Technical Guide

Microsoft 365 Authentication

Release: 2023-04-18

Doc Rev. No: R4

Table of Contents

1 Introduction

This guide will provide basic configurations to quickly set up Microsoft 365 Authentication.

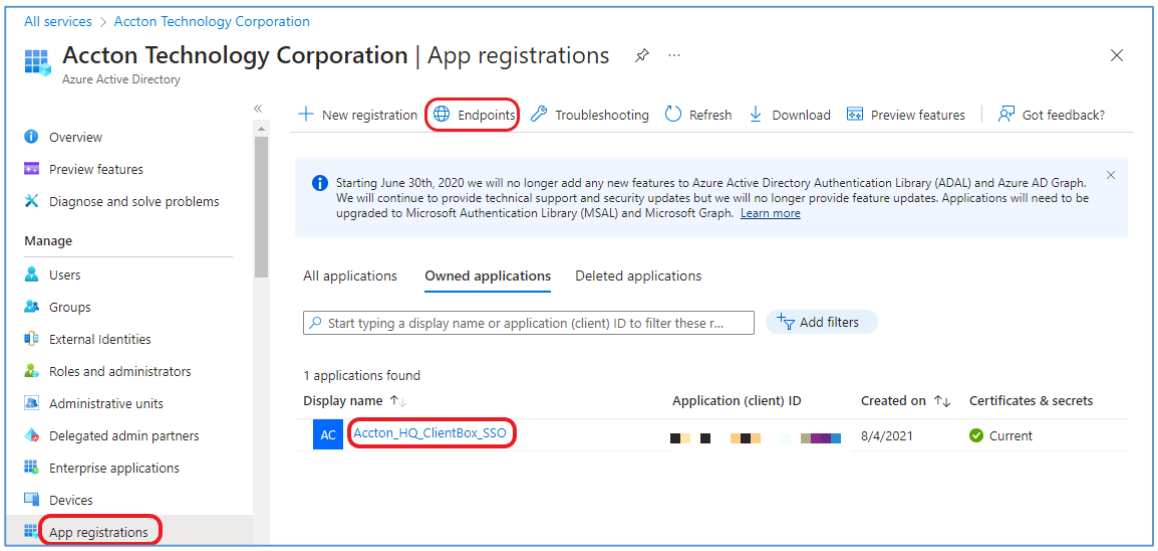
Microsoft 365 Authentication is an authentication mechanism which enables users to login through Microsoft 365 authentication server.

Microsoft 365 Authentication also allows LDAP authorization, which allow MIS to restrict user with different permission to access company network.

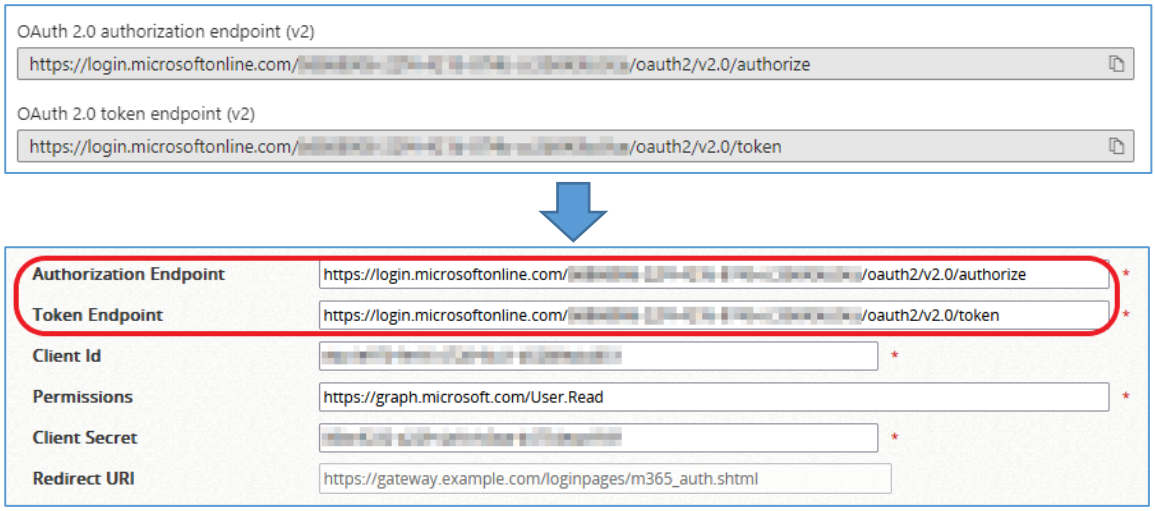
2 Pre-configure on Microsoft 365 Azure

This chapter will guide you in generating values for controller configurations from your existing registration in Microsoft 365 Azure.

