



ALCATEL-LUCENT RAINBOW™

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

Glossary.....	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

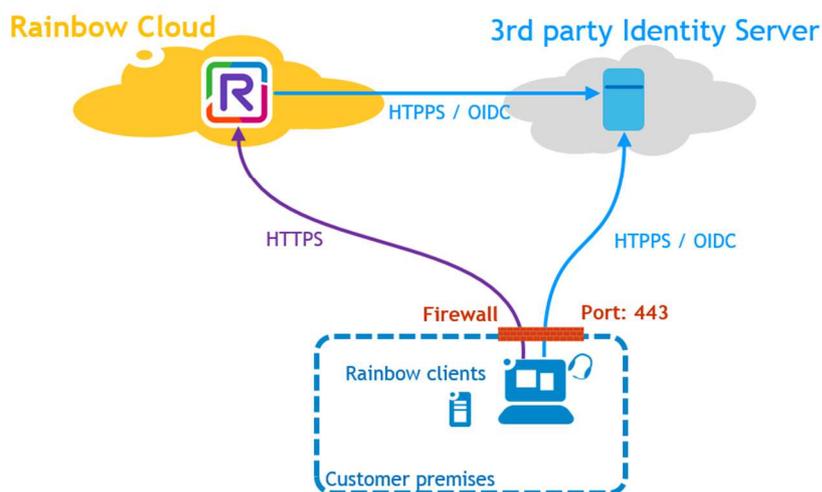
ALE:	Alcatel-Lucent Enterprise
SSO:	Single Sign On
SAML:	Security assertion markup language
IDP:	Identity Provider
OIDC:	Open ID Connect

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. Microsoft 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

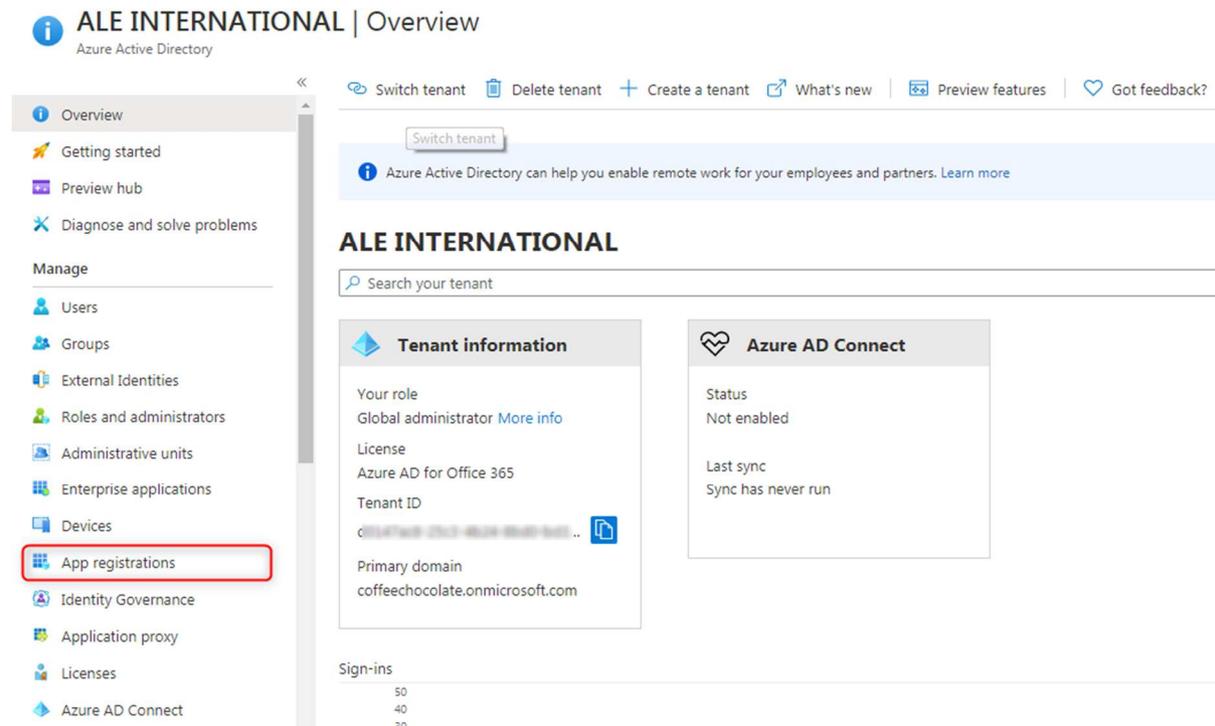
1. [How to Activate the Single Sign-On between Azure Active Directory and my Company \(using SAML\)?](#)
2. [How to Activate the Single Sign-On between ADFS and my Rainbow Company \(using SAML\)?](#)

