WLEPIDE QUICK START GUIDE

MICROSOFT 365

Table of Contents

1	Intro	oductic	ח	4				
2	Excl	Exchange Online						
	2.1	Prerequisites						
	2.2	Steps	to Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing	4				
	2.3	Assigr	ning the Role to the Application	5				
	2.4	.4 Permissions for Auditing, DDC, & CPA						
		2.4.1	Permissions for Auditing	5				
		2.4.2	Permissions for Data Discovery & Classification	6				
		2.4.3	Permissions for Current Permissions Analysis	6				
	2.5	Install	the Exchange Online Management Module	6				
	2.6	Gener	ate a ThumbPrint	7				
	2.7 How to Install a Certificate for DDC and FSA Agent			8				
	2.8 Adding an Exchange Online Component							
	2.9	2.9 Viewing the Reports						
3	Office 365 Component							
	3.1 Prerequisites							
	3.2	OneDrive						
		3.2.1	Steps to Register an App and Generate the Client ID and Secret Key for OneDrive Auditing	.18				
		3.2.2	Steps to Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification	.20				
		3.2.3	Steps to Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis	.21				
	3.3	3 Azure						
		3.3.1	Steps to Register an App and Generate the Client ID and Secret Key for Azure Auditing	.22				
	3.4	Team	5	.23				
		3.4.1	Steps to Register an App and Generate the Client ID and Secret Key for Teams Auditing	.23				
	3.5	Skype	for Business	.24				
		3.5.1	Steps to Register an App and Generate the Client ID and Secret Key for Skype for Business Auditing	.24				

	3.6	Adding Azure Active Directory, OneDrive for Business, Skype for Business & Microsoft Teams25
	3.7	Viewing the Reports
4	Sha	rePoint Online
	4.1	Prerequisites
	4.2	Steps to Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing.31
	4.3	Steps to Generate the Client ID and Secret Key for SharePoint Online Data Discovery & Classification
	4.4	Steps to Generate the Client ID and Secret Key for SharePoint Online Current Permissions Analysis. 34
	4.5	Adding a SharePoint Online Component
	4.6	Viewing the Reports
5	Sup	port
6	Trac	demarks

1 Introduction

The Lepide Data Security Platform performs comprehensive auditing and reporting on critical changes on Microsoft 365 components. The components supported for Microsoft 365 are: Exchange Online, SharePoint Online, Azure Active Directory, OneDrive for Business, Skype for Business and Microsoft Teams.

This guide takes you through the process of standard configuration of the Lepide Data Security Platform for Microsoft 365 Components. For information on installation, please see our <u>Installation and Prerequisites Guide</u>.

If you have any questions at any point in the process, you can contact our Support Team. The contact details are listed at the end of this document.

2 Exchange Online

2.1 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

2.2 Steps to 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

2.3 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.

2.4 Permissions for Auditing, DDC, & CPA

2.4.1 Permissions for Auditing

For Office 365 Exchange Online (Delegated And Application)

Exchange.ManageAsApp Application Exchange Online

Graph Api (Delegated and Application)

User.Read	Application	Graph API
MailboxSetting.Read	Application	Graph API

Office365 Management APIs

ActivityFeed.Read	Delegated	Management API
ActivityFeed.Read	Application	Management API

2.4.2 Permissions for Data Discovery & Classification

Graph Api (Delegated and Application)

MailboxSettings.ReadWrite	Application	Graph API
User.ReadWrite.All	Application	Graph API
Directory.ReadWrite.All	Application	Graph API
Mail.ReadWrite	Application	Graph API
Calendars.ReadWrite	Application	Graph API
Contacts.ReadWrite	Application	Graph API
Tasks.ReadWrite.All	Application	Graph API

2.4.3 Permissions for Current Permissions Analysis

For Office 385 Exchange Online (Delegated And Application)

Exchange.ManageAsApp Application Exchange Online

2.5 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

2.6 Generate a ThumbPrint

The steps to install the Exchange Online PowerShell module are as follows:

- A. Open Windows PowerShell, run as Administrator
- B. 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
- C. 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"
- D. To install the ExchangeOnline PowerShell module run the command below: "Install-Module -Name ExchangeOnlineManagement"

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

- A. Run the following PowerShell commands:
- a. \$mycert = New-SelfSignedCertificate -DnsName "YourDomainName.com" -CertStoreLocation
 "cert:\LocalMachine\My"-NotAfter (Get-Date).AddYears(NumberofYears) -KeySpec
 KeyExchange -FriendlyName "scriptfile"
 Note: "scriptfile" should be the User Defined Name for the certificate
- b. \$mycert | Select-Object -Property Subject,Thumbprint,NotBefore,NotAfter
 Note: User should copy Thumbprint value as it is required for Login Information
- c. \$mycert | Export-Certificate -FilePath "C:\temp\scriptfile.cer" **Note**: FilePath should ends with a (.cer) file type
- d. \$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
- B. Install the Certificate in the "trusted root certification Authorities Store" of Agent's System Machine

- a. Open the certificates of .cer and .pfx as filetype (generated in the above steps)
- b. Install the certificates with "local machine" as the store location option
- c. In case of a (.pfx) certificate, enter the "password value" mentioned in the above step
- d. Choose the "windows can automatically select a certificate store" as an option for the "Certificate Store" path

The steps to upload the certificate for your client application are as follows:

In the App registrations tab for the client application:

- A. Select Certificates & secrets, Certificates
- B. Click on Upload certificate and select the certificate file to upload
- C. Click **Add**. Once the certificate is uploaded, the thumbprint, start date and expiration values are displayed

NOTE: The User should copy the Client ID and ThumbPrint as this will be needed for Login Information

2.7 How to Install a Certificate for DDC and 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
- 4. Choose the 'windows can automatically select a certificate Store' as the option for 'Certificate Store' path

2.8 Adding an Exchange Online Component

The Lepide Data Security Platform tracks the changes inside Exchange Online and gives detailed reporting on any configuration changes, for example Mailbox Modifications, Exchange Group Modifications, etc.

To add an Exchange online component:

• From the Component Management screen, click on **Exchange Online**:



Figure 1: Component Management Screen

The Global Administrator App Credentials dialog box appears:



		×
Global Administrator	Ann Credentials	
Please provide the global ad	ministrator and Client ID and Secret Value Key	
Flease provide the global ad	ministrator app ciencito and secret value key.	
Tenant Name		
	Enter like: Your domain name.onmicrosoft.com	
Subscription Type	Enterprise plan *	0
		0
Client ID		
Secret Key		
ThumbPrint		0
	- Back Next >	Cancel
	< Dack Next >	

Figure 2: App Credentials

• Enter the Tenant Name, choose the Subscription Type and enter the Client ID, Secret Key and ThumbPrint

NOTE: The instructions to generate the **Client ID** and **Secret Key** are given in Section 2.2. The instructions to generate the **ThumbPrint** are given in Section 2.6 - Generate a ThumbPrint

- Click Next
- The Add Mailboxes to Audit dialog box is displayed:

						×
Add Mailbox(e	s) to audit					
Please select the ma	ailbox(es) to audit.					
Audit:	All Mailboxes				-	
				E 4444		
	pe To Search>		Q	<type search="" to=""></type>	Q	
<		ш			>	
				< <u>B</u> ack <u>N</u>	ext >	Cancel

Figure 3: Add Mailboxes to Audit

- Select the Mailboxes you would like to audit. The options are:
 - All Mailboxes this is the default option
 - Selected Only
 - All but Excluding Selected
- To audit specific mailboxes, choose **Selected Only** from the drop-down list and the mailboxes are displayed with checkboxes to select those to be **included** in auditing:



Figure 4: Add Selected Mailboxes to Audit

- To audit all **except** specific mailboxes, choose **All but Excluding Selected** from the dropdown list and the checked mailboxes will be **excluded** from auditing.
- Click **Next**
- The Add Objects to Audit dialog box is displayed:

Audi	t:	Selected Only			*
		Dbjects List		Description	^
Q	<ty< td=""><td>pe To Search></td><td>Q</td><td><type search="" to=""></type></td><td></td></ty<>	pe To Search>	Q	<type search="" to=""></type>	
		Address Book		Global Address list, Address L	1
		Auditing Mailbox Access		Mailbox Access Audit Log Search	
	0.	loumaling		Journal Rule	
		Add-in		Apps	
		Auditing		Admin Audit Log Search, Mailbox	4
		Client Access		Outlook Web App, Mobile Device,	1
		Mail Flow		Accepted Domains, Message Trac	=
		n-place eDiscovery & hold		Mailbox Search	
		Exchange Group		Distribution Group.Sequrity Group	
		Federation And Hybrid		Fedration and Hybrid Configuration	
		Sharing		Organization,Organization Relation	
		Mail User		Mail User	
		Mail Contact		Mail Contact	
		nformation Right Management (IRM)		IRM Configuration, RMS Template	
		Data Loss Prevention		DLP Policy, Data Classification, Fi	
		Hole Based Access Control (RBAC)		Management Role, Management	
	H	Public Folder		Public Folder	
	1	nule		Iransport Hules	
-		Protection	_	Maiware Filter, Connection Filter,	\sim
<		ш		>	

Figure 5: Add Objects to Audit

- Select the Objects you would like to audit. The options are:
 - All Objects this is the default option
 - Selected Only
 - All but Excluding Selected
- To audit specific objects, choose **Selected Only** from the drop-down list and the objects are displayed with checkboxes to select those to be **included** in auditing:
- To audit all **except** specific objects, choose **All but Excluding Selected** from the drop-down list and the checked objects will be **excluded** from auditing.
- Click **Next**
- The Database Settings dialog box is displayed:

					×
Database Settings					
Please provide SQL server d	letails to store the audit	data			
Configure SQL Se	erver				
SQL Server:	192.168.40.238				
	Authentication				
	Windows Aut	entication			
	SQL Authentic	ation			
	User Name:	sa			
	Password:	•••••			
			Test 0	Connection	
Select Database:	Lepide_Exch_Onlin	ne			*
Collect Changes F	wany 5	linutes			
conect changes i	very.	iniutes.			
			< Back	Next >	Cancel
			(Door	Trank P	Ganoor

Figure 6: Database Settings

- From this dialog box you can do the following:
 - Add the **SQL Server** name. Click the _____ icon to select a server
 - In the **Select Database** box, type in a name and the Solution will create a database with this name
 - Collect **Changes Every:** Set the frequency to collect the changes from the M365 portal. The minimum is 5 minutes

- Click Finish
- A message box will be displayed asking for confirmation to restart the solution:



Figure 7: Confirm Restart

• Click **Yes** to restart

2.9 Viewing the Reports

Exchange Online reports are available from the States & Behavior screen.

- Click the Users & Entity behavior icon to display the States & Behavior screen
- From the tree structure to the left side of the screen expand Exchange Online.
- There will be a separate Node for Exchange Online for the tenant which has been added. Expand this Node
- The example below shows the All Modifications in Exchange Online Report:





Figure 8: All Modifications in Exchange Online Report



3 Office 365 Component

3.1 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.

3.2 OneDrive

3.2.1 Steps to Register an App and Generate the Client ID and Secret Key for OneDrive 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 an Office 365 component for OneDrive

- 4. Click on the API permission tab for the given Client ID and select Add a Permission
- 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
Office 365 Managemer	nt API's
ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Application

NOTE: Every permission change required must be granted admin consent



3.2.2 Steps to Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification

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** 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.

- 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" /> <AppPermissionRequest Scope="http://sharepoint/social/tenant" Right="Read" /> </AppPermissionRequests>

7. Click **Create**

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

3.2.3 Steps to Generate the Client ID and Secret Key for OneDrive 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 OneDrive for Business environment.

