SP Marketplace

Prerequisites for Provisioning thru MS PowerShell

SP Marketplace uses the Microsoft recommended, and only way, to provision Modern SharePoint sites through PnP PowerShell commands. The PnP community has release a new version of PnP PowerShell and will no longer support prior versions of PnP PowerShell. The new version extends the functionality and uses modern authentication. Here is the Microsoft article explaining the new Cross Platform PnP PowerShell.

New Version of the PnP PowerShell - Open-source cross-platform PowerShell module to manage Microsoft 365 - Microsoft 365 Developer Blog

We have migrated our PnP Provisioning code to use this new Cross Platform version of PnP PowerShell.

A prerequisite for using this version of PnP PowerShell, previously not required, is the need for us to register an Azure AD Application, which allows our provisioning code to authenticate – this is required due to the new and improved authentication support used by the new version.

This is done with a single PowerShell command, which is `Register-PnPManagementShellAccess`.

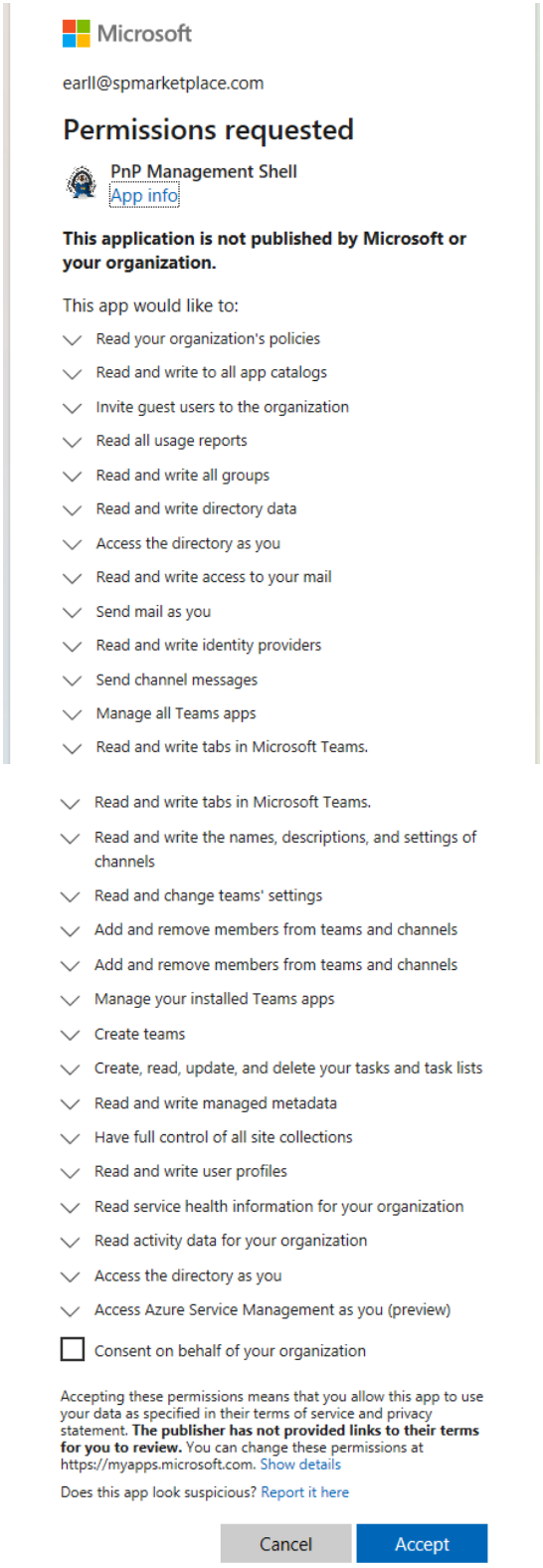
Here is a detailed article on this process and a special case situation for GCC accounts.
`Authentication | PnP PowerShell`

SP Marketplace can do this registration process but it requires Global Admin on the install/service account because Global Admin is the required to register an Azure Ad Application. Without Global Admin, customers will have to create the Azure AD App before we can run our PnP PowerShell scripts that install our products.

Here are the steps required for Non GCC accounts – for GCC Accounts refer to the above article.

1. Open PowerShell ISE
2. Set-ExecutionPolicy –ExecutionPolicy Unrestricted –Scope CurrentUser
3. Install-Module -Name PnP.Powershell -Scope CurrentUse
4. Register-PnPManagementShellAccess
5. Login with an Office/365 user that has Global Admin Role
6. Check the Consent box and then Click on Accept at the next prompt. (Shown below)

SP Marketplace



NOTE: Not all of the above permissions are currently being used in our scripts. Below is a list of permissions that our scripts do not utilize. We do not recommend removing these permissions as future iterations of our scripts may call them, however if it is absolutely necessary, a customer may remove some of the listed permissions by navigating to the Azure AD, locate the App Registration, and remove individual permissions.

Specific Permissions/Actions that are not used in our PnP Provisioning Scripts

1. Invite Guest users to the organization
2. Read all usage reports
3. Read and access to your mail
4. Send mail as you
5. Send Channel Messages
6. Read and write managed metadata
7. Read and write user profiles
8. Read service health information for your organization
9. Read activity Data for your organization
10. Create, read, update and delete your tasks and task lists