GETTING STARTED GUIDE

ALCATEL-LUCENT RAINBOW™

SSO OIDC Configuration guide

Ed 1

NOVEMBER 2020

Author: Cloud Services

Alcatel·Lucent Enterprise

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

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

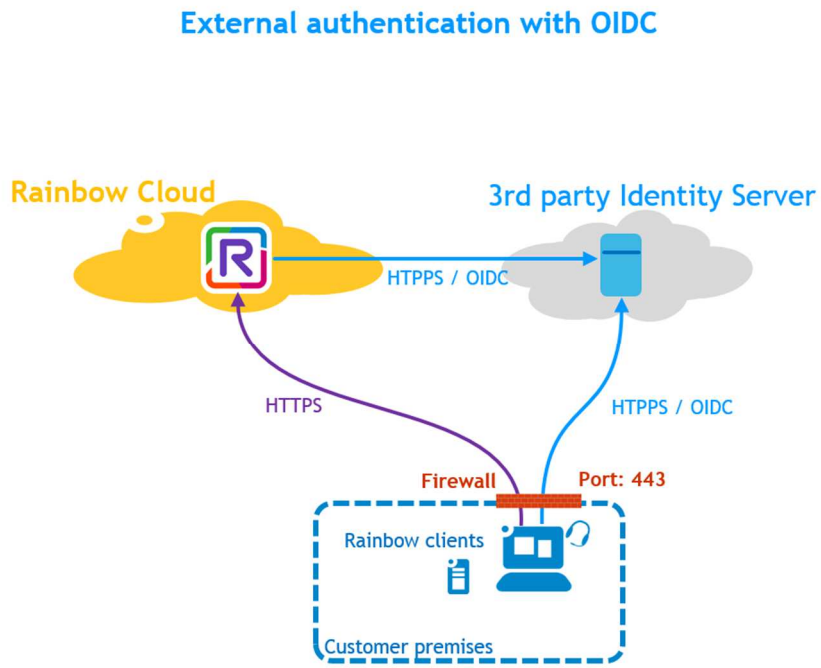
IDP: Identity Provider

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:



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

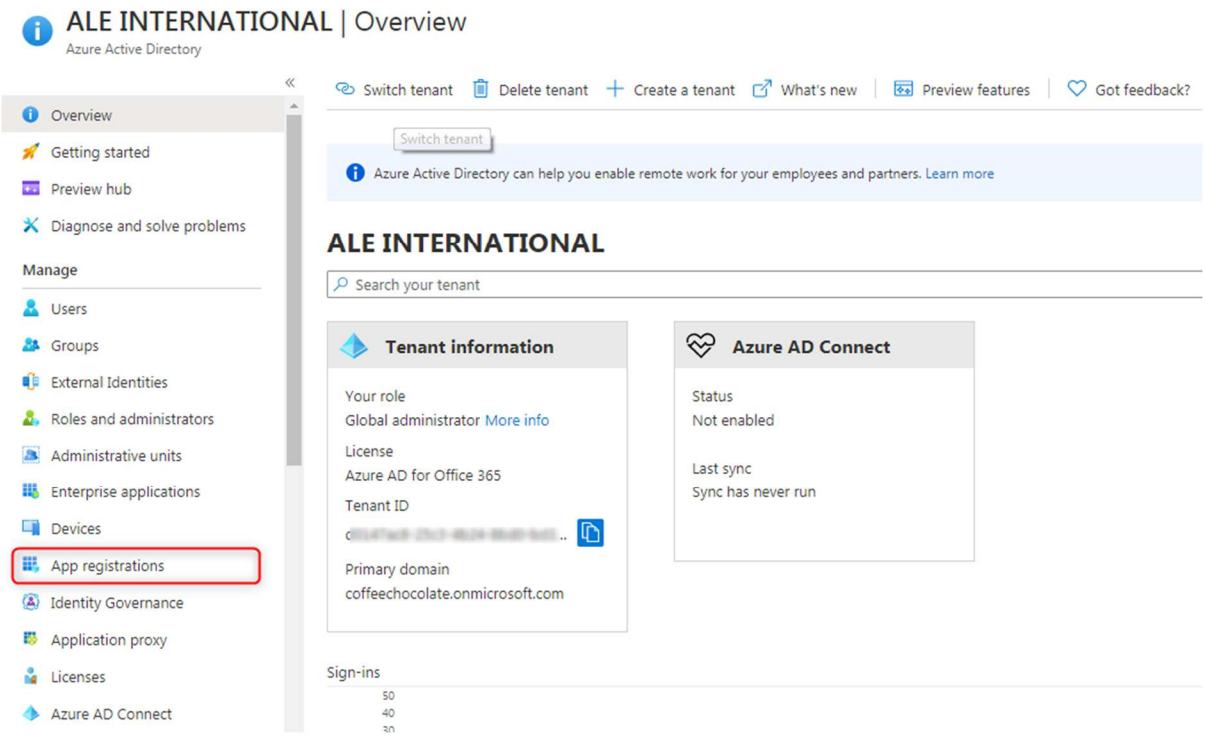
1. How to Activate the Single Sign-On between Azure Active Directory and my Company (using SAML)?
2. How to Activate the Single Sign-On between ADFS and my Rainbow Company (using SAML)?