- 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 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>

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

3.3 Azure

3.3.1 Steps to 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 Graph API's

Sites.Read.AllDelegatedOffice 365 Management API'sActivityFeed.ReadDelegatedActivityFeed.ReadApplicationActivityFeed.ReadDlpDelegatedActivityFeed.ReadDlpApplication



3.4 Teams

3.4.1 Steps to 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
- Select Microsoft API's and API's my organization uses as follows: Microsoft Graph API's

Sites.Read.AllDelegatedOffice 365 Management API'sActivityFeed.ReadDelegatedActivityFeed.ReadApplicationActivityFeed.ReadDlpDelegatedActivityFeed.ReadDlpApplication



3.5 Skype for Business

3.5.1 Steps to 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
- Select Microsoft API's and API's my organization uses as follows: Microsoft Graph API's

Sites.Read.All Delegated

Office 365 Management API's

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

3.6 Adding Azure Active Directory, OneDrive for Business, Skype for Business & Microsoft Teams

The Lepide Data Security Platform audits the changes inside Azure AD, OneDrive, Skype for Business and MS Teams and all these components can be added in one go under the component name Office 365.

NOTE: We can audit azure file storage if synced with an on-premise file server

1. From the Component Management screen, click on **Office 365** to add your Tenant.



Figure 9: Component Management Screen

The Global Administrator App Credentials dialog box appears:



		×
Global Administrator	App Credentials	
Please provide the global adr	ninistrator app Client ID and Secret Value Key.	
Tenant Name	Lepidesoftware.onmicrosoft.com	
	Enter like: Your domain name.onmicrosoft.com	
Subscription Type	Enterprise plan *	(?) .
Client ID	748b10d9-11f5-4424-920d-a1dfbc3c9a96	
Secret Vev	•••••	
benetikey	· · · ·	
	< <u>B</u> ack <u>N</u> ext	> Cancel

Figure 10: App Credentials

- 2. Enter the Tenant Name, choose the Subscription Type and enter the Client ID and Secret Key.
- 3. The instructions to generate the Client ID and Secret Key are given in Sections 3.2 to 3.5 of this guide
- 4. Close this dialog box once finished and click **Next**

The Components dialog box is displayed:



				Х
Components Please select component(s) to configure			
	<u> </u>	S	T	
OneDrive	Azure	Skype for Buisness	Microsoft Teams	
			< Back Next >	Cancel

Figure 11: Components

- 5. Select the components you would like to audit. You can add any one or more components as required.
- 6. Click **Next**

					Х
Database Setting Please enter SQL serv	gs er details to store t	the audit data			
Configure SOL Server					
SOL Server:	192.168.40.238				
	Authentication				
	🔘 Windows	Authentication			
	💿 SQL Auth	nentication (recommended)			
	User Name:	sa			
	Password:	•••••			
	1 325/10/10.			Test Connection	
				rest connection	
	Select Databa	ase: Lepide_0365		•	
			< Back	Next > Can	cel

Figure 12: Database Settings

- 7. The database settings dialog box is displayed:
- 8. From this dialog box you can do the following:
 - Add the SQL Server name. Click the $\boxed{ \dots }$ icon to select a server
 - In the Select Database box, type in a name and the Solution will create a database with this name
- 9. Click **Finish**

10. A message box will be displayed asking for confirmation to restart the solution:



Figure 13: Confirm Restart

11. Click Yes to restart

3.7 Viewing the Reports

- Click the Users & Entity behavior icon for the display the States & Behavior screen
- The All-Environment Changes Report holds all the changes for these components
- From the tree structure to the left side of the screen click on **All Environment Changes**.
- The example below shows the All Environment Changes Report:



