

Microsoft 365.

quick start guide.

Contents

1	Introduction	3
2	Exchange Online.....	3
2.1	Prerequisites	3
2.2	Steps to Register an App and Generate the Client ID and Secret Key for Exchange Online Auditing...	3
2.3	Assigning the Role to the Application	4
2.4	Permissions for Auditing, DDC, & CPA	4
2.4.1	Permissions for Auditing Exchange Online	4
2.4.2	Permissions for Data Discovery & Classification of Exchange Online	5
2.4.3	Permissions for Current Permissions Analysis	6
2.5	Install the Exchange Online Management Module.....	6
2.6	Generate a ThumbPrint.....	6
2.7	How to Install a Certificate for DDC and FSA Agent	7
2.8	Adding an Exchange Online Component.....	8
3	Office 365 Component	11
3.1	Prerequisites	11
3.2	OneDrive	12
3.2.1	Steps to Register an App and Generate the Client ID and Secret Key for OneDrive Auditing	12
3.2.2	Steps to Generate the Client ID and Secret Key for OneDrive Data Discovery & Classification	13
3.2.3	Permissions for Data Discovery & Classification for OneDrive	14
3.3	Steps to Generate the Client ID and Secret Key for OneDrive Current Permissions Analysis.....	14
3.3.1	Permissions for Current Permissions Analysis for OneDrive	15
3.4	Azure	15
3.4.1	Register an App and Generate the Client ID and Secret Key for Azure Auditing.....	15
3.4.2	Generate the Client ID and Secret Key for Azure Current Permission Analysis	16
3.5	Permissions for Current Permission Analysis for Azure	16
3.6	Teams.....	17

3.6.1	Register an App and Generate the Client ID and Secret Key for Teams Auditing.....	17
3.6.2	Permissions for the Auditing of Teams	17
3.7	Microsoft Copilot	18
3.7.1	Steps to Generate the Client ID and Secret key	18
3.8	Permissions for Copilot	18
3.9	Adding an Azure, OneDrive, MS Teams and Copilot Component	20
4	SharePoint Online	24
4.1	Prerequisites	24
4.2	Steps to Register an App and Generate the Client ID & Secret Key for SharePoint Online Auditing..	25
4.3	Permissions for Auditing SharePoint Online	25
4.4	Steps to Generate the Client ID & Secret Key for SharePoint Online Data Discovery & Classification	26
4.5	Permissions for Data Discovery and Classification of SharePoint Online.....	27
4.6	Steps to Generate the Client ID & Secret Key for SharePoint Online Current Permissions Analysis ..	28
4.7	Permissions for Current Permission Analysis of SharePoint Online.....	29
4.8	Adding a SharePoint Online Component	30
5	Support.....	34
6	Trademarks	34

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, Microsoft Copilot 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 [Installation and Prerequisites Guide](#).

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 Exchange Online

Microsoft Graph

MailboxSetting.Read	Application	For Enumerating the User Mailbox who has Exchange Online License for Auditing	
User.Read.All	Application	For Enumerating the User Mailbox who has Exchange Online License for Auditing	Role: Exchange Administrator

Office 365 Exchange Online

Exchange.ManageAsApp	Application	For Providing the Permission to Client Id and Secret Key to Manage Exchange as Application	Role: Global Reader
MailboxSetting.ReadWrite	Delegated	For Enumerating the User Mailbox who has Exchange Online License for Auditing	



Office365 Management APIs

ActivityFeed.Read	Delegated	For Providing Permission to application to Read Activity Data of your Organization for Auditing.
ActivityFeed.Read	Application	For Providing Permission to application to Read Activity Data of your Organization for Auditing.

2.4.2 Permissions for Data Discovery & Classification of Exchange Online**Microsoft Graph**

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

Office 365 Exchange Online

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



MailboxSettings.ReadWrite	Delegated	For Enumeration Of User Mailbox
---------------------------	-----------	---------------------------------

2.4.3 Permissions for Current Permissions Analysis

For Office 365 Exchange Online

Exchange.ManageAsApp	Application	For Providing the Permission to Client Id and Secret key to Manage Exchange as Application	Role: Exchange Administrator
----------------------	-------------	--	------------------------------

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

5. 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

6. 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:

Run the following PowerShell commands:

1.

```
$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 your certificate and "YourDomainName" should be the name of your Tenant

2.

```
$mycert | Select-Object -Property Subject,Thumbprint,NotBefore,NotAfter
```

Note: User should copy Thumbprint value as it is required for Login Information

3.

```
$mycert | Export-Certificate -FilePath "C:\temp\scriptfile.cer"
```

Note: FilePath should ends with a (.cer) file type

4.