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



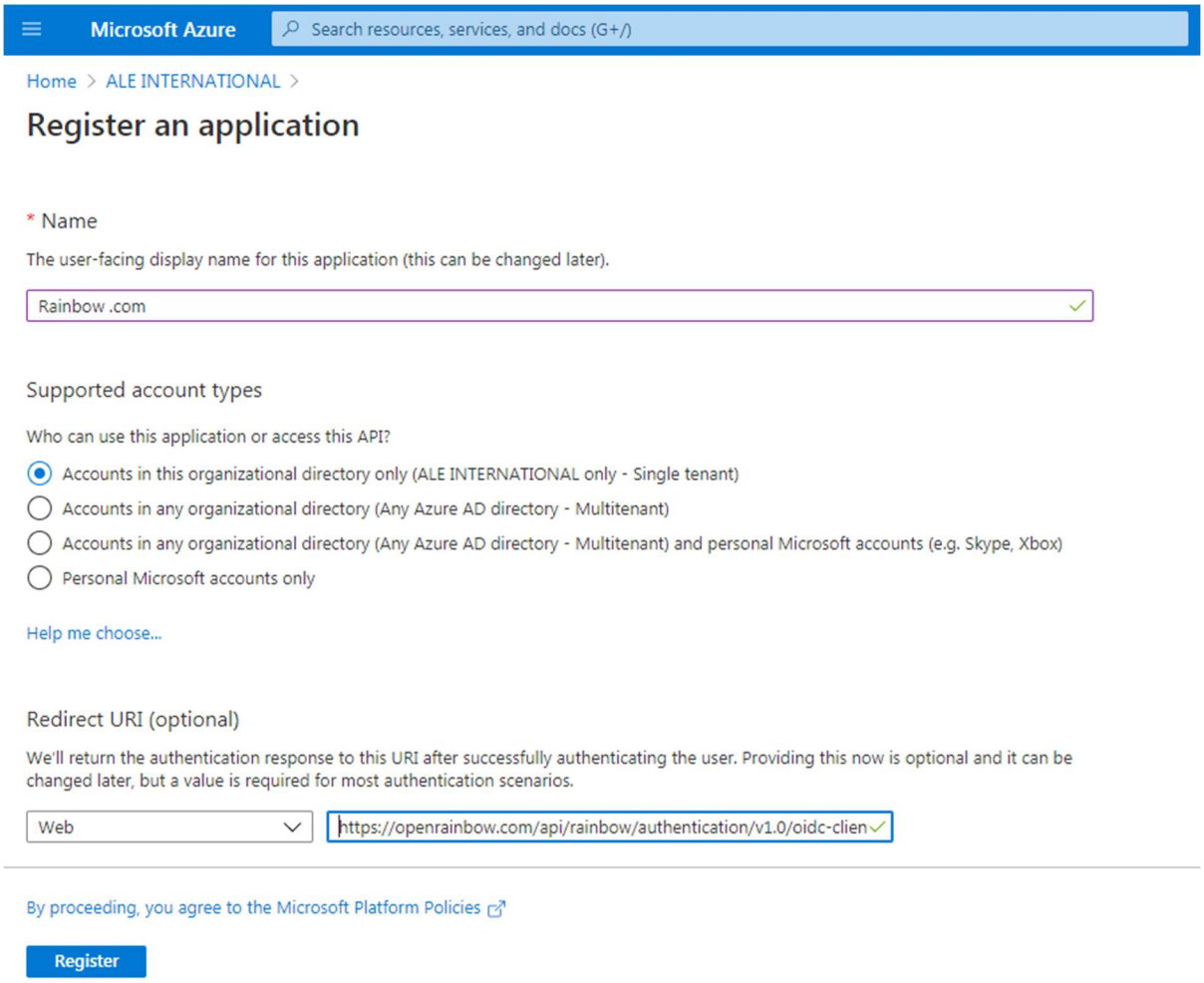
Select **New registration**

Enter a **Name** for the app

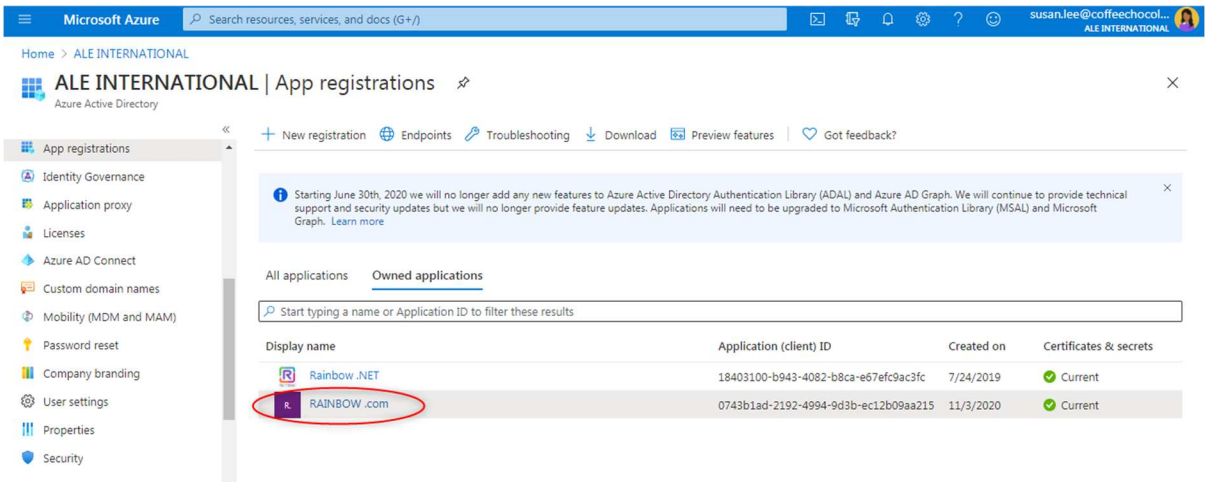
