	3.2	What's Not Available?	20
	3.3	Minimum Rights Required	20
	3.4	Adding the Windows File Server with Least Privileges	20
4	Net/	App Cluster Mode	22
	4.1	Minimum Rights Required	22
	4.2	Adding the NetApp Cluster Mode with Least Privileges	23
5	Exch	ange Online	25
	5.1	Prerequisites	25
	5.2	Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing	25
	5.3	Assigning the Role to the Application	25
	5.4	Permissions for Auditing, DDC, & CPA	26
		5.4.1 Permissions for Auditing	26
		5.4.2 Permissions for Data Discovery & Classification	27
		5.4.3 Permissions for Current Permissions Analysis	27
	5.5	Install the Exchange Online Management Module	27
	5.6	Generate the Certificate for Tenant on the LDSP Server	28
	5.7	Install the Certificate on DDC Agent \ FSA Agent	28
	5.8	Register your Certificate with Microsoft Identity Platform	29
6	Shar	ePoint Online	30
	6.1	Prerequisites	30
	6.2	Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing	30
	6.3	Generate the Client ID and Secret Key for SharePoint Online Data Discovery & Classification	31
	6.4	Generate the Client ID and Secret Key for SharePoint Online Current Permissions Analysis	33
	6.5	Permissions	35
		6.5.1 Auditing Permissions	35
		6.5.2 Data Discovery and Classification Permissions	35

		6.5.3	Current Permissions Analysis Permissions
7	036	5 Com	ponent
	7.1	Prere	quisites
	7.2	OneD	0rive
		7.2.1	Register an App and Generate the Client ID and Secret Key for OneDrive Auditing
		7.2.2	Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification
		7.2.3	Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis
	7.3	Azure	
		7.3.1	Register an App and Generate the Client ID and Secret Key for Azure Auditing
		7.3.2	Azure Current Permission Analysis
	7.4	Team	ıs
		7.4.1	Register an App and Generate the Client ID and Secret Key for Teams Auditing
	7.5	Skype	e for Business
		7.5.1	Register an App and Generate the Client ID and Secret Key for Skype for Business Auditing 42
	7.6	Perm	issions
		7.6.1	Auditing Permissions
		7.6.2	Data Discovery and Classification Permissions
		7.6.3	Current Permissions Analysis Permissions
8	Supp	oort	
9	Trad	emark	s46

1 Introduction

The purpose of this document is to detail the Principle of Least Privilege (POLP) minimum rights and privileges required for configuring the specific components for auditing and the steps which are needed to complete the configuration for a successful setup.

2 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 Services Profile			COM+						
General	Address	Account	Profile	Telephones	Organi	zation					
Membe	er Of	Dial-in	Env	ironment	Sessio	ons					
Member of:											
Name		Active Directo	ry 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> in	ndow <u>H</u> elp						
🛅 Console Root	Name						
		There are no items to show in this view.					

Figure 2: Microsoft Management Console

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

5		_							
-	File	Action	View	Favorites	Window	Help			
		New				Ctrl+N			
		Open				Ctrl+O			
		Save				Ctrl+S			
		Save As							
	Add/Remove Snap-in Ctrl+M								
		Options							
		1 C:\Windows\system32\secpol							
		2 C:\Wind	ows\sy:	stem32\ever	ntvor				
		3 C:\Wind	ows\sy:	stem32\serv	ices				
		4 C:\Wind	ows\sy:	stem32\dsa					
		Exit							

Figure 3: File Menu

The following dialog box is displayed:

ap-ip	Vendor		1	Concole Poot	Edit Extensions
aphin Failover Cluster Man	Microsoft Cor	Ĥ		Console ROOL	
Folder	Microsoft Cor				Remove
Group Policy Manag	Microsoft Cor				
Group Policy Manag	Microsoft Cor				
Group Policy Object	Microsoft Cor				Move Up
Group Policy Starter	Microsoft Cor				Move Down
Internet Informatio	Microsoft Cor	≡	<u>A</u> dd >		
Internet Informatio	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor				
Local Backup	Microsoft Cor				
Local Users and Gro	Microsoft Cor				
NAP Client Configur	Microsoft Cor	~			Ad <u>v</u> anced
ription:					
ription:					