Lepide Data Security Platform

	States & Behavior 🕅 🕅	All Environment Chan	ges								Y
		7.0	-		×						
	- All Environment Changes	Component Name	+ when	Component Name	<u> </u>						
0	Anomaly Analysis	Y Server Name	+ Today	EqualTo	×						
	. SQL Server Reports	√ Object Path	+	Azure Active Direc	tory ,						
•	192.168.20.70(SharePoint)	Y Object Type	+	Business , Microso	't Teams						
6	E-I LPDE1.local	Y Who	+								
е. С	kovt.onmicrosoft.com/Exchange (Y When	+								
	lepidesoftware.onmicrosoft.com(E	V Operation	+								
	I SIVASOFT.ONMICROSOFT.COM(E	V unese									
	+ kpvt-admin.sharepoint.com(Share	* where	-								
	repidesoftware-admin.sharepoint.	Y Criticality	+								
E.	Explore Backup										Generate Report
	Console Auditing	Data a set and based as based									
		brag a coumn header here to	group by that column.							• u _	
_		Component Name	For Server Name	J Object Path	7 Object Type	Who	When	r	√7 What	Vhere	Details
S		م	P	. م	م م	3	D	Q	Q	<u>0</u>	
		Microsoft Teams	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	Member	sudesh@lepidesoftware.on	3/4/2021 3:42:23 PM	Teams Session Started	User 'sudesh@lepidesof	twa N/A	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:34:18 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:34:16 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesn@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:34:01 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesni@iepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	2/4/2021 3:33:59 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
8		Azure Active Directory	lepidesoftware.onm	crosoft c sudesh@epidesoftware.onmicrosoft c	User	sudesh@lepidesoftware.on.	3/4/2021 3:33:31 PM	User Logged In	Sudesh@lepidesoftware	on 14.102	
		Microsoft Teams	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	. Member	sudesh@lepidesoftware.on	3/4/2021 3:31:41 PM	Teams Session Started	User 'sudesh@lepidesof	twa N/A	
		Microsoft Teams	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	Member	sudesh@lepidesoftware.on	3/4/2021 3:31:35 PM	Teams Session Started	User 'sudesh@lepidesof	twa N/A	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:29:57 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:29:54 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:28:56 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:28:54 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:27:52 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:27:50 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:27:38 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:27:36 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesni@iepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	2/4/2021 3:27:32 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onm	consoft c sudesh@epidesoftware.ormicrosoft.c.	lleer	sudesh@lepidesoftware.on.	3/4/2021 3:26:45 PM	User Logged In	Sudesh@lepidesoftware	on 14.102	
		Azure Active Directory	lepidesoftware onmi	crosoft c sudesh@lepidesoftware onmicrosoft c	User	sudesh@lepidesoftware.on	3/4/2021 3:24:57 PM	User Logged In	Sudesh@lepidesoftware	on 14.102	
		Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:24:38 PM	User Logged In	Sudesh@lepidesoftware	on 14.102	
		Microsoft Teams	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	Member	sudesh@lepidesoftware.on	3/4/2021 3:22:01 PM	Teams Session Started	User 'sudesh@lepidesoft	twa N/A	
	< >	Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:09:01 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:08:59 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
	States & Behavior	Azure Active Directory	lepidesoftware.onm	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:08:58 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
		Azure Active Directory	lepidesoftware.onmi	crosoft.c sudesh@lepidesoftware.onmicrosoft.c.	User	sudesh@lepidesoftware.on	3/4/2021 3:04:21 PM	User Logged In	Sudesh@lepidesoftware	on 14.102.	
	Regulatory Compliance	4 Anuna Activa Directory	lenideenftware onm	oment o leudaeh@lanidaentwara.onmioment o	Hear	eudach@lanidaenftwara.on	3/4/2021 3-04-19 PM	Lieer Looped In	Surdaeh Rianidaen Awara	00 14 102	

Figure 14: All Environment Changes Report

4 SharePoint Online

4.1 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.



4.2 Steps to Register an App and Generate the Client ID and Secret Key for SharePoint Online Auditing

Log onto the Microsoft 365 Admin Center

- 1. Select Azure Active Directory from the Admin Center
- 2. 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.

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

Microsoft Graph API's

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



4.3 Steps to 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

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.

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



4.4 Steps to 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**
- 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>

- 11. You will now be prompted to trust the add-in for all the permissions that it requires
- 12. 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

4.5 Adding a SharePoint Online Component

The Lepide Data Security Platform tracks the changes inside SharePoint Online and gives detailed reporting on any configuration changes. For example, Document Modifications, SharePoint Group Modifications, etc.