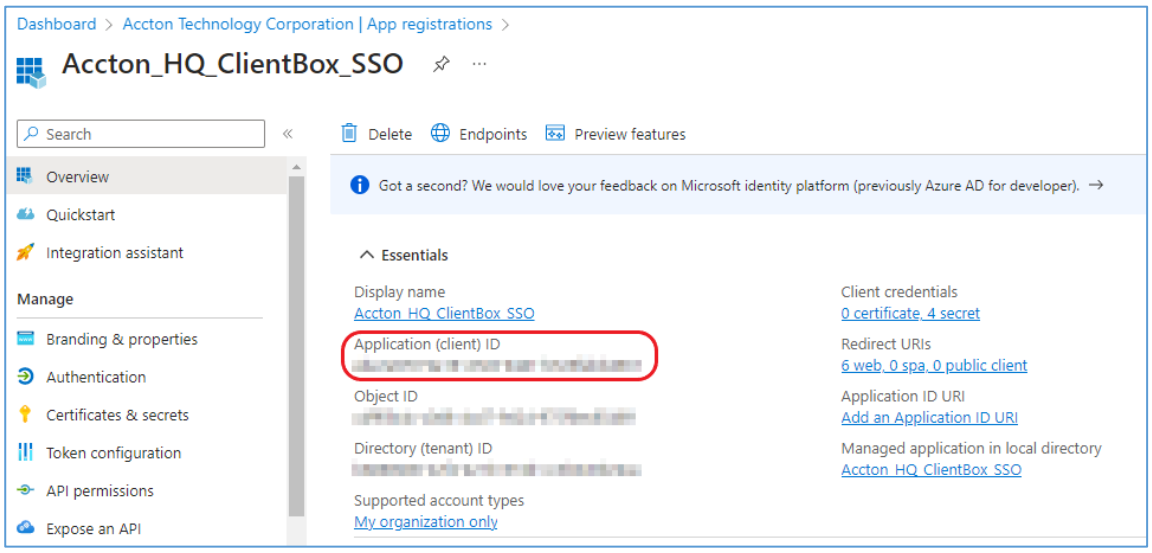
1. Go to *App registrations > the created registration*, click “Endpoints” to generate the parameters for the controller

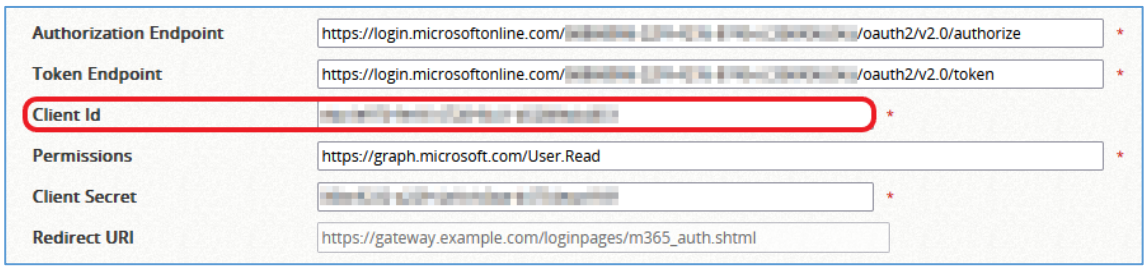


2. Copy the URL address and paste to the controller
   a. OAuth 2.0 authorization endpoint (v2) – Paste the value to Authentication Endpoint (Controller)
      ex. https://login.microsoftonline.com/**<Directory (tenant) ID>**/oauth2/v2.0/authorize
   b. OAuth 2.0 token endpoint (v2) - Paste the value to Token Endpoint (Controller)
      ex. https://login.microsoftonline.com/**<Directory (tenant) ID>**/oauth2/v2.0/token

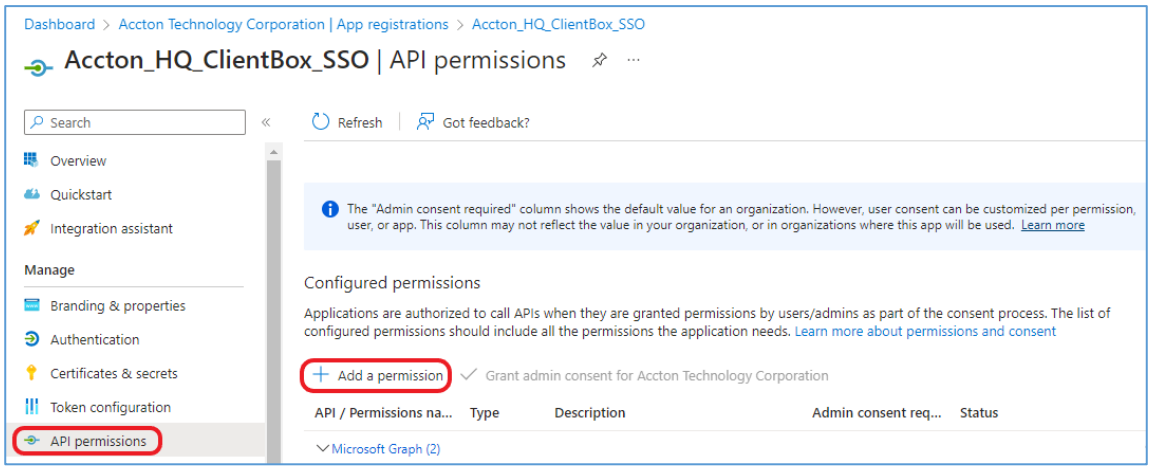


3. Go to *App registrations > the created registration*, Application (client) ID – Paste the value to Client ID (Controller)

