

# Microsoft 365 Developer Certification

## Identity and Security



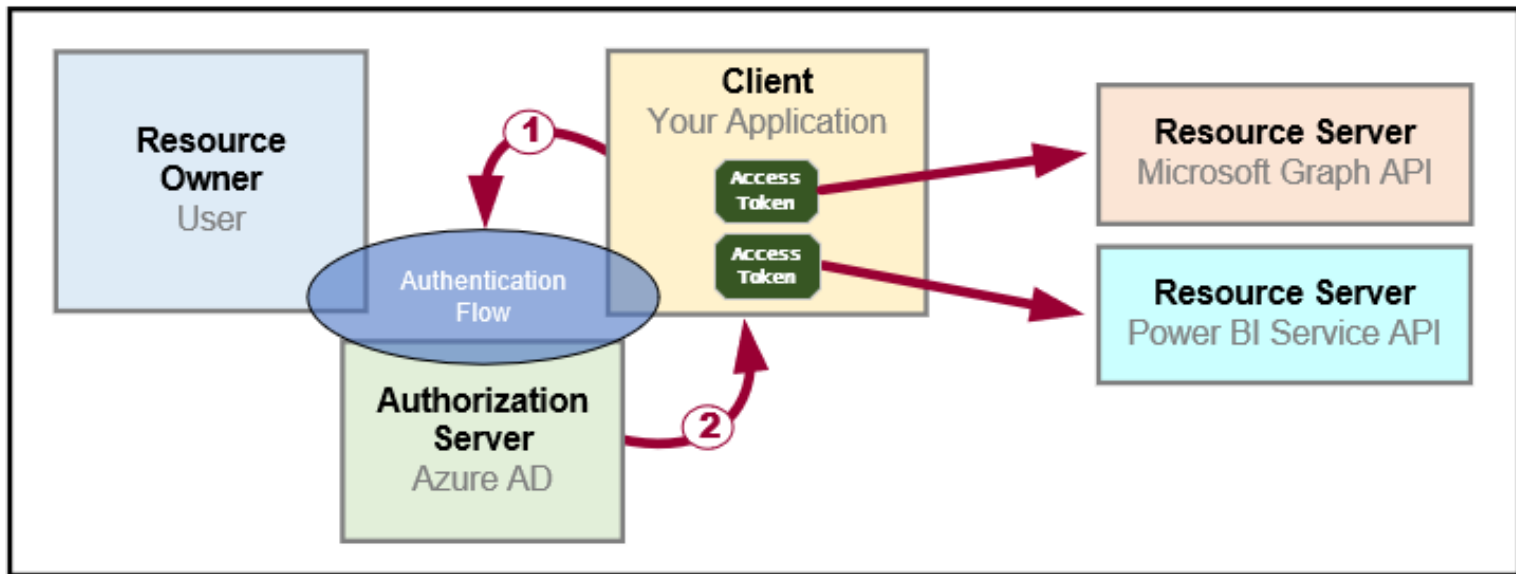
# Agenda

- OAuth and OpenID Connect Primer
- Register an Application
- Implement Authentication
- Configure Permissions to Consume an API
- Implement Authorization to Consume an API
- Implement Authorization in an API
- Create a Service to Access Microsoft Graph



# OAuth 2.0 Fundamentals

- Client application calls to resource server on behalf of a user
  - Client implements authentication flow to acquire access token
  - Access token contains permission grants for client to call resource server
  - Client passes access token when calling to resource server
  - Resource server inspects access token to ensure client has permissions



# Access Token is a Bearer Token

- It can be used by any who bears (e.g. steals) it
  - Always encrypt with HTTPS when transmitting access tokens

```
{
  "iss": "https://sts.windows.net/f995267b-5b7d-4e65-b929-d3d3e11784f9/",
  "amr": [ "pwd" ],

  "iat": 1542829619, "nbf": 1542829619, "exp": 1542833519,

  "tid": "f995267b-5b7d-4e65-b929-d3d3e11784f9",

  "appid": "b52f8e53-d0bf-45c2-9c39-d9c1e96e572c",

  "aud": "https://analysis.windows.net/powerbi/api",

  "scp": "Dashboard.Read.All Dataset.Read.All Group.Read.All Report.ReadWrite.All",

  "oid": "32573058-0ac0-4935-a39d-cd57d5a5a894",
  "unique_name": "maxwells@sharepointconfessions.onmicrosoft.com",
  "upn": "maxwells@sharepointconfessions.onmicrosoft.com",
  "name": "Maxwell Smart",
  "family_name": "Maxwell",
  "given_name": "Smart",

  "ipaddr": "47.200.98.132",

  "ver": "1.0"
}
```



# OAuth 2.0 Client Registration

- Client must be registered with authorization server
  - Authorization server tracks each client with unique Client ID
  - Client should be registered with one or more Reply URLs
  - Reply URL should be fixed endpoint on Internet
  - Reply URL used to transmit security tokens to clients
  - Client registration tracks permissions and other attributes