Figure 15: Component Management Screen

• From the Component Management screen click on **SharePoint Online**.

The Global Administrator App Credentials dialog box is displayed:



				×
Global Administrato	r App Credentials			
Please provide the global ad	dministrator app Client ID and Secret Value Key.			
				_
			-	
Central Admin URL	https://lepidesoftware-admin.sharepoint.com	(?	
	NOTE: Please add the Central Admin URL correctly.			
	"https://domainName-admin.sharepoint.com"			
Tenant Name	lepidesoftware.onmicrosoft.com			
	Enter like: Your domain name.onmicrosoft.com			
Client ID	7ad32845-9848-462b-a55e-f98d7bb5adcd			
Secret Key	••••••			
	< <u>B</u> ack <u>N</u> ext	>	Cance	1
	Figure 16: Ann Credentials			

- Figure 16: App Credentidis
- Enter the Central Admin URL, Tenant Name and the Client ID and Secret Key.
- The instructions to generate the Client ID and Secret Key are given in Section 4.2 to 4.4 of this guide
- Close this dialog box once finished and click Next

The Add Objects to Audit dialog box is displayed:

					×
Add Objects to a	ıdit				
Places collector collector	- to sudt				
Please select the object	is to audit.				
Audit:	Selected Only			-	
	Diects List				
S <ty< td=""><td>pe To Search></td><td></td><td></td><td>0</td><td></td></ty<>	pe To Search>			0	
	Document			-	
🗆 [Document Library				
🗖 F	Folder				
	àroup				
	ink				
	jst				
	ust item				
	Site Collection				
	Sharing and Access				
	lenant				
·/					
		г			
			< <u>B</u> ack	<u>N</u> ext > (Cancel

Figure 17: Add Objects to Audit

- Select the Objects you would like to audit. The options are: •
 - All Objects this is the default option •
 - Selected Only

- All but Excluding Selected
 - To audit specific objects, choose **Selected Only** from the drop-down list and the objects are displayed with checkboxes to select those to be **included** in auditing:
 - To audit all except specific objects, choose All but Excluding Selected from the drop-down list and the checked objects will be excluded from auditing.
- Click **Next**

The Add Operations dialog box is displayed:



					×
Add Operations t	o audit				
Please select the operation	tions to audit				
Please select the opera					
Audit:	Selected Only		+		
	perations List		^		
🔎 <Ту;	e To Search>		2		
	ccessed		=		
	heck Out Discarded				
	hecked In				
	hecked Out				
	Compliance Setting Changed				
	Copied				
	Deleted				
	Downloaded				
	ile Deleted First Stage Recycle Bin				
	ile Deleted Second Stage Recycle Bin				
	ile Previewed				
	ile Version Recycled				
	Ile Versions All Minors Recycled				
	And the d				
	nodmed				
	loved				
			~		
		< Back	Next	>	Cancel

Figure 18: Add Operations to Audit



- Select the Operations you would like to audit. The options are:
 - All this is the default option
 - Selected Only
 - All but Excluding Selected
 - To audit specific operations, choose **Selected Only** from the drop-down list and the operations are displayed with checkboxes to select those to be **included** in auditing:
 - To audit all except specific operations, choose All but Excluding Selected from the drop-down list and the checked operations will be excluded from auditing.
- Click **Next**

The Database Settings dialog box is displayed:

					×
Database Settings					
Please enter SQL server de	tails to store the audit da	ita			
Configure SQL S	erver				
SOL Server:	192, 168, 40, 238				
	Authentication				
	Windows Auth	entication			
	SQL Authentic	ation			
	User Name:	sa			
	Password:	•••••			
			Test	Connection	
Select Database:	Lepide_SP_Online				.
		[< <u>B</u> ack	<u>N</u> ext >	Cancel
					
	Figure 19: L	Database Setting	S		

- From this dialog box you can do the following:
 - Add the **SQL Server** name. Click the _____ icon to select a server
 - In the **Select Database** box, type in a name and the Solution will create a database with this name
- Click **Finish**
- A message box will be displayed asking for confirmation to restart the solution:



Figure 20: Confirm Restart

• Click **Yes** to restart

4.6 Viewing the Reports

- Click the Users & Entity behavior icon 🖆 to display the States & Behavior screen
- From the tree structure to the left side of the screen expand SharePoint Online.
- There will be a separate Node for SharePoint Online for the tenant which has been added. Expand this Node
- The example below shows the All Modifications in SharePoint Online Report:

States & Behavior 😵	kpvt-admin.sharepoint.com	m(SharePoint Online)\All	Modifications in ShareP	oint Online					Υ
Search P	Object Name	+ When	8						
All Environment Changes	7 Who	+ Curtom Date Range							
- 🐔 Anomaly Analysis		6/1/2019 12:00 A	M To						
🕀 🙀 SQL Server Reports	Y When	* 3/4/2021 11:59 P	M						
192.168.20.70(SharePoint)	Y Operation	+							
HI LPDE1.local	V Object Type	+							
File Server Reports	▼ Site UDI								
KIVASOFT ONMICROSOFT COM(Exchange Online)	- one one								
knyt-admin sharenoint.com(SharePoint Online)	Y From	+							
A SharePoint Online Modification Reports									Generate Report
All Modifications in SharePoint Online									
Document Modification Reports	Grid View Graph View								
🔓 🔝 Folder Modification Reports	Drag a column header here to grou	p by that column.						💾 Q 🗎	
Permission Modification Reports	1 01	-				17 CH 1101			
Tenant Modification Reports	Object Name	Who 🖓	When n	Operation	V Object Type	V Site URL V	What 🖓	From	Details
Generation Modification Reports	٩ ٩	م	P		<u>٨</u>	م م	P	<u>م</u>	
S SharePoint Group Reports	contentTuneHub	SHAREPOINT/system	12/22/2019 12:50:20 PM	Ste Deleted	Site Collection	https://knut.sharepoint.com	ContentTyneHub : Ste Dala	N/A	Object Name: Sanchit_share
Sharing And Access Reports	ComplianceRoliceCenter	SHAREPOINT/system	12/22/2019 12:50:19 PM	Ste Deleted	Ste Collection	https://kput.sharepoint.com	CompliancePoliceCenter - Si	N/A	Who: SHAREPOINT\system
Pavontes	http://fundamental_denatide	CHAREPOINT) Car Deside	12/22/2010 12:50.17 PM	Created	Ste Collection	http://fundamental_denatide	Ste Cellectice "http://funda	N/A	 When: 12/22/2019 12:50:32 PM
Explore Backup	1	SUAPEPOINT/suternovisio	12/22/2010 12:00:07 PM	Ste Deleted	Ste Collection	http://dridalier.ta_donotde	1 : Ste Deleted	N/A	Operation: Site Deleted
Console Auditing	1004	SHAREPOINT system	12/0/2010 12:02:01 PM	Site Deleted	Site Collection	https://kpvt.sharepoint.com	1224 - Can Deleted	N/A	Object Type: Site Collection
* • ·	4254225422	SHAREFOINT system	12/0/2010 12:02:01 PM	Ske Deleted	Site Collection	https://kpvt.sharepoint.com	4254225422 Che Deleted	N/A	Site URL: https://kpvt.sharepoint.com/sites/
	4304323423	SHAREFOINT system	12/0/2019 12:02:01 PM	Site Deleted	Site Collection	https://kpvt.sharepoint.com	4334323423 . Site Deleted	N/A	From: N/A
2	AccountsDepartment	SHAREFOINT system	12/0/2010 12:02:01 PM	Ske Deleted	Ske Collection	https://kpvt.sharepoint.com	RocourtisDepartment - Site	N/A	What:
	search	SHAREFOINT system	12/0/2019 12:02:00 PM	Site Deleted	web	https://kpvt.snarepoint.com	Search . Site Deleted	N/A	Sanchit_share : Site Deleted
	Community	SHAREFOINT system	12/0/2010 12:01:50 PM	Ske Deleted	Web	https://kpvt.sharepoint.com	Hub , ske beleted	N/A	
	Community	SHAREFOINTSystem	12/6/2019 12:01:56 PM	Site Deleted	web	https://kpvt.snarepoint.com	Community : Site Deleted	N/A	