```
$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

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

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

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

2.8 Adding an Exchange Online Component

From the Web Console Manage Component window, click on the **Exchange Online** component and the Add Credential for Exchange Online window is displayed with the Component Credential category selected:

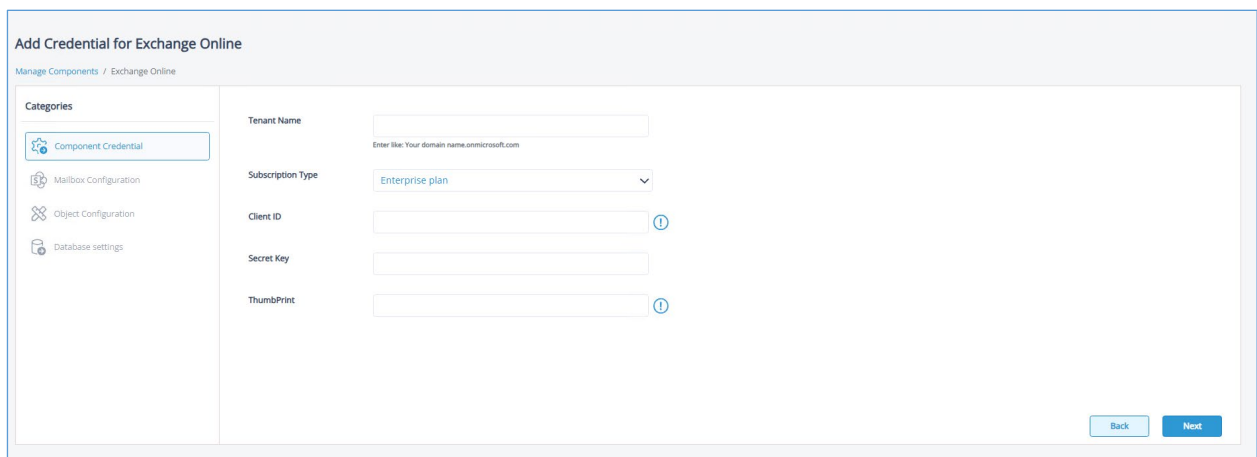


Figure 1: Component Credential

Add the component credentials as follows:

- Enter the **Tenant Name**
- Select the **Subscription Type** from the following options:

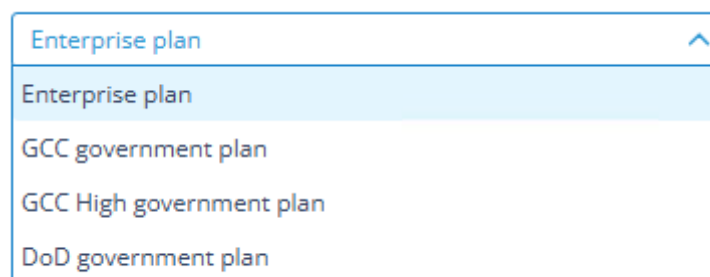



Figure 2: Subscription Types

- Add the **Client Id**
- Add the **Secret Key**
- Add the **ThumbPrint**

Click the  icon to display the steps on how to generate the Client ID, Secret Key and ThumbPrint

NOTE: Within this guide, the instructions on how 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.

- Click **Next** to continue

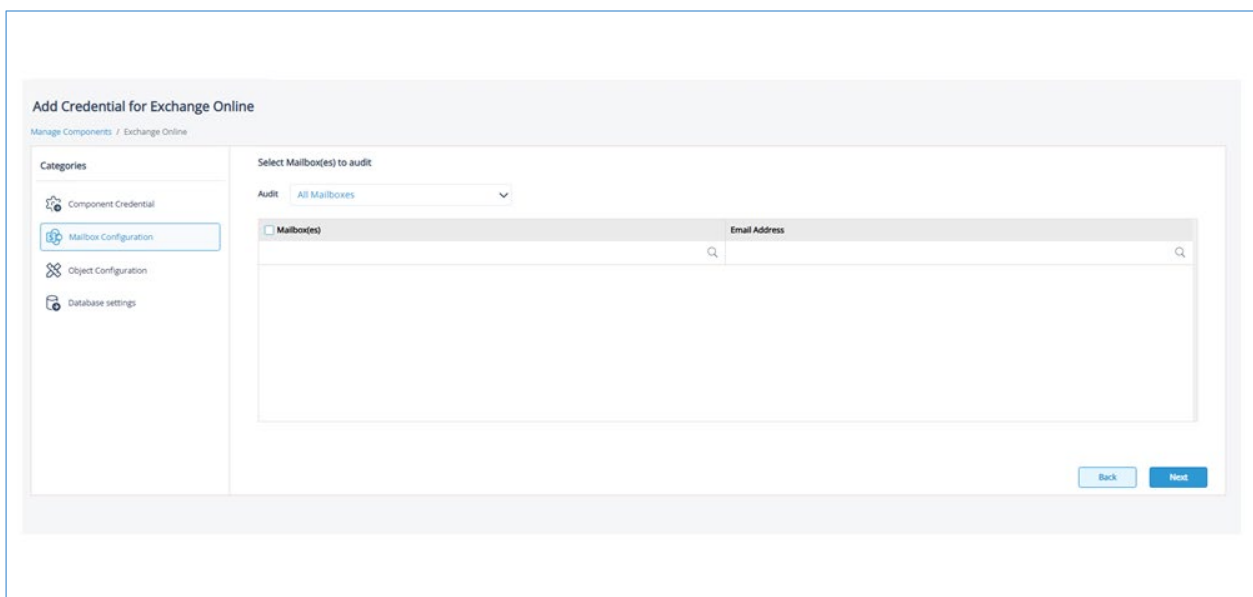



Figure 3: Mailbox Configuration

The Mailbox Configuration window is selected:

- Select one or more of the Mailboxes to be audited
- To select all Mailboxes, check the box next to **Mailbox(es)**
- To search by Mailbox or Email ID, click the relevant search box next to the search icon  and enter the text to search for
- Click **Next** to continue

The Object Configuration window is selected:

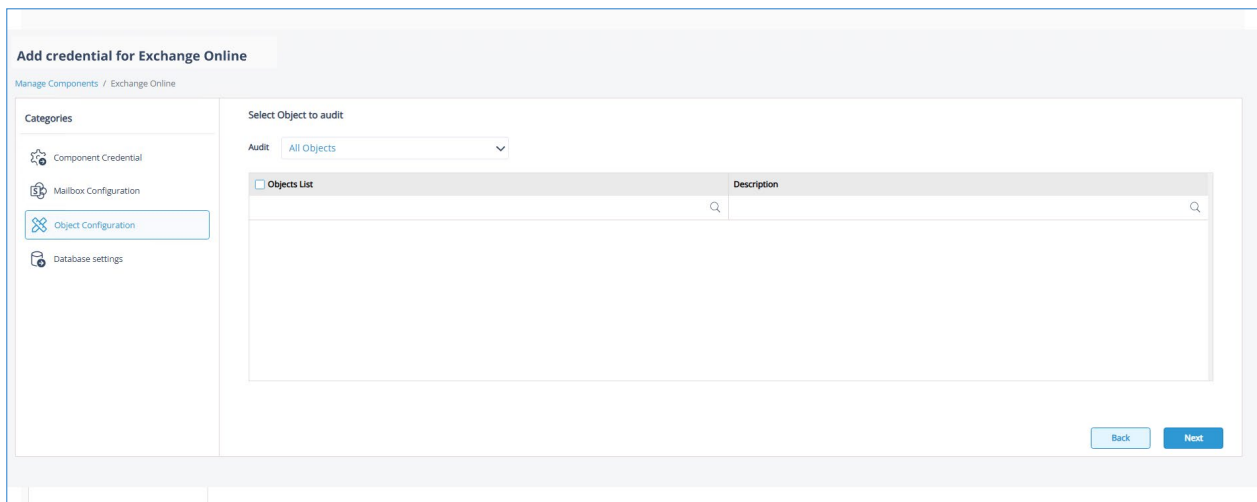


Figure 4: Object Configuration

- Select one or more objects to be audited
- To select all objects, check the box next to **Objects List**
- To search by Object or Description, click the relevant search box next to the search icon 🔍 and enter the text to search for
- Click **Next** to continue

The Database Settings window is displayed:

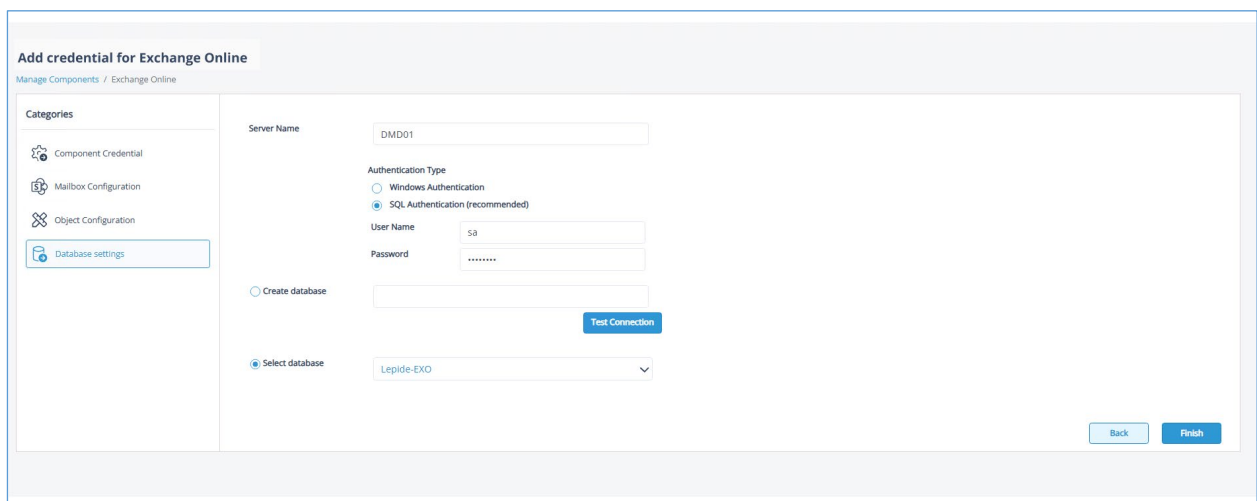


Figure 5: Database Settings

Add the Database Settings as follows:

- **Server Name** – enter the name of the server
- **Authentication Type** – choose from either:

- Windows Authentication or
- SQL Authentication – add the User Name and Password
- Select to either **Create database** – enter the database name and click **Test Connection** to test the database connection

Or

- **Select database** – use the drop-down arrow to select the name of an existing database
- Click **Finish**

The added component will be displayed in the Manage Component window:

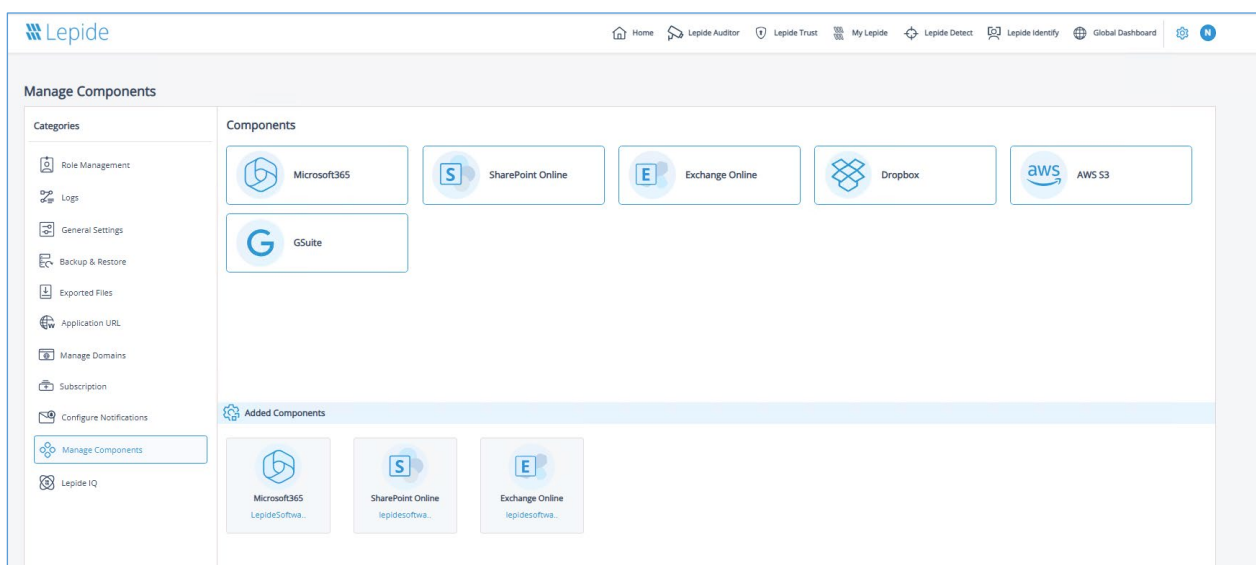


Figure 6: Manage Components

3 Office 365 Component

3.1 Prerequisites

- To add OneDrive, Azure, Teams or Copilot 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 be 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**
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

AuditLog.Read.All	Application
-------------------	-------------

Office 365 Management API's

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

NOTE: Every permission change required must be granted admin consent



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

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 Permissions for Data Discovery & Classification for OneDrive

Office 365 SharePoint Online

Sites.Full.Control.All	Application
User.Read.All	Application

3.3 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



3.3.1 Permissions for Current Permissions Analysis for OneDrive

Office 365 SharePoint Online

Sites.FullControl.All	Application
User.Read.All	Application

3.4 Azure

3.4.1 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

AuditLog.Read.All	Application
Directory.Read.All	Application

Office 365 Management API's

ActivityFeed.Read	Delegated
ActivityFeed.ReadDlp	Delegated



ActivityFeed.Read	Application
ActivityFeed.ReadDlp	Application

NOTE: Every permission change required must be granted admin consent

- Now add the components with Client ID and Secret Key

3.4.2 Generate the Client ID and Secret Key for Azure Current Permission Analysis

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

- Click on the API permission tab for the given Client ID and select **Add a Permission**

3.5 Permissions for Current Permission Analysis for Azure

Exchange.ManageAsApp	Application
----------------------	-------------

NOTE: Every permission change required must be granted admin consent

- Now add the components with Client ID and Secret Key

3.6 Teams

3.6.1 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**

3.6.2 Permissions for the Auditing of Teams

1. 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

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

Microsoft Graph API's

AuditLog.Read.All	Application
-------------------	-------------

NOTE: Every permission change required must be granted admin consent

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



3.7 Microsoft Copilot

3.7.1 Steps to Generate the Client ID and Secret key

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

NOTE: The user should copy Client ID and Secret Key as needed for Login Information

4. Click on the **API Permission Tab** for the given Client ID, click on **Request API Permissions**

3.8 Permissions for Copilot

1. The permissions required for running Copilot Reports are:

Office 365 Management APIs

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

Microsoft Graph Permissions

AuditLog.Read.All	Delegated
AuditLog.Read.All	Application
AuditLogsQuery-OneDrive.Read.All	Application
AuditLogsQuery-SharePoint.Read.All	Application
AuditLogsQuery.Read.All	Application
Directory.Read.All	Application
Files.Read.All	Application
InformationProtectionPolicy.Read.All	Application
Organization.Read.All	Application
User.Read.All	Application

2. Grant Admin consent for Domain (Lepide Data Security Software) after API Permissions selection

NOTE: Every Permission change required must be granted Admin Consent for a given Domain.

NOTE: The user should be a member of the EDiscovery Manager Role to run a Content Search and Export query using PowerShell. This role should be assigned to the user whose email address was provided at the time of Copilot configuration.