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)							
O Another computer:	B <u>r</u> owse						
Allow the selected computer to be changed when launching from the commonly applies if you save the console.	iand 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:

a	Cor	nsole1 - [Console Root\Local U	Isers and Groups (Local)\Groups]		- • ×			
🚡 Eile Action View Favorites Wind	low <u>H</u> elp				_ 8 ×			
Console Root	Name	Description		Actions				
⊿ Set Local Users and Groups (Local)	Access Control Assist	Members of this group can remot		Groups				
Users	Administrators	Administrators have complete an		More Actions	•			
Groups	A Backup Operators	Backup Operators can override se			· ·			
	Rentificate Service DC	Members of this group are allowe		Administrators	^			
	🚇 Cryptographic Operat	Members are authorized to perfor		More Actions	•			
	Distributed COM Users	Members are allowed to launch, a						
	🚇 Event Log Readers	Members of this group can read e						
	A Guests	Guests have the same access as m						
	Byper-V Administrators	Members of this group have com						
	A IIS_IUSRS	Built-in group used by Internet Inf						
	Network Configuratio	Members in this group can have s						
	A Performance Log Users	Members of this group may sche						
	Arrow Monitor	Members of this group can acces						
	A Power Users	Power Users are included for back						
	A Print Operators	Members can administer printers						
	ADS Endpoint Servers	Servers in this group run virtual m						
	🌆 RDS Management Ser	Servers in this group can perform						
	ADS Remote Access S	Servers in this group enable users						
	🌆 Remote Desktop Users	Members in this group are grante						
	🌆 Remote Management	Members of this group can acces						
	A Replicator	Supports file replication in a dom						
	🜆 Users	Users are prevented from making						
	A WinRMRemoteWMIU	Members of this group can acces						
]]				

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 ? ×									
General									
Administrators									
Description: Administrators have complete and unrestricted access to the computer/domain									
Members:									
Administrator	Administrator & LPDE1\Domain Admins LPDE1\Svc-Lepide (Svc-Lepide@LPDE1.local)								
Add	Add Remove Changes to a user's group membership are not effective until the next time the user logs on.								
(OK	Cancel	Apply	Help					

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 Action View Help	
ADSI Edit Connect to View	Welcome to ADSI Ec
Refresh Help	Active Directory Services Interf Editor (ADSI Edit) is a low-level editor for Active Directory Don Services / Active Directory Lightweight Directory Services

Figure 8: Connect To.. Menu

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>s</u> erver: (Server Domain [:port])						
×						
• Default (Domain or server that you logged in to)						
Use SSL-based Encryption						
Ad <u>v</u> anced 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:

Z							
File Action View Help							
🗢 🄿 📶 💥 🗐 🖬 🗟 🖬							
ADSI Edit Default naming context [H-EX13.w DC=www,DC=Idp13,DC=com	/ww.ldp13.com]						
	New 🕨						
	View 🕨						
	Rename						
	Refresh						
	Export List						
	Properties						
	Help						

Figure 10: Select Properties

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

JC=EFDET,DC=local Properties		?	×
Attribute Editor Security			
Group or user names:			
Administrators (LPDE1\Administrators Pre-Windows 2000 Compatible Access Incoming Forest Trust Builders (LPDE ENTERPRISE DOMAIN CONTROLL	s) ss (LPDE1\Pre-Wi 1\Incoming Fores ERS	ndows 20 t Trust Bu	^
Svc Lepide (Svc-Lepide@LPDE1.loc	al)		
			~
	Add	Remove	
Permissions for Svc Lepide	Allow	Deny	
Full control	Ξ,		^
	•		
Read			
Read Write			
Read Write Create all child objects			
Read Write Create all child objects Delete all child objects			~
Read Write Create all child objects Delete all child objects For special permissions or advanced settin Advanced.	gs, click	- - - - Advanced	*
Read Write Create all child objects Delete all child objects For special permissions or advanced settin Advanced.	y , , , , gs, click	Advanced	~
Read Write Create all child objects Delete all child objects For special permissions or advanced settin Advanced.	gs, dick	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 ×
Name: Default naming context
Path: LDAP://H-EX13.www.ldp13.com/Default naming context
Connection Point
O Select or type a <u>Distinguished Name or Naming Context</u> :
v
Select a well known Naming Context:
Default naming context 🗸 🗸
Default naming context
Configuration ComplexetDSE
⊖ Se Schema
×
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced 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		^
Sector Antipage Sector Antipage Sector Antipage Sector Antipage An	ent)	
Belegated Setup (LPDE1\Delegated Setup)		
Exchange Servers (LPDE1\Exchange Servers)		
Exchange Trusted Subsystem (LPDE1\Exchange Trusted S	Subs	
Kchange Windows Permissions (LPDE1\Exchange Windo	ws	
A <u>d</u> d <u>R</u>	<u>l</u> emove	е
Permissions for Organization	2	
Management Allow	Deny	
Full control		Ê I
Read 🗸		
Create all child objects		
		~
For special permissions or advanced settings, click Adv	anced	
Participation (
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:

File Action View Help	
	7 🗕 🕱
Active Directory Users and Computers [DCD01.LPDE1.local] Seved Queries	Name Builtin Computers ForeignSecurityf Austin Computer Pool Delhi Domain Control Group Pool Lepide 2020 Microsoft Exchan NYC test User 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	×
Users or Groups Select one or more users or groups to whom you want to delegate control.	5
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.local)
Add Remove

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) III Create a custom task to delegate 	
< Back Next > Cancel	Help

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:
 Only the following objects in the folder: transportStack objects Trusted Domain objects User objects x25Stack 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	×
Permissions Select the permissions you want to delegate.	R
Show these permissions: General Property-specific Creation/deletion of specific child objects	
Pemissions: Full Control Read Write Create All Child Objects Petete 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	x
	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: LPDE1Jocal/ The groups, users, or computers to which you have given control are: Sam (Sam@LPDE1Jocal) They have the following permissions: V	
	< 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 Windows File Server Auditing

3.1 What's Available?

- a. All File Server Modification reports ie States and Changes.
- b. Permission Analysis.
- c. Alerting and Scheduling.
- d. Full reporting under Web Console.

3.2 What's Not Available?

All the features that are available on a Full Privileged Model are also available with the Least Privileged Model. The only difference is the specific rights and configuration that is required to be done.

3.3 Minimum Rights Required

- a. A Domain User Account.
- b. This account should have db_owner and 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 Local Administrators Group on the File Server.
- d. This account should be a member of the Local Administrators Group on the Lepide Server.
- e. This account should have List Folder/Read Data, Traverse Folder/Execute File and Read Permissions rights on the Shares which are to be audited.
- f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.
- g. The SYSTEM account should have Modify rights on the folder where the agent is installed.

3.4 Adding the Windows File Server with Least Privileges

Follow the steps below to add a File Server with the Least Privileges:

1. Create a Shared Folder on the File Server and assign **Modify** rights to the Domain User account.

Permissions for Lepide		×
Security		
Object name: C:\Company Share	e\Lepide	
Group or user names:		
Security Sec		
SYSTEM		
Administrators (DM-101/Administratore)	strators)	
Svc Lepide (Svc-Lepide@LPD)	E1.local)	
	Add	Remove
Permissions for Svc Lepide	Allow	Deny
Permissions for Svc Lepide Full control	Allow	Deny
Permissions for Svc Lepide Full control Modify	Allow	Deny
Permissions for Svc Lepide Full control Modify Read & execute	Allow	Deny
Permissions for Svc Lepide Full control Modify Read & execute List folder contents	Allow	Deny
Permissions for Svc Lepide Full control Modify Read & execute List folder contents Read	Allow	Deny
Permissions for Svc Lepide Full control Modify Read & execute List folder contents Read	Allow	Deny
Permissions for Svc Lepide Full control Modify Read & execute List folder contents Read	Allow	Deny

Figure 22: Permissions

 Add the file server with the Name or IP and provide the path to the Shared folder in the column Share Path instead of selecting Use Admin\$ for Agent. Also, provide the user account created in the fields given at the bottom of the window.

File Server Name/IP:	LEPIDE-NAS	Add
Domain/Workgroup:	LPDE1	
Cluster Name/IP:		
Use Admin\$ for Ag	ent	
Share path:	\/LEPIDE-NAS/Lepide	0
Authentication:		
OCurrent user (LPD)E1\nick)	
• The following use	er:	
User Name:	LPDE1\svc-Lepide	
Password:	•••••	

Figure 23: Add File Server

- 3. The next steps are similar to the Full Privilege Model installation.
- Permission Analysis can also be done in the same way once the rights are adjusted according to Section
 3.1.2 above.

4 NetApp Cluster Mode

Everything, except the **Permission Analysis Module** is available for NetApp Filers in the Least Privilege Model.

