Sample: Conditional Access API access using PowerShell

# Call CA API with PowerShell script

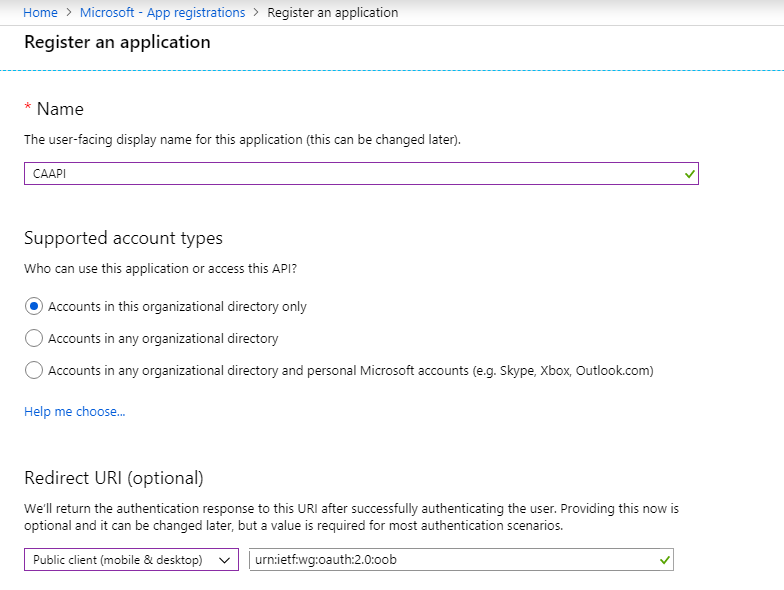
The Conditional Access API and the Named Location API are standard REST Based API, the below example covers how these APIs can be called using the PowerShell to create more complex operations.

We have created a PowerShell script Sample that calls the API. In order to use this script, please take the following steps:

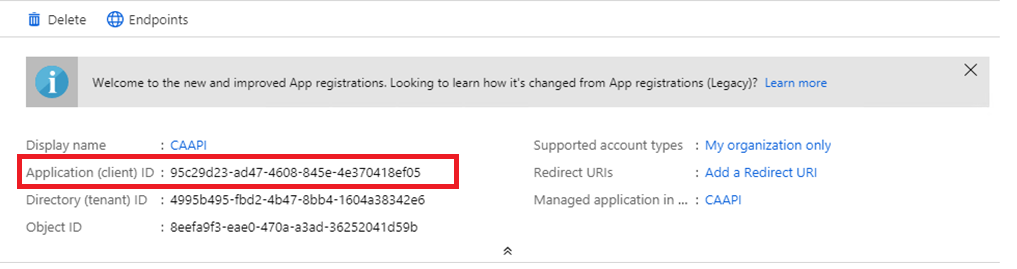
## Register an Azure AD application which has permissions to call the API

The Graph authorization model requires that an application must be consented by a user or administrator prior to accessing an organization’s data.

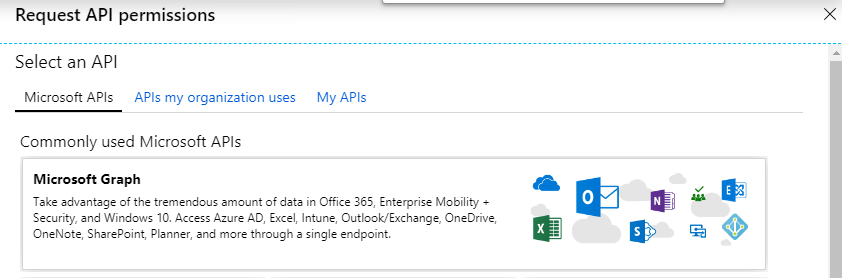
1. Log into the Azure portal as a global administrator.
2. Navigate to the Azure Active Directory Blade , and click on “**App registrations”**.
3. Click on “**New registration**” button at the top of the page.
4. Provide a name for the application that is different from any other application in your tenant’s directory (e.g., “CA API”), change the **Supported account types** to **Accounts in this organizational directory only**, and provide the following as the Redirect URI: choose “**Public client (mobile & desktop)”** and type **urn:ietf:wg:oauth:2.0:oob**