Assigning the eDiscovery Manager Role in Microsoft Purview

Follow the steps below to assign the eDiscovery Manager role to a user in Microsoft Purview:

Steps to Assign the Role:

1. **Access Microsoft Purview:**
 - Open your web browser and navigate to [Microsoft Purview](#)
2. **Navigate to Role Management:**
 - Go to **Settings**
 - Select **Roles and Scope**
 - Click on **Role Group**
3. **Edit the eDiscovery Manager Role Group:**
 - Locate and select **eDiscovery Manager**
 - Click **Edit**
4. **Choose the Users for Role Assignment:**
 - Click on **Choose Users**
 - Select the users whom you want to assign the role



- Click **Select**
 - Click **Next**
- 5. Confirm Role Assignment:
 - Ensure that the **Manage eDiscovery Manager role** is assigned
- 6. This role should be assigned to the user whose email address provided at the time of Co-pilot configuration.
 - Click **Save** to finalize the role assignment

By following the above steps, you can successfully assign the eDiscovery Manager role to the necessary users in Microsoft Purview.

Steps to Install the Online PowerShell Module

1. Open Windows PowerShell, run as Administrator
 - Run the following commands firstly in Windows PowerShell(x86) then in Windows PowerShell
2. To Ensure that you have Execution policy set as "Remote Signed " run the below command.

```
Get-ExecutionPolicy
```

3. If Execution policy is not RemoteSigned then run the below command.

```
Set-ExecutionPolicy RemoteSigned
```

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

```
Get-Module -ListAvailable -Name NuGet
```

3.9 Adding an Azure, OneDrive, MS Teams and Copilot Component

From the Web Console Manage Component window, click on the **Microsoft 365** component and the Add Credential for Microsoft 365 window is displayed with the Select Component category selected:

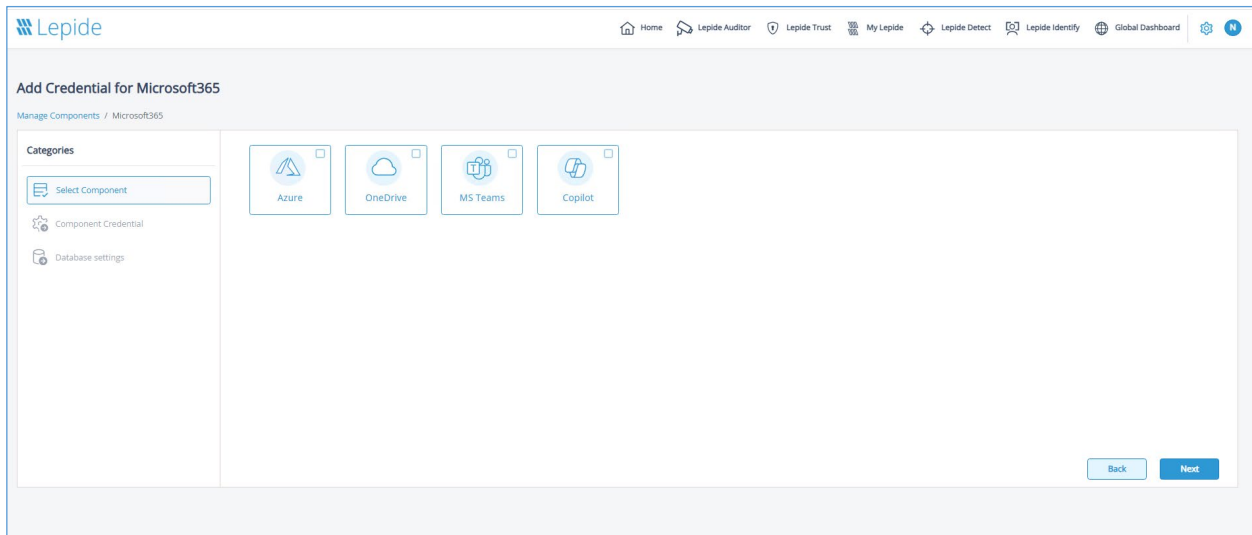


Figure 7: Select Component

From the Select Component category:

- Select the Component(s) you want to add. This can be one or more of the following:
 - Azure
 - OneDrive
 - MS Teams
 - Copilot

