FlexNet Beacon does not store the user credentials but instead requests a token from Azure AD and stores it. Azure AD requires that the application requesting a token states what **resource** it needs to access and specifies the **permissions** required to access the objects it intends to act upon, finally it requires that a **user** with roles containing those permissions log into the Azure AD and consent to those permissions.

FlexNet Beacon, for Microsoft 365 connector, uses the **Microsoft Graph** APIs to **read** **user**, **subscribed SKU** and **usage** information. The permissions to read the user, sku and usage information are contained only in an administrator role hence it becomes imperative that a user with administrator role requests this token. Also, when FlexNet Beacon requests this token, FlexNet Beacon is registered as an Enterprise App in Azure AD so that administrators can view and monitor the app & permissions and can revoke the permissions for a particular user or delete the app altogether blocking all accesses.

Since only a Cloud Application Administrator can register the apps in Azure AD, we recommend that a user with Cloud Application Administrator logs in Azure AD in the process of generating token since it has both rights to register the app and read the user, sku and usage information.

Following is a detailed list of permissions and why Microsoft 365 connector requires them. It reads data on these objects from Office 365:

* Users
* Subscribed SKUs
* Reports

Microsoft 365 connector uses Microsoft Graph APIs to get this data. Now there are certain permissions required to get the data on above objects. Here are examples of reading some attributes on those objects and required permissions, with links to Microsoft documentation:

* [List of Users](https://docs.microsoft.com/en-us/graph/api/user-list?view=graph-rest-1.0)

| **Permission type** | **Permissions (from least to most privileged)** |
| --- | --- |
| Delegated (work or school account) | User.ReadBasic.All, User.Read.All, User.ReadWrite.All, Directory.Read.All, Directory.ReadWrite.All, Directory.AccessAsUser.All |

* [Subscribed SKUs](https://docs.microsoft.com/en-us/graph/api/subscribedsku-list?view=graph-rest-1.0)

| **Permission type** | **Permissions (from least to most privileged)** |
| --- | --- |
| Delegated (work or school account) | Directory.Read.All, Directory.ReadWrite.All, Directory.AccessAsUser.All |

* [Outlook Usage Reports](https://docs.microsoft.com/en-us/graph/api/reportroot-getemailappusageuserdetail?view=graph-rest-1.0)

| **Permission type** | **Permissions (from least to most privileged)** |
| --- | --- |
| Delegated (work or school account) | Reports.Read.All |

So above are the bare minimum permissions required for FlexNet Beacon to read the data it needs to read. Now if we go and check Azure AD to see who can consent for these permissions, we find that these permissions must be consented by an admin:

| **Permission** | **Display String** | **Description** | **Admin Consent Required** | **Microsoft Account supported** |
| --- | --- | --- | --- | --- |
| [*Directory.Read.All*](https://docs.microsoft.com/en-us/graph/permissions-reference#directory-permissions) | Read directory data | Allows the app to read data in your organization's directory, such as users, groups and apps. **Note**: Users may consent to applications that require this permission if the application is registered in their own organization’s tenant. | Yes | No |
| [Reports.Read.All](https://docs.microsoft.com/en-us/graph/permissions-reference#reports-permissions) | Read all usage reports | Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Office 365 and Azure Active Directory. | Yes | No |

Finally, we need that FlexNet Beacon can connect to Microsoft Graph APIs on a given schedule and get this data, we need to request [offline\_access](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent#offlineaccess) permission which requests Azure AD to return a Refresh Token that can be used by FlexNet Beacon. The refresh token is used to authenticate with Microsoft in a given user’s context, for a specific resource (Microsoft Graph in this case) and for specific permissions (Directory.Read.All and Reports.Read.All). This token cannot be used for any other purpose.