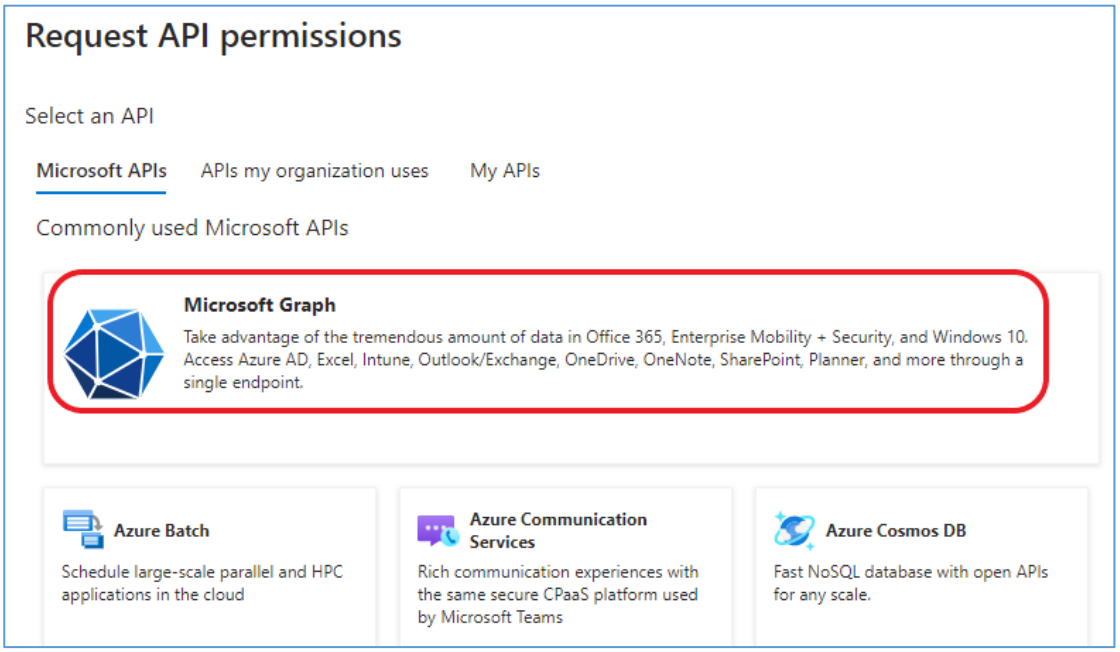




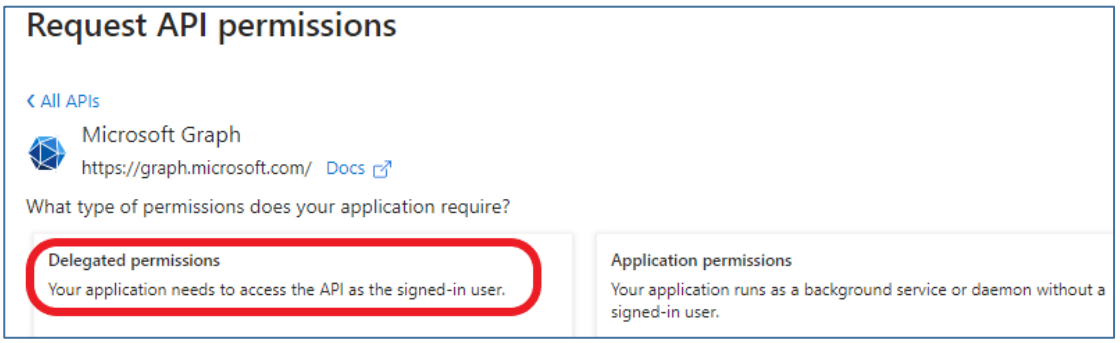
4. Go to *App registrations > the created registration > API permissions*
   a. Click “Add a permission”



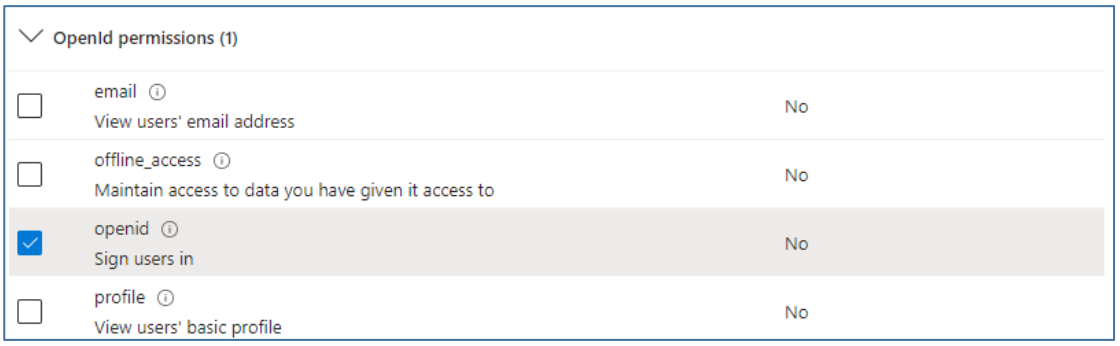
b. Click “Microsoft Graph”

