Lepide

CONFIGURATION GUIDE

CONFIGURING LEPIDE FOR MICROSOFT 365 WITHOUT GLOBAL ADMINISTRATOR RIGHTS

Table of Contents

1. User Admin Roles

The User Admin Roles are only required while creating app (Client ID and Secret Key) for authentication. After adding a component, the Global Administrator role can be removed and the permissions set up as described below.

2. OneDrive, Azure, MS Team Auditing

2.1. Prerequisites

To add Microsoft 365 server for Auditing, a user must have Global Administrator permissions of the tenant environment.

2.2. To Generate Client ID and Secret Key

1. Log into the Microsoft 365 account through global admin
2. Select **Azure Active Directory Account** through 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 (Global Administrator)
   - 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** (with expiry period) and a Secret ID will be generated which the user can copy for future use

> NOTE: Copy Client ID and Secret Key for adding Microsoft 365 components

4. Click on the API permission tab for the given Client ID and select **Request API Permissions**
5. Select **API my organization uses** as follows:

   Microsoft 365 Management APIs and select permission type(s) as detailed below:

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

6. Grant Admin consent for registered Domain after API Permissions selection

> NOTE: Every permission change required must be granted admin consent for a given Domain

7. Go to the Azure Active Directory Dashboard and select **Tab Roles and Administrators**
8. Under Roles and Administrator select **Global Administrator**
   Double click to **Add Assignments**
   In Add Assignments go to **Select Member(s)** and select newly created members
9. Assignment type will be eligible. Unlock permanently eligible and selection assignment duration and click **Assign**
10. Now add the components with Client ID and Secret Key
11. After adding a component, you can remove global administrator roles and auditing will still work normally

3. Exchange Online Auditing

3.1. Prerequisites

To add Exchange Online server for Auditing, a user must have the following:

- Global Administrator permissions of the tenant environment
- Exchange Administrator permissions of the tenant (for non-owner auditing)

3.2. Generate Client ID and Secret Key

1. Log into the Microsoft 365 account through global admin
2. Select **Azure Active Directory Account** through 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

> NOTE: Copy Client ID and Secret Key for adding a component

4. Click on the API permission tab for the given Client ID
   Select **Request API Permissions**
5. Select **API my organization uses** as follows:

   Microsoft 365 Exchange Online(Delegated and Application)

   >EAS.AccessAsUser.All Delegated

>EWS.AccessAsUser.All	Delegated
>Exchange.Manage	Delegated
>Exchange.ManageAsApp	Application
>Mailboxsettings.Read Write	Delegated
>Tasks.ReadWrite.Shared	Delegated
>Users.ReadWrite	Delegated

Microsoft 365 Management APIs

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

6. 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

7. Go to Azure Active Directory Dashboard and select the tab **Roles and Administrators**
8. Under Roles and Administrators select **Global Administrator** and double click on it to Add assignments
   In Add Assignments go to Select Member(s) and select the newly created members
9. Then the Assignment Type will be eligible. Unlock permanently eligible and selection assignment duration and click **Assign**
10. Now add the components with Client ID and Secret Key
11. After adding a component, you can remove the global administrator roles and auditing will still work normally

4. SharePoint Online Auditing

4.1. Prerequisites

To add SharePoint Online server for Auditing, a user must have Global Administrator permissions of the tenant environment.

4.2. To Generate Client ID and Secret Key

1. Log into the Microsoft 365 account through Global Admin
2. Select **Azure Active Directory Account** through 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
     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

> NOTE: Copy Client ID and Secret Key as this will be needed for Login Information

4. Click on the API Permission Tab for the given Client ID
   Select Request API Permissions
5. Select API my organization uses as follows:

   Microsoft 365 Management APIs

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

   SharePoint (Delegated and Application)

>ActivityFeed.ReadDlp	Delegated
>AllSites.FullControl	Delegated

>Sites.FullControl.All	Application
>Sites.Manage.All	Application
>Sites.Read.All	Application
>Sites.ReadWrite.All	Application

6. 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

7. Go to the **Azure Active Directory Dashboard** and select tab roles and administrators
8. Under Roles and Administrator select **Global Administrator** and double click on it to Add assignments
   In Add assignments go to Select Member(s) and select newly created members
9. Assignment type will be eligible
   Unlock permanently eligible and selection assignment duration and click **Assign**
10. Now add the components with Client ID and Secret Key
11. After adding a component, you can remove the global administrator roles and auditing will still work normally

5. DDC SharePoint Online

5.1. Prerequisites

To add SharePoint Online server for Auditing, a user must have the following:

- Global Administrator permissions of the tenant environment.
- SharePoint Administrator permissions.

5.2. To Generate Client ID and Secret Key

1. Go to **https://<Tenant>-admin.sharepoint.com/_layouts/15/appregnew.aspx**
2. On that page, click the two **Generate** buttons to generate a Client ID and a Client Secret. Enter the title, app domain, and Redirect URI.

> NOTE: Save the retrieved Client ID and Client Secret. They are the credentials for the administrator account, so that read or update actions can be performed on your SharePoint Online

3. Go to **https://<Tenant>-admin.sharepoint.com/_layouts/15/appinv.aspx** Enter the generated client ID in the App Id field and click Lookup.
4. 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. Click the **Trust It** button to trust the app

Now add the components with Client ID and Secret Key

After adding a component, you can remove global administrator roles and classification will still work normally

4. 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/.

5. Trademarks

Lepide Data Security Platform, 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.