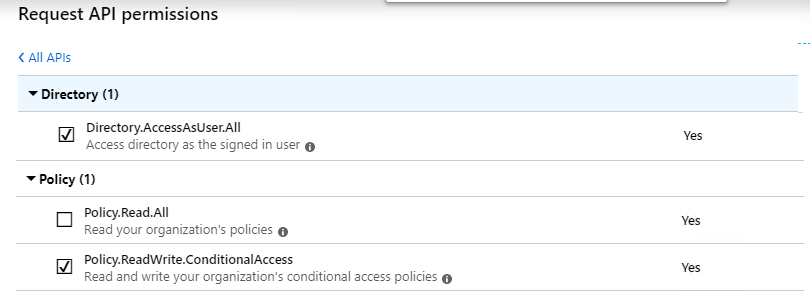
1. Click “Register”.
2. When the application is registered, copy the **Application (Client) ID value**, and save the value for later – we will use it in the script.



1. Click on Settings, then click on “**API Permissions**” under Manage Blade.
2. Click on “**Add a permission**”
3. Select “**Microsoft Graph**” under “**Microsoft APIs”**

****

1. Select the following: Select ***Directory.AccessAsUser.All*** and ***Policy.ReadWrite.ConditionalAccess***, sign in and read user profile. Then click “**Add permissions**”



1. Review the Permissions

A screenshot of a social media post

Description automatically generated

## Install PowerShell Prerequisites

1. Download and install [**Azure AD PowerShell V2**](https://github.com/Azure/azure-docs-powershell-azuread/blob/master/docs-conceptual/azureadps-2.0/install-adv2.md)**.**
2. Install[**MSCloudIdUtils**](https://www.powershellgallery.com/packages/MSCloudIdUtils/). This module provides several utility cmdlets including:
   1. The ADAL libraries needed for authentication
   2. Access tokens from user, application keys, and certificates using ADAL
   3. Graph API handling paged results
3. If it's your first time using the module run **Install-MSCloudIdUtilsModule**.

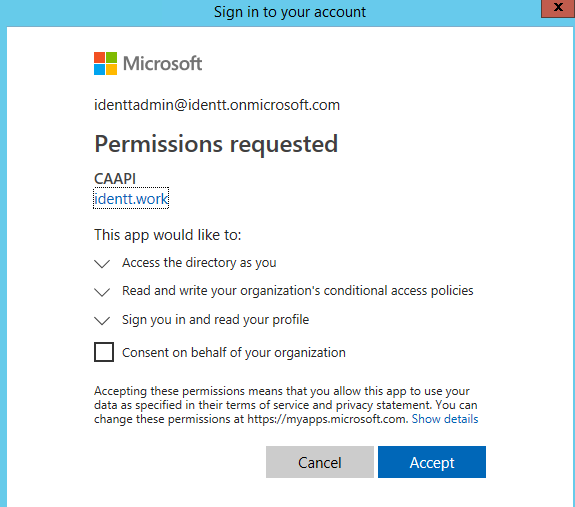
## Edit PowerShell Script

1. Open CAAPI.PSM1 and change the following:
   1. Replace $tenantDomain with the domain of your tenant
   2. Replace $clientID with the App ID you created earlier.



## Using the PowerShell Script

1. Open PowerShell and navigate to the folder where you saved the **CAAPI.psm1** file.
2. Load the script.\ **CAAPI.psm1** and authenticate with a Global Administrator.
3. You will the below Dialog with requested permission **“Accept”** to login



1. Available functions:

* **New-CAPolicy**
* **Start-CAPolicyBackup**
* **Start-CAPolicyRestore**
* **Get-CAPolicy**
* **Set-CAPolicy**

1. You can add your own customizations using Microsoft Graph API

<https://developer.microsoft.com/en-us/graph/docs/concepts/auth_overview>

# Known Issues / Limitations

The List is mainted and updated here

<https://github.com/jeevanbisht/CAPSModule/blob/master/KnownIssuesTracker>

# Additional Information

**Can I use this capability in production?**

The purpose of the early preview is to gather feedback and find issues and is part of getting the APIs into a production ready state; we do not recommend that you use this feature in production.

**Who can I call when things go wrong?**

The Azure AD engineering team will directly support each Private Preview customer. Please reach out to your GTP representative with any issues or questions.

**How about Breaking changes and functional takebacks?**

There is a high degree of ongoing change during a Private Preview that is hard to predict. Therefore, we limit Private Previews to a restricted set of customers working directly with engineering. Customer should assess risk when deploying Private Preview features in production.

**What is the time frame to next milestone?**

Private Preview capabilities may be withdrawn and possibly redesigned before reaching further milestones.