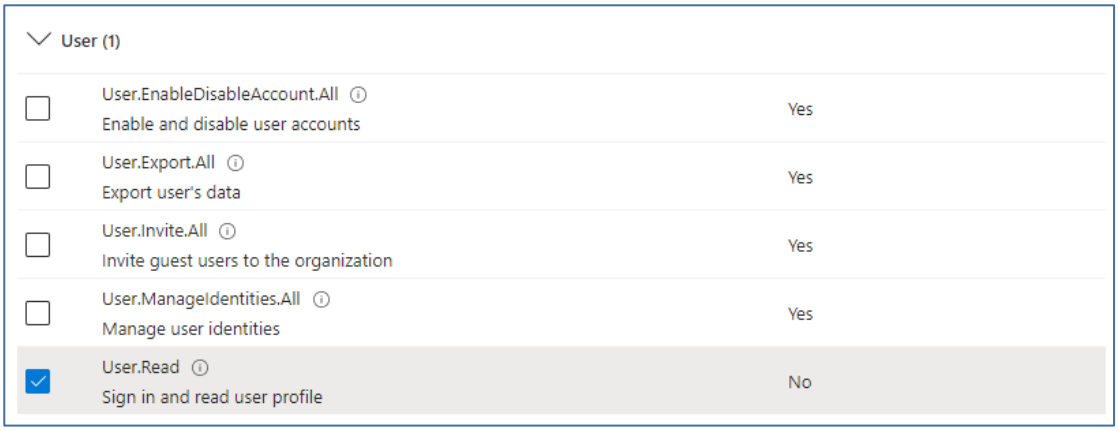


c. Click “Delegated permissions”

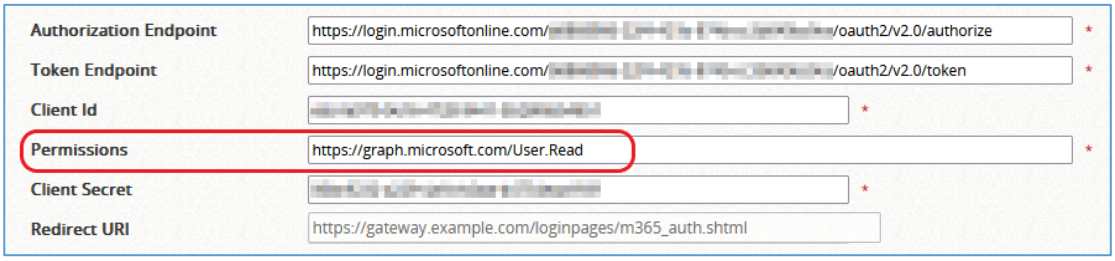


d. Enable “openid” and “User.Read”

