



Technical Guide

Microsoft 365 Authentication

Release: 2023-04-18

Doc Rev. No: R4

Copyright Notification

Edgecore Networks Corporation

© Copyright 2023 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

Table of Contents

1	Introduction	2
2	Pre-configure on Microsoft 365 Azure	3
3	Configuration steps on the controller	9
	3.1 Enable Microsoft 365 Authentication Option for the desired Service Zone:.....	9
	3.2 Configure Microsoft 365 Settings	10
	3.3 Configure LDAP Group Mapping (Optional).....	11
3	Microsoft 365 Login Flow.....	12
4	Remarks.....	13

1 Introduction

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

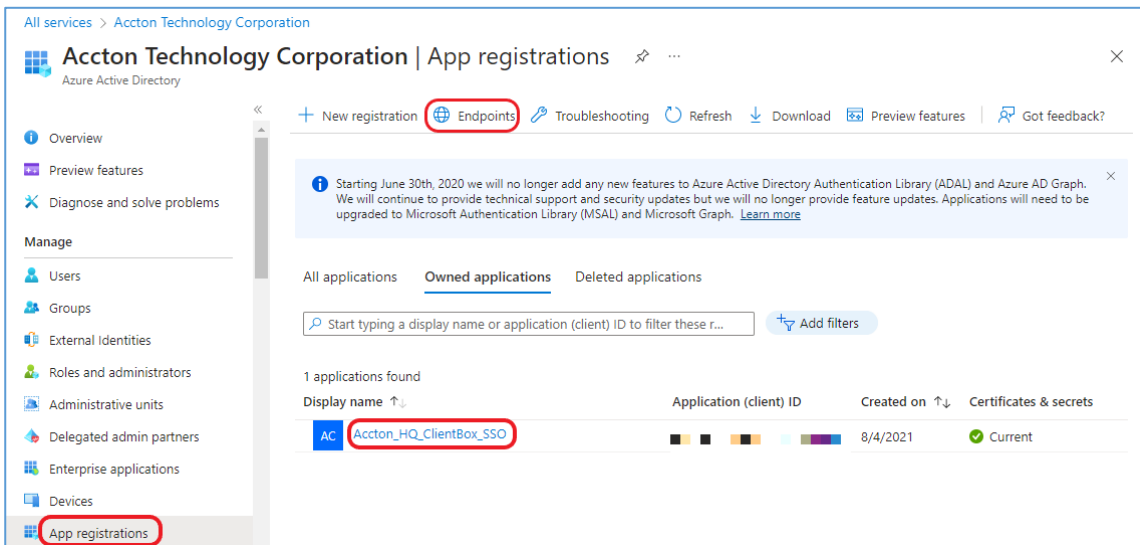
Microsoft 365 Authentication is an authentication mechanism which enables users to login through Microsoft 365 authentication server.

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

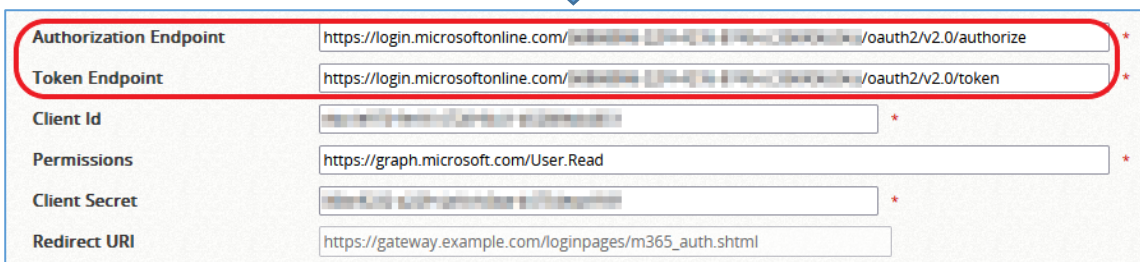
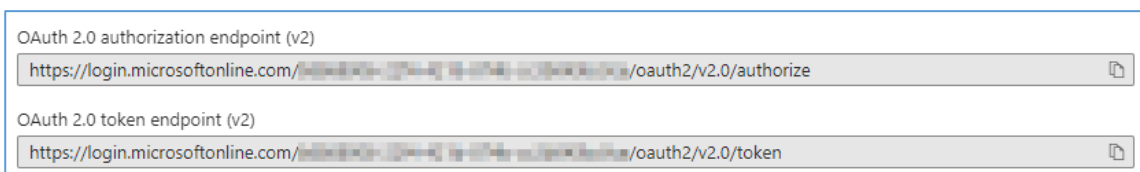
2 Pre-configure on Microsoft 365 Azure