Select the desired option for **Who can use this application or access this API?**

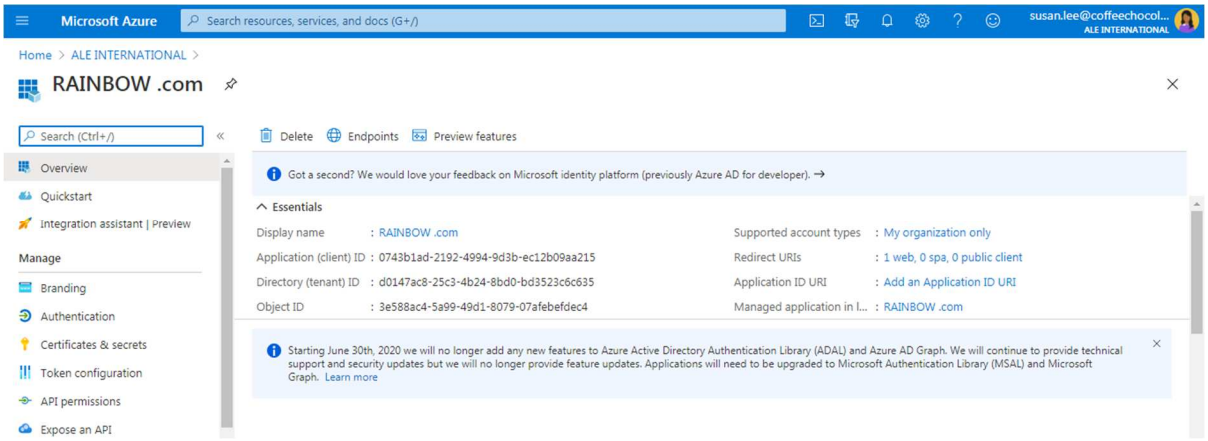
Enter the following URL into the **Redirect URI** field:

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



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





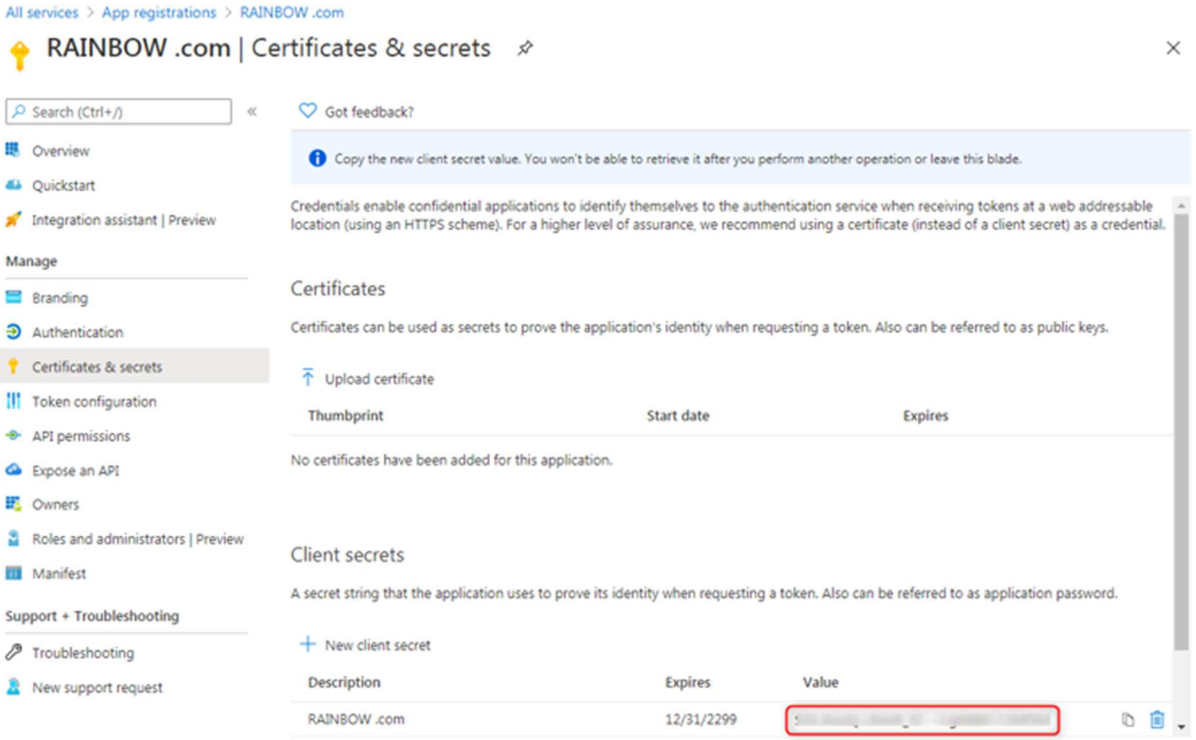
Select the **Certificates & secrets** link under the Manage menu.

Select the **New client secret** button.

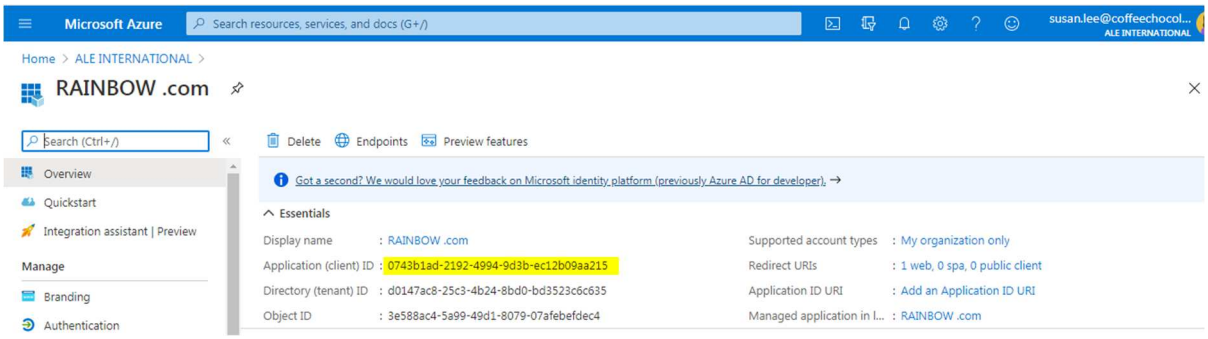
Enter an optional description and select your preferred expiration period.

Select the **Add** button.