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

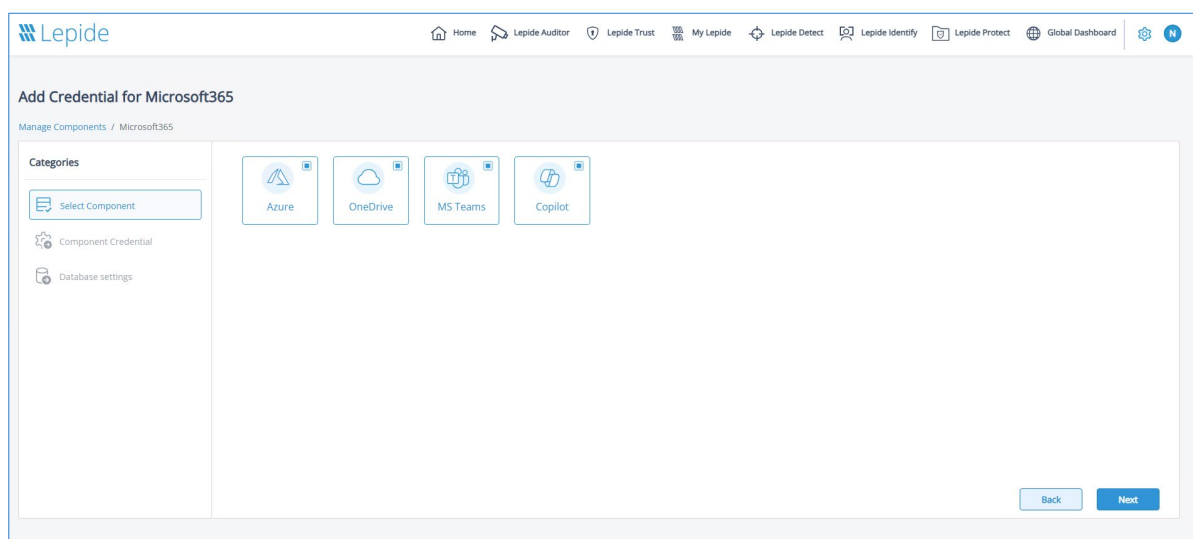


Figure 8: All Microsoft 365 Components Selected

- Click **Next** to continue

The Component Credential window is selected:

The screenshot shows the 'Add Credential for Microsoft365' interface. On the left, a sidebar lists 'Categories' with options: 'Select Component', 'Component Credential' (highlighted), and 'Database settings'. The main area contains a form with the following fields: 'Tenant Name' (with an example: 'Your domain name.onmicrosoft.com'), 'Subscription Type' (a dropdown menu currently showing 'Enterprise plan'), 'Client ID' (with an information icon), 'Secret Key', 'Email ID' (with a note: 'Note: This input is intended for Copilot.'), and 'Password' (with a note: 'Note: This input is intended for Copilot.'). At the bottom right of the form are 'Back' and 'Next' buttons.


Add the component credentials as follows:

- Enter the **Tenant Name**
- Select the **Subscription Type** from the following options:

The screenshot shows a dropdown menu for 'Subscription Type'. The menu is open, displaying a list of options: 'Enterprise plan' (which is highlighted and has an upward arrow icon), 'Enterprise plan', 'GCC government plan', 'GCC High government plan', and 'DoD government plan'.

Figure 10: Subscription Types

- Add the **Client Id**
- Add the **Secret Key**

For steps on how to generate the Client ID and Secret Key, click the  icon

NOTE: Within this guide, the instructions on how to generate the **Client ID** and **Secret Key** are given in Section 3.2 to 3.5.

For Microsoft Copilot:

- Add the **Email ID**
- Add the **Password**

NOTE: We are running PowerShell command to get client chat, and run some graph query to get Sensitive label, so we need Email ID and password of the user who has above permissions and privileges for Copilot.

- Click **Next** to continue

The Database Settings window is selected:

The screenshot shows the 'Add credential for Microsoft 365' window with the 'Database Settings' tab selected. The 'Categories' sidebar on the left includes 'Select Components', 'Component Credential', and 'Database Settings'. The main form contains the following fields and options:

- Server Name:** 192.168.30.332
- Authentication Type:** ☒ Windows Authentication, ☐ SQL Authentication
- User Name:** [Empty text box]
- Password:** [Empty text box]
- Create database:** ☒ (Selected), with a text box containing 'Richard_Data1' and a 'Test Connection' button.
- Select database:** ☐ (Unselected), with a dropdown menu showing 'Select'.

At the bottom right of the window are 'Back' and 'Finish' buttons.

Figure 11: Database Settings

Add the Database Settings as follows:

- **Server Name** – enter the name of the server
- **Authentication Type** – choose from either:
 - Windows Authentication or
 - SQL Authentication – add the User Name and Password
- Select to either **Create database** – enter the database name and click **Test Connection** to test the database connection

Or

- **Select database** – use the drop-down arrow to select the name of an existing database
- Click **Finish**

The added component will be displayed in the Manage Component window:

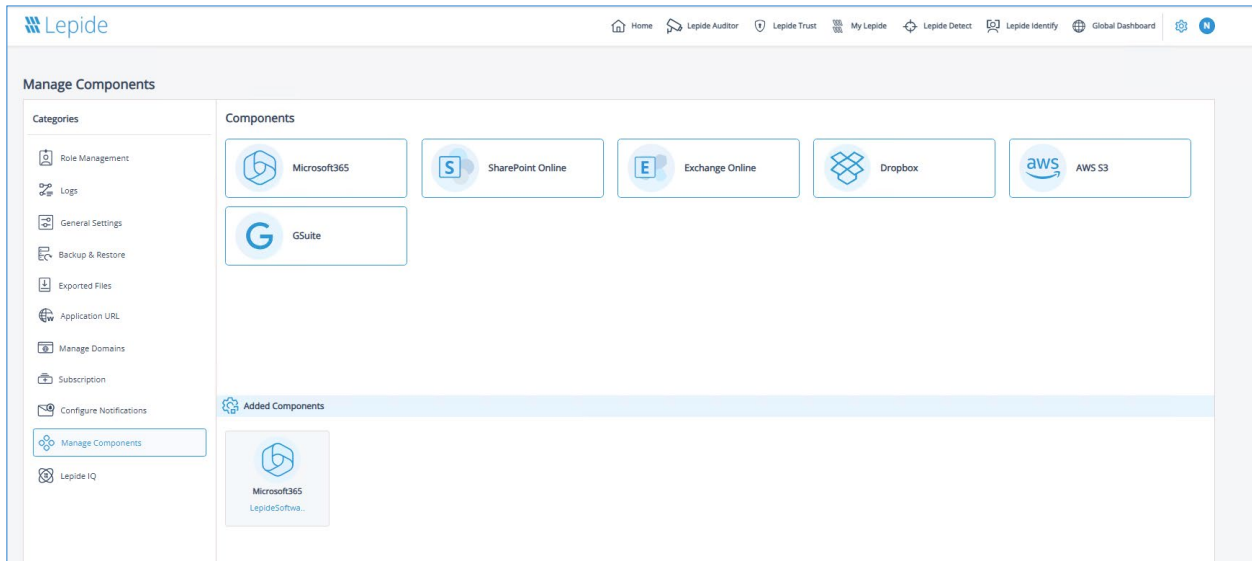


Figure 12: Added Microsoft 365 Component

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 be grayed out.

4.2 Steps to Register an App and Generate the Client ID & 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**

4.3 Permissions for Auditing SharePoint Online

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

Office 365 Management API's

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

NOTE: Every permission change required must be granted admin consent

Now add the components with Client ID and Secret Key

4.4 Steps to Generate the Client ID & 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 in 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
```

4.5 Permissions for Data Discovery and Classification of SharePoint Online

The permissions given to the Client ID are as follows:

Office 365 SharePoint Online

Sites.FullControl.All	Application
User.ReadWrite.All	Application

Office 365 Management API's

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

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

4.6 Steps to Generate the Client ID & 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>
```

5. You will now be prompted to trust the add-in for all the permissions that it requires
6. 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

4.7 Permissions for Current Permission Analysis of SharePoint Online

Office 365 SharePoint Online

Sites.FullControl.All	Application
User.ReadWrite.All	Application

Office 365 Management API's

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

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

4.8 Adding a SharePoint Online Component

From the Web Console Manage Component window, click on the **SharePoint Online** component and the Add Credential for SharePoint Online window is displayed with the Component Credential category selected:

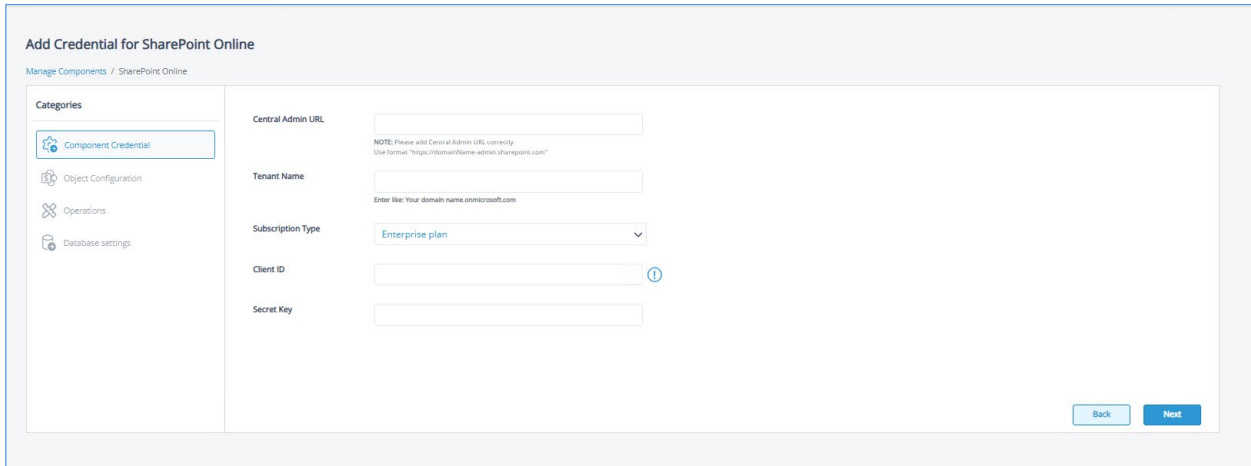


Figure 13: Component Credential

Add the component credentials as follows:

- Enter the **Central Admin URL**
- Enter the **Tenant Name**
- Select the **Subscription Type** from the following options:

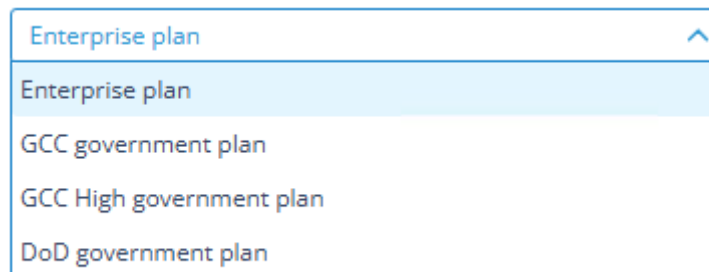



Figure 14: Subscription Types

- Add the **Client Id**
- Add the **Secret Key**

For steps on how to generate the Client ID and Secret Key, click the  icon

NOTE: Within this guide, the instructions on how to generate the **Client ID** and **Secret Key** for SharePoint Online are given in Section 4.2 to 4.4.