5 Step 1: Configure Azure AD as an OIDC provider

Log in to your Azure portal at <https://portal.azure.com/>

Select **Azure Active Directory**

Select the **App registrations** link under the **Manage** menu



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>

Microsoft Azure Search resources, services, and docs (G+)

Home > ALE INTERNATIONAL >

Register an application

* Name

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

Rainbow .com ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (ALE INTERNATIONAL only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Help me choose...

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 ✓ ✓

By proceeding, you agree to the Microsoft Platform Policies ↗

Register

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

Microsoft Azure Search resources, services, and docs (G+)

Home > ALE INTERNATIONAL

ALE INTERNATIONAL | App registrations

App registrations Identity Governance Application proxy Licenses Azure AD Connect Custom domain names Mobility (MDM and MAM) Password reset Company branding User settings Properties Security

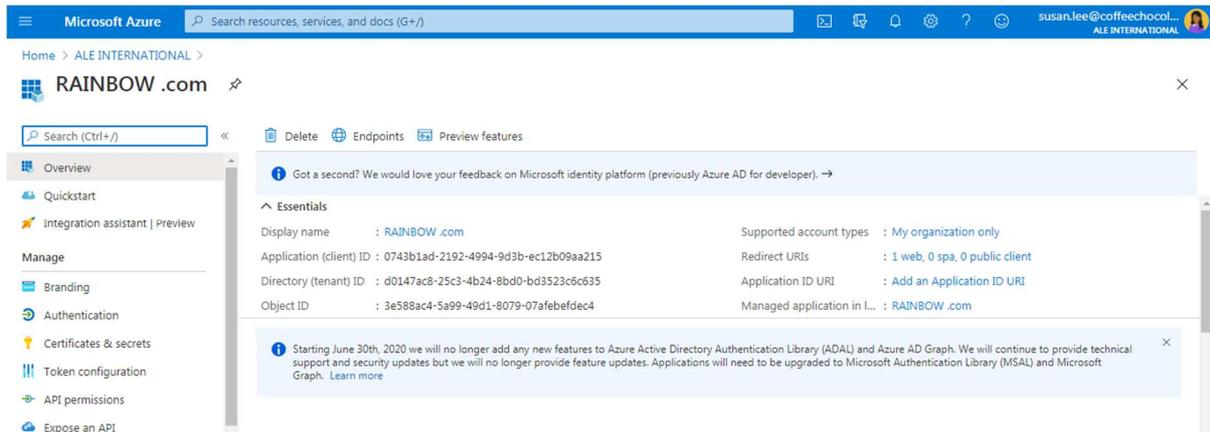
+ New registration Endpoints Troubleshooting Download Preview features Got feedback?

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

All applications Owned applications

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
Rainbow .NET	18403100-b943-4082-b8ca-e67efc9ac3fc	7/24/2019	Current
RAINBOW .com	0743b1ad-2192-4994-9d3b-ec12b09aa215	11/3/2020	Current