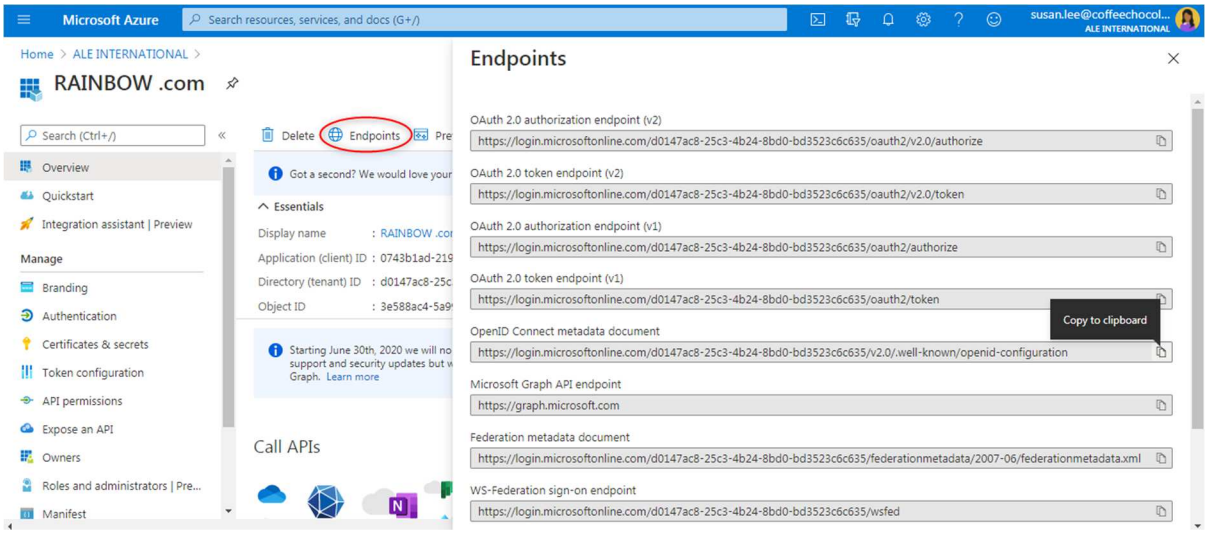
The client secret appears under the Client secrets section. Copy its value for later use in a text editor, because you won't be able to view it again.



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



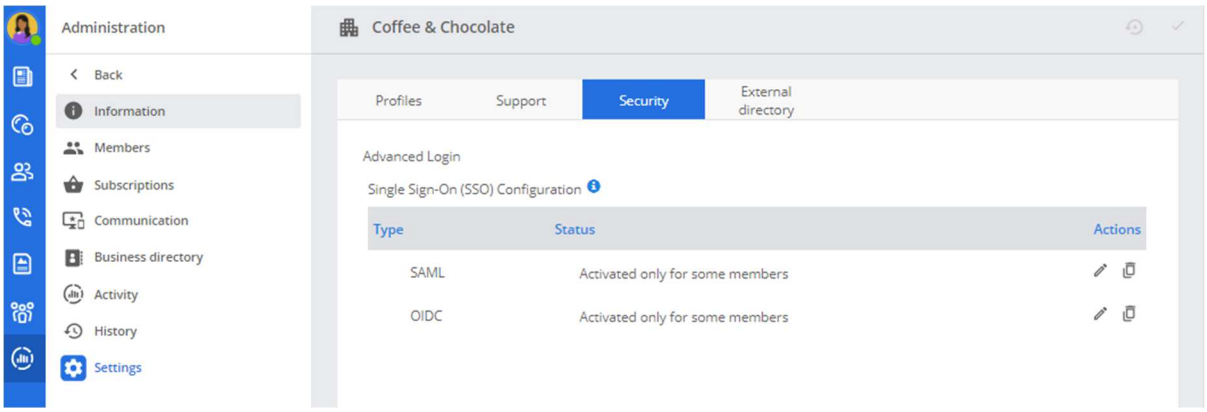
Click on **Endpoints** and copy **OpenID Connect metadata document** URL:

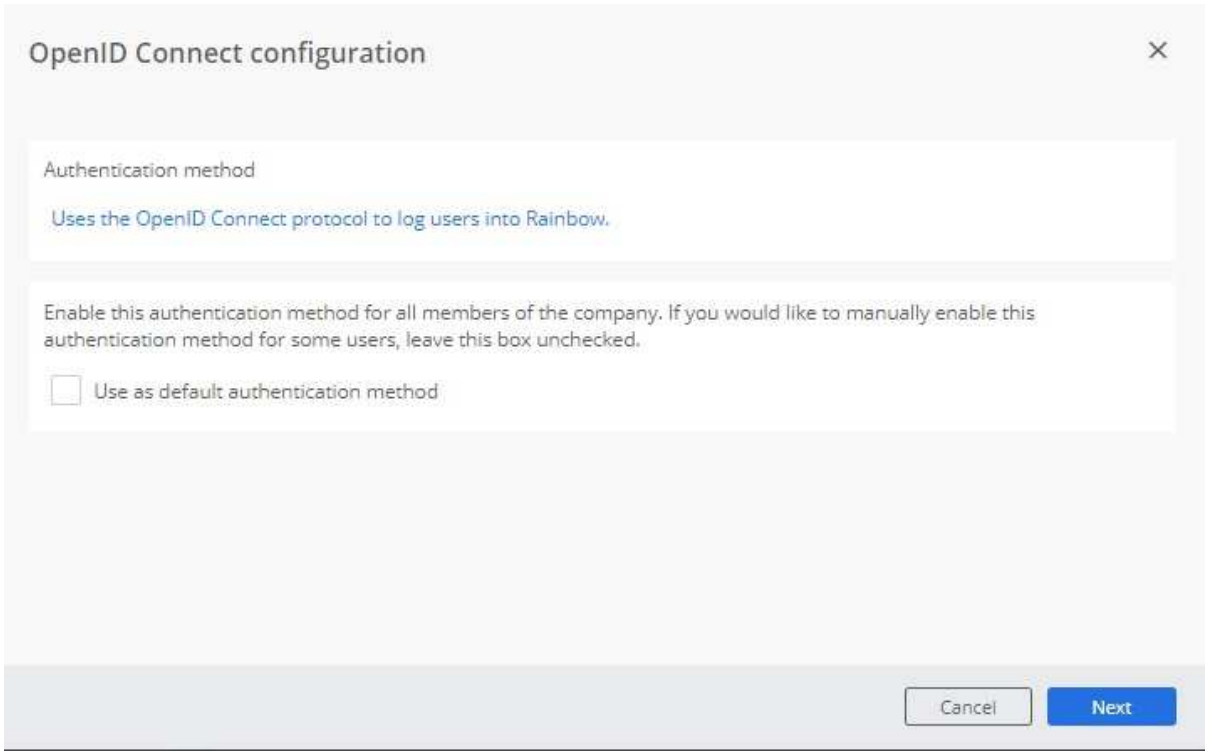


6 Step 2: Configure SSO OIDC in Rainbow Admin GUI

In the administration menu of Rainbow, open My Company > Settings > Security tab

Add a configuration of an SSO server based on OIDC protocol.



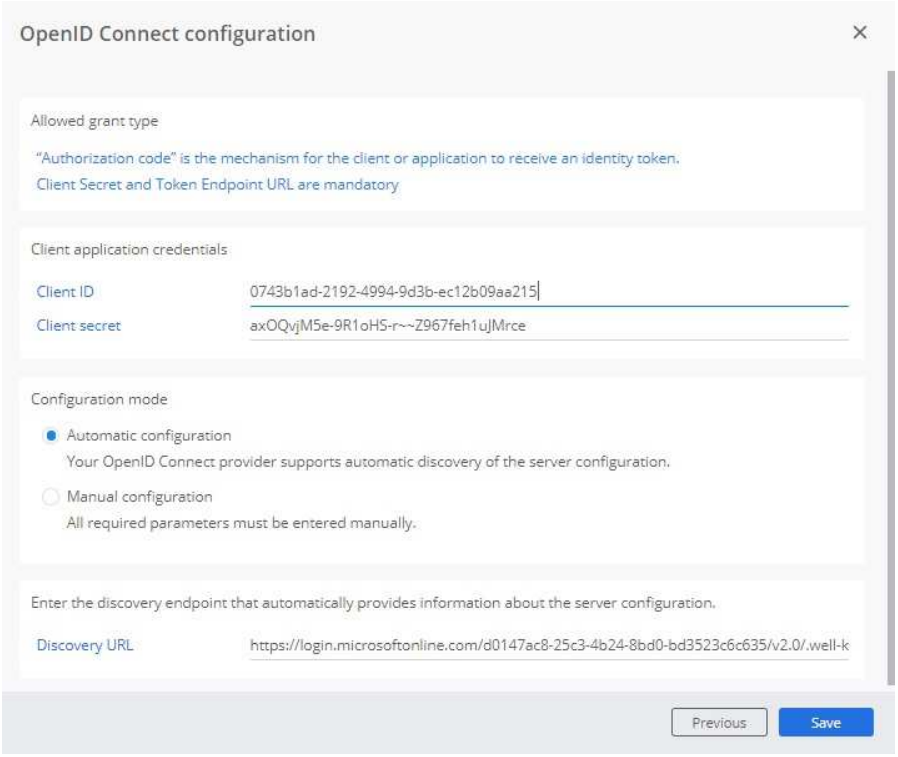


You can choose to use this authentication method as the default one for the whole company, else leave unchecked to activate it on a user-basis.