- Click **Next** to continue

The Object Configuration window is selected:

The screenshot shows the 'Add credential for SharePoint Online' window. The left sidebar has four categories: 'Component Credential', 'Object Configuration' (selected), 'Operations', and 'Database Settings'. The main area is titled 'Select Object to audit'. It features an 'Audit' dropdown set to 'Selected Only' and a list box titled 'Object List'. The list contains the following items: Document, Document Library, Folder, Group, Link, Link Item, Site, Site Collection, Sharing and Access, and Tenant. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 15: Object Configuration

- Select one or more of the objects to be audited
- To select all objects, check the box next to **Object List**
- Click **Next** to continue

The Operations window is selected:

The screenshot shows the 'Add credential for SharePoint Online' window. The left sidebar has four categories: 'Component Credential', 'Object Configuration', 'Operations' (selected), and 'Database Settings'. The main area is titled 'Select Operation to audit'. It features an 'Audit' dropdown set to 'Selected Only' and a list box titled 'Operation List'. The list contains the following items: Accessed, Check Out Discarded, Checked In, Checked Out, Compliance Settings Changed, Copied, Deleted, File Deleted First Stage Recycle Bin, File Deleted Second Stage Recycle Bin, File Version All Recycle Bin, and Modified. At the bottom right, there are 'Back' and 'Next' buttons.

Figure 16: Operations

- Select one or more operations to be audited

- To select all operations, check the box next to **Operation List**
- Click **Next** to continue

The Database Settings window is displayed:

Add credential for SharePoint Online
Manage Component / SharePoint Online

Categories

- Component Credential
- Object Configuration
- Operations
- Database Settings**

Server Name: 192.168.30.332

Authentication Type:
☒ Windows Authentication
☐ SQL Authentication

User Name:

Password:

☒ Create database: Richard_Data1

☐ Select database:

Figure 17: Database Settings

Add the Database Settings as follows:

- **Server Name** – enter the name of the server
- **Authentication Type** – choose from either:
 - Windows Authentication or
 - SQL Authentication – add the User Name and Password
- Select to either **Create database** – enter the database name and click **Test Connection** to test the database connection

Or

- **Select database** – use the drop-down arrow to select the name of an existing database
- Click **Finish**

The added component will be displayed in the Manage Component window:

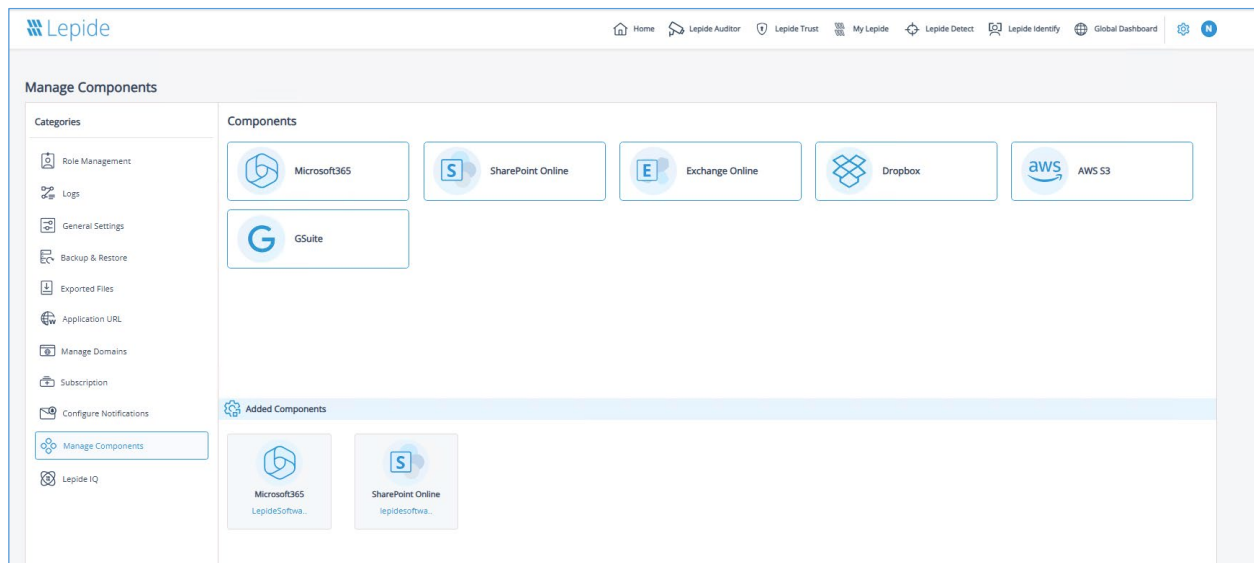


Figure 18: Added SharePoint Online Component

5 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

Alternatively, visit <https://www.lepide.com/contactus.html> to chat live with our team. You can also email your queries to the following addresses:

sales@Lepide.com

support@Lepide.com

To read more about the solution, visit <https://www.lepide.com/data-security-platform/>.

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

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.