4.1 Minimum Rights Required

- a. A Domain User Account.
- b. This account should have db_owner and db_creator rights over the SQL databases. An SQL account with the mentioned privileges can also be used.
- c. This account should have **Change** Permission on the C\$ in NetApp.
- d. This account should have Modify Rights on the Audit Log Volume.
- e. This account should be a member of the Local **Administrators** Group on the Lepide Server.

f. This account should be used to Logon to the Lepide Server to Configure the File Server for Auditing.

4.2 Adding the NetApp Cluster Mode with Least Privileges

To add the NetApp Filer Cluster Mode for auditing, the native auditing should be enabled manually, and it should meet the following pre-requisites:

- a. The minimum Log File Size (rotate-size) should be 1 MB.
- b. The format of auditing should be XML.
- c. The size of selected audit log volume should be at least 2 GB.
- d. The rotate limit should be applied to the auditing configuration.
- 1. On the first page, provide the IP address and the domain user account. Please ensure to **Uncheck** the **I have Management Access** option.

Please provide NetA	pp filer information.	×
NetApp Filer Name/IP :	Lepide-Netapp	
Password :	•••••	
Minimum rights needed to a	ccess. Iudit NetApp filer.	
	< <u>B</u> ack <u>N</u> ext > Cancel He	lp

Figure 24: NetApp Filer Information

2. In the Least Privilege Model, the **ShareInfo.txt** file is not created itself by the solution. The users will have to create this file manually in a txt format and should have the entries like this for every Share:

SharePath#JunctionPath#ShareName

Share Path: This can be taken from the OnTap Manager in the Share section.

Junction Path: This can be taken from the OnTap Manager in the Volume section

3. On the next page, please provide the audit log volume details along with the version of the NetApp and the location of the **ShareInfo.txt** file.

Audit log configurati	on settings.	×
Audit Log Configuration		
Log Volume Name :	log	
NetApp Version :	9.6 and above ×	
Share Folder Information :	C:\Program Files (x86)\LepideAuditor Suite\FSA\FSM(
	< <u>B</u> ack <u>N</u> ext > Cancel He	lp

Figure 25: Audit Log Configuration Settings

4. All the other steps are the same as the Full Privilege Model where the next step is to put in the SQL server details where the audit logs will be stored.



5 Exchange Online

All the reports and functionalities available for Exchange Online auditing with the Least Privilege model are the same as with the Full Privilege model.

5.1 Prerequisites

The following are prerequisites to add an Exchange Online component to the Lepide Data Security Platform:

- The Lepide Server and Agent's Machine need to be logged in with Admin User
- The Lepide Server and Agent's Machine are required to be Remote signed
- Dot Net FrameWork 4.6.2 Developer Pack is required on the Lepide Server and Agent's Machine.
- Tls 1.2 is required for the Lepide Server and Agent's Machine

5.2 Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing

- 1. Log into the Microsoft 365 account through Global Admin
- 2. Select Azure Active Directory Account through the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration and select supported account type
 - Click on **Register Account** and client ID will be displayed which the user can copy for future reference
 - For the given Client ID generated in the Azure Account Dashboard, click on Certificates and Secrets
 - Click on Add New Client Secret (with expiry period) and a Secret ID will be generated which the user can copy for future reference

5.3 Assigning the Role to the Application

- 1. Go to Azure Active Directory Dashboard and select the tab **Roles and Administrators**
- 2. Under Roles and Administrators select **Global Reader** and double click on it to Add assignments In Add Assignments go to Select Member(s) and select the newly created Application.

- 3. Then the Assignment Type will be eligible. Unlock permanently eligible and selection assignment duration and click **Assign**
- 4. Under Roles and Administrators assign **Exchange Administrator** by following above steps.

NOTE:	
Global Reader:	This Is required for providing permission to the Application so that it can read different audit log events by using different technologies.
Exchange Administrator:	This is required for providing permission to the Application so that it can manage all aspects of Exchange Online so that we can Read Mailbox Audit Logs by using Exchange Online PowerShell.

5.4 Permissions for Auditing, DDC, & CPA

5.4.1 Permissions for Auditing

For Office 365 Exchange Onl	ine (Delegate	d And Application)		
Exchange.ManageAsApp	Application	Exchange Online	For Providing the Permission to Client Id and Secret Key to Manage Exchange as Application	
Graph Api (Delegated and A	pplication)			
User.Read	Application	Graph API	For Enumerating the User Mailbox who has Exchange Online License for Auditing	
MailboxSetting.Read	Application	Graph API	For Enumerating the User Mailbox who has Exchange Online License for Auditing	
Office365 Management APIs	;			
ActivityFeed.Read	Delegated	Management API	For Providing Permission to application to Read Activity Data of your Organization for Auditing.	
ActivityFeed.Read	Application	Management API	For Providing Permission to application to Read Activity Data of your Organization for Auditing.	

