**Step-by-Step Guide to Configure PnP PowerShell with SharePoint Online and Entra ID App Using Sites.Selected Permission**

This guide outlines how to set up the PnP PowerShell module to interact with SharePoint Online using an Entra ID app registration with the Sites.Selected permission for app-only authentication. This approach ensures secure, unattended script execution with minimal permissions, adhering to the principle of least privilege.

**Prerequisites**

* **PowerShell 7.2 or later**: Required for the PnP PowerShell module. Download from Microsoft's PowerShell GitHub.
* **PnP PowerShell Module**: Install the module if not already installed.
* **Microsoft Entra ID Permissions**: You need Application Developer or Global Administrator role to register an app, and Global Administrator or SharePoint Administrator role to grant permissions.
* **SharePoint Site URL**: The specific site(s) you want the app to access (e.g., https://yourtenant.sharepoint.com/sites/yoursite).
* **Administrative Access**: Access to the Microsoft Entra admin center and SharePoint Online admin center.

**Step 1: Install the PnP PowerShell Module**

1. Open PowerShell 7.2 or later as an administrator.
2. Install the PnP PowerShell module by running:

Install-Module -Name PnP.PowerShell -Force

1. Verify the installation:

Get-Module -Name PnP.PowerShell -ListAvailable

**Step 2: Register an Entra ID Application**

1. **Access the Entra Admin Center**:
   * Navigate to Microsoft Entra admin center.
   * Sign in with an account that has Application Developer or Global Administrator permissions.
2. **Register a New Application**:
   * Go to **Identity** > **Applications** > **App registrations**.
   * Click **+ New registration**.
   * Enter a name (e.g., PnP-PowerShell-App).
   * Set **Supported account types** to "Accounts in this organizational directory only."
   * Leave **Redirect URI** blank or set to http://localhost for app-only scenarios.
   * Click **Register**.
   * Note down the **Application (client) ID** from the app’s Overview page.
3. **Add Sites.Selected Permission**:
   * In the app registration, go to **API permissions** > **Add a permission**.
   * Select **Microsoft APIs** > **SharePoint**.
   * Choose **Application permissions** (not Delegated).
   * Expand **Sites** and select **Sites.Selected**.
   * Click **Add permissions**.
   * Under **Configured permissions**, click **Grant admin consent for [your tenant name]**.
   * Confirm by clicking **Yes** (requires Global Administrator privileges). If the button is greyed out, contact a Global Administrator to perform this step.

**Step 3: Create and Upload a Self-Signed Certificate**

1. **Generate a Self-Signed Certificate**:
   * In PowerShell, use the New-PnPAzureCertificate cmdlet to create a certificate:

$cert = New-PnPAzureCertificate -OutPfx "pnp.pfx" -OutCert "pnp.cer" -ValidYears 1

* + This generates a .pfx (private key) and .cer (public key) file in your current directory.
  + Note the **Thumbprint** and **Base64 encoded key** from the command output.

1. **Upload the Certificate to Entra ID**:
   * Return to the Entra ID app registration in the Entra admin center.
   * Go to **Certificates & secrets** > **Certificates** tab.
   * Click **Upload certificate**.
   * Select the pnp.cer file generated above and click **Add**.
2. **Install the Certificate Locally** (for script execution):
   * Double-click the pnp.pfx file and follow the wizard to import it into the **Current User** > **My** certificate store.
   * Alternatively, use PowerShell to import:

Import-PfxCertificate -FilePath "pnp.pfx" -CertStoreLocation Cert:\CurrentUser\My

**Step 4: Grant Sites.Selected Permission to Specific SharePoint Sites**

1. **Connect to SharePoint Online**:
   * Use an account with SharePoint Administrator or Global Administrator permissions to connect to the SharePoint tenant:

Connect-PnPOnline -Url "https://yourtenant.sharepoint.com" -Interactive

* + Sign in with your credentials and complete any multi-factor authentication if prompted.

1. **Grant Permissions to Specific Sites**:
   * For each site you want the app to access, run the Grant-PnPAzureADAppSitePermission cmdlet. Replace the placeholders with your values:
   * $siteUrl = "https://yourtenant.sharepoint.com/sites/yoursite"
   * $clientId = "<Your Application (client) ID>"

Grant-PnPAzureADAppSitePermission -AppId $clientId -DisplayName "PnP PowerShell App" -Permissions Read -Site $siteUrl

* + Replace Read with Write, Manage, or FullControl based on your needs (e.g., Write for modifying content, FullControl for full administrative access).
  + Repeat for additional sites (e.g., https://yourtenant.sharepoint.com/sites/othersite).

1. **Verify Permissions**:
   * Check the permissions granted to the app:

Get-PnPAzureADAppSitePermission -Site $siteUrl

**Step 5: Connect to SharePoint Online Using the Entra ID App**

1. **Prepare Connection Parameters**:
   * Gather the following:
     + $siteUrl: The SharePoint site URL (e.g., https://yourtenant.sharepoint.com/sites/yoursite).
     + $clientId: The Application (client) ID from Step 2.
     + $thumbprint: The certificate thumbprint from Step 3.
     + $tenant: Your tenant name (e.g., yourtenant.onmicrosoft.com).
2. **Connect Using the Certificate**:
   * Run the following command to connect:

Connect-PnPOnline -Url $siteUrl -ClientId $clientId -Thumbprint $thumbprint -Tenant $tenant

* + This establishes an app-only connection to the specified site.

1. **Test the Connection**:
   * Verify the connection by retrieving site details:

Get-PnPSite

* + If successful, it returns details of the connected site. If you encounter a (401) Unauthorized error, ensure the Sites.Selected permission was granted correctly for the site and the certificate is installed.

**Step 6: Example Usage**

Once connected, you can perform tasks on the site, limited to the permissions granted (e.g., Read, Write, Manage, or FullControl). Examples:

* **List All Lists**:

Get-PnPList

* **Add an Item to a List** (requires Write or higher permission):

Add-PnPListItem -List "YourListName" -Values @{"Title" = "New Item"}

* **Retrieve Site Permissions**:

Get-PnPAzureADAppSitePermission

**Step 7: Disconnect and Clean Up**

1. **Disconnect the Session**:
   * When finished, disconnect from SharePoint:

Disconnect-PnPOnline

1. **Secure the Certificate**:
   * Store the .pfx file securely and delete it from unsecured locations.
   * If using Azure KeyVault for certificate storage, refer to Microsoft Learn for integration steps.