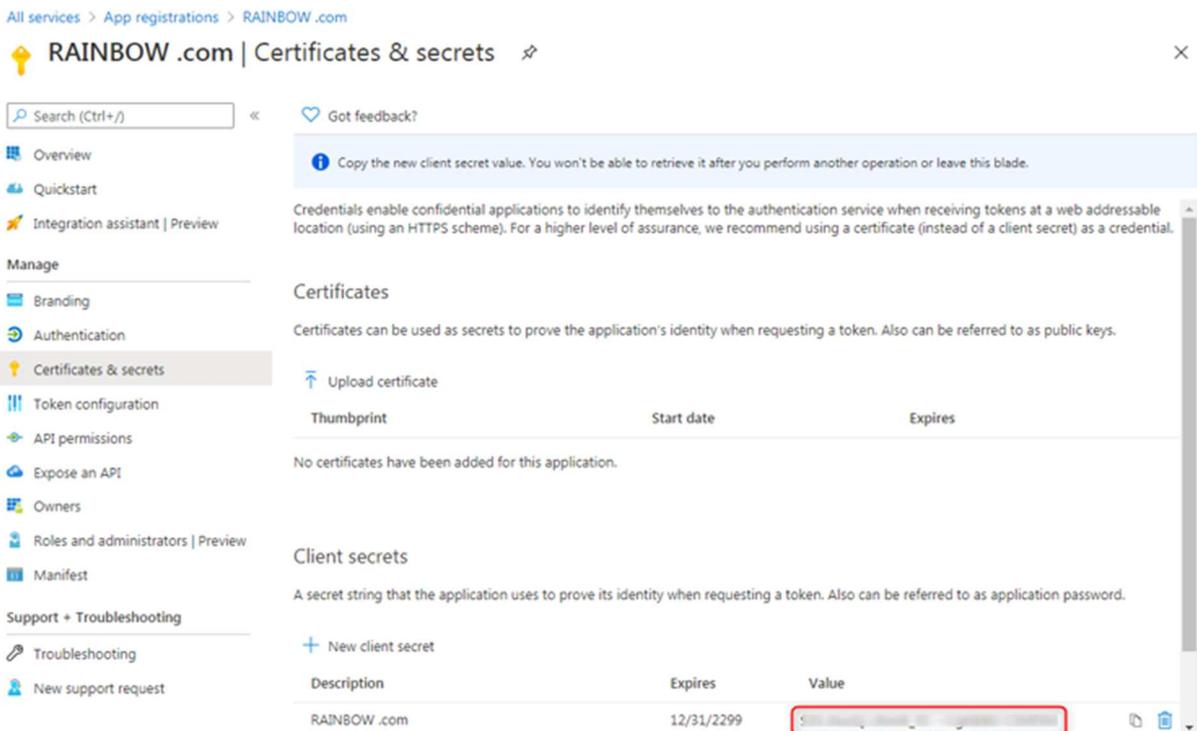
Select the **Certificates & secrets** link under the **Manage** menu.

Select the **New client secret** button.

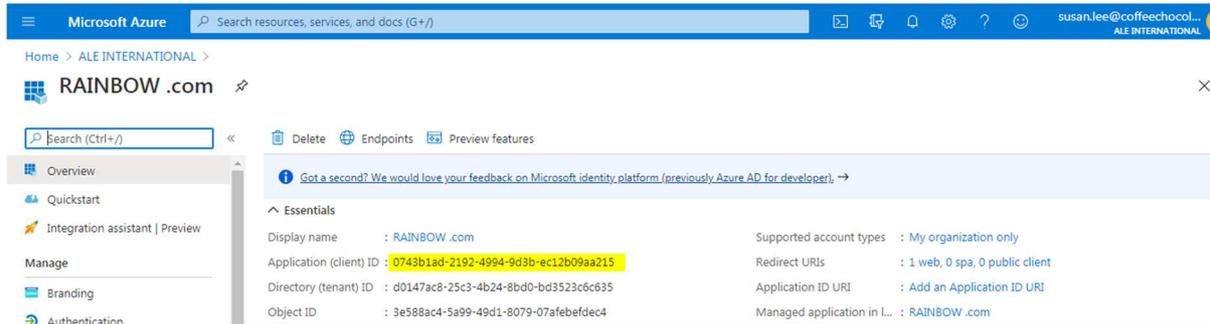
Enter an optional description and select your preferred expiration period.

Select the **Add** button.

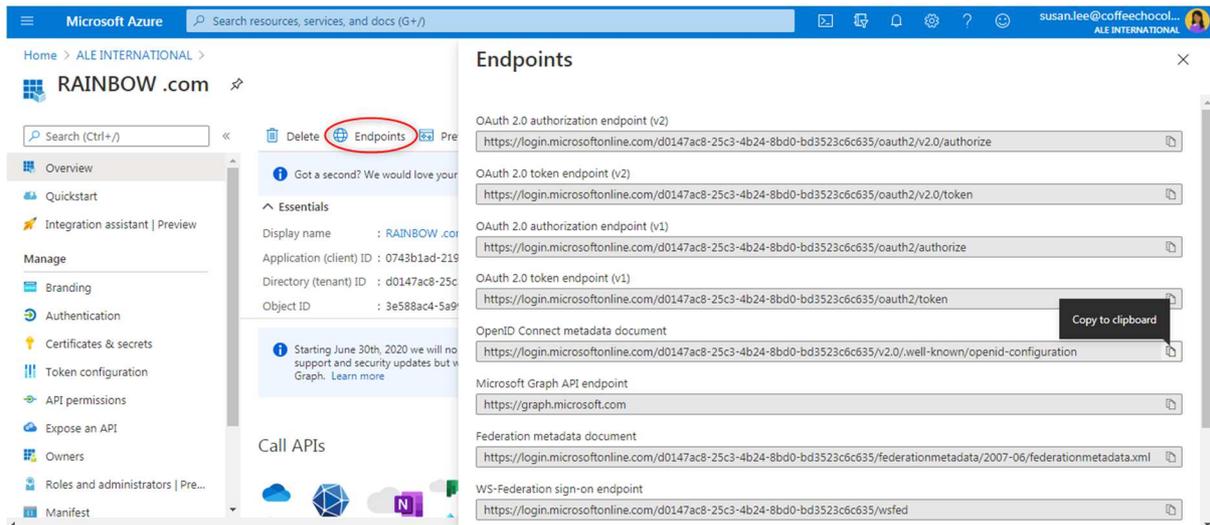
The client secret appears under the **Client secrets** section. Copy its value for later use in a text editor, because you won't be able to view it again.



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

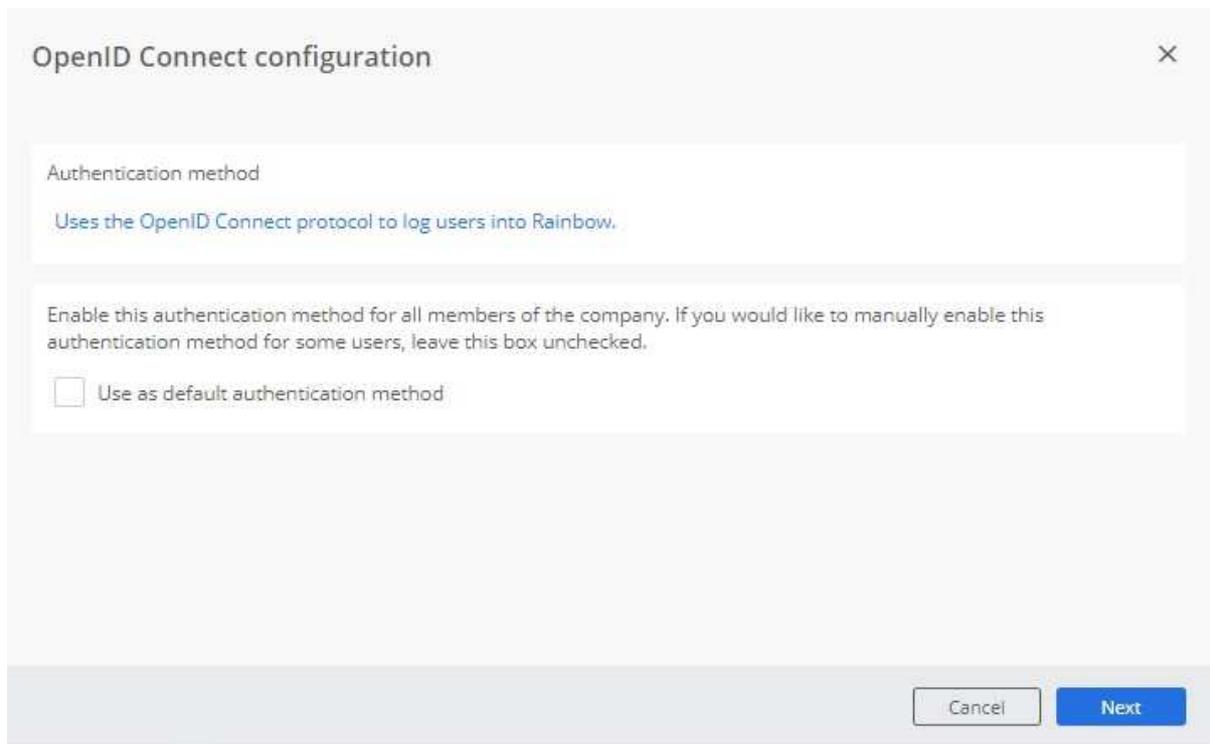
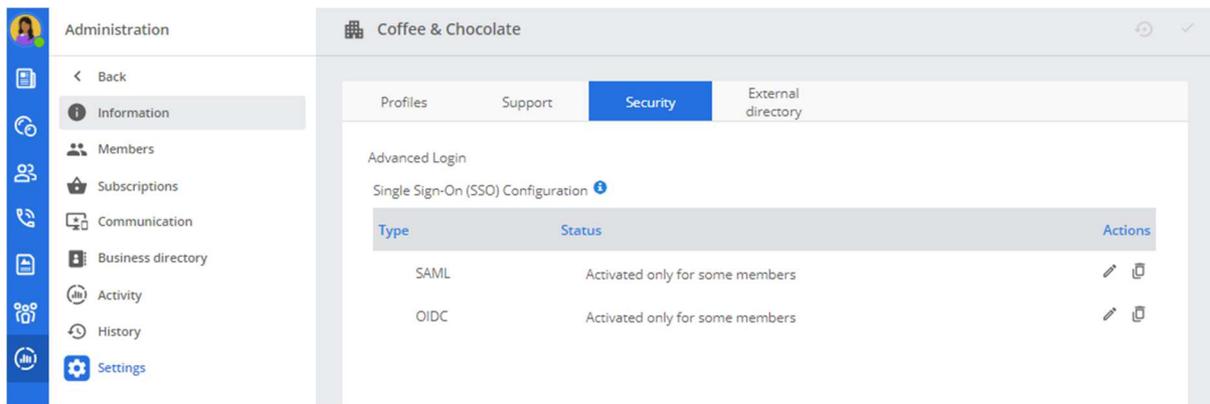


