## GETTING STARTED GUIDE



# **ALCATEL-LUCENT RAINBOW<sup>™</sup>**

# SSO OIDC Configuration guide

Ed 1

NOVEMBER 2020

Author: Cloud Services



#### Disclaimer

This documentation is provided for reference purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, this documentation is provided "as is" without any warranty whatsoever and to the maximum extent permitted.

In the interest of continued product development, ALE International reserves the right to make improvements to this document and the products it describes at any time without notice or obligation.

#### Copyright

©2020 ALE International. Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for a commercial purpose is prohibited unless prior permission is obtained from Alcatel-Lucent.

Alcatel-Lucent, OmniPCX, and OpenTouch and Rainbow are either registered trademarks or trademarks of Alcatel-Lucent.

All other trademarks are the property of their respective owners.

## Contents

Glo	ssary	4
1	Introduction	5
2	Overview	6
3	History	6
4	Related documents	6
5	Step 1: Configure Azure AD as an OIDC provider	. 7
6	Step 2: Configure SSO OIDC in Rainbow Admin GUI	11

# Glossary

ALE:	Alcatel-Lucent Enterprise
SSO:	Single Sign On
SAML:	Security assertion markup language
IDP:	Identity Provider
OIDC:	Open ID Connect

## 1 Introduction

Rainbow is able to connect to a third party identity provider (IDP) to perform user authentication through Single Sign On (SSO) based on SAML or OIDC protocols.

The network flows are the following:

### **External authentication with OIDC**



Supported authentication use cases in Rainbow are described in following article:

https://support.openrainbow.com/hc/en-us/articles/360012699219-Rainbow-Authentication-Getting-Started-Guide

As stated in Rainbow-Authentication-Getting-Started-Guide document, following IDP have been tested with SSO OIDC:

- 1. Microsof Azure
- 2. Ping Identity

For other IDP service providers deployment or interoperability tests using OIDC, please contact Rainbow customer care services for consulting.

## 2 Overview

This guide provides technical details to configure Rainbow Single Sign On (SSO) based on OIDC protocol in front of Microsoft Azure.

## 3 History

Modifications	Date	Edition
Creation of document	04/11/2020	Ed 1

## 4 Related documents

- 1. <u>How to Activate the Single Sign-On between Azure Active Directory and my Company (using SAML)?</u>
- 2. How to Activate the Single Sign-On between ADFS and my Rainbow Company (using SAML)?

# 5 Step 1: Configure Azure AD as an OIDC provider

Log in to your Azure portal at <a href="https://portal.azure.com/">https://portal.azure.com/</a>

#### Select Azure Active Directory

Select the App registrations link under the Manage menu

ALE INTERNA Azure Active Directory	ATIONAL   Overview		
<ul> <li>Overview</li> <li>Getting started</li> <li>Preview hub</li> <li>Diagnose and solve proble</li> </ul>	Switch tenant     Switch tenant     Switch tenant     Aure Active Directory can help you enable	<ul> <li>Create a tenant <sup>2</sup> What's new         <sup>2</sup> Preview         <sup>2</sup></li></ul>	v features OG feedback?
Manage			
Groups	Tenant information	💝 Azure AD Connect	
<ul> <li>External Identities</li> <li>Roles and administrators</li> <li>Administrative units</li> <li>Enterprise applications</li> <li>Devices</li> <li>App registrations</li> </ul>	Your role Global administrator More info License Azure AD for Office 365 Tenant ID c	Status Not enabled Last sync Sync has never run	
Identity Governance     Application proxy     Licenses     Azure AD Connect	Sign-ins		

#### Select New registration

Enter a Name for the app

Select the desired option for **Who can use this application or access this API**? Enter the following URL into the **Redirect URI** field:

https://openrainbow.com/api/rainbow/authentication/v1.0/oidc-client/callback



Select the Register button to save and open the new app.