5.4.2 Permissions for Data Discovery & Classification

Graph Api	(Delegated	and	Application)
-----------	------------	-----	----------------------

MailboxSettings.ReadWrite	Application	Graph API	For Enumeration Of User Mailbox
User.ReadWrite.All	Application	Graph API	For Enumerating the Basic Details Required for DDC
Directory.ReadWrite.All	Application	Graph API	For Enumerating the Folders of User's Mailbox so that we can classify all the Mail Folder's Sensitive data
Mail.ReadWrite	Application	Graph API	For Enumerating the Mail content of User's Mailbox so that we can classify the sensitive data and add the Lepide Tags
Calendars.ReadWrite	Application	Graph API	For Enumerating the meeting and appointment content so that we can classify the sensitive data and add the Lepide Tags
Contacts.ReadWrite	Application	Graph API	For Enumerating the contact content so that we can classify the sensitive data and add the Lepide Tags
Tasks.ReadWrite.All	Application	Graph API	For Enumerating the Task Event content so that we can classify the sensitive data and add the Lepide Tags

5.4.3 Permissions for Current Permissions Analysis

For Office 385 Exchange Online (Delegated And Application)

Exchange.ManageAsApp	Application	Exchange Online	For Prov	viding	the l
			Secret	kev	to

For Providing the Permission to Client Id and Secret key to Manage Exchange as Application

5.5 Install the Exchange Online Management Module

1. Open Windows PowerShell by run as Administrator

NOTE: Run the following commands firstly in Windows PowerShell(x86) then in Windows PowerShell

2. To Ensure that you have Nuget Package installed run the below command.

Get-Module -ListAvailable -Name NuGet

3. If you don't have a NuGet Package then to install the module run the below command

Install-Module -Name NuGet -Force



4. To Ensure that you have a version of PowerShellGet and PackageManagement newer than 1.0.0.1 installed, run the command below:

Get-Module PowerShellGet, PackageManagement -ListAvailable

- If you have an older version of PowerShellGet and PackageManagement then to install the latest version, run the command below: Install-Module PowerShellGet -Force -AllowClobber
- To install the Exchange Online PowerShell module run the command below: Install-Module -Name ExchangeOnlineManagement -RequiredVersion 3.1.0 -Force

5.6 Generate the Certificate for Tenant on the LDSP Server

Follow the steps below to create the certificate:

The steps to create a certificate for your domain name are as follows:

• Run the following PowerShell commands:

```
$mycert = New-SelfSignedCertificate -DnsName "YourDomainName.com" -
CertStoreLocation "cert:\LocalMachine\My"-NotAfter (Get-
Date).AddYears(NumberofYears) -KeySpec KeyExchange -FriendlyName "scriptfile"
Note: "scriptfile" should be User Defined Name for certificate and "YourDomainName" should be name
of your Tenant
```

\$mycert | Select-Object -Property Subject, Thumbprint, NotBefore, NotAfter
Note: User should copy Thumbprint value as it is required for Login Information

\$mycert | Export-Certificate -FilePath "C:\temp\scriptfile.cer"
Note: FilePath should ends with a (.cer) file type

\$mycert | Export-PfxCertificate -FilePath "C:\temp\scriptfile.pfx" -Password \$(ConvertTo-SecureString -String "Password value" -AsPlainText -Force) Note: Password value is the User Defined Password Value for certificate

5.7 Install the Certificate on DDC Agent \ FSA Agent

The Certificate should be installed in the '**Trusted Root Certification Authorities Store'** of the Agent's System Machine

- 1. Open the certificates of .cer and .pfx as filetype (generated in the above steps).
- 2. Install the certificates with 'local machine' as the store location option
- 3. In the case of a (.pfx) certificate enter the **'password value'** mentioned in the above step
- Choose the 'windows can automatically select a certificate Store' as the option for 'Certificate Store' path

5.8 Register your Certificate with Microsoft Identity Platform

- 1. In the Microsoft Entra admin center, in **App registrations**, select your application
- 2. In the App Registrations Tab for the client application select **Certificates & Secrets**, **Certificates**
- 3. Click on Upload Certificate and select the certificate file to upload
- 4. Click **Add**. Once the certificate is uploaded, the thumbprint, start date, and expiration values are displayed

6 SharePoint Online

All the reports and functionalities available for SharePoint Online auditing with the Least Privilege model are the same as with the Full Privilege model.

6.1 Prerequisites

- To add SharePoint Online to the Lepide Data Security Platform for Auditing, an app must be registered on the Microsoft 365 portal.
- Login to the Office 365 Tenant needs to be done by a User with a Global Administrator account. This is because if the user does not have global admin rights then they will not be able to grant admin consent permissions to the Tenant.
- Without Global Admin rights, the Grant permission option in Microsoft will grayed out.

6.2 Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on Certificates and Secrets.
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding a SharePoint Online component.

- 4. Click on the API permission tab for the given Client ID and select Add a Permission
 - 5. Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's

Name Type

Sites.Read.All Delegated

Office 365 Management API's

ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

6.3 Generate the Client ID and Secret Key for SharePoint Online Data Discovery & Classification

Modern Authentication for SharePoint Online

- 1. Log into the Office 365 account through SharePoint Administrator / Global Administrator
- 2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
- 3. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key** and set the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: https://www.localhost.com/

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials, you are using and allow read or update actions to be performed on your SharePoint Online for Data Discovery and Classification.

- 4. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
- 5. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
- 6. In the App's Permission Request XML field, enter the code below to grant appropriate access:

<AppPermissionRequests AllowAppOnlyPolicy="true">

<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />
</AppPermissionRequests>

- 7. You will now be prompted to trust the add-in for all the permissions that it requires
- 8. Click **Trust It** to grant the requested access

Please run the command below at SharePoint Online Management Shell:

function Enable-SPDisableCustomAppAuthentication {

Write-Host "Please specify sharepoint organisation name." -ForegroundColor Green

Write-Host "For example if your sharepoint site is https://contoso.sharepoint.com value should be contoso: " -ForegroundColor Green -NoNewline

\$orgName = Read-Host

\$orgName = \$contosh

Write-Verbose "Connecting to: https://contoso-admin.sharepoint.com" -Verbose

Connect-SPOService -Url "https://contosh-admin.sharepoint.com"

Set-SPOTenant -DisableCustomAppAuthentication \$false

}

Enable-SPDisableCustomAppAuthentication

Please run the command below:

Set-SPOTenant -DisableCustomAppAuthentication \$false

Now, Create a profile in Data Discovery & Classification and Classify it

6.4 Generate the Client ID and Secret Key for SharePoint Online Current Permissions Analysis

Modern Authentication for OneDrive for Business

- 1. Log into the office 365 account through **SharePoint Administrator / Global Administrator**.
- 2. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
- 3. Click the two Generate buttons to generate a Client ID and a Secret Key
- 4. Specify the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: https://www.localhost.com/

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials, you are using and allow read or update actions to be performed on your SharePoint Online for Current Permission Analysis.

- 5. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx
- 6. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
- 7. In the App's Permission Request XML field, enter the code below to grant appropriate access:

<AppPermissionRequests AllowAppOnlyPolicy="true">

<AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" />

</AppPermissionRequests>

- 9. You will now be prompted to trust the add-in for all the permissions that it requires
- 10. Click **Trust It** to grant the requested access

Please run the command below at SharePoint Online Management Shell:

function Enable-SPDisableCustomAppAuthentication {

Write-Host "Please specify sharepoint organisation name." -ForegroundColor Green

Write-Host "For example if your sharepoint site is https://contoso.sharepoint.com value should be contoso: " -ForegroundColor Green -NoNewline

\$orgName = Read-Host

\$orgName = \$contosh

Write-Verbose "Connecting to: https://contoso-admin.sharepoint.com" -Verbose

Connect-SPOService -Url "https://contosh-admin.sharepoint.com"

Set-SPOTenant

Now, Create a dataset in Current permission scan settings and Scan it

6.5 Permissions

The permissions required for the different functionality of SharePoint Online are as follows:

6.5.1 Auditing Permissions

The permissions required are as follows:

Microsoft Graph API's

Name	Туре	Detail
Sites.Read.All	Delegated	Read items in all site collections
Office 365 Managemen	t API's	
ActivityFeed.Read	Delegated	Read activity data for your organization
ActivityFeed.Read	Application	Read activity data for your organization
ActivityFeed.ReadDlp	Delegated	Read DLP policy events including detected sensitive data
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data

6.5.2 Data Discovery and Classification Permissions

The permissions given to the Client ID are as follows:

Scope: <u>http://sharepoint/content/tenant</u> Full Control

Full control is required here as **Read permission** is required to read the file and content, **Write permission** is required to be able to add the tags and the **Manage permission** is required to be able to manage both the added and existing tags on the file. By using the Full Control permission, all this options are available.

6.5.3 Current Permissions Analysis Permissions

The permissions given to the Client ID are as follows:

Scope: <u>http://sharepoint/content/tenant</u> Full Control

The scope need full control because we need to get all the permission levels not just the permission for a specific object. So to get all the permission levels we need to have full control access of the content/tenant scope.

7 O365 Component

The O365 Component in the Lepide Data Security Platform covers the following four components of M365:

- OneDrive
- Azure Active Directory
- Teams
- Skype for Business

All the reports and functionalities available for O365 auditing with the Least Privilege model are the same as with the Full Privilege model.

7.1 Prerequisites

- To add OneDrive, Azure, Teams or Skype for Business components to the Lepide Data Security Platform for Auditing, an app must be registered on the Microsoft 365 portal.
- Login to the Office 365 Tenant needs to be done by a User with a Global Administrator account. This is because if the user does not have global admin rights then they will not be able to grant admin consent permissions to the Tenant.
- Without Global Admin rights, the Grant permission option in Microsoft will grayed out.

7.2 OneDrive

7.2.1 Register an App and Generate the Client ID and Secret Key for OneDrive Auditing

- 7. Log onto the Microsoft 365 Admin Center
- 8. Select Azure Active Directory from the Admin Center
- 9. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets.**
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding an Office 365 component for OneDrive

10. Click on the API permission tab for the given Client ID and select Add a Permission

11. Select Microsoft API's and API's my organization uses as follows:

Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph APTS			
AuditLog.Read.All	Delegated		
AuditLog.Read.All	Application		
Office 365 Management API's			
ActivityFeed.Read	Application		
ActivityFeed.ReadDlp	Application		

Microsoft Craph ADI's

NOTE: Every permission change required must be granted admin consent

12. Now add the components with Client ID and Secret Key



Lepide Data Security Platform

7.2.2 Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification

Modern Authentication for OneDrive for Business

- 11. Log into the office 365 account through SharePoint Administrator / Global Administrator
- 12. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
- 13. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key** and set the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: https://www.localhost.com/

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials, you are using and allow read or update actions to be performed on your OneDrive for Business environment.

14. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx

- 15. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
- 16. In the App's Permission Request XML field, enter the code below to grant appropriate access:

<AppPermissionRequests AllowAppOnlyPolicy="true"> <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" /> <AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" /> </AppPermissionRequests>

- 17. Click Create
- 18. You will now be prompted to trust the add-in for all the permissions that it requires
- 19. Click **Trust It** to grant the requested access
- 20. Now, Create a profile in Data Discovery & Classification and Classify it

Lepide Data Security Platform

7.2.3 Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis

Modern Authentication for OneDrive for Business

- 8. Log into the office 365 account through **SharePoint Administrator / Global Administrator**.
- 9. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx
- 10. Click the two **Generate** buttons to generate a **Client ID** and a **Secret Key**
- 11. Specify the following options:
 - Title: Enter a name for the app
 - App Domain: www.localhost.com
 - Redirect URL: https://www.localhost.com/

NOTE: Save the retrieved Client ID and Secret Key. They are the credentials, you are using and allow read or update actions to be performed on your OneDrive for Business environment.

12. Go to https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx

- 13. Enter the generated **Client ID** in the **App Id** field and click **Lookup**
- 14. In the App's Permission Request XML field, enter the below code to grant appropriate access:

<AppPermissionRequests AllowAppOnlyPolicy="true"> <AppPermissionRequest Scope="http://sharepoint/content/tenant" Right="FullControl" /> <AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" /> </AppPermissionRequests>

- 15. Click Create
- 16. You will be prompted to trust the add-in for all the permissions that it requires
- 17. Click **Trust It** to grant the requested access
- 18. Now, Create a dataset in Current permission scan settings and Scan it



7.3 Azure

7.3.1 Register an App and Generate the Client ID and Secret Key for Azure Auditing

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets.**
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Azure

