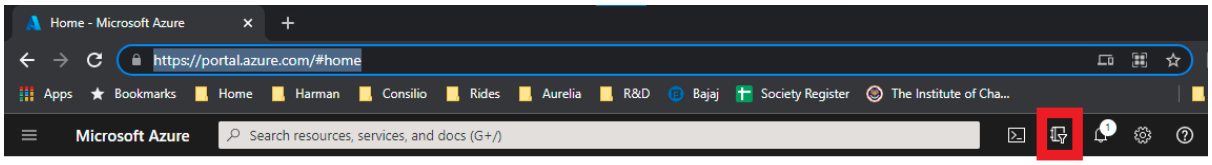
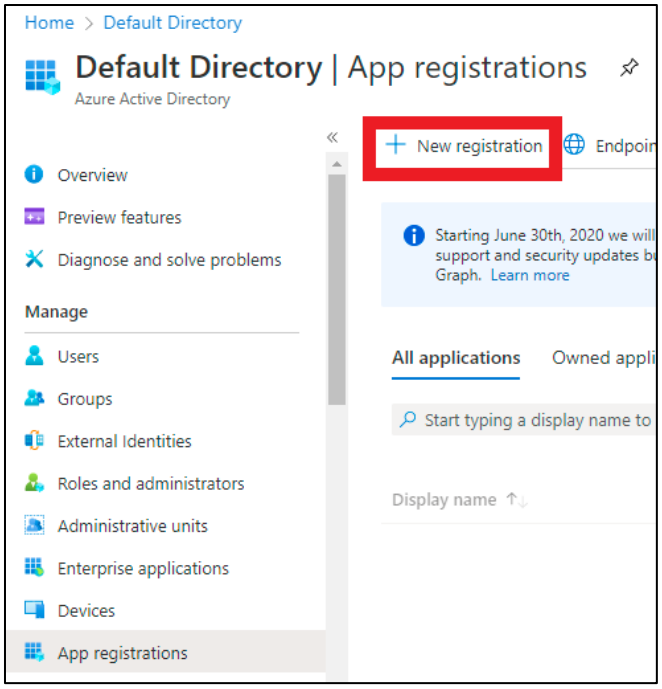
Microsoft365 Connector Technical Setup and App Registration

Steps to follow

1. Go to https://portal.azure.com/
2. Login with a Global Admin account or other appropriate administrator account
3. If there are multiple tenants, select the applicable tenant from the filter on the top right



4. Once the tenant is selected, go to Azure Active Directory from the left side menu. Alternatively, you may search for Azure Active Directory from the search box.
5. Go to **App registrations** from the left side navigation bar.
6. Click on **+ New Registration**
7. In the registration page, give a name for the application, e.g., Sightline Connector.
8. In the Supported Account Types, select "Single tenant".
    a. Since each Sightline client will create their own application, Single tenant should be used. If there is a case where a single application is going to be used to connect to multiple tenants, then select the Multi-tenant option.
9. Click on **Create Application**
10. The application will be created, and you will be redirected to the application properties page.



11. From this page, copy the **Application ID** and the **Tenant ID**. This is required while creating the source in Sightline. Tenant ID can be obtained from the Azure portal's home page as well.

Create application secret

1. Click on the **Certificates & secrets** menu item from the left side navigation section from the newly created application details page.
2. Click **+ New client secret**
3. In the Add a client secret section, give a Description, select the expiration date, and click **Add.**
4. A new client secret will be created, and the details will be displayed
5. Copy the client secret (Value). This is required for Source Location creation in Sightline.
    a. **Please note that this key cannot be accessed again once you leave this page.**

Permissions and Admin Consent

1. Click on **API Permissions** on the left navigation bar.
2. From the permissions page, click **Add a permission**.
3. From the Request API permissions, select **Microsoft Graph.**
4. Use the chart below to set the appropriate permissions.

API / Permissions name	Type	Admin Consent	Outlook	Teams	OneDrive	SharePoint
Calendars.Read	Application	Yes	YES	NO	NO	NO
Calendars.ReadBasic.All	Application	Yes	YES	NO	NO	NO
Calendars.ReadWrite	Application	Yes	YS	NO	NO	NO
CallRecords.Read.All	Application	Yes	NO	YES	NO	NO
ChannelMember.Read.All	Application	Yes	NO	YES	NO	NO
ChannelMessage.Read.All	Application	Yes	NO	YES	NO	NO
Chat.Read.All	Application	Yes	NO	YES	NO	NO
Chat.Read.WhereInstalled	Application	Yes	NO	YES	NO	NO
Directory.Read.All	Application	Yes	NO	YES	NO	NO
Files.Read.All	Application	Yes	NO	YES	YES	YES
Group.Read.All	Application	Yes	NO	YES	NO	NO
Mail.Read	Application	Yes	YES	NO	NO	NO
Mail.ReadBasic	Application	Yes	YES	NO	NO	NO
Mail.ReadBasic.All	Application	Yes	YES	NO	NO	NO
Mail.ReadWrite	Application	Yes	YES	NO	NO	NO
OnlineMeetings.Read.All	Application	Yes	NO	YES	NO	NO
Sites.Read.All	Application	Yes	NO	NO	NO	YES
Team.ReadBasic.All	Application	Yes	NO	YES	NO	NO
TeamMember.Read.All	Application	Yes	NO	YES	NO	NO
TeamsActivity.Read.All	Application	Yes	NO	YES	NO	NO
User.Read	Delegated	No	YES	YES	NO	NO
User.Read.All	Application	Yes	YES	YES	NO	NO

Limiting Permissions to Specific Mailboxes

Administrators who want to limit app access to specific mailboxes can create an application access policy by using the **New-ApplicationAccessPolicy** PowerShell cmdlet. For more information, please visit: https://learn.microsoft.com/en-us/graph/auth-limit-mailbox-access

Helpful Links

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app