## Authorization Server

Azure AD

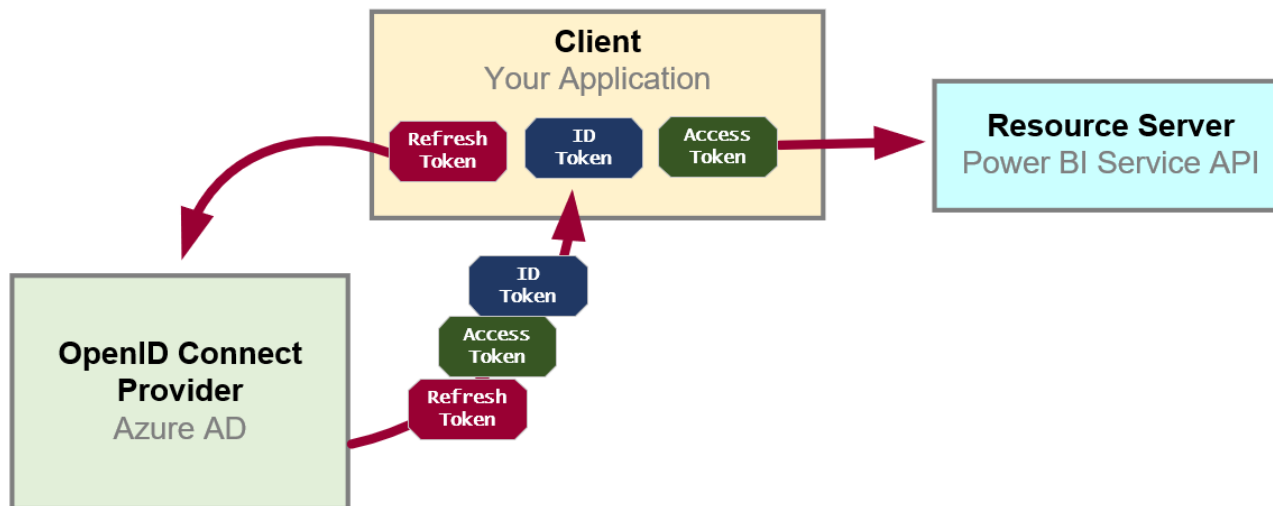
### Registered Applications

Name	App ID	Permissions	Reply URL	Credentials
App1	guid1	...	none	none
App2	guid2	...	...	secret key
App3	guid3	...	...	X.509 Certificate



# OpenID Connect Extends OAuth 2.0

- OAuth 2.0 has shortcomings with authentication & identity
  - It does not provide client with means to validate access tokens
  - Lack of validation makes client vulnerable to token forgery attacks
- Open ID Connect is standard which extends OAuth 2.0
  - OpenID Connect provider passes ID token in addition to OAuth 2.0 tokens
  - OpenID Connect provider provides client with keys for token validation





# Inquiring Minds Want To Know...

- Where are my users
  - Inside a single tenant
  - Inside any Microsoft 365 tenant
  - Inside a Microsoft 365 tenant or
- Where does the application run
  - Public client versus Confidential client
- Should the app work on behalf of a user or work as itself
  - Should access tokens be created as user tokens or app-only tokens
- When and how should permissions be requested and granted
  - when should the app ask the user for permissions to a resource



# Authentication Flows

- **User Password Credential Flow** *(public client)*
  - Used in Native clients to obtain access code
  - Requires passing user name and password across network
- **Device Code Flow** *(public client)*
  - New style of authentication introduced with Azure AD v2 Endpoint
- **Client Credentials Flow** *(confidential client)*
  - Authentication based on password or certificate held by application
  - Used to obtain app-only access tokens
- **Authorization Code Flow** *(confidential client)*
  - Client first obtains authorization code sent back to browser
  - Client then obtains access token in server-to-server call
- **Implicit Flow** *(public client)*
  - Used in SPAs built with JavaScript and AngularJS
  - Application obtains access token w/o acquiring authorization code