😑 Microsoft Azure 🔎 Se	earch resources, services, and docs (G+/)	ыландар 🛛 🕞 Д 🍈 ? 😳 susan.lee@coffeechocol 🌘
Home > ALE INTERNATIONAL >		
RAINBOW .com	\$	×
Search (Ctrl+/)	« 间 Delete 🜐 Endpoints 🐱 Preview features	
Uverview	Got a second? We would love your feedback on Microsoft identity platform (pr	eviously Azure AD for developer). $ ightarrow$
🍪 Quickstart	∧ Essentials	
💉 Integration assistant   Preview	Display name : RAINBOW .com	Supported account types : My organization only
Manage	Application (client) ID : 0743b1ad-2192-4994-9d3b-ec12b09aa215	Redirect URIs : 1 web, 0 spa, 0 public client
Branding	Directory (tenant) ID : d0147ac8-25c3-4b24-8bd0-bd3523c6c635	Application ID URI : Add an Application ID URI
Authentication	Object ID : 3e588ac4-5a99-49d1-8079-07afebefdec4	Managed application in I : RAINBOW .com
Certificates & secrets	Starting June 30th, 2020 we will no longer add any new features to Azure Active	e Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical
Token configuration	support and security updates but we will no longer provide feature updates. Ap Graph. Learn more	splications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft
API permissions		
🙆 Expose an API		

Select the Certificates & secrets link under the Manage menu.

Select the New client secret button.

Enter an optional description and select your preferred expiration period.

Select the Add button.

The client secret appears under the Client secrets section. Copy its value for later use in a text editor, because you won't be able to view it again.

All services > App registrations > RAINB	30W.com			~
Search (Ctrl+/)     «	♥ Got feedback?			^
<ul> <li>Øverview</li> <li>Quickstart</li> </ul>	Copy the new client secret value. Yo	u won't be able to retrieve it after you perf	form another operation or leave this blade.	
💉 Integration assistant   Preview	Credentials enable confidential application location (using an HTTPS scheme). For a	ons to identify themselves to the auther higher level of assurance, we recomme	ntication service when receiving tokens at a web a nd using a certificate (instead of a client secret) a	addressable A
<ul> <li>Branding</li> <li>Authentication</li> </ul>	Certificates Certificates can be used as secrets to pro	we the application's identity when requ	esting a token. Also can be referred to as public i	keys.
📍 Certificates & secrets	↓ Upload certificate			
Token configuration     API permissions	Thumbprint	Start date	Expires	_
Expose an API     Owners	no ceruncates nave veen auteu no uns	ahhiranni		
<ul> <li>Roles and administrators   Preview</li> <li>Manifest</li> </ul>	Client secrets	to prove its identity when requesting a	token. Also can be referred to as application pass	sword.
Support + Troubleshooting	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			
Troubleshooting	+ New client secret			
New support request	Description	Expires	Value	
	RAINBOW .com	12/31/2299	Statute And Property Control	r 💼 🗸

In App registrations > Your app menu, copy the Application (client) ID value and save it in a text file

E Microsoft Azure	Search resources, services, and docs (G+/)		P	Ω			٢	susan.lee@coffeechocol
Home > ALE INTERNATIONAL >								
RAINBOW .com	#							×
	« 📋 Delete 🕀 Endpoints 🐻 Preview features							
Uverview	Got a second? We would love your feedback on Microsoft identity, platform (previously Azure AD for	leveloper), →						
📣 Quickstart								
🚀 Integration assistant   Preview	Display name : RAINBOW .com Supp	orted account	types	: Му	organiz	ation o	nly	
Manage	Application (client) ID : 0743b1ad-2192-4994-9d3b-ec12b09aa215 Redi	ect URIs		:1w	eb, 0 sp	a, 0 pu	blic client	
Branding	Directory (tenant) ID : d0147ac8-25c3-4b24-8bd0-bd3523c6c635 Appl	ation ID URI		: Ad	d an Ap	plicatio	n ID URI	
Authentication	Object ID : 3e588ac4-5a99-49d1-8079-07afebefdec4 Man	ged application	on in I	: RAI	NBOW	.com		

Click on Endpoints and copy OpenID Connect metadata document URL:

	h resources, services, and docs (G+/)	ы 🖓 🖓 🖓 😳 susanlee@coffeechocol 🔒
Home > ALE INTERNATIONAL >		Endpoints ×
Search (Ctrl+/)     «	Delete Endpoints 🐼 Pre	OAuth 2.0 authorization endpoint (v2) https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/authorize
Overview     Quickstart     Integration assistant   Preview	Got a second? We would love your     Essentials	OAuth 2.0 token endpoint (v2)  https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/token  OAuth 2.0 authorization endpoint (v1)
Manage	Application (client) ID : 0743b1ad-219 Directory (tenant) ID : d0147ac8-25c	https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/authorize
Authentication     Certificates & secrets     Token configuration	Object ID : 3e588ac4-5a9 Starting June 30th, 2020 we will no support and security updates but w	OpenID Connect metadata document         Copy to clipboard           https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/v2.0/.well-known/openid-configuration         D
API permissions     Expose an API	Graph. Learn more	Microsoft Graph API endpoint           https://graph.microsoft.com         D           Federation metadata document         D
<ul> <li>Owners</li> <li>Roles and administrators   Pre</li> </ul>	Call APIs	https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/federationmetadata/2007-06/federationmetadata.xml 🗅
Manifest •		https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/wsfed

