Application Manager for Intune Description

Last Modified on 08.24.23

Application Manager for Intune integrates into the Customer's Microsoft Intune management system. The integration is done through the **Recast Azure AD Connector** and **Application Manager for Intune Azure AD Application** background applications, and Application Manager background services.

The Intune management system deploys the desired applications onto those workstations that are members of both Intune and the Azure AD groups, configured in Intune as the deployments' target.

Recast Software is not responsible for the Intune environment's operation. Instead, it's the customer's responsibility to take care of the environment's operation, other related services, and deployment of any necessary background applications.

Background Applications

Recast Azure AD Connector

Application Manager Portal, where you manage Application Manager for Intune, requires access to the customer's Azure tenant to be able to read the Azure AD users, devices, and groups that are used to target deployments. Recast Azure AD Connector is an Azure AD registered application that needs the customer's Azure AD administrator's (Global Admin's) consent to access the customer's Azure AD tenant.

Recast Azure AD Connector requires the following permissions to the Customer's tenant:

API name	Permissions	Type	Granted through
Microsoft Graph	Read directory data	Application	Admin consent
Windows Azure Active Directory	Sign in and read user profile	Delegated	Admin consent or User consent

Before allowing the Customer User to link a new Azure AD tenant, the Recast Portal uses Recast Azure AD Connector to verify the Customer User's permission for the action. Verification requires one of the following permissions from the Customer User, signed into Recast Portal:

- Global Admin role in the linked Azure AD tenant
- Added as a member in the Recast Azure AD Connector enterprise application in the linked Azure AD tenant

If the Customer User who is linking the new Azure AD tenant does not have the Global Admin role, the Customer User first needs a permission from the Global Admin, who then needs to add the Customer User as a member to the consented Recast Azure AD Connector enterprise application.

Recast Azure AD Connector registered application is used only by the Azure Functions which are protected by Azure AD authentication. Only a 'Recast Portal' Azure AD registered application can access the functions. The Recast Portal application can be accessed only by Azure AD authenticated Customers.

Application Manager for Intune Permissions

The automation that creates Intune applications and deployments needs access to both the Customer's Azure tenant, for verifying consent, and to Intune, for managing applications. Application Manager for Intune is an Azure AD registered application that needs the Customer's Azure AD administrator's (Global Admin's) consent to access the Customer's Azure AD tenant and Intune.

Application Manager for Intune requires the following permissions to the Customer's tenant:

API name	Permissions	Type	Granted through
Microsoft Graph	Read and write Microsoft Intune applications	Application	Admin consent
Microsoft Graph	Read Microsoft Intune devices	Application	Admin consent
Microsoft Graph	Read organization's information	Application	Admin consent
Windows Azure Active Directory	Sign in and read user profile	Delegated	Admin consent or User consent

If the Customer User who is implementing Application Manager for Intune does not have the Global Admin role, the Customer User first needs permission from the Global Admin, who then needs to add the Customer User as a member to the AM for Intune enterprise application.

The Application Manager for Intune registered application is used only by the Azure Functions and Azure Automation runbook, where Azure Functions are protected by Azure AD authentication. Only a 'Recast Portal' Azure AD registered application can access the functions. The Portal application can be accessed only by Azure AD authenticated Customers. Azure Automation runbook is only accessible by the Provider's authorized development and support personnel.