Recast

Microsoft Intune Settings

Last Modified on 2026-08-17

These settings are visible when **Microsoft Intune** is enabled as a data source for application migration.

Before configuring these Intune settings, you must create an Azure App Registration with the following **Application Permissions** granted in Microsoft Entra ID:

- DeviceManagementApps.Read.All
- DeviceManagementManagedDevices.Read.All

Configure Azure Environment Options

- **Intune Tenant ID**: Azure Active Directory tenant GUID
- **Intune Client ID**: App registration client/application ID
- **Intune Client Secret**: Client secret for the app registration (stored encrypted)
- **Azure Environment**: The Microsoft cloud environment for your tenant

Environment	Graph API Endpoint	Token Authority	Use When
Commercial	graph.microsoft.com	login.microsoftonline.com	Standard Azure public cloud (default)
GCC High	graph.microsoft.us	login.microsoftonline.us	US Government GCC High tenants
DoD	dod-graph.microsoft.us	login.microsoftonline.us	US Government Department of Defense tenants
China	microsoftgraph.chinacloudapi.cn	login.chinacloudapi.cn	Azure operated by 21Vianet (China)

If you are unsure which environment to use, select **Commercial**.
GCC High and DoD are used exclusively by US Government tenants.
China applies only to tenants in the Azure China regions operated by 21Vianet.

Click **Test Intune Connection** to verify.

> **Intune Deploy Import Requirements**
>
> The **Intune Deploy Import** tab requires that the application be **run as Administrator** and the machine running the tool to be **Intune-enrolled**. These conditions are checked automatically and the tab is hidden if either requirement is not met. Additionally, any application you wish to import must be assigned as **Available** (not Required) to the machine in **Company Portal** – the tool downloads content through the Intune SideCar service, which only exposes apps that are available to the device.