# The Azure Portal

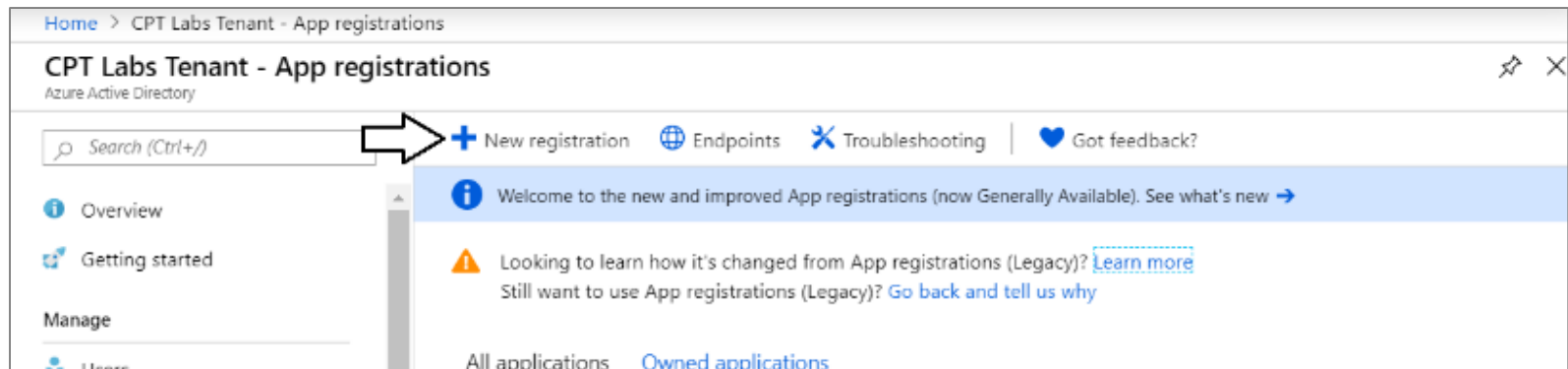
- Azure portal allows you to register Azure AD applications
  - Azure Portal accessible at <https://portal.azure.com>
  - No Azure subscription required to register applications

The screenshot displays the Microsoft Azure portal interface. On the left, the navigation pane shows the 'App registrations' link highlighted. The main content area is titled 'Critical Path Training - App registrations' and shows a table of applications. An arrow points from the 'App registrations' link in the sidebar to the table, and another arrow points from the 'My Public Client App' entry in the table to the 'New registration' button.

DISPLAY NAME	APPLICATION (CLIENT) ID
MP My Public Client App	0e5a8b4c-1c1e-4fdf-bc2a-c5e7a8f5835a

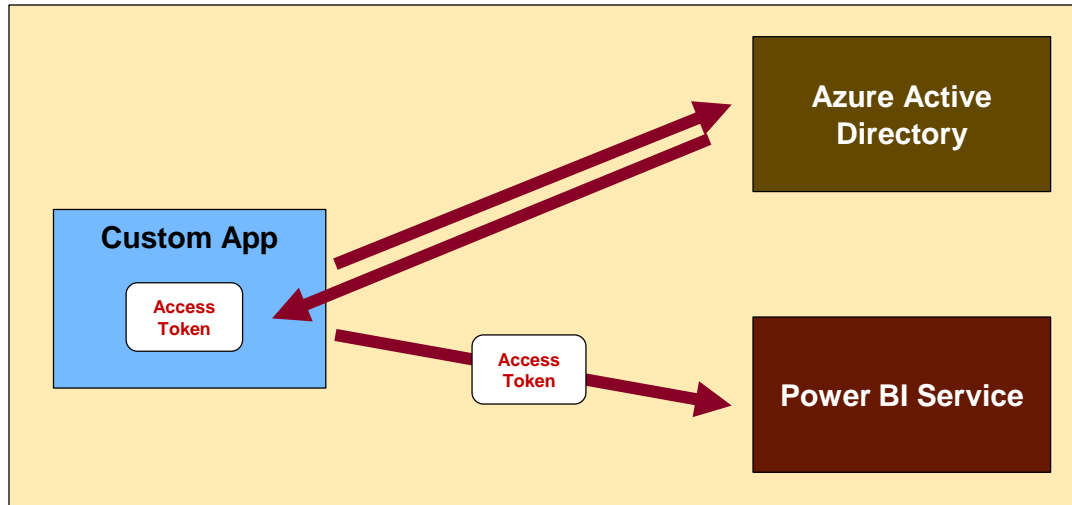
# Azure AD Applications

- Creating applications required for AAU authentication
  - Applications are as Native application or Web Applications
  - Application identified using GUID known as application ID
  - Application ID often referred to as client ID or app ID



# Authenticating with Azure AD

- Custom applications must authenticate with Azure AD
  - Your code implements and authentication flow to obtain access token
  - Access token must be passed when calling Power BI Service API

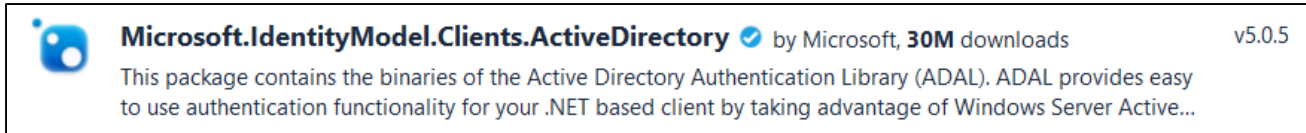


- Microsoft supports two endpoints for programming authentication
  - Azure AD V1 endpoint (released to GA over 8 years ago)
  - Azure AD V2 endpoint (released to GA in May 2019)