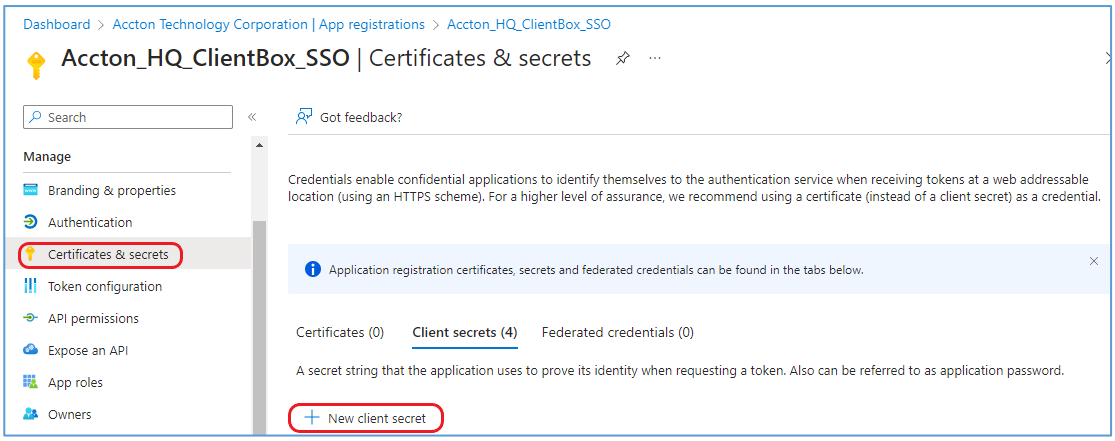




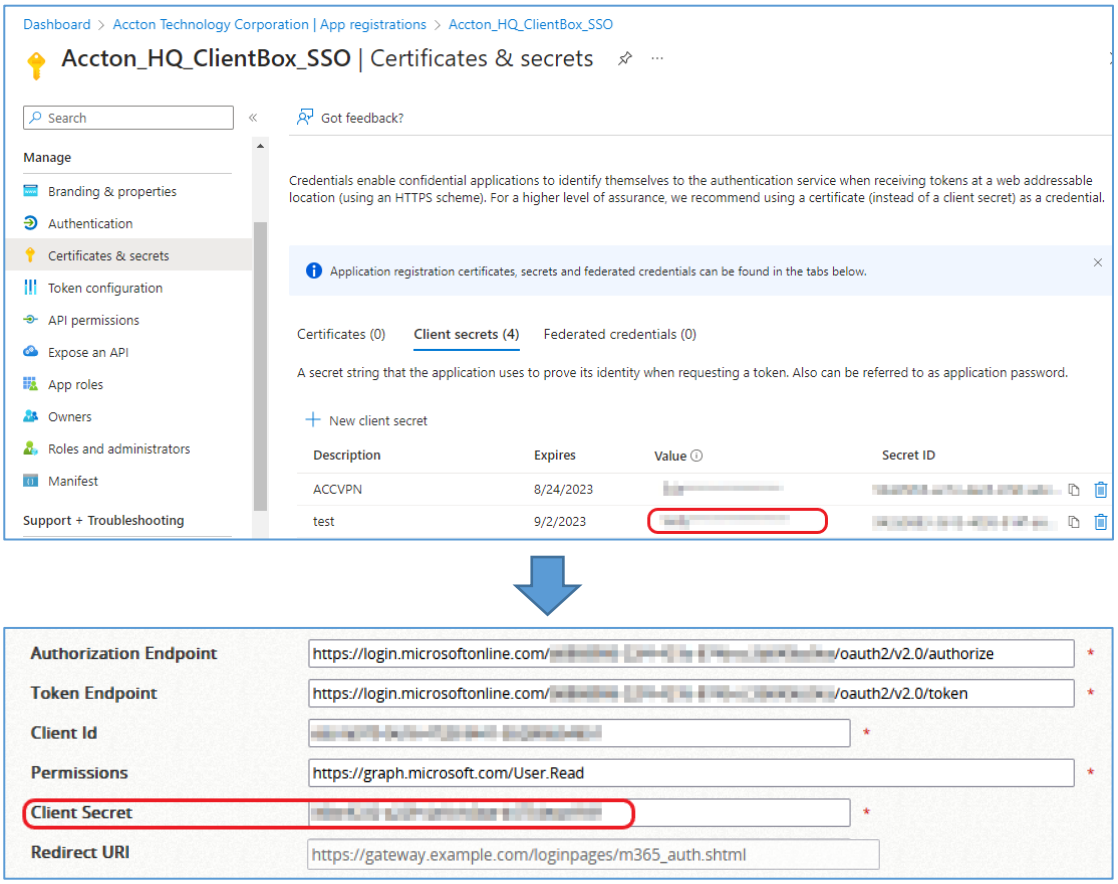
e. Type in “openid https://graph.microsoft.com/User.Read” to the controller



5. Go to *App registrations > the created registration > Certificates & secrets*
   a. Click “New Client secret”

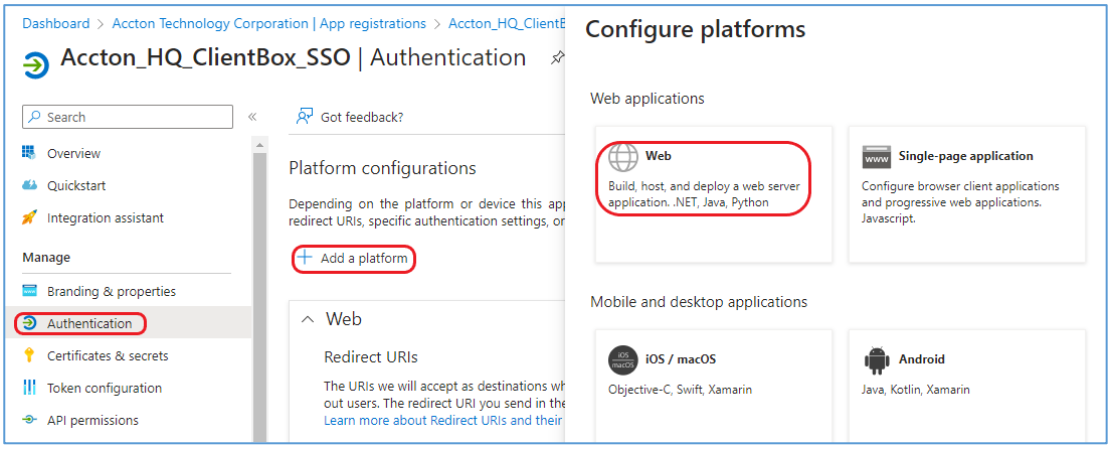


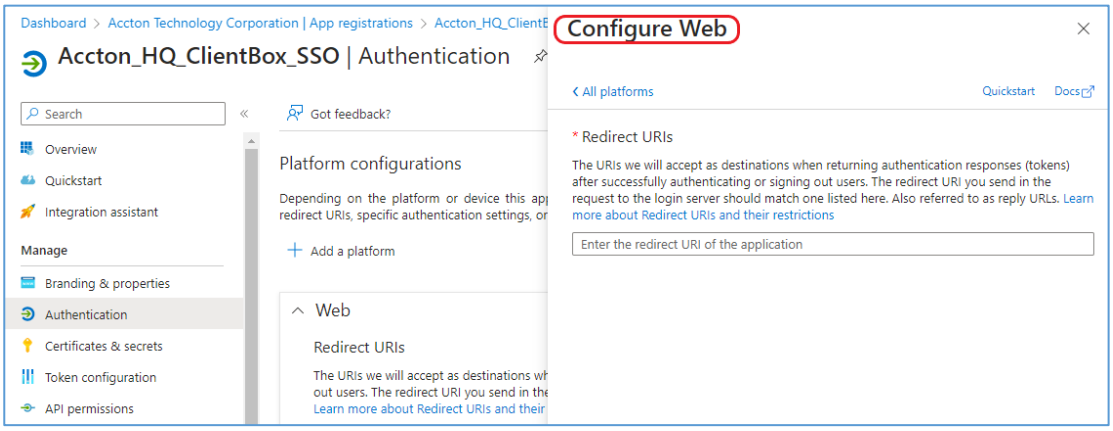
b. Copy the “Value” and paste to the “Client Secret” in the controller



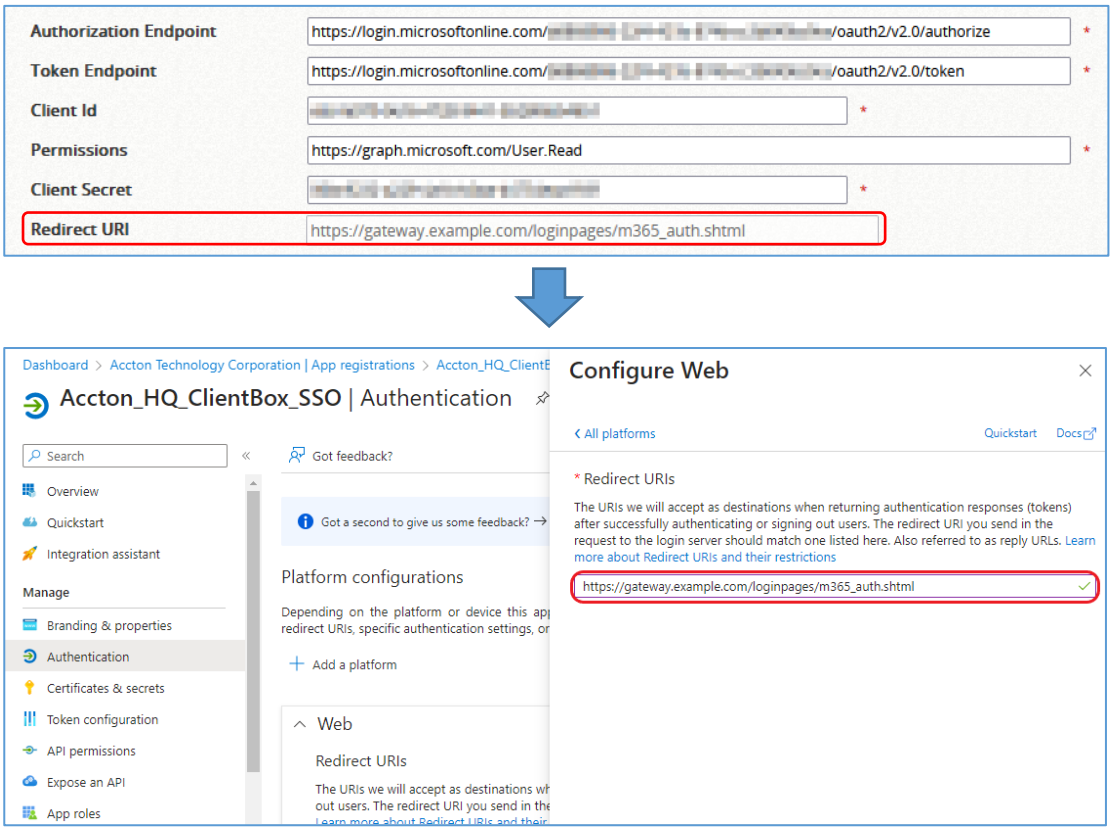
6. Go to *App registrations > the created registration > Authentication*

a. Click “Add a platform” and select “Web” to enter “Configure Web” page





b. Copy the “Redirect URI” from the controller and paste to the “Redirect URIs” in “Configure Web” page



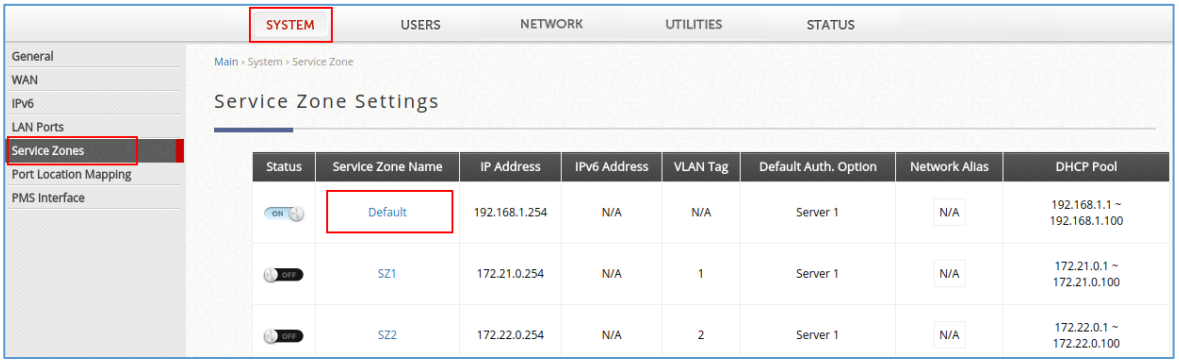
Attention:

1. Email address must fill in the user’s information on Microsoft 365 authentication SSO system, it is critical message during the communication.
2. SSL Login must be enabled on the controller.
3. The two-stage authentication will only happen when the device is logged in for the first time. Unless there are settings in the management system that need to be re-authenticated, the two-stage authentication will not appear on the device after that, because the system will record the logged-in device.