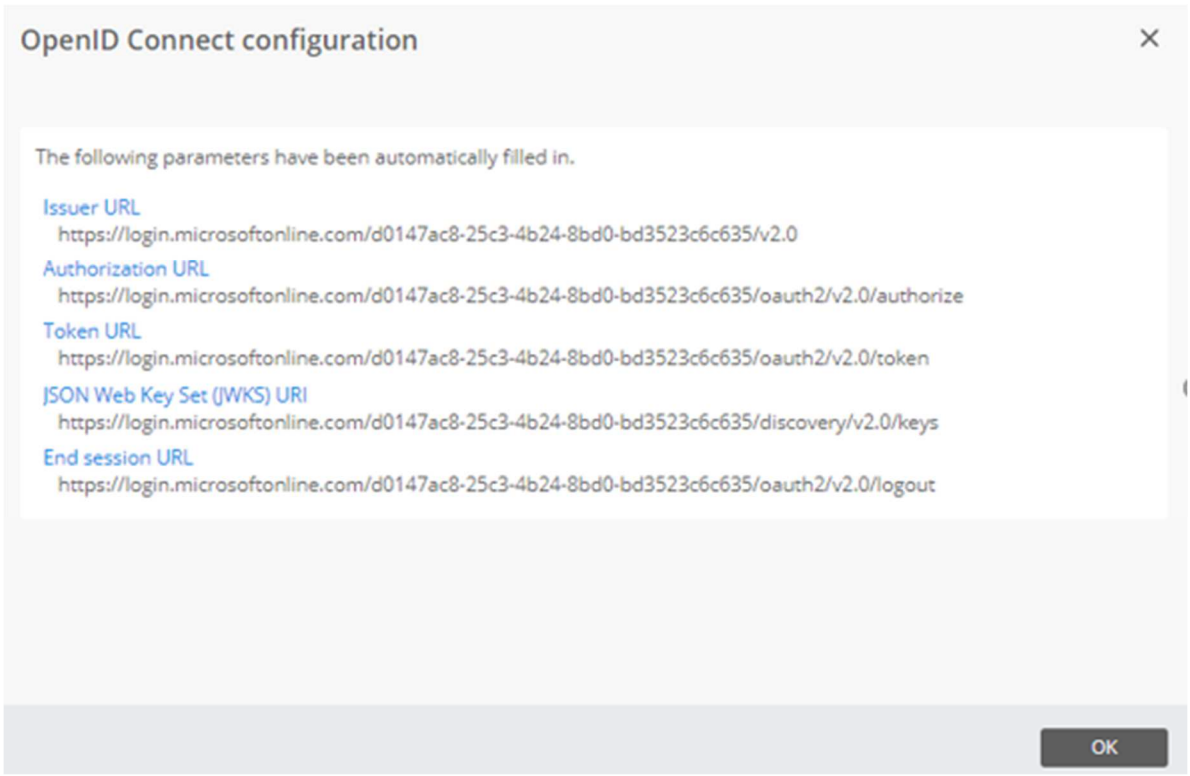
Click next

Enter previously saved parameters:

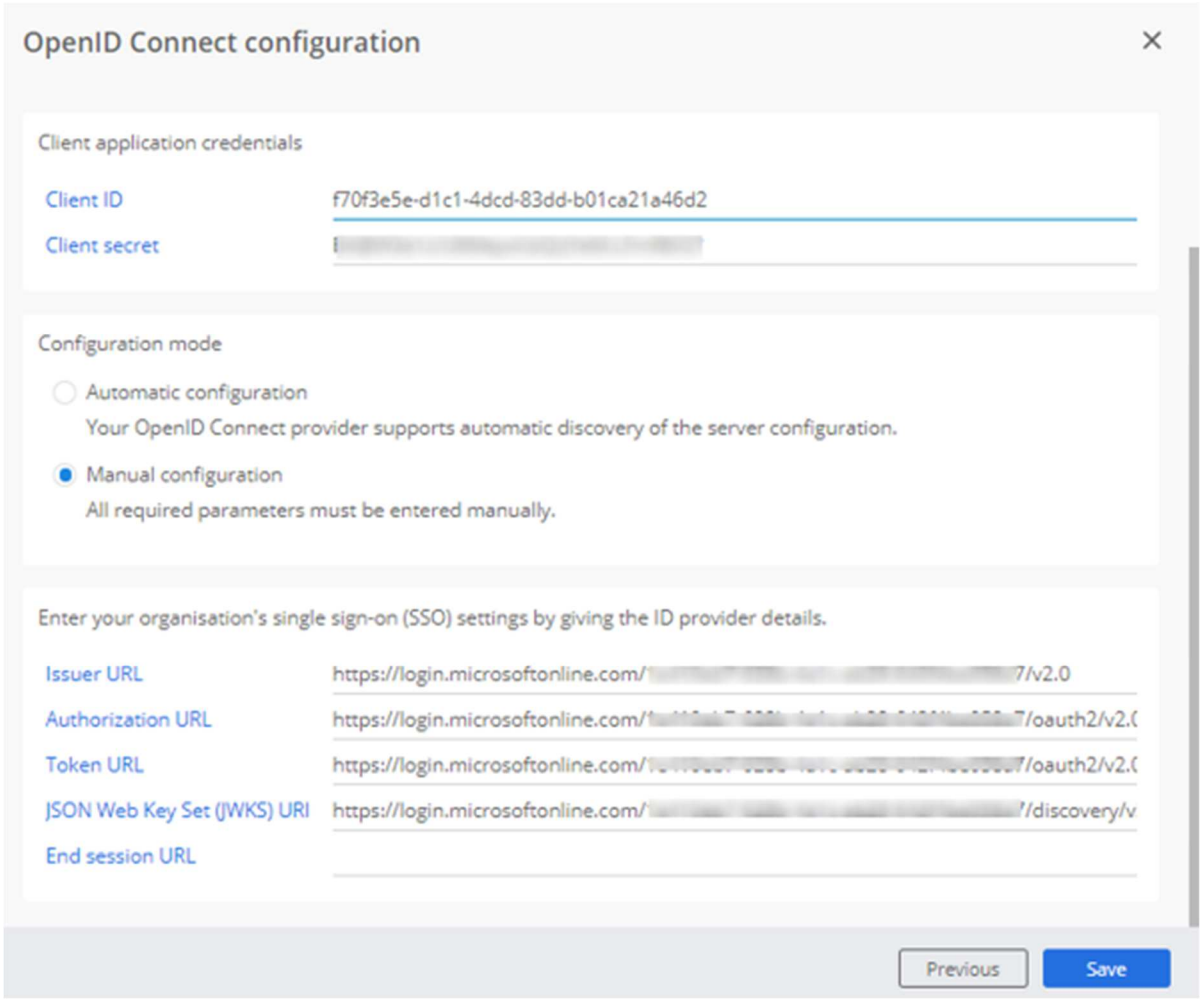
1. Client ID
2. Secret
3. Discovery URL



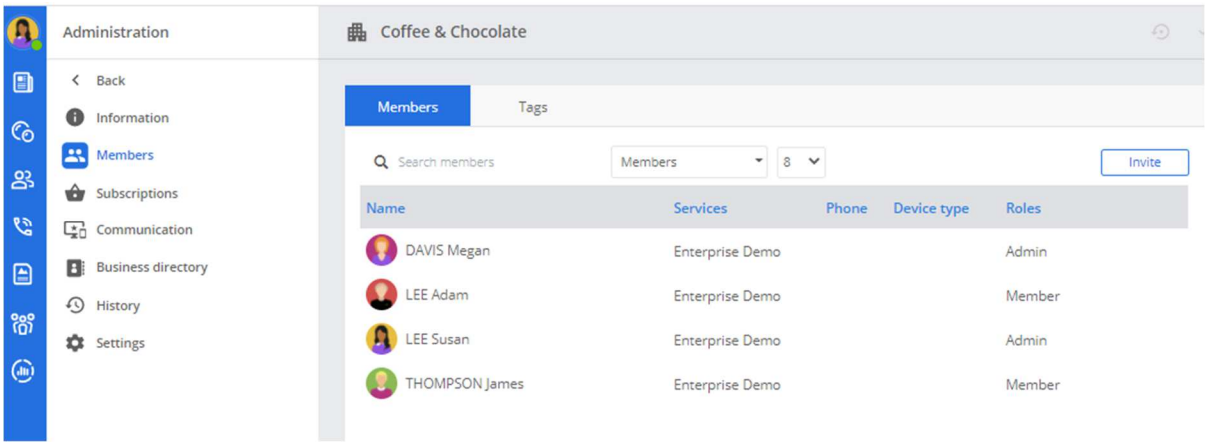
Save the configuration and upon success, you should get this screen:


OpenID Connect configuration
The following parameters have been automatically filled in.
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/token
JSON Web Key Set (JWKS) URI
https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/discovery/v2.0/keys
End session URL
https://login.microsoftonline.com/d0147ac8-25c3-4b24-8bd0-bd3523c6c635/oauth2/v2.0/logout
OK

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



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: