Lepide

CONFIGURATION GUIDE

THE PRINCIPLE OF LEAST PRIVILEGE FOR SHAREPOINT ONLINE

Table of Contents

1. Introduction

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

2. Least Privilege Model for SharePoint Online

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

3. 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.

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

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

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

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

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

Microsoft Graph API's

Name	**Type**
Sites.Read.All	Delegated

Office 365 Management API's

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

NOTE: Every permission change required must be granted admin consent

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

3.2. 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
```

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

3.3. 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**
7. In the App's Permission Request XML field, enter the code below to grant appropriate access:

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

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

Please run the command below at SharePoint Online Management Shell:

```
function Enable-SPDisableCustomAppAuthentication {
Write-Host "Please specify sharepoint organisation name." -ForegroundColor Green
```

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

    $orgName = Read-Host

    $orgName = $contosh

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

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

Set-SPOTenant
```

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

4. Permissions

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

4.1. Auditing Permissions

The permissions required are as follows:

Microsoft Graph API's

Name	Type	Detail
Sites.Read.All	Delegated	Read items in all site collections
Office 365 Management API's		
ActivityFeed.Read	Delegated	Read activity data for your organization
ActivityFeed.Read	Application	Read activity data for your organization
ActivityFeed.ReadDlp	Delegated	Read DLP policy events including detected sensitive data
ActivityFeed.ReadDlp	Application	Read DLP policy events including detected sensitive data

4.2. Data Discovery and Classification Permissions

The permissions given to the Client ID are as follows:

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

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

4.3. Current Permissions Analysis Permissions

The permissions given to the Client ID are as follows:

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

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

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 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/.

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.