Application Manager for Intune Permissions

Last Modified on 08.03.23

Application Manager for Intune requires individually registered Azure AD enterprise applications with specific permissions for the Intune tenant.

Recast Azure AD Connector Enterprise Application

- Reads Azure AD users, devices and groups in the customer's tenant.
- Requires customer's Azure AD administrator (Global Administrator) to grant the application permissions.
- Used by the Recast Portal to verify that an end user is allowed to link the tenant to AM for Intune. The logged-in user in the Recast Portal must be either Global Administrator or added as a member to Recast Azure AD Connector Enterprise application.

Required Permissions

API name	Permissions	Description	Type	Granted through
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 consent
Microsoft Graph	Sign in and read user profile	Allows users to sign into the app, and allows the app to read the profile of signed-in users. Also allows the app to read basic company information of signed-in users.	Delegated	Admin consent or User consent

Application Manager for Intune Permissions

- Manages Intune apps and deployments.
- Requires customer's Azure AD administrator (Global Administrator) to grant the application permissions.

Required Permissions

API name	Permissions	Description	Type	Granted through
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

API name	Permissions	Description	Type	Granted through
Microsoft Graph	Read Microsoft Intune devices	Allows the app to read the properties of devices managed by Microsoft Intune.	Application	Admin consent
Microsoft Graph	Read organization information	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
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 allow the app to read basic company information of signed-in users.	Delegated	Admin consent or User consent

Application Group Permissions

Manages memberships of devices to specified groups.

Required Permissions

API name	Permissions	Description	Type	Granted Through
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	Admin consent
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	Admin consent
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	Admin consent

API name	Permissions	Description	Type	Granted Through
Microsoft Graph	Read and write all group memberships	Allows the app to list groups, read basic properties, read and update the membership of the groups this app has access to without a signed-in user. Group properties and owners cannot be updated and groups cannot be deleted.	Application	Admin consent
Microsoft Graph	Read all devices	Allows the app to read your organization's devices' configuration information without a signed-in user.	Application	Admin consent

Accept Additional Permissions

The Application Group feature requires additional permissions for Azure AD and Intune tenants.

To accept additional permissions for **Application Manager For Intune Application Groups:**

1. Log into your Microsoft account with Global Administrator credentials.

2. **Accept** the requested permissions.