	Document.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 4:40:15 PM	File Previewed	File	https://kpvt.snarepoint.com	Document.dock : Hie Previe	20.190.145.178	
	Fact dock	tarun@kpvt.onmicrosoft.com	12/6/2019 4:40:14 PM	File Previewed	rie Die	https://kpvt.sharepoint.com	Con1 docx : File Previewed	20.190.145.176	
	Sen Ldocx	tarun@kpvt.onmcrosoft.com	12/6/2019 4:40:14 PM	File Previewed	File	https://kpvt.snarepoint.com	Sen Loocx : Hie Previewed	20.190.145.178	
	Latest.docx	tarun@kpvt.onmcrosoft.com	12/6/2019 12:39:36 PM	File Previewed	rie	https://kpvt.snarepoint.com	Latest.docx : File Freviewed	20.190.145.177	
	Document.docx	tarun@kpvt.onmcrosoft.com	12/6/2019 12:39:38 PM	Hie Previewed	HIE	https://kpvt.snarepoint.com	Document.dock : Hie Previe	20.190.145.177	
	1/oC1.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:39:38 PM	Hie Previewed	hie	https://kpvt.sharepoint.com	1/oC1.docx : Hie Previewed	20.190.145.177	
	Sen1.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:39:38 PM	Hie Previewed	Hie	https://kpvt.sharepoint.com	Sen1.docx : Hie Previewed	20.190.145.17/	
	1/oC1.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:33:43 PM	Hie Previewed	Hie	https://kpvt.sharepoint.com	1/oC1.docx : Hie Previewed	20.190.145.177	
	Latest.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:33:43 PM	He Previewed	Hle	https://kpvt.sharepoint.com	Latest.docx : Hie Previewed	20.190.145.177	
	Document.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:33:43 PM	File Previewed	File	https://kpvt.sharepoint.com	Document.docx : File Previe	20.190.145.177	
	Sen1.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:33:43 PM	File Previewed	File	https://kpvt.sharepoint.com	Sen1.docx : File Previewed	20.190.145.177	
	Document.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:21:59 PM	File Previewed	File	https://kpvt.sharepoint.com	Document.docx : File Previe	20.190.145.179	
	17oCT.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:21:58 PM	File Previewed	File	https://kpvt.sharepoint.com	17oCT.docx : File Previewed	20.190.145.179	
	Sen1.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:21:56 PM	File Previewed	File	https://kpvt.sharepoint.com	Sen1.docx : File Previewed	20.190.145.179	
	Latest.docx	tarun@kpvt.onmicrosoft.com	12/6/2019 12:21:56 PM	File Previewed	File	https://kpvt.sharepoint.com	Latest.docx : File Previewed	20.190.145.175	
D. market	https://kpvt-admin.sharepoi	SHAREPOINT\system	12/5/2019 12:01:32 PM	Tenant DNS Deleted	Tenant	https://kpvt-admin.sharepoi	Https://kpvt-admin.sharepoi	N/A	
States & Behavior	x4.txt	tarun@kpvt.onmicrosoft.com	12/5/2019 11:56:45 AM	Accessed	File	https://kpvt.sharepoint.com	File "x4.txt" : Accessed	125.63.125.71	
	x4.bt	tarun@kpvt.onmicrosoft.com	12/5/2019 11:55:53 AM	Modified	File	https://kpvt.sharepoint.com	File "x4.txt" : Modified	125.63.125.71	
Kegulatory compliance	4	tanun@kout.opmicrosoft.com	12/5/2019 11:55:52 AM	Uninadad	File	https://kout.sharepoint.com	File "v1 txt" - Uninsdad	125 62 125 71	

Figure 21: All Modifications in SharePoint Online Report



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 <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/.

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.

