Lepide

CONFIGURATION GUIDE

THE PRINCIPLE OF LEAST PRIVILEGE FOR EXCHANGE ONLINE

Table of Contents

1. Introduction

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

2. Least Privilege Model for Exchange Online

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

3. 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

4. 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

5. 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.

6. Permissions for Auditing, DDC, & CPA

6.1. Permissions for Auditing

For Office 365 Exchange Online (Delegated And Application)

Exchange.ManageAsApp	Application	Exchange Online	For Providing the Permission to Client Id and Secret Key to Manage Exchange as Application

Graph Api (Delegated and Application)

User.Read	Application	Graph API	For Enumerating the User Mailbox who has Exchange Online License for Auditing
MailboxSetting.Read	Application	Graph API	For Enumerating the User Mailbox who has Exchange Online License for Auditing

Office365 Management APIs

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

6.2. Permissions for Data Discovery & Classification

Graph Api (Delegated and Application)

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

6.3. Permissions for Current Permissions Analysis

For Office 385 Exchange Online (Delegated And Application)

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

7. 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

8. Generate the Certificate for Tenant on the LDSP Server

Follow the steps below to create the certificate:

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

- Run the following PowerShell commands:

  ```
  $mycert = New-SelfSignedCertificate -DnsName "YourDomainName.com" -
  CertStoreLocation "cert:\LocalMachine\My"-NotAfter   (Get-
  Date).AddYears(NumberofYears) -KeySpec KeyExchange -FriendlyName "scriptfile"
  ```

  Note: "scriptfile" should be User Defined Name for certificate and "YourDomainName" should be name of your Tenant

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

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

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

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

  ```
  $mycert | Export-PfxCertificate -FilePath "C:\temp\scriptfile.pfx" -Password
  $(ConvertTo-SecureString -String "Password value" -AsPlainText -Force)
  ```

  Note: Password value is the User Defined Password Value for certificate

9. Install the Certificate on DDC Agent \ FSA Agent

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

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

10. 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

11. 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/.

12. 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.