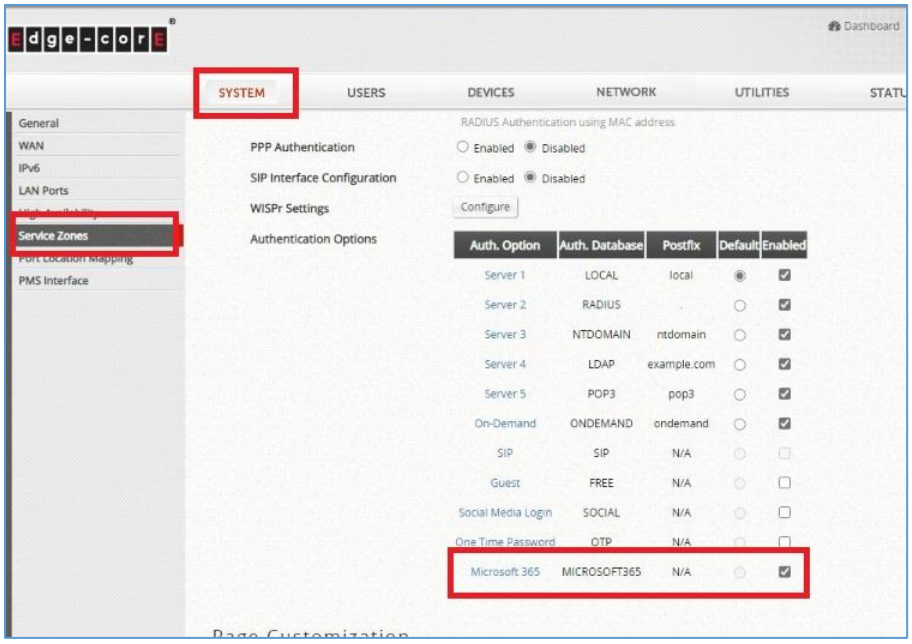
3 Configuration steps on the controller

3.1 Enable Microsoft 365 Authentication Option for the desired Service Zone:

a. Go to *Main Menu > SYSTEM > Service Zones*, in this sample case, “Default” Service Zone is selected:

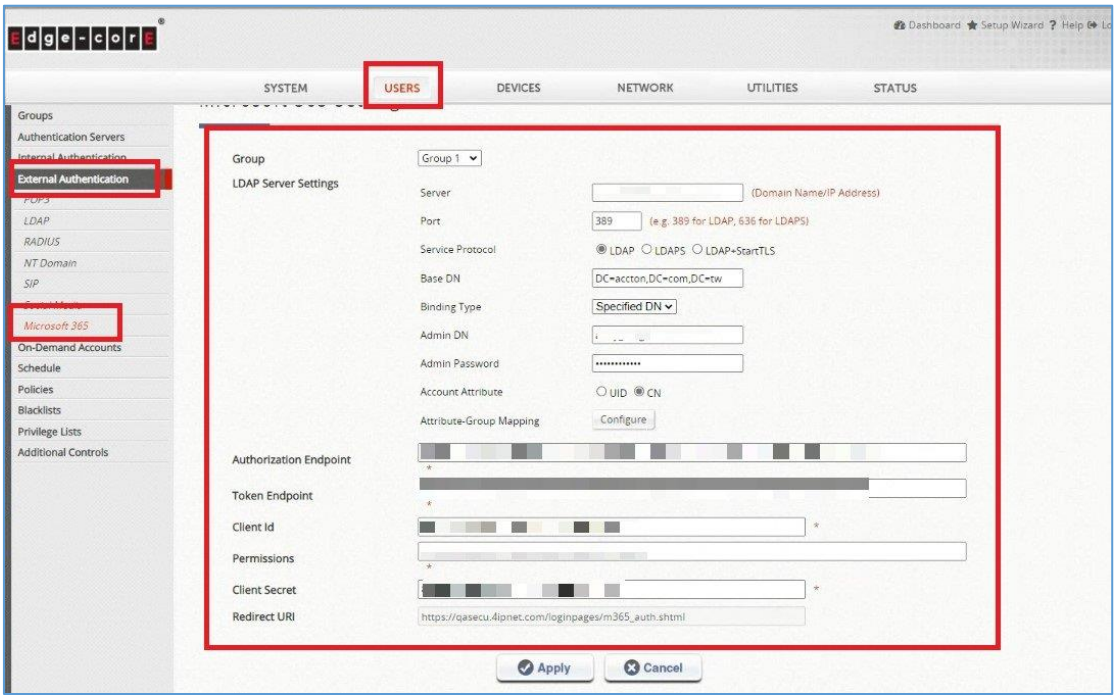


b. Scroll down to Authentication Options of Default Service Zone and ensure the option entry of “Microsoft 365 Authentication” is enabled.



