

Technical Guide

Microsoft 365 Authentication

Release: 2023-04-18 Doc Rev. No: R4

Copyright Notification

Edgecore Networks Corporation

 $\ensuremath{\mathbb{C}}$ 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

Intro	duction	2
Pre-c	onfigure on Microsoft 365 Azure	3
Confi	guration steps on the controller	9
3.1	Enable Microsoft 365 Authentication Option for the desired Service Zone:	9
3.2	Configure Microsoft 365 Settings	
3.3	Configure LDAP Group Mapping (Optional)	11
Micro	osoft 365 Login Flow	12
Rema	ırks	13
	Introd Pre-cc Confi 3.1 3.2 3.3 Micro Rema	 Introduction Pre-configure on Microsoft 365 Azure Configuration steps on the controller 3.1 Enable Microsoft 365 Authentication Option for the desired Service Zone: 3.2 Configure Microsoft 365 Settings 3.3 Configure LDAP Group Mapping (Optional) Microsoft 365 Login Flow Remarks

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

All services > Accton Technology Corp	oration
Accton Technology	<pre>r Corporation App registrations</pre>
Overview	+ New registration 🌐 Endpoints 🤌 Troubleshooting 🖒 Refresh 🞍 Download 🐼 Preview features 🛛 🞘 Got feedback?
 Preview features X Diagnose and solve problems 	Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more
Manage	
🚨 Users	All applications Owned applications Deleted applications
🚨 Groups	
External Identities	C Start typing a display name or application (client) ID to filter these r
🎝 Roles and administrators	1 applications found
Administrative units	Display name ↑↓ Application (client) ID Created on ↑↓ Certificates & secrets
🚸 Delegated admin partners	AC Accton_HQ_ClientBox_SSO
Enterprise applications	
Devices	
App registrations	

- 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

OAuth 2.0 authorization endpoin	t (v2)	
https://login.microsoftonline.co	m/ /oauth2/v2.0/authorize	D
OAuth 2.0 token endpoint (v2)		
https://login.microsoftonline.co	m/ //////oauth2/v2.0/token	D
Authorization Endpoint	https://login.microsoftonline.com/	*
Token Endpoint	https://login.microsoftonline.com/	*
Client Id	And the second s	
Permissions	https://graph.microsoft.com/User.Read	*
Client Secret	Histori dihammiantifikaantit	
Redirect URI	https://gateway.example.com/loginpages/m365_auth.shtml	

Microsoft 365 Authentication

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

Dashboard > Accton Technology	Corporation App registrations >	
Accton_HQ_Clie	ntBox_SSO 🖈 …	
₽ Search	« 📋 Delete Endpoints 💀 Preview features	
Overview	Got a second? We would love your feedback on M	licrosoft identity platform (previously Azure AD for developer). $ ightarrow$
🗳 Quickstart	-	
🚀 Integration assistant		
Manage	Display name Accton HQ ClientBox SSO	Client credentials <u>0 certificate, 4 secret</u>
Branding & properties	Application (client) ID	Redirect URIs
Authentication	Object ID	<u>6 web, 0 spa, 0 public client</u> Application ID LIRI
📍 Certificates & secrets	atting one of the Constant	Add an Application ID URI
Token configuration	Directory (tenant) ID	Managed application in local directory
 API permissions 	Supported account types	Accorn no clientos 350
Expose an API	My organization only	
Authorization Endpoint	https://login.microsoftonline.com/	• • • • /oauth2/v2.0/authorize
Token Endpoint	https://login.microsoftonline.com/	/oauth2/v2.0/token
Client Id	ALCONF. CONTRACTOR AND ALCONF.	*
Permissions	https://graph.microsoft.com/User.Read	
Client Secret	Next 20 compared to the second	*
Redirect URI	https://gateway.example.com/loginpages/m365_au	uth shtml

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



Technical Guide

Microsoft 365 Authentication

b. Click "Microsoft Graph"

Request API permission	15	
Select an API		
Microsoft APIs APIs my organization	n uses My APIs	
Commonly used Microsoft APIs		
Microsoft Graph Take advantage of the tree Access Azure AD, Excel, In single endpoint.	nendous amount of data in Office 365, Enterpris tune, Outlook/Exchange, OneDrive, OneNote, Sh	e Mobility + Security, and Windows 10. arePoint, Planner, and more through a
Azure Batch Schedule large-scale parallel and HPC applications in the cloud	Rich communication experiences with the same secure CPaaS platform used by Microsoft Teams	Azure Cosmos DB Fast NoSQL database with open APIs for any scale.

c. Click "Delegated permissions"



d. Enable "openid" and "User.Read"

∨ Оре	✓ OpenId permissions (1)				
	email 🛈 View users' email address	No			
	offline_access ① Maintain access to data you have given it access to	No			
	openid 🕕 Sign users in	No			
	profile ① View users' basic profile	No			

