C vidual regist ed Azure AD enter ri e ap ic ions o e co se ted with spe ific

Centero Azure AD Connector:

- Reads Azure AD users, devices and groups in the customers tenant.
- Requires customers Azure AD administrator (Global Administrator) to consent the application permissions.
- Is used by Centero Portal to verify that Customer's User is allowed to link the tenant to CSM for Intune.
    - The Customer's user signed in the Centero Portal must be either Global Administrator or added as a member to Centero Azure AD Connector Enterprise application.
- Requires the following permissions to Customers tenant:

API name	Permissons	Description	Type	Granted troug
Microsoft Graph	Read directory data	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.	Application	Admin conser
Windows Azure Active Directory	Sign in and read user profile	Allows users to sign in to the app, and allows the app to read the profile of signed-in users. It also allow the app to read basic company information of signed-in users.	Delegated	Admin conser User consent

CSM for Intune

- Manages Intune apps and deployments.
- Requires customers Azure AD administrator (Global Administrator) to consent the application permissions.
- Requires the following permissions to Customers tenant:

API name	Permissons	Description	Type	Granted trough
Microsoft Graph	Read and write Microsoft Intune apps	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune.	Application	Admin consent
Microsoft Graph	Read Microsoft Intune devices	Allows the app to read the properties of devices managed by Microsoft Intune.	Application	Admin consent

M		Allows the app to read the organization and related resources, without a signed-in user. Related resources include things like subscribed skus and tenant branding information.	Application	Admin consent
Windows Azure Active Directory	Sign in and read user profile	Allows users to sign in to the app, and allows the app to read the profile of signed-in users. It also allow the app to read basic company information of signed-in users.	Delegated	Admin consent or User consent

CSM For Intune Application Groups

- Manages memberships of devices to specified groups

API name	Permissions	Description	Type	G T
Microsoft Graph	Sign in and read user profile	Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.	Delegated	A c
Microsoft Graph	Read Microsoft Intune devices	Allows the app to read the properties of devices managed by Microsoft Intune, without a signed-in user.	Application	A c
Microsoft Graph	Read all devices	Allows the app to read your organization's devices' configuration information without a signed-in user.	Application	A c
Microsoft Graph	Read and write all groups	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.	Application	A c
Microsoft Graph	Read Microsoft Intune apps	Allows the app to read the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.	Application	A c