3.2 Configure Microsoft 365 Settings

a. Go to Microsoft 365 Authentication Page: *Main Menu > USERS > External Authentication > Microsoft 365*.



To configure Microsoft 365, select each setting and specify necessary parameters:

LDAP Server Settings: Settings for LDAP Authorization (Optional).
Authorization Endpoint: Set the endpoint for Microsoft 365 authentication server
Token Endpoint: Token for Microsoft 365 authorization
Client Id: Set the Client ID for Microsoft 365 authorization server
Permissions: Permission to Read/Write Microsoft 365 authorization server
Client Secret: Set the Client Secret for Microsoft 365 authorization server

Note:

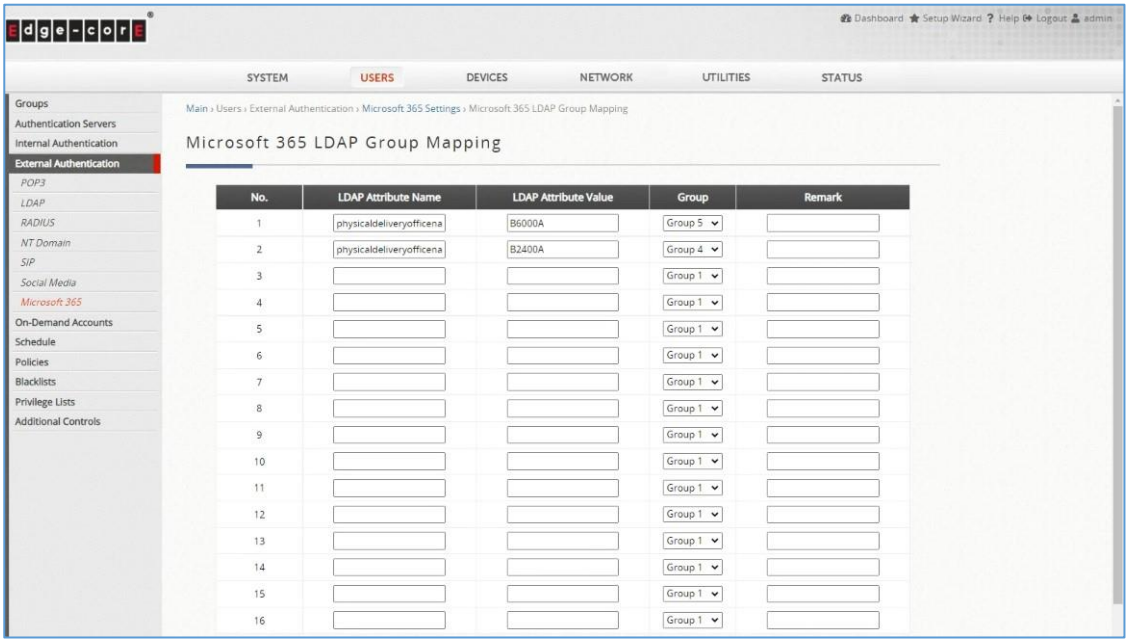
Above parameters are obtain by MIS/Admintrators granting access to

https://portal.azure.com/#view/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/~/RegisteredApps

Check the **Chapter 2: Pre-configure on Microsoft 365 Azure** for more detail configuration

3.3 Configure LDAP Group Mapping (Optional)

a. Configure the LDAP Group Mapping:



To configure LDAP attribute mapping, select each setting and specify necessary parameters:

LDAP Attribute Name: Set the LDAP attribute name.
LDAP Attribute Value: Set the correspond value to match LDAP attribute
Group: Group which mapping to this LDAP attribute value

3 Microsoft 365 Login Flow

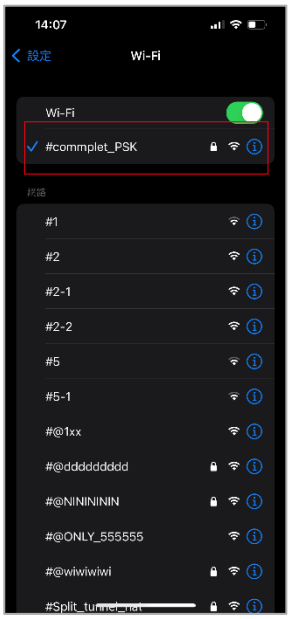
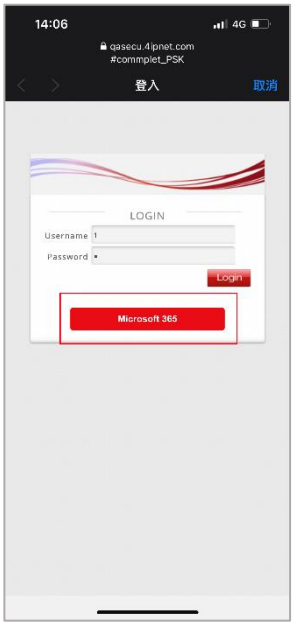


Figure 3.1- Associate to the SSID



3.2- Click 'Microsoft 365' button

3.3 – Login with Microsoft 365 account

Figure 3.4 –Finish Microsoft 365 identification

3.5- Logged In Successfully

4 Remarks

Please contact Technical Support Team for additional inquiries.