## 6 Step 2: Configure SSO OIDC in Rainbow Admin GUI

In the administration menu of Rainbow, open My Company > Settings > Security tab Add a configuration of an SSO server based on OIDC protocol.

8	Administration	Coffee & Chocol	ate	
	< Back		Enternal	
6	1 Information	Profiles	Support Security directory	
	Members	Advanced Login		
쏭	Subscriptions	Single Sign-On (SSO)	)) Configuration 🟮	
0	Communication	Туре	Status	Actions
	Business directory	SAML	Artivated only for some members	ı ō
900	(iii) Activity	0105	readers only to some memory a	4.5
(0)	History	OIDC	Activated only for some members	U V
•	Settings			

OpenID Connect configuration	×
Authentication method Uses the OpenID Connect protocol to log users into Rainbow.	
Enable this authentication method for all members of the company. If you would like to manually enable this authentication method for some users, leave this box unchecked.	
Cancel	Next

You can choose to use this authentication method as the default one for the whole company, else leave unchecked to activate it on a user-basis.

### Click next

Enter previously saved parameters:

- 1. Client ID
- 2. Secret
- 3. Discovery URL

\llowed grant type		
"Authorization code" is	s the mechanism for the client or application to receive an identity token.	
Client Secret and Toke	n Endpoint URL are mandatory	
Client application crede	entials	
Client ID	0743b1ad-2192-4994-9d3b-ec12b09aa215	
Client secret	axOQvjM5e-9R1oHS-r~~Z967feh1uJMrce	
<ul> <li>Automatic configure</li> <li>Your OpenID Configure</li> <li>Manual configure</li> <li>All required parameter</li> </ul>	uration nect provider supports automatic discovery of the server configuration. tion meters must be entered manually.	
inter the discovery end	dpoint that automatically provides information about the server configuration.	
	https://lippin.co/accenteration.com/20147a-2026-204624.8b-20.b-22522-6-6254.204	11.14

Save the configuration and upon success, you should get this screen:

# OpenID Connect configuration × The following parameters have been automatically filled in. Issuer URL Issuer URL https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/v2.0 Authorization URL https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/authorize Token URL https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/authorize Token URL https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/token JSON Web Key Set (WKS) URI https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/tokens End session URL https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/togout

## You can also choose the manual configuration and enter all the URLs manually, like this:

OpenID Connect config	guration	×
Client application credentials		
Client ID	f70f3e5e-d1c1-4dcd-83dd-b01ca21a46d2	
Client secret		
Configuration mode Automatic configuration Your OpenID Connect pro Manual configuration All required parameters n Enter your organisation's single	vider supports automatic discovery of the server configuration. nust be entered manually.	
Issuer URL	https://login.microsoftonline.com/ 7/v2.0	
Authorization URL	https://login.microsoftonline.com/1 7/oauth2/v	2.0
Token URL	https://login.microsoftonline.com/	2.0
JSON Web Key Set (JWKS) URI	https://login.microsoftonline.com/ //discovery	/v
End session URL		
	Previous	e

To activate the new login method for a user, go into Members tab:

8	Administration	Coffee & Chocolate		
	< Back			
6	1 Information	Members Tags		
00	Aembers	Q Search members	Members - 8 -	Invite
رت	Subscriptions	Name	Services Phone Device type	Roles
3	Communication			
	Business directory	DAVIS Megan	Enterprise Demo	Admin
000	Ilistory	LEE Adam	Enterprise Demo	Member
້ຳດ້ຳ	Settings	LEE Susan	Enterprise Demo	Admin
۲		THOMPSON James	Enterprise Demo	Member

Select the user you want to modify and in Security tab choose OIDC as sign-in method:

formation LEE Susan ×										
Information	Phone	Services	Roles	Permissions	Security					
User's Authenticati	ion Policy									
Sign-in method	SSO cr	edentials (OIDC)	~							
						Clore				
						ciose	жрру			