How-To: Set Up App Registrations for Automated Entra ID Administration

Field	Details
Document Type	How-To Guide / Runbook
Applies To	Microsoft Entra ID, PowerShell, Microsoft Graph SDK
Audience	Systems Administrators / DevOps
Author	AK. Udofeh
Last Updated	April 2026

Overview

This article provides a structured guide on creating and configuring a Microsoft Entra ID App Registration. This setup allows for secure authentication from a local terminal or automated scripts to perform administrative tasks such as SSO configuration and directory management.

Background

To interact with Entra ID via automation or the command line without using personal user credentials, a Service Principal is required. Standard user accounts often have MFA or conditional access policies that interfere with headless automation; an App Registration provides a controlled, auditable, and secure method for programmatic access.

Before You Start

Check	Where
Sufficient Permissions	Ensure you have 'Application Developer' or 'Cloud Application Administrator' roles.
Microsoft Graph SDK	Install the module: `Install-Module Microsoft.Graph`
Client Credentials	Have a naming convention ready (e.g., `Svc-Entra-Config`).

Configuration Steps

1. **Register the Application**:
    - Navigate to https://entra.microsoft.com> Entra ID > App Registrations > New Registration.

- Enter a meaningful display name (e.g. AppName SSO).
- Under Supported account types, select Accounts in this organisational directory only (Single tenant) unless multi-tenant access is required.
- Leave the Redirect URI blank.
- Click Register.

2. **Generate Credentials**:
   - Go to **Certificates & secrets > Client secrets**.
   - Create a new secret.
   - Give it a description for future reference.

> Copy the secret Value immediately; it will be masked permanently once you leave the blade.

3. **Configure API Permissions**:

   - Go to **API permissions > Add a permission > Microsoft Graph**.
   - Select **Application permissions**.
   - Add `Application.ReadWrite.All` (for SSO/App config) and `Directory.Read.All`.
   - Select:, G**rant admin consent for [Tenant]**.

4. **Elevate via Directory Roles (Conditional)**:

> Only perform this step if API permissions above result in "Access Denied" for specific administrative tasks.

   - Navigate to **Identity > Roles & admins**.
   - Search for **Cloud Application Administrator**.
   - Select **Add assignments** and search for the **Name** of your App Registration to assign the role directly.

Automated / Script Option - PowerShell

```
# Define connection variables
$TenantId = "your-tenant-id"
$ClientId = "your-client-id"
$ClientSecret = "your-client-secret" | ConvertTo-SecureString -AsPlainText -Force

# Create credential object for non-interactive login
$Credential = New-Object System.Management.Automation.PSCredential($ClientId, $ClientSecret)

# Connect to Microsoft Graph using the App Registration
# This uses the Client Credentials flow
Connect-MgGraph -TenantId $TenantId -Credential $Credential
```

```
# Success Indicator: Retrieve Tenant details to verify connection
Get-MgOrganization | Select-Object DisplayName, Id
```

Script Breakdown

- **Variable Definition**: Stores the IDs and secrets generated in the portal. The secret is converted to a `SecureString` for compatibility with PowerShell credential objects.
- **Connect-MgGraph**: Establishes the session. Because a `Credential` object is passed, it bypasses the interactive browser login.
- **Get-MgOrganization**: A simple test command. If the terminal returns your organisation's name, the authentication was successful.

Automated / Script Option - zsh

```
export ARM_CLIENT_ID="your-app-id"
export ARM_CLIENT_SECRET="your-app-password"
export ARM_SUBSCRIPTION_ID="your-sub-id"
export ARM_TENANT_ID="your-tenant-id"
```

Troubleshooting

Access Denied (403 Error)

- **Cause**: The App Registration lacks the specific Graph API scope or the Directory Role required for the task.
- **Fix**: Ensure **Admin Consent** was clicked in the portal. If the error persists, assign the **Cloud Application Administrator** directory role to the app as detailed in the manual steps.

Conflicting Authentication Context

- **Cause**: An existing interactive session is active in the terminal.
- **Fix**: Run `Disconnect-MgGraph` before attempting to connect with the App Registration credentials.

Expected Outcome

Metric	Detail
Resolution Time	10–15 Minutes
User Impact	None (Backend configuration only)
Recurrence Risk	Low (Credentials expire based on secret lifetime)

Revision #4
Created 2026-04-15 10:57:09 UTC by AK. Udofeh
Updated 2026-04-15 15:51:02 UTC by AK. Udofeh