Technical Guide

Microsoft 365 Authentication

∨ Us	∨ User (1)				
	User.EnableDisableAccount.All ① Enable and disable user accounts	Yes			
	User.Export.All ① Export user's data	Yes			
	User.Invite.All ① Invite guest users to the organization	Yes			
	User.Manageldentities.All 🕕 Manage user identities	Yes			
<u>~</u>	User.Read 🛈 Sign in and read user profile	No			

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

Authorization Endpoint	https://login.microsoftonline.com/	/oauth2/v2.0/authorize	*	
Token Endpoint	https://login.microsoftonline.com/			
Client Id	and the second second second second	*		
Permissions	https://graph.microsoft.com/User.Read		*	
Client Secret	Ne-Crit CD-printer Efforcement	*		
Redirect URI	https://gateway.example.com/loginpages/m365_auth.shtm	1		

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

a. Click "New Client secret"

Dashboard > Accton Technolo	ogy Corpor	ation App registrations > Accton_HQ_ClientBox_SSO	
Accton_HQ_CI	lientBo	x_SSO Certificates & secrets 👒 …	>
₽ Search	«	A Got feedback?	
Manage	*		
Branding & properties		Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressabl location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a creden	ie tial.
Authentication	- 11		
Certificates & secrets		Anniiration renistration certificates secrets and federated credentials can be found in the tabs below	×
Token configuration			
API permissions		Certificates (0) Client secrets (4) Eederated credentials (0)	
🔷 Expose an API			
App roles		A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.	
🎎 Owners		+ New client secret	

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

P Search «	Got feedback?					
lanage	A					
Branding & properties	Credentials enable confidential a location (using an HTTPS schem	applications to identify the	emselves to the authenticatio surance, we recommend usin	n service when receiving tokens at a web addressa q a certificate (instead of a client secret) as a cred		
Authentication		, <u>,</u>	,	<u> </u>		
Certificates & secrets			and an electricity and the forward in t	ale a de la classe		
Token configuration	Application registration cer	tificates, secrets and federat	ted credentials can be found in t	the tabs below.		
API permissions	Certificates (0) Client ser	rets (4) Federated o	edentials (0)			
Expose an API			edentiais (0)			
App roles	A secret string that the applica	tion uses to prove its iden	tity when requesting a token	. Also can be referred to as application password.		
Owners	+ New client secret					
Roles and administrators	Description	Expires	Value ①	Secret ID		
Manifest	ACCVPN	8/24/2023	10			
upport + Troubleshooting	test	9/2/2023		000000-000-000-000-00		
Authorization Endpoint	https://login.microsoftc	online.com/	De-Co-Decision	/oauth2/v2.0/authorize		
Token Endpoint	https://login.microsoftc	online.com/	(Property and the second	/oauth2/v2.0/token		
Client Id		• • • •				
	https://graph.microsoft.com/User.Read					
Permissions	https://graph.microsoft	ceon ober need				

- 6. Go to App registrations > the created registration > Authentication
 - a. Click "Add a platform" and select "Web" to enter "Configure Web" page



Microsoft 365 Authentication

Dashboard > Accton Technology Corporation | App registrations > Accton_HQ_ClientE \times Accton_HQ_ClientBox_SSO | Authentication Accton_HQ_ClientBox_SSO | Authentication < All platforms Quickstart Docs ₽ Search 📯 Got feedback? * Redirect URIs Overview Platform configurations The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions Quickstart Depending on the platform or device this appredirect URIs, specific authentication settings, or 💉 Integration assistant Enter the redirect URI of the application + Add a platform Manage Branding & properties ∧ Web Authentication Redirect URIs 📍 Certificates & secrets The URIs we will accept as destinations whout users. The redirect URI you send in the Learn more about Redirect URIs and their Token configuration API permissions

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

Authorization Endpoint	https://login.microsoftonline.com/	/0.	auth2/v2.0/authorize *			
Token Endpoint	https://login.microsoftonline.com/	https://login.microsoftonline.com/				
Client Id	101070-001-001-0000	Here and a second s	*			
Permissions	https://graph.microsoft.com/User.R	ead	*			
Client Secret	Re-Citi dit-primiter efficie		*			
Redirect URI	https://gateway.example.com/log	inpages/m365_auth.shtml				
Dashboard > Accton Technology Corpor	ation App registrations > Accton_HQ_ClientE	Configure Web	×			
Accton_HQ_ClientBo	x_SSO Authentication ☆					
	🖗 Got feedback?	< All platforms * Redirect LIRIs	Quickstart Docs㎡			
 Overview Quickstart 	(i) Got a second to give us some feedback? $ ightarrow$	The URIs we will accept as destinations when retu after successfully authenticating or signing out us request to the locin carrier should match and lists	irring authentication responses (tokens) sers. The redirect URI you send in the			
💉 Integration assistant	Platform configurations	more about Redirect URIs and their restrictions https://gateway.example.com/loginpages/m365	auth.shtml			
Branding & properties	Depending on the platform or device this appredirect URIs, specific authentication settings, or					
Authentication	+ Add a platform					
📍 Certificates & secrets						
Token configuration	∧ Web					
API permissions	Redirect URIs					
 Expose an API App roles 	The URIs we will accept as destinations we out users. The redirect URI you send in the Learn more about Redirect URIs and their					