- 4. Click on the API permission tab for the given Client ID and select Add a Permission
- 5. Select Microsoft API's and API's my organization uses as follows:

Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's

Directory.Read.All	Application
AuditLog.Read.All	Application
Office 365 Management A	Pl's
ActivityFeed.Read	Delegated
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Delegated
ActivityFeed.ReadDlp	Application

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

7.3.2 Azure Current Permission Analysis

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center

- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets.**
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Azure. The app created needs the Global reader role only

- 4. Click on the API permission tab for the given Client ID and select Add a Permission
- 5. Select Microsoft API's and API's my organization uses as follows:

Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Office 365 Management API's

Exchange.ManageAsApp Application

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

7.4 Teams

7.4.1 Register an App and Generate the Client ID and Secret Key for Teams Auditing

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets.**
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Teams

- 4. Click on the API permission tab for the given Client ID and select Add a Permission
- 5. Select Microsoft API's and API's my organization uses as follows:

Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's			
AuditLog.Read.All	Delegated		
AuditLog.Read.All	Application		
Directory.Read.All	Application		
Office 365 Management API's			
ActivityFeed.Read	Delegated		
ActivityFeed.Read	Application		
ActivityFeed.ReadDlp	Delegated		
ActivityFeed.ReadDlp	Application		

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

7.5 Skype for Business

7.5.1 Register an App and Generate the Client ID and Secret Key for Skype for Business Auditing

- 1. Log onto the Microsoft 365 Admin Center
- 2. Select Azure Active Directory from the Admin Center
- 3. Click on **App Registration** and follow the steps below to generate Client ID and Secret Key:
 - Select **New Registration** and provide a valid name for the registration.
 - Click on **Register Account** and the Client ID will be displayed which the user can copy for future use
 - For the given Client Id generated in the Azure Account Dashboard, click on **Certificates and Secrets.**
 - Click on Add New Client Secret and a Secret Value will be generated which the user can copy for future use.

NOTE: Copy the Client ID and Secret value for adding Office 365 component for Skype

4. Click on the API permission tab for the given Client ID and select Add a Permission

5. Select **Microsoft API's** and **API's my organization uses** as follows:

Microsoft 365 Graph API's, Office 365 Management API's and select permission type(s) as detailed below:

Microsoft Graph API's				
AuditLog.Read.All	Delegated			
AuditLog.Read.All	Application			
Directory.Read.All	Application			
Office 365 Management API's				
ActivityFeed.Read	Delegated			
ActivityFeed.Read	Application			
ActivityFeed.ReadDlp	Delegated			
ActivityFeed.ReadDlp	Application			

NOTE: Every permission change required must be granted admin consent

6. Now add the components with Client ID and Secret Key

7.6 Permissions

The permissions required for the different functionality of O365 components are as follows:

7.6.1 Auditing Permissions

The permissions required are as follows:

Graph API's

Name	Туре	Detail
AuditLog.Read.All	Delegated	Read audit log data
Directory.Read.All	Application	Read directory data
AuditLog.Read.AllApplica	ition Read all a	udit log data

Management API's

Name	Туре	Deta	il
ActivityFeed.Read		Delegated	Read activity data for your organization
ActivityFeed.Read		Application	Read activity data for your organization

ActivityFeed.ReadDlp	Delegated	Read DLP policy events including detected sensitive Data.
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive Data.

7.6.2 Data Discovery and Classification Permissions

The permissions given to the Client ID are as follows:

Scope: http://sharepoint/content/tenant Full Control

Full control is required here as Read permission is required to read the file and content, Write permission is required to be able to add the tags and the Manage permission is required to be able to manage both the added and existing tags on the file. By using the Full Control permission, all this options are available.

Scope: http://sharepoint/social/tenant Read

This acts as a central location where users can track their tasks and access the documents and sites they are following so Read permission is sufficient here.



7.6.3 Current Permissions Analysis Permissions

The permissions given to the client ID are as follows:

Scope: <u>http://sharepoint/content/tenant</u> Full Control

The scope need full control because we need to get all the permission levels not just the permission for a specific object. So to get all the permission levels we need to have full control access of the content/tenant scope.

Scope: <u>http://sharepoint/social/tenant</u> Read

This acts as a central location where users can track their tasks and access the documents and sites they are following so Read permission is sufficient here.



8 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 <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/.

9 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.