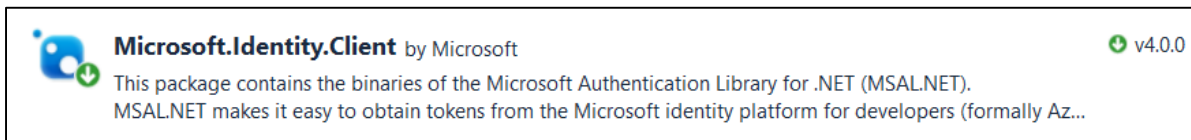


# Azure AD Endpoints and Libraries

- Authenticating with the Azure AD V1 Endpoint
  - Heavily used over the last 5-6 years
  - Accessed through **Azure AD Authentication Library (ADAL)**



- Authenticating with the Azure AD V2 Endpoint
  - Moved from preview to GA in May 2019
  - Accessed through **Microsoft Authentication Library (MSAL)**



- Why move to the Azure AD V2 Endpoint?
  - Dynamic Incremental consent
  - New authentication flows (e.g. device code flow)



# Application Types

- Azure AD Application Types
  - Public client (mobile and desktop)
  - Web

## Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web



*e.g. https://myapp.com/auth*

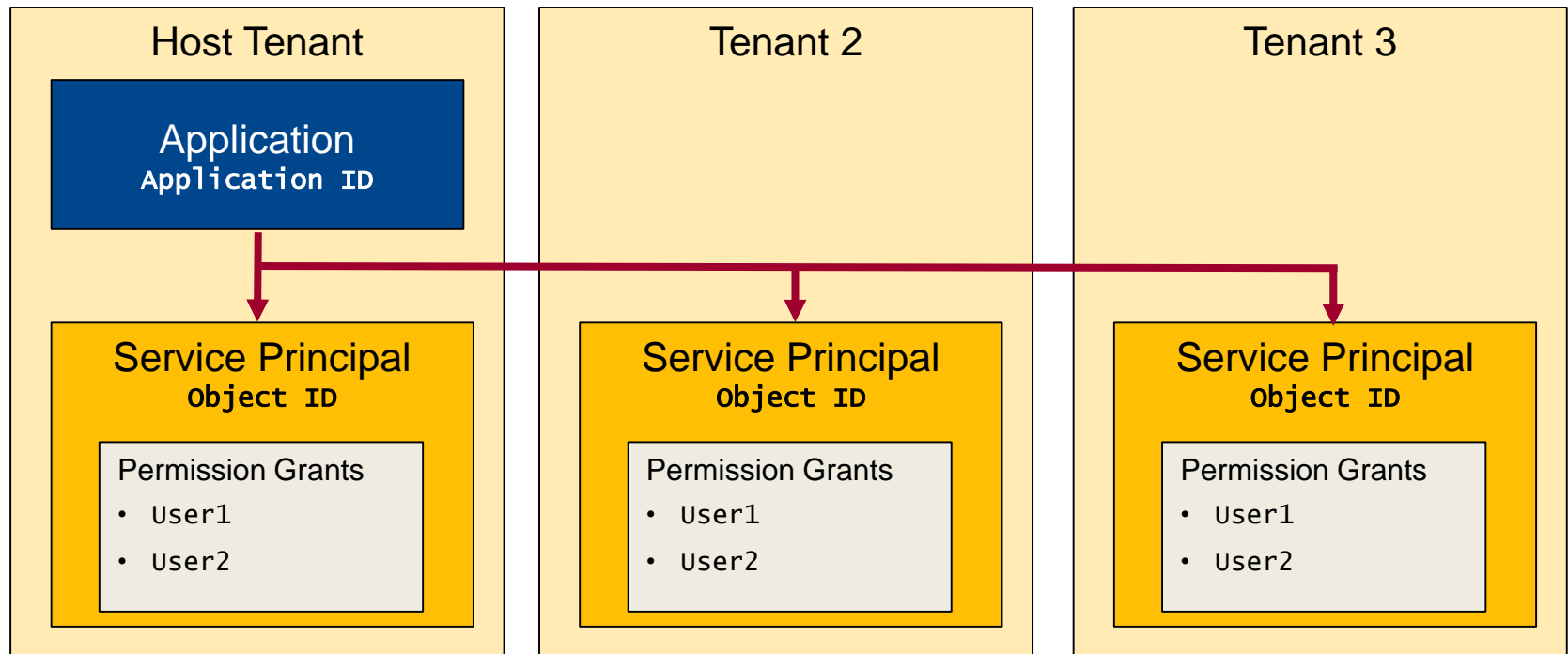
Public client (mobile & desktop)

Web



# Applications and Service Principals

- Azure AD creates service principal(s) for each application
  - Service principle created once per tenant
  - Service principle acts as first-class AAD security principal



# Applications versus Service Principle

- Application defined once across all tenants
  - Identified using global Application ID
  - Application object lives in tenant where it's registered
  - Defines auth type, secrets and required permissions
- Service principal created once per tenant
  - Identified using tenant-specific Object ID
  - Used to track permission grants for user consent