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:

		SYSTEM	USERS	NETWO	ORK	UTILITIES	STATUS		
neral Main > System > Service Zone									
Service Zone Settings									
e Zones		Status	Service Zone Name	IP Address	IPv6 Address	VLAN Tag	Default Auth. Option	Network Alias	DHCP Pool
nterface			Default	192.168.1.254	N/A	N/A	Server 1	N/A	192.168.1.1 ~ 192.168.1.100
		G OFF	SZ1	172.21.0.254	N/A	1	Server 1	N/A	172.21.0.1 ~ 172.21.0.100
		OFF	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.

d g e - c o r 崖								To Dashboard
	SYSTEM	USERS	DEVICES	NETWO	RK	UTIL	ITIES	STA
ieneral			RADIUS Authenticat	tion using MAC at	ddress			
/AN	PPP Auth	nentication	🔿 Enabled 🔘 Dis	abled				
∿6	SIP Inter	face Configuration	🔿 Enabled 🔘 Dis	abled				
AN Ports	WISPr Se	ttings	Configure					
ervice Zones	Authenti	cation Options	Auth. Option	Auth. Database	Postfix	Default	Enabled	
Port cocation Mapping	- 10 A		Server 1	LOCAL	local	۲	2	
MS Interface			Server 2	RADIUS		0		
			Server 3	NTDOMAIN	ntdomain	0		
			Server 4	LDAP	example.com	0		
			Server 5	POP3	рорз	0		
			On-Demand	ONDEMAND	ondemand	0		
			SIP	SIP	N/A			
			Guest	FREE	N/A		0	
			Social Media Login	SOCIAL	N/A		0	
			One Time Password	OTP	N/A	0	0	
			Microsoft 365	MICROSOFT365	N/A		2	

3.2 Configure Microsoft 365 Settings

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

SYSTEM	USERS DEVICES	NETWORK	UTILITIES	STATUS
s				
Group	Group 1 🗸			
LDAP Server Settings	Server		(Domain Name/IP Addre	ss)
	Port	389 (e.g. 389 for LDA	P, 636 for LDAPS)	
	Constan Deserved			
	Service motocon	CLUAP OLDAPS OLDAP	-+startitus	
	Base DN	DC=accton,DC=com,DC=tw		
	Binding Type	Specified DN 🗸		
	Admin DN	·		
	Admin Password			
		0.00	_	
	Account Attribute	UID @ CN		
	Attribute-Group Mapping	Configure		
Authorization Endpoint				
, and a second point	*			
Token Endpoint		and the second second	and the shares	
Client Id			*	
Dermissions				
Permissions	*			
Client Secret			*	
Redirect URI	https://gasecu.4ipnet.com/log	tinpages/m365 auth.shtml		

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)

Edge-corE	0					🍰 Dashboard 🚖 Seti	ip Wizard ? Help 🕪 Logout 👗 admin
	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Groups Authentication Servers Internal Authentication External Authentication	Main > Users > External Authe	entication) Microsoft 365 Setting	pping)AP Group Mapping			
POP3	No.	LDAP Attribute Name	LDAP	Attribute Value	Group	Remark	
RADIUS	1	physicaldeliveryofficena	B6000A		Group 5 🖌		
NT Domain	2	physicaldeliveryofficena	B2400A	A	Group 4 🖌		
Social Media	3		-		Group 1 👻		
Microsoft 365	4				Group 1 👻		
On-Demand Accounts	5				Group 1 🗸		
Policies	6		[Group 1 👻		
Blacklists	7		-		Group 1 🗸		
Privilege Lists Additional Controls	8		[Group 1 🖌		
	9				Group 1 👻		
	10				Group 1 👻		
	11				Group 1 🖌		
	12				Group 1 🖌		
	13		[Group 1 🖌		
	14				Group 1 🖌		
	15		[Group 1 🖌		
	16]	Group 1 👻		

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 attributeGroup: Group which mapping to this LDAP attribute value

3 Microsoft 365 Login Flow

14:07		at	∻ ∎
く 設定	Wi-Fi		
			_
Wi-Fi			
🗸 #commple	et_PSK	٩	∻ (j)
抗路			
#1			∻ (j)
#2			∻ (j)
#2-1			∻ (j)
#2-2			∻ (j)
#5			₹ (j)
#5-1			₹ (j)
#@1xx			∻ (j)
#@ddddd	dddd	۵	∻ (j)
#@NININI	NIN	۵	∻ (j)
#@ONLY_	555555		∻ (j)
#@wiwiwi	wi	٩	∻ (j)
#Split_tu n	nei_nat	-	奈 (i)

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.