software manager

Description of CSM for Intune

CSM for Intune integrates into the Customer's Microsoft Intune management system. The integration is done through the **Centero Azure AD Connector** and **CSM for Intune Azure AD Application** background applications, and CSM background services. CSM for Intune configures the assignments, and certain other things, into the Intune management system based on the configuration is the Management Portal.

As a result, 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.

The Provider 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

Centero Azure AD Connector

Centero Management Portal, where you manage the CSM for Intune, needs 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. Centero 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.

Centero 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 Centero Portal uses Centero 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 Centero Portal:

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 Centero Azure AD Connector enterprise application.

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

CSM for Intune

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. CSM 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.

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

API name	Permissons	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 CSM for Intune 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 CSM for Intune enterprise application.

CSM 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 'Centero Portal' Azure AD registered application can access the functions. The Centero Portal

applic_____by Azure AD-authenticated_____s. A___e Aut___mation
runbo_____Provider's authorized development and support personnel.