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)

The screenshot shows the 'App registrations' page for 'Accton_HQ_ClientBox_SSO'. The 'Application (client) ID' field is highlighted with a red circle. The page includes a navigation sidebar on the left with options like 'Overview', 'Quickstart', and 'Manage'. The main content area shows various details for the application, including 'Display name', 'Object ID', 'Directory (tenant) ID', and 'Supported account types'.



The screenshot shows the 'API permissions' configuration form. The 'Client Id' field is highlighted with a red circle. The form includes fields for 'Authorization Endpoint', 'Token Endpoint', 'Permissions', 'Client Secret', and 'Redirect URI'. The 'Permissions' field contains the value 'https://graph.microsoft.com/User.Read'.

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

The screenshot shows the 'API permissions' page for 'Accton_HQ_ClientBox_SSO'. The 'Add a permission' button is highlighted with a red circle. The page includes a navigation sidebar on the left with options like 'Overview', 'Quickstart', and 'Manage'. The main content area shows a table of 'Configured permissions' and a 'Microsoft Graph (2)' section.

b. Click “Microsoft Graph”

The screenshot shows the 'Request API permissions' interface. At the top, it says 'Select an API' with three tabs: 'Microsoft APIs' (selected), 'APIs my organization uses', and 'My APIs'. Below this, it lists 'Commonly used Microsoft APIs'. The 'Microsoft Graph' card is highlighted with a red border. It features the Microsoft Graph logo and the text: '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.' Below this are three other API cards: 'Azure Batch', 'Azure Communication Services', and 'Azure Cosmos DB'.

c. Click “Delegated permissions”

The screenshot shows the 'Request API permissions' page for 'Microsoft Graph'. It includes a breadcrumb '< All APIs' and the URL 'https://graph.microsoft.com/ Docs'. The question 'What type of permissions does your application require?' is followed by two options: 'Delegated permissions' (highlighted with a red border) and 'Application permissions'. The 'Delegated permissions' option includes the text: 'Your application needs to access the API as the signed-in user.'

d. Enable “openid” and “User.Read”

The screenshot shows a list of 'OpenId permissions (1)'. The list includes the following items:

Permission	Description	Status
<input type="checkbox"/> email ⓘ	View users' email address	No
<input type="checkbox"/> offline_access ⓘ	Maintain access to data you have given it access to	No
<input checked="" type="checkbox"/> openid ⓘ	Sign users in	No
<input type="checkbox"/> profile ⓘ	View users' basic profile	No

User (1)		
<input type="checkbox"/>	User.EnableDisableAccount.All ⓘ Enable and disable user accounts	Yes
<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	No

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

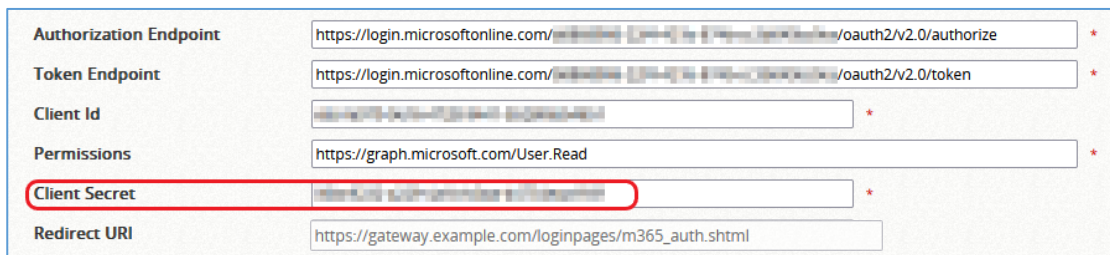
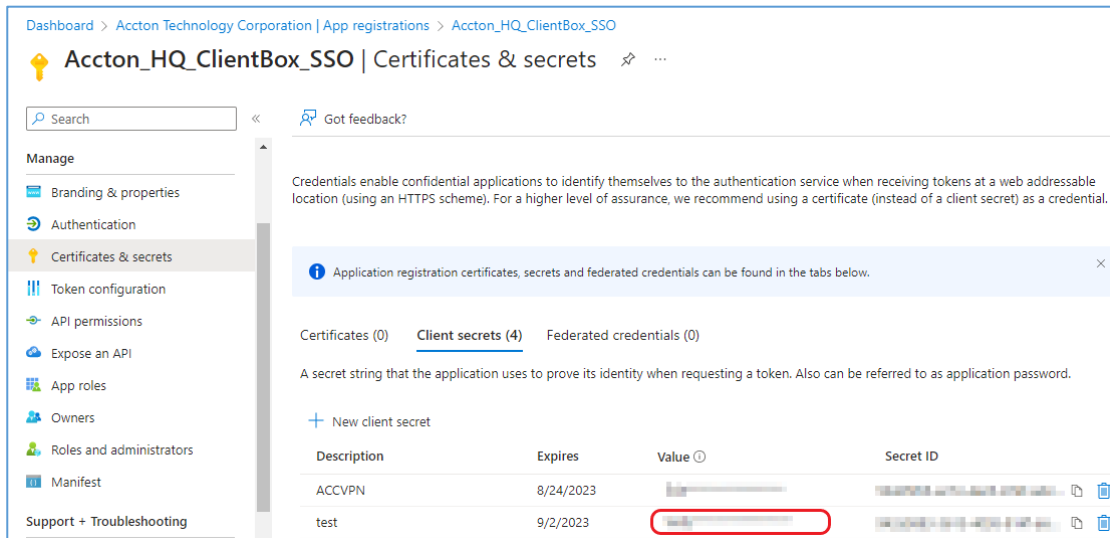
Authorization Endpoint	<input type="text" value="https://login.microsoftonline.com/.../oauth2/v2.0/authorize"/>	*
Token Endpoint	<input type="text" value="https://login.microsoftonline.com/.../oauth2/v2.0/token"/>	*
Client Id	<input type="text" value="..."/>	*
Permissions	<input type="text" value="https://graph.microsoft.com/User.Read"/>	*
Client Secret	<input type="text" value="..."/>	*
Redirect URI	<input type="text" value="https://gateway.example.com/loginpages/m365_auth.shtml"/>	

5. Go to *App registrations > the created registration > Certificates & secrets*

a. Click “New Client secret”

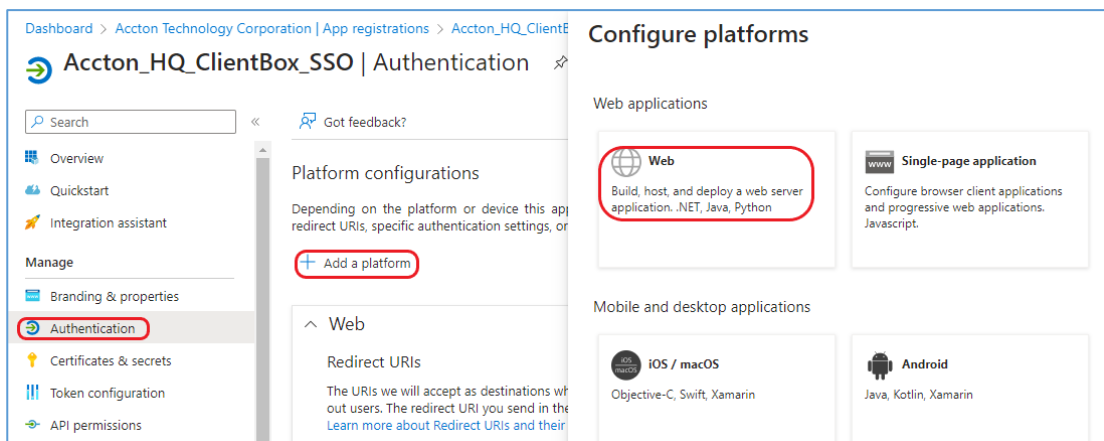
The screenshot shows the Azure AD portal interface for an application registration named 'Accton_HQ_ClientBox_SSO'. The left-hand navigation pane is expanded to 'Certificates & secrets'. The main content area displays a message about credentials and shows that there are 4 client secrets. A '+ New client secret' button is highlighted with a red circle.

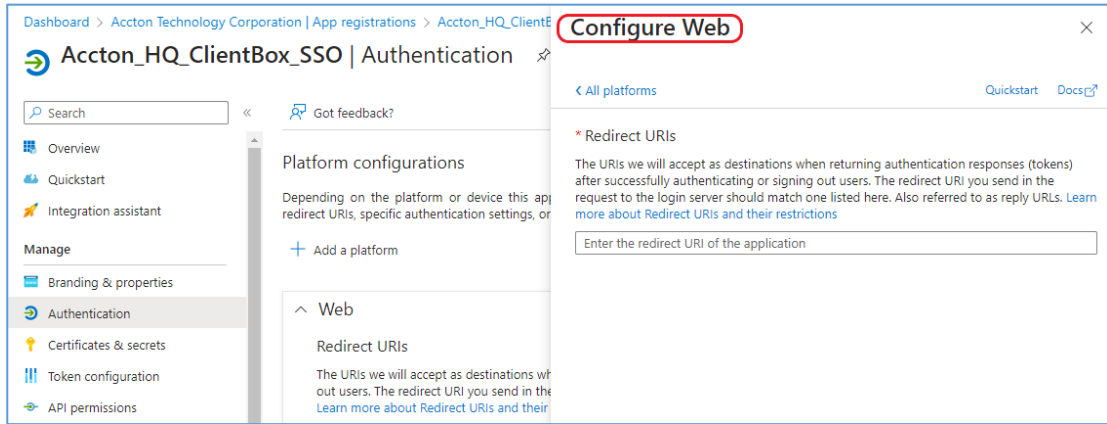
- b. Copy the “Value” and paste to the “Client Secret” in the controller



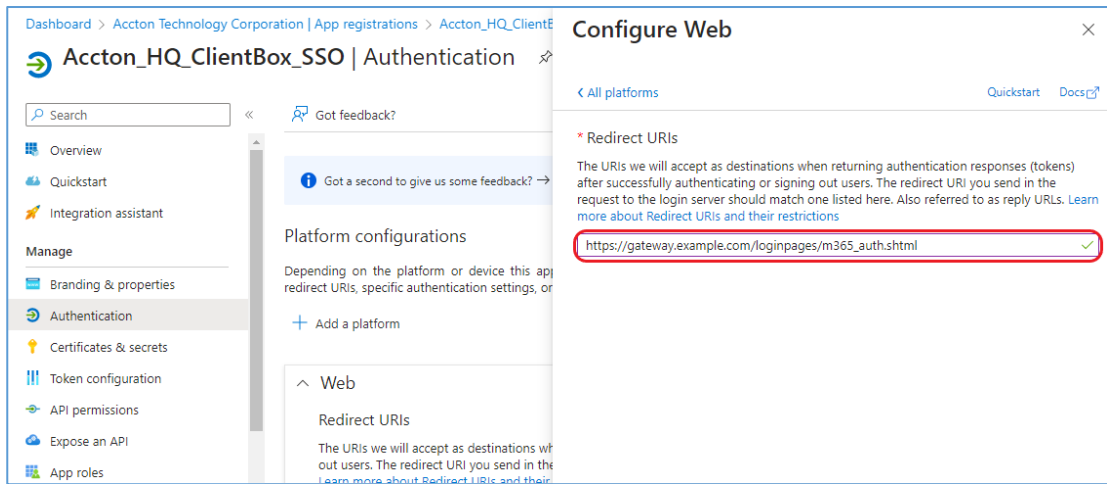
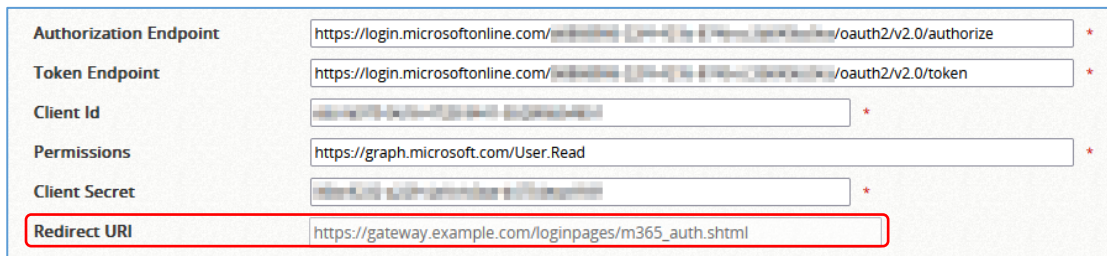
6. Go to *App registrations > the created registration > Authentication*

- 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:

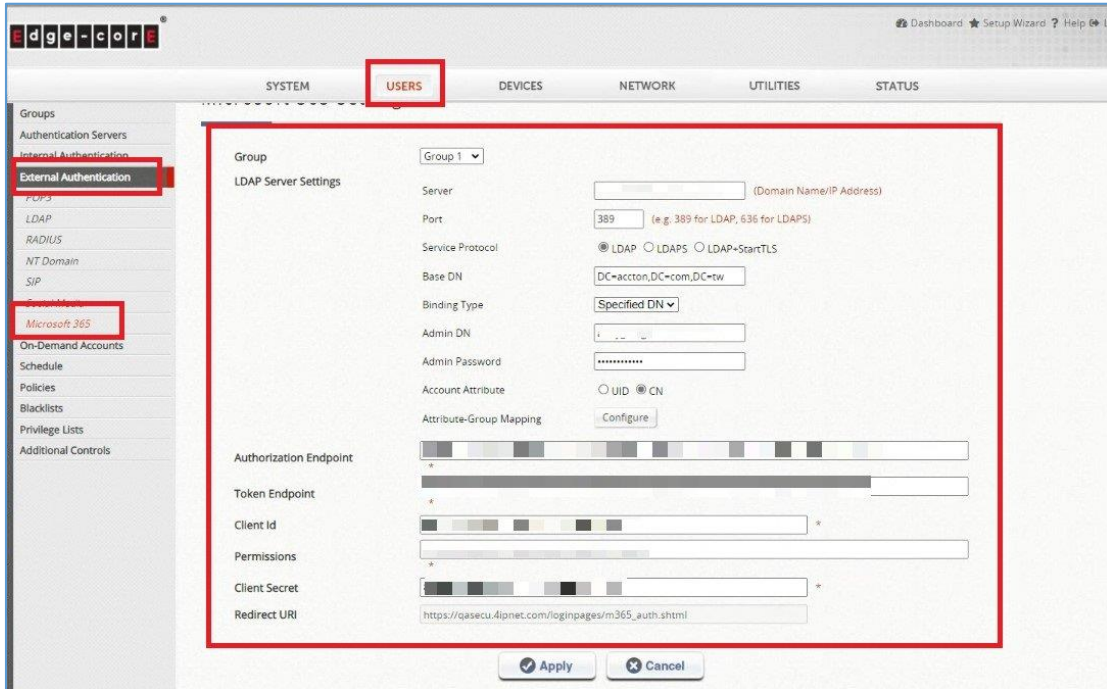
Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
<input checked="" type="checkbox"/>	Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
<input type="checkbox"/>	SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 ~ 172.21.0.100
<input type="checkbox"/>	SZ2	172.22.0.254	N/A	2	Server 1	N/A	172.22.0.1 ~ 172.22.0.100

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

Auth. Option	Auth. Database	Postfix	Default	Enabled
Server 1	LOCAL	local	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
Server 2	RADIUS		<input type="radio"/>	<input checked="" type="checkbox"/>
Server 3	NTDOMAIN	ntdomain	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 4	LDAP	example.com	<input type="radio"/>	<input checked="" type="checkbox"/>
Server 5	POP3	pop3	<input type="radio"/>	<input checked="" type="checkbox"/>
On-Demand	ONDEMAND	ondemand	<input type="radio"/>	<input checked="" type="checkbox"/>
SIP	SIP	N/A	<input type="radio"/>	<input type="checkbox"/>
Guest	FREE	N/A	<input type="radio"/>	<input type="checkbox"/>
Social Media Login	SOCIAL	N/A	<input type="radio"/>	<input type="checkbox"/>
One Time Password	OTP	N/A	<input type="radio"/>	<input type="checkbox"/>
Microsoft 365	MICROSOFT365	N/A	<input type="radio"/>	<input checked="" type="checkbox"/>

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:

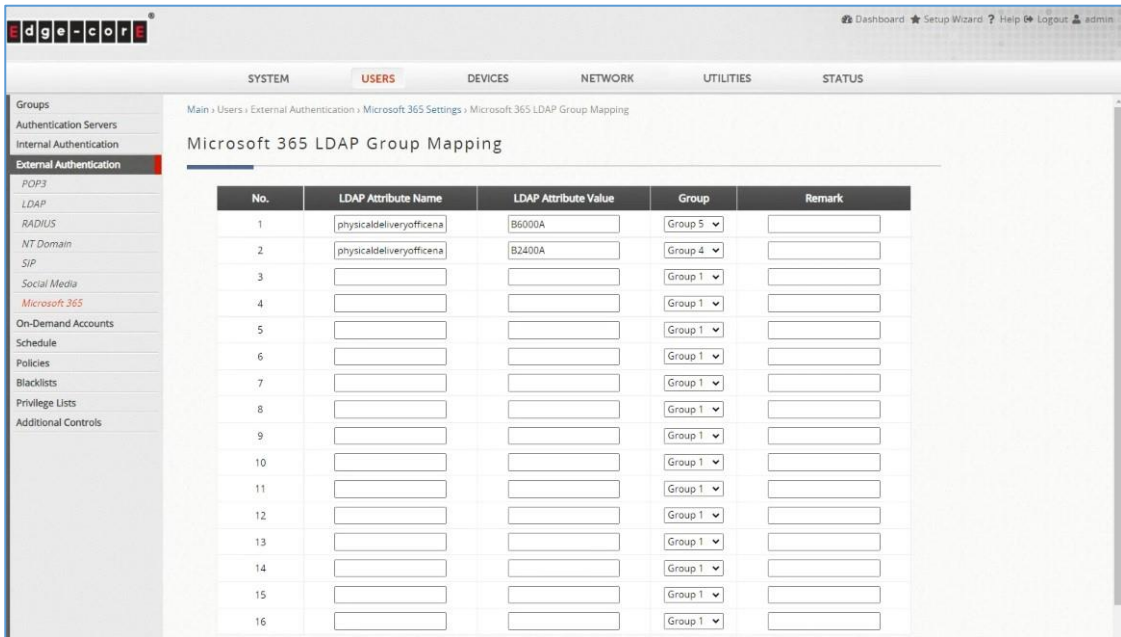
Above parameters are obtain by MIS/Admintrators granting access to

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

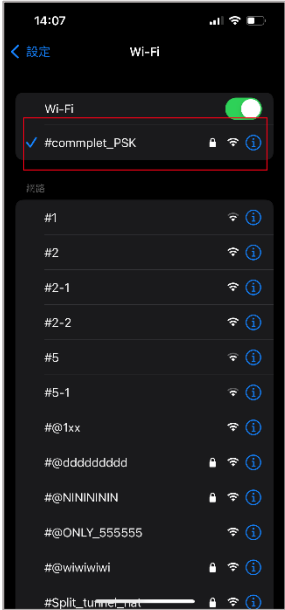
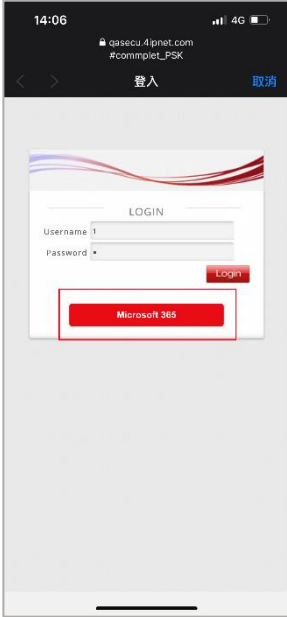


Figure 3.1- Associate to the SSID



3.2- Click 'Microsoft 365' button



3.3 – Login with Microsoft 365 account

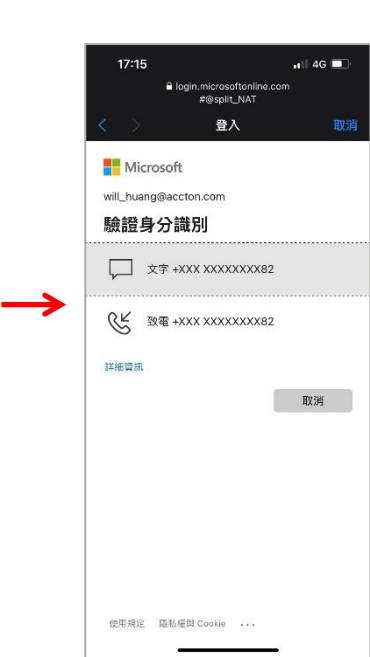


Figure 3.4 –Finish Microsoft 365 identification



3.5- Logged In Successfully

4 Remarks

Please contact Technical Support Team for additional inquiries.