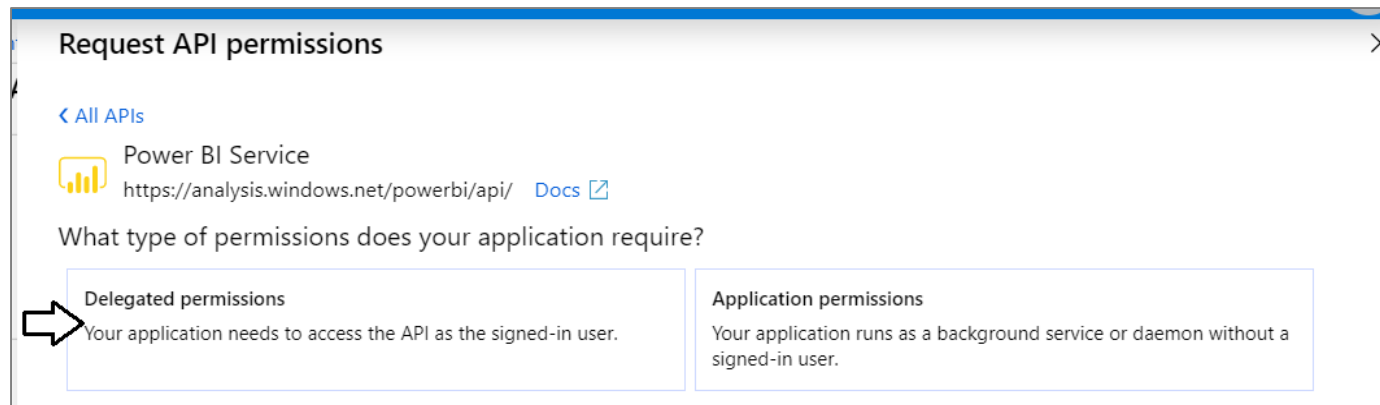
# Identity Topology Options

- Consumer
  - Microsoft personal accounts (Outlook, OneDrive, MSN, or Xbox LIVE)
- Enterprises
  - Organizational accounts defined inside Azure AD tenant
- Business to Business (B2B)
  - Organization accounts added as guest user in other tenants
- Business to Customer (B2C)
  - Provides customer identity access management (CIAM) solution



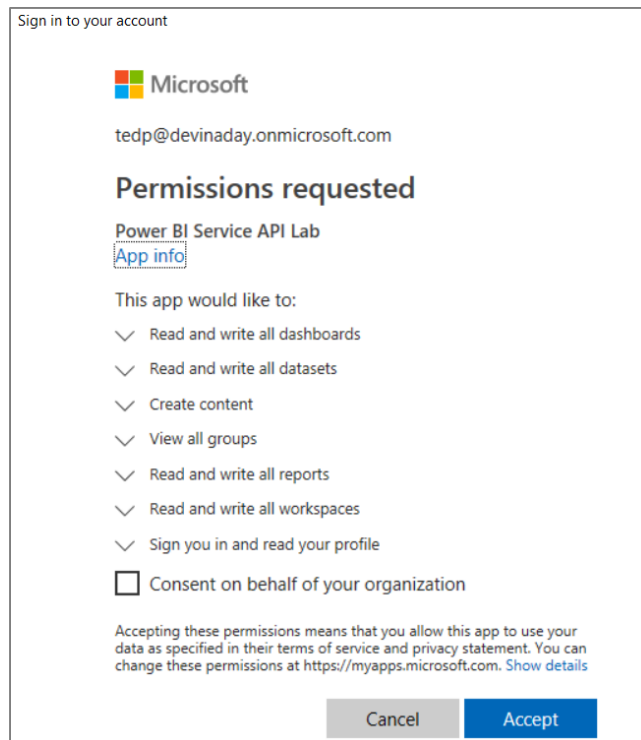
# Delegated Permissions vs Application Permissions

- Permissions categorized into two basic types
  - Delegated permissions are (app + user) permissions
  - Application permissions are app-only permissions (far more powerful)
  - Not all application types and APIs support application permissions
  - Power BI Service API does not support application permission




# Interactive Consent for Delegated Permissions

- Users must consent to delegated permissions
  - User prompted during first log in
  - User must click Accept
  - Only occurs once for each user



Sign in to your account

 Microsoft

tedp@devinaday.onmicrosoft.com

**Permissions requested**

Power BI Service API Lab  
[App info](#)

This app would like to:

- ✓ Read and write all dashboards
- ✓ Read and write all datasets
- ✓ Create content
- ✓ View all groups
- ✓ Read and write all reports
- ✓ Read and write all workspaces
- ✓ Sign you in and read your profile
- ☐ Consent on behalf of your organization

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)



# Creating a Public Client Application

- Power BI supports Public Client Applications
  - Used for native applications and desktop applications
  - Requires Redirect URI for interactive logins

### Register an application

**\* Name**

The user-facing display name for this application (this can be changed later).

➡ Power BI Service API Lab ✓

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

➡ Public client (mobile & desktop) ▼ ➡ https://localhost/app1234 ✓

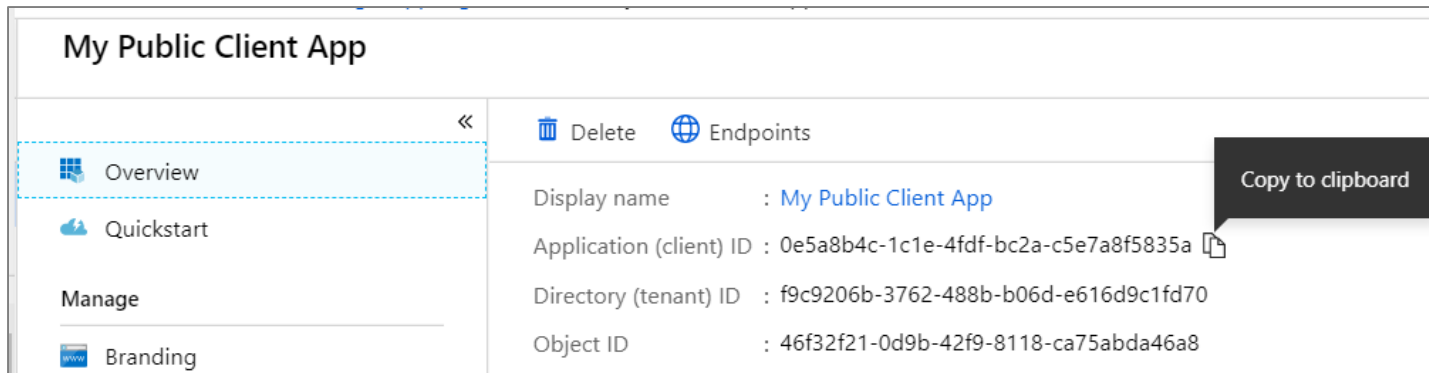
By proceeding, you agree to the [Microsoft Platform Policies](#)

➡ **Register**



# Copying the Application ID

- Each new application created with Application ID
  - You cannot supply your own GUID for application ID
  - Azure AD will always create this GUID
  - You can copy the application ID from the Azure portal



- Don't forget this confusing fact...
  - Application ID == Client ID



# Configuring Required Permissions

- Application configured with permissions
  - Default permissions allows user authentication – but that's it
  - To use APIs, you can assign permissions to the application

Power BI Service API Lab - API permissions

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Microsoft Graph (1)			
User.Read	Delegated	Sign in and read user profile	-

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)



# Choosing an API

- There are lots of APIs to choose from
  - Microsoft Graph, Power BI Service, etc.

Request API permissions


Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

**Microsoft Graph**

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



**Azure Rights Management Services**

Allow validated users to read and write protected content

**Azure Service Management**

Programmatic access to much of the functionality available through the Azure portal

**Dynamics 365 Business Central**

Programmatic access to data and functionality in Dynamics 365 Business Central

**Flow Service**


Embed flow templates and manage flows

**Intune**

Programmatic access to Intune data

**Office 365 Management APIs**

Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

 **Power BI Service**

Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

**SharePoint**

Interact remotely with SharePoint data

**Skype for Business**

Integrate real-time presence, secure messaging, calling, and conference capabilities





# Granting Delegated Permissions

- It can be helpful to Grant Permissions in Azure portal
  - Prevents the need for interactive granting of application by user
  - Might be required when authenticating in non-interactive fashion

### API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

[+ Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED
▼ Power BI Service (3)			
<a href="#">Dashboard.Read.All</a>	Delegated	View all dashboards	-  Granted for Critical Pa
<a href="#">Report.Read.All</a>	Delegated	View all reports	-  Granted for Critical Pa
<a href="#">Tenant.Read.All</a>	Delegated	View all content in tenant	Yes  Granted for Critical Pa

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. [See best practices for requesting permissions](#)

### Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Critical Path Training](#)



# Registering AAD Apps with PowerShell

```
$authResult = Connect-AzureAD

# display name for new public client app
$appDisplayName = "My Power BI Service App"

# get user account ID for logged in user
$user = Get-AzureADUser -ObjectId $authResult.Account.Id

# get tenant name of logged in user
$tenantName = $authResult.TenantDomain

# create Azure AD Application
$replyUrl = "https://localhost/app1234"
$aadApplication = New-AzureADApplication `
    -DisplayName $appDisplayName `
    -PublicClient $true `
    -AvailableToOtherTenants $false `
    -ReplyUrls @($replyUrl)

# create service principal for application
$appId = $aadApplication.AppId
$serviceServicePrincipal = New-AzureADServicePrincipal -AppId $appId

# assign current user as application owner
Add-AzureADApplicationOwner -ObjectId $aadApplication.ObjectId -RefObjectId $user.ObjectId
```



# Configuring Delegated Permissions

```
# create Azure AD Application
$replyUrl = "https://localhost/app1234"
$aadApplication = New-AzureADApplication `
    -DisplayName $appDisplayName `
    -PublicClient $true `
    -AvailableToOtherTenants $false `
    -ReplyUrls @($replyUrl)

# configure delegated permissions for the Power BI Service API
$requiredAccess = New-Object -TypeName "Microsoft.Open.AzureAD.Model.RequiredResourceAccess"
$requiredAccess.ResourceAppId = "00000009-0000-0000-c000-000000000000"

# create first delegated permission - Report.Read.All
$permission1 = New-Object -TypeName "Microsoft.Open.AzureAD.Model.ResourceAccess" `
    -ArgumentList "4ae1bf56-f562-4747-b7bc-2fa0874ed46f", "Scope"

# create second delegated permission - Dashboards.Read.All
$permission2 = New-Object -TypeName "Microsoft.Open.AzureAD.Model.ResourceAccess" `
    -ArgumentList "2448370f-f988-42cd-909c-6528efd67c1a", "Scope"

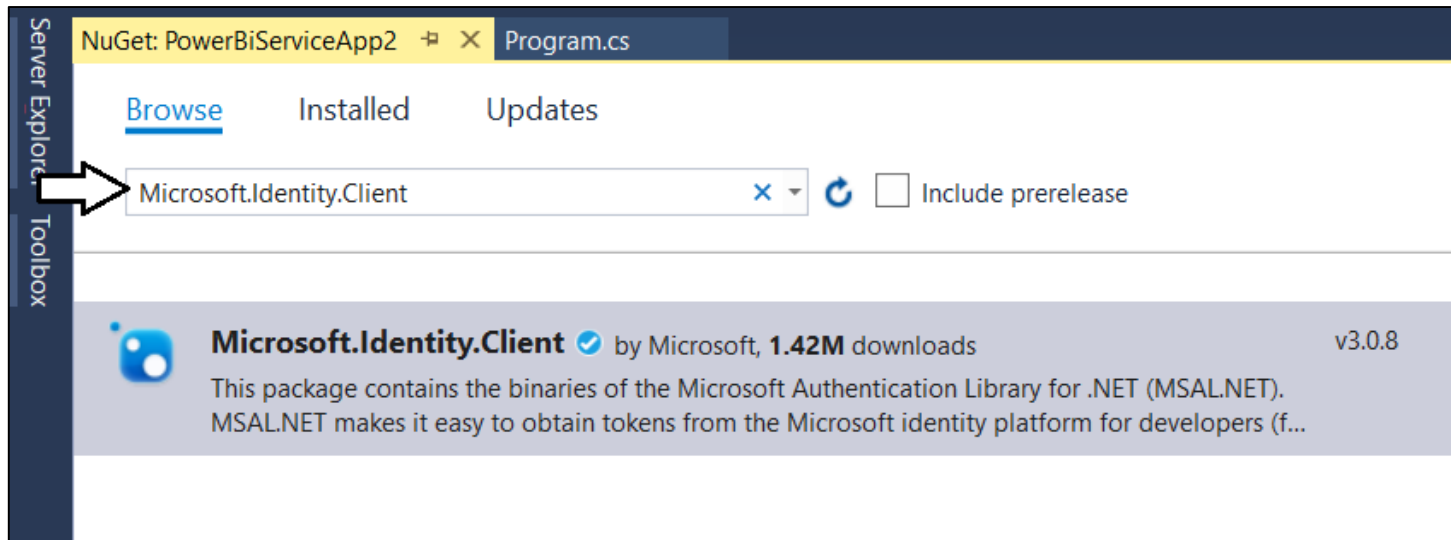
# add permissions to ResourceAccess list
$requiredAccess.ResourceAccess = $permission1, $permission2

# add permissions by updating application with RequiredResourceAccess object
Set-AzureADApplication -ObjectId $aadApplication.ObjectId -RequiredResourceAccess $requiredAccess
```



# Microsoft Authentication Library (.NET)

- Developing with the Microsoft Authentication Library
  - Provides access to Azure AD V2 Endpoint
  - Added to project as `Microsoft.Identity.Client` NuGet package
  - Provides different classes for *public clients* vs *confidential clients*



# Power BI Service API Scopes

- Azure AD V2 endpoint requires passing scopes
  - Scopes define permissions required in access token
  - Scopes defined as **resource** + **permission**

<https://analysis.windows.net/powerbi/api/> + **Report.ReadWrite.All**

```
static string[] scopesDefault = new string[] {  
    "https://analysis.windows.net/powerbi/api/.default"  
};  
  
static string[] scopesReadWorkspaceAssets = new string[] {  
    "https://analysis.windows.net/powerbi/api/Dashboard.Read.All",  
    "https://analysis.windows.net/powerbi/api/Dataset.Read.All",  
    "https://analysis.windows.net/powerbi/api/Report.Read.All"  
};  
  
static string[] scopesReadUserApps = new string[] {  
    "https://analysis.windows.net/powerbi/api/App.Read.All"  
};  
  
static string[] scopesManageWorkspaceAssets = new string[] {  
    "https://analysis.windows.net/powerbi/api/Content.Create",  
    "https://analysis.windows.net/powerbi/api/Dashboard.ReadWrite.All",  
    "https://analysis.windows.net/powerbi/api/Dataset.ReadWrite.All",  
    "https://analysis.windows.net/powerbi/api/Group.Read.All",  
    "https://analysis.windows.net/powerbi/api/Report.ReadWrite.All",  
    "https://analysis.windows.net/powerbi/api/Workspace.ReadWrite.All"  
};
```



# Interactive Access Token Acquisition

## Using MSAL with public client application

- Flow implemented using `PublicClientApplication` object
  - Created using `PublicClientApplicationBuilder` object
  - Requires passing redirect URI
  - You can control prompting behavior

```
static string GetAccessTokenInteractive(string[] scopes) {  
    var appPublic = PublicClientApplicationBuilder.Create(clientId)  
        .WithAuthority(tenantCommonAuthority)  
        .WithRedirectUri(redirectUri)  
        .Build();  
  
    var authResult = appPublic.AcquireTokenInteractive(scopes)  
        .WithPrompt(Prompt.SelectAccount)  
        .ExecuteAsync().Result;  
  
    return authResult.AccessToken;  
}
```



# User Credential Password Flow

## Using MSAL with public client application

- MSAL supports user credential password flow
  - Supported in .NET runtime but not in .NET CORE
  - Microsoft recommends against using this flow

```
static string GetAccessTokenWithUserPassword(string[] scopes) {  
    var appPublic = PublicClientApplicationBuilder.Create(clientId)  
        .WithAuthority(tenantCommonAuthority)  
        .Build();  
  
    string username = "chuckster@devinaday2019.onmicrosoft.com";  
    string userPassword = "myCAT$rightLEG";  
    SecureString userPasswordSecure = new SecureString();  
    foreach (char c in userPassword) {  
        userPasswordSecure.AppendChar(c);  
    }  
  
    var authResult = appPublic.AcquireTokenByUsernamePassword(scopes, username, userPasswordSecure)  
        .ExecuteAsync().Result;  
  
    return authResult.AccessToken;  
}
```





# Device Code Flow

## Using MSAL with public client application

- MSAL introduced this new flow with MSAL
  - Much more secure than user password credential flow
  - Not available in ADAL

```
static string GetAccessTokenWithDeviceCode(string[] scopes) {  
    // device code authentication requires tenant-specific authority URL  
    var appPublic = PublicClientApplicationBuilder.Create(clientId)  
        .WithAuthority(tenantSpecificAuthority)  
        .Build();  
  
    // this method call will block until you have logged in using the generated device code  
    var authResult = appPublic.AcquireTokenWithDeviceCode(scopes, deviceCodeCallbackParams => {  
        // retrieve device code and verification URL from deviceCodeCallbackParams  
        string deviceCode = deviceCodeCallbackParams.UserCode;  
        string verificationUrl = deviceCodeCallbackParams.VerificationUrl;  
  
        Console.WriteLine("When prompted by the browser, copy-and-paste the following device code: " + deviceCode);  
  
        Console.WriteLine("Opening Browser at " + verificationUrl);  
        Process.Start("chrome.exe", verificationUrl);  
  
        Console.WriteLine("This console app will now block until you enter the device code and log in");  
  
        // return task result  
        return Task.FromResult(0);  
    }).ExecuteAsync().Result;  
  
    Console.WriteLine("The call to AcquireTokenWithDeviceCode has completed and returned an access token");  
  
    return authResult.AccessToken;  
}
```

# Client Credentials Flow

## Using MSAL with confidential client application

- Client credentials flow used to obtain app-only token
  - Requires passing app secret (e.g. app password or certificate)
  - Requires passing tenant-specific endpoint

```
const string clientId = "e6a54dc4-7345-495d-b029-88c6349b62d2";
const string clientSecret = "M2MwODBhOTEtOWUyYi00NWQlLWJmMTQzMjMlZTAzMzZjOTMx=";
const string tenantName = "devinaday2019.onmicrosoft.com";

// endpoint for tenant-specific authority
const string tenantSpecificAuthority = "https://login.microsoftonline.com/" + tenantName;

static string GetAppOnlyAccessToken() {

    var appConfidential = ConfidentialClientApplicationBuilder.Create(clientId)
        .WithClientSecret(clientSecret)
        .WithAuthority(tenantSpecificAuthority)
        .Build();

    string[] scopesDefault = new string[] { "https://analysis.windows.net/powerbi/api/.default" };

    var authResult = appConfidential.AcquireTokenForClient(scopesDefault).ExecuteAsync().Result;

    return authResult.AccessToken;
}
```