Click on **Endpoints** and copy **OpenID Connect metadata document URL**:



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.



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:

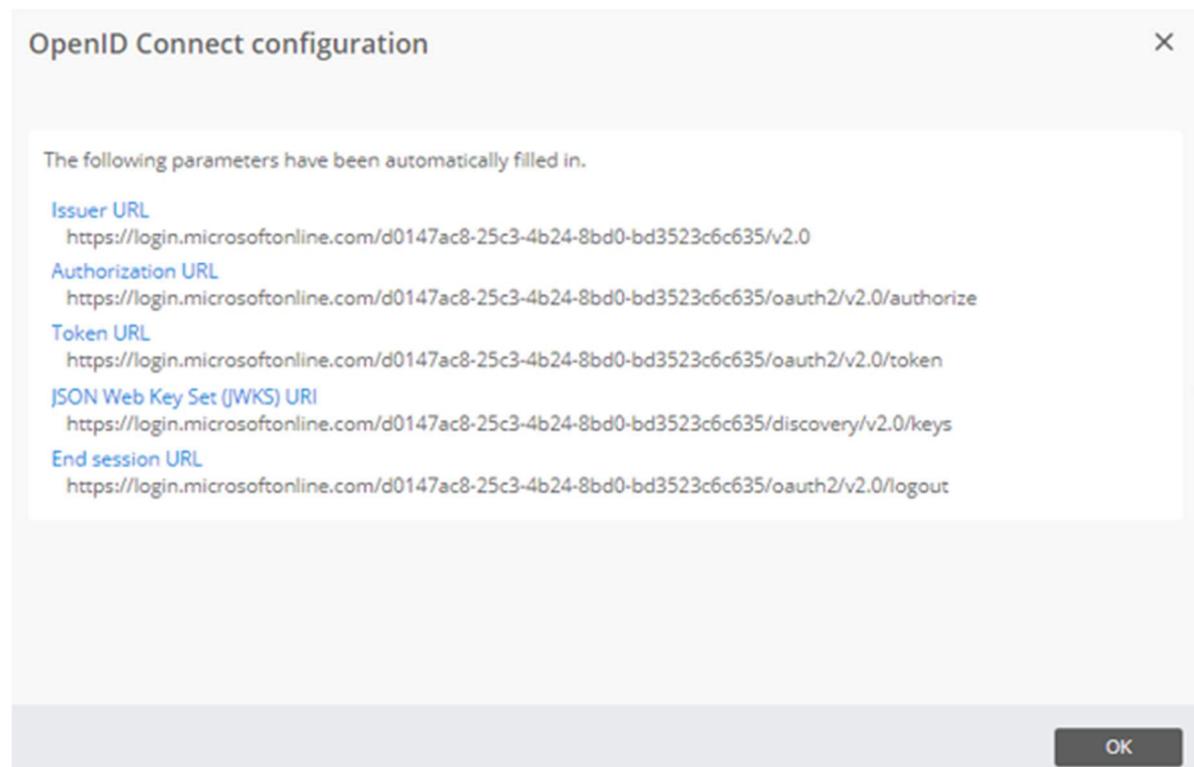
1. Client ID
2. Secret
3. Discovery URL

The screenshot shows a dialog box titled "OpenID Connect configuration" with a close button (X) in the top right corner. The dialog is divided into several sections:

- Allowed grant type:** A text box containing "Authorization code" with a tooltip that reads: "Authorization code" is the mechanism for the client or application to receive an identity token. Client Secret and Token Endpoint URL are mandatory.
- Client application credentials:** Two text boxes. The first is labeled "Client ID" and contains the value "0743b1ad-2192-4994-9d3b-ec12b09aa215". The second is labeled "Client secret" and contains the value "axOQvjM5e-9R1oH5-r~-Z967feh1ujMrce".
- Configuration mode:** Two radio buttons. The first is "Automatic configuration" (selected) with the subtext "Your OpenID Connect provider supports automatic discovery of the server configuration." The second is "Manual configuration" with the subtext "All required parameters must be entered manually."
- Discovery URL:** A text box containing the URL "https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/v2.0/.well-k".

At the bottom right of the dialog, there are two buttons: "Previous" (disabled) and "Save" (active).

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



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

OpenID Connect configuration [X]

Client application credentials

Client ID: f70f3e5e-d1c1-4dcd-83dd-b01ca21a46d2

Client secret: [Masked]

Configuration mode

Automatic configuration
Your OpenID Connect provider supports automatic discovery of the server configuration.

Manual configuration
All required parameters must be entered manually.

Enter your organisation's single sign-on (SSO) settings by giving the ID provider details.

Issuer URL: https://login.microsoftonline.com/.../v2.0

Authorization URL: https://login.microsoftonline.com/.../oauth2/v2.0

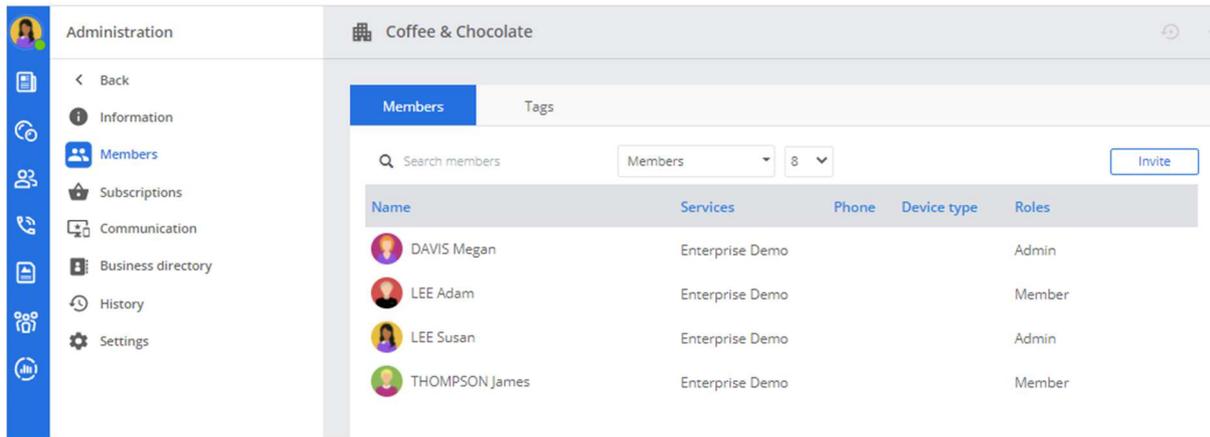
Token URL: https://login.microsoftonline.com/.../oauth2/v2.0

JSON Web Key Set (JWKS) URI: https://login.microsoftonline.com/.../discovery/v...

End session URL: [Empty]

[Previous] [Save]

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



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

