**Resolve – User Guide**

**Version 1.0**

**School of Dentistry**

**University of Washington, Seattle**



**Revision and Signoff Sheet**

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Author** | **Version** | **Change Reference** |
| 21st July 2020 | Palash Jhamnani | 1.0 | First Draft |

**Reviewers**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Reviewer** | **Version** | **Comments** |
|  | Anya L. Levysmith | 1.0 |  |

Contents

[Introduction 4](#_Toc48216951)

[Know Issues 4](#_Toc48216952)

[Azure Portal 5](#_Toc48216953)

[Application Registration 5](#_Toc48216954)

# Introduction

Resolve is a case/request management software

# Know Issues

Same person/approver should not belong in multiple groups.

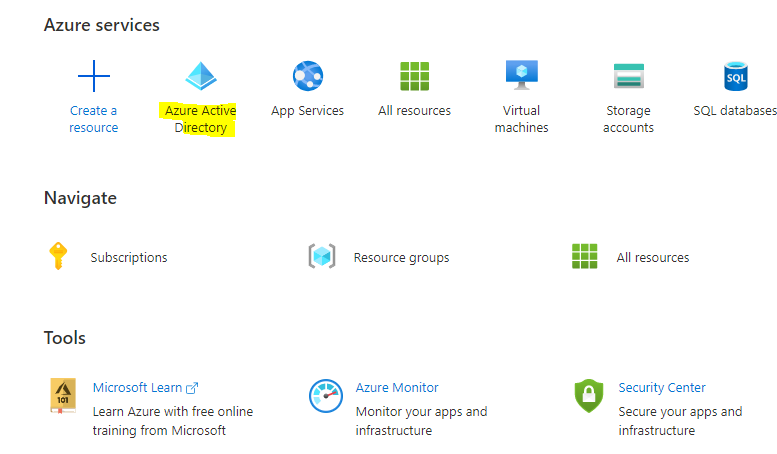
This is due to the database schema, where the key for approver table is composite, comprising of UserID and CaseID, so for the same case, a person cannot be an approver twice. This behavior can be modified with schema changes; however, it is not advised to change the schema as it will require changes at multiple places in the codebase. The current schema adheres to the business requirement and meets segregation of duty (SOD) principle. According to SOD, one person should not handle 2 conflicting approvals concurrently. E.g. A person belonging to HR group may approve a hiring request and if he/she belong to the Finance group as well then, they could approve/modify the hiring budget as well.

# Azure Portal

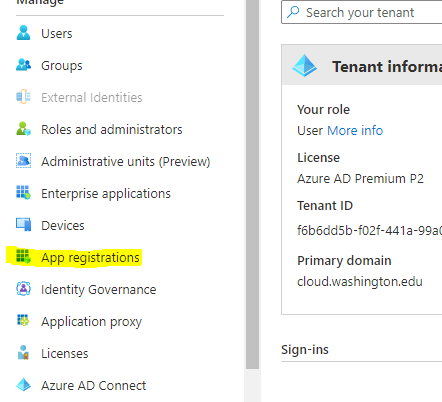
## Application Registration

Step1: Login to <https://portal.azure.com/#home> with your UW net id

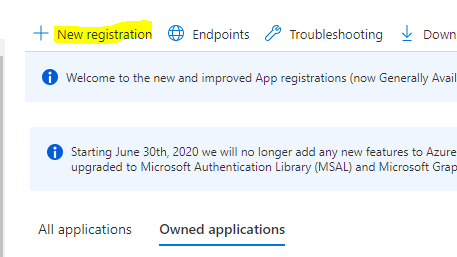
Step2: Go to Azure Active Directory



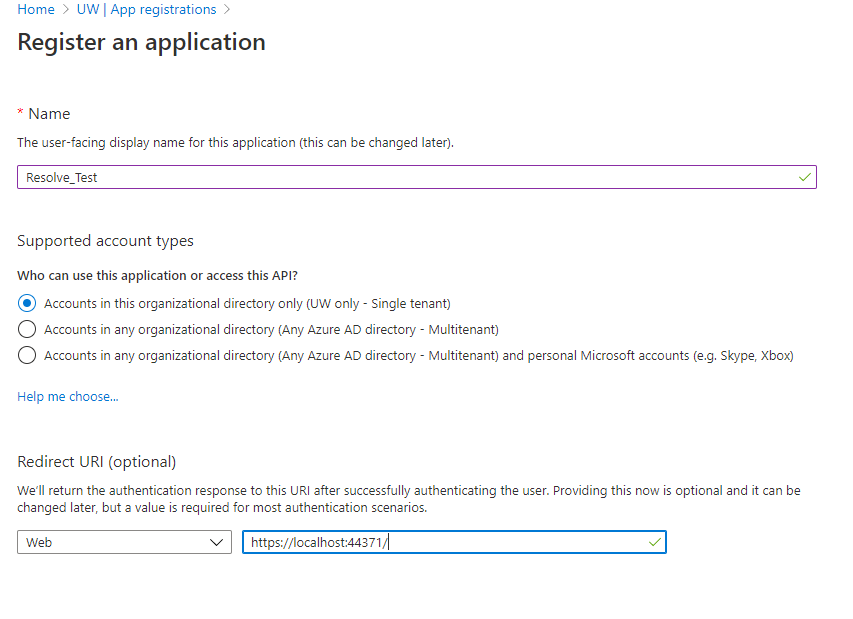
Step3: Go to App Registrations



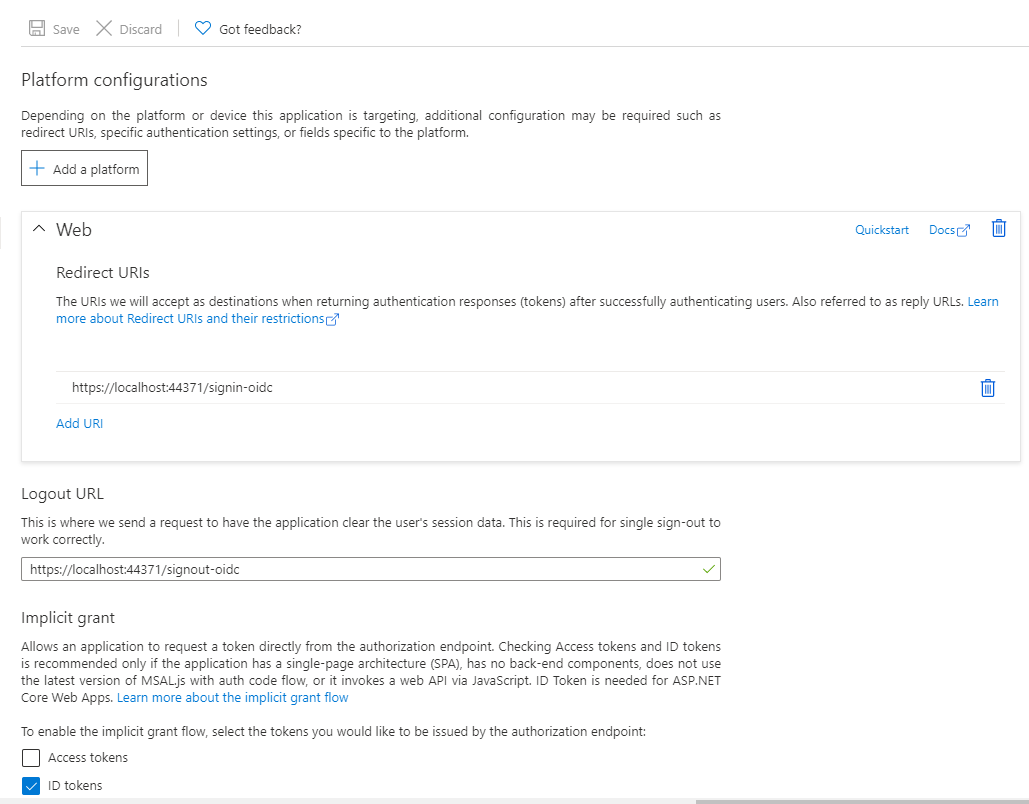
Step4: Click New registration



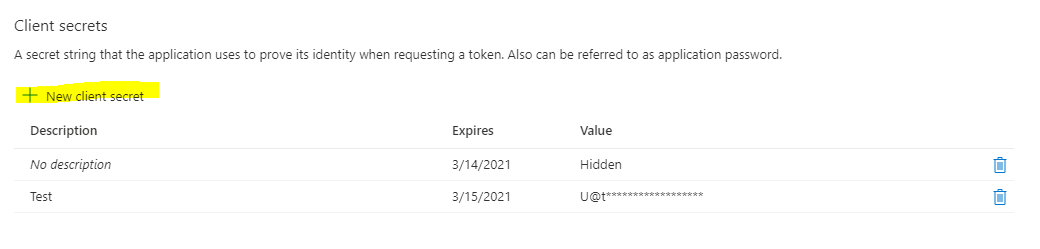
Step5:



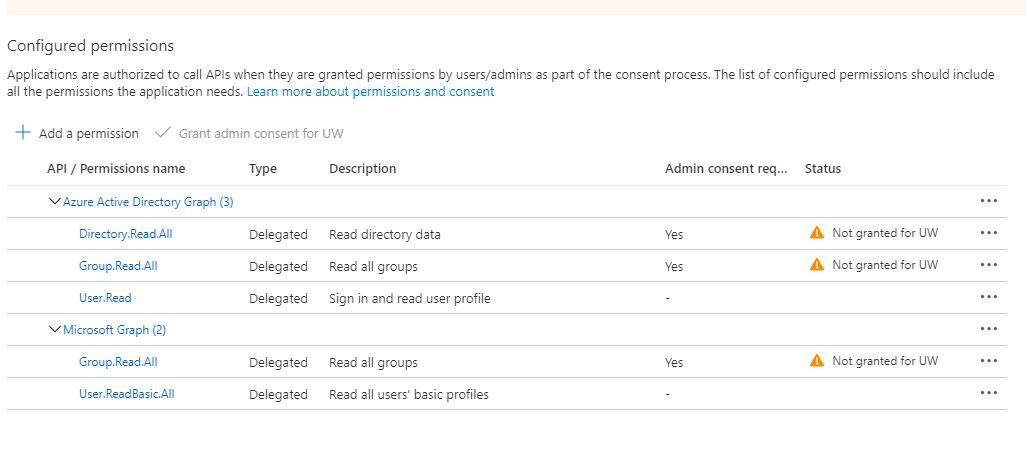
Step6: Go to Authentication and configure URL’s as shown below (According to hostname applicable)



Step7: Create a new client secret (note it down, will not be able to retrieve later)



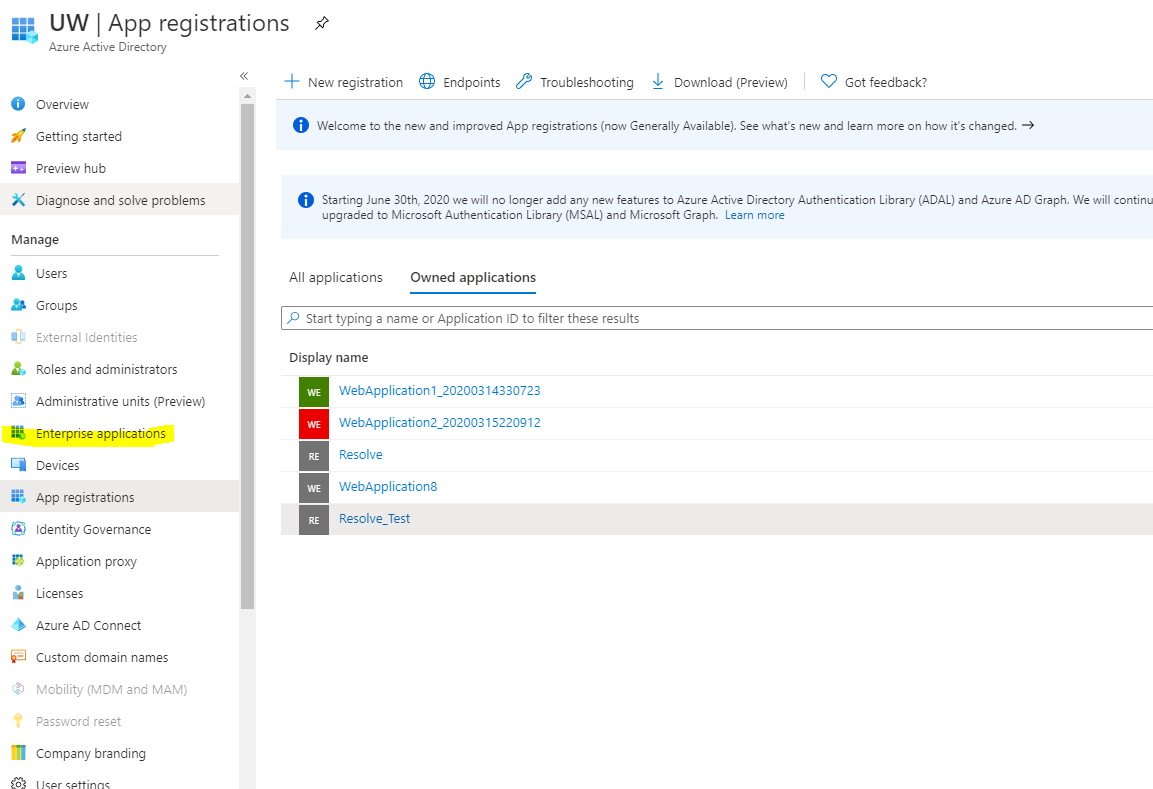
Step8: API Permissions



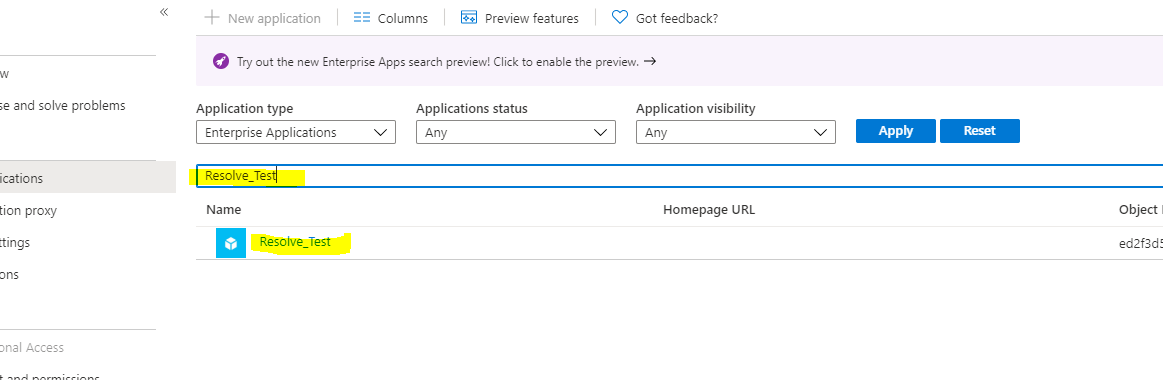
Step9: Modify the Manifest



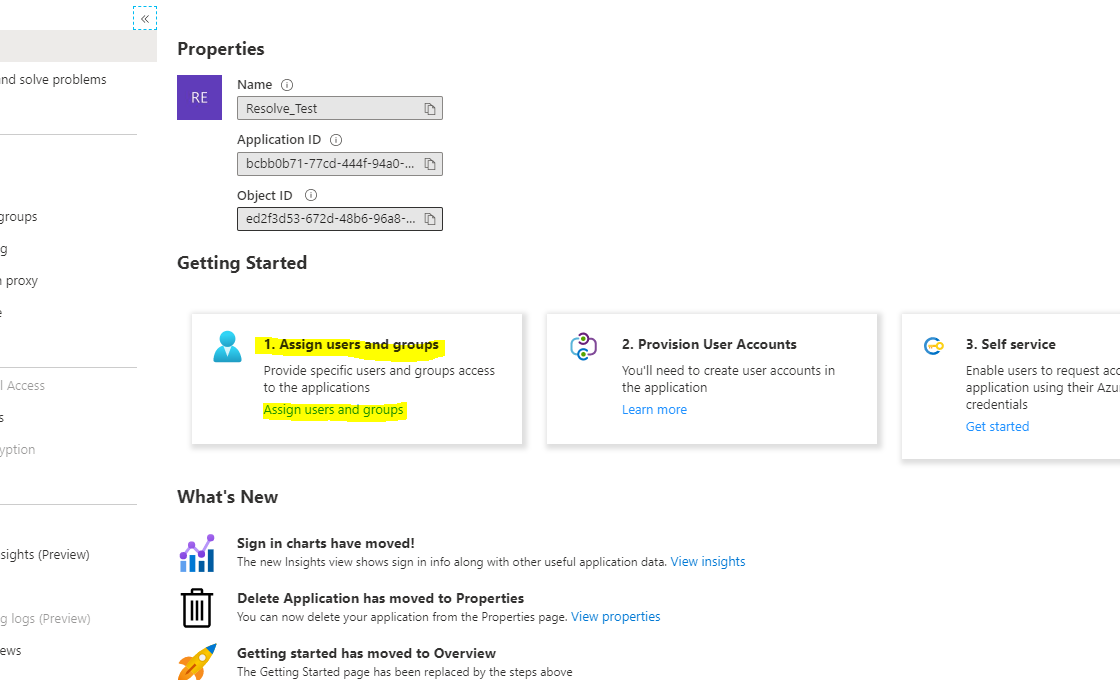
Step9: Now add the associated groups to the application by going to Enterprise Applications



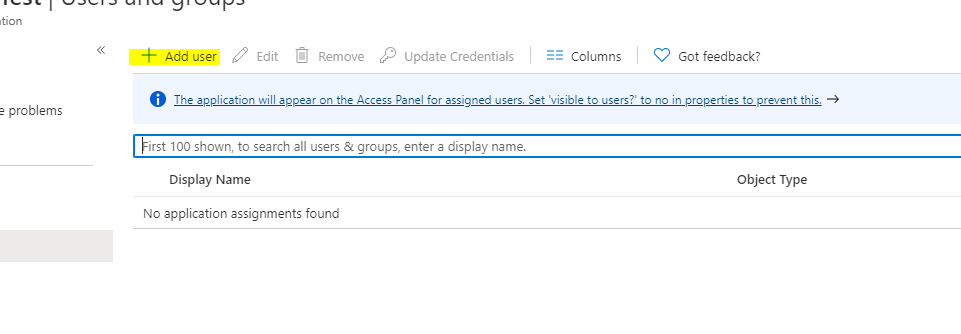
Step10: Search for your Application



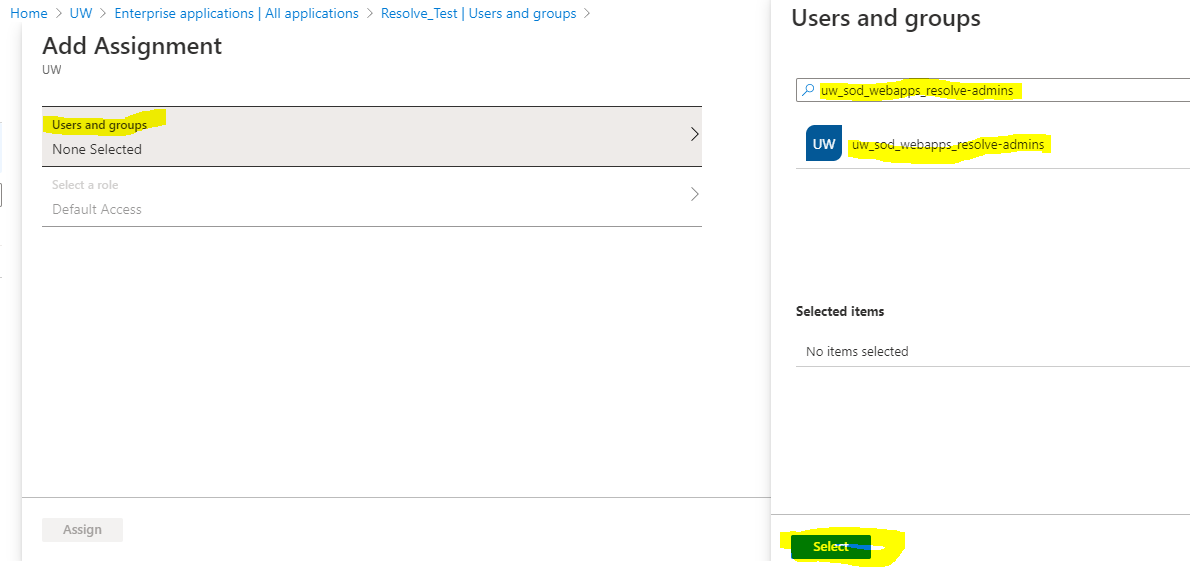
Step11: Assign Users and Groups



Step12: Add User



Step 13: Add the group



Step 14: Add all other groups relevant to Resolve at this place in Azure Portal

Step 15: Now use all the above details and fill in the appsettings.json file for your application as shown below

{

"AzureAd": {

"Instance": "https://login.microsoftonline.com/",

"Domain": "cloud.washington.edu",

"TenantId": "f6b6dd5b-f02f-441a-99a0-162ac5060bd2",

"ClientId": "0f6bc5f5-5dfb-43aa-93b5-6bc621f3d5f6",

"CallbackPath": "/signin-oidc",

"ClientSecret": "U@t3rA4h:\_8E[esK6aNXqs=.\_prSp@@E"

},

"Logging": {

"LogLevel": {

"Default": "Information",

"Microsoft": "Warning",

"Microsoft.Hosting.Lifetime": "Information"

}

},

"Smtp": {

"FromAddress": "sodforms@uw.edu",

"Server": "smtp.washington.edu",

"Password": "JAc@7H&C&+",

"Port": 587

},

"Launch": {

"Host\_Name": "localhost",

"Host\_Port": 44371

//"Host\_Name": "devapps.dental.uw.edu",

//"Host\_Port": 443

},

"AllowedHosts": "\*",

"GraphApiUrl": "https://graph.microsoft.com/beta",

"ConnectionStrings": {

//"ResolveContext": "Server=sod-d-sql-001.dental.uw.edu;Database=ResolveV1;Trusted\_Connection=True;MultipleActiveResultSets=true",

"ResolveContext": "Server=.\\SQLExpress;Database=ResolveV2;Trusted\_Connection=True;MultipleActiveResultSets=true"

}

}

With these steps your app should be ready to authenticate and integrate Azure AD into your .Net Core App.

# Initial Onboarding of Users

There are 2 ways through which users can sign up for Resolve. Both ways are described down below.

## Sign up through first login

A user can login to Resolve, provided they have a UW NetID account, and their profile will be created automatically. The admin needs to ensure that the user has already been added to the right groups on <https://groups.uw.edu/> before their first login, or else the user will need to visit their home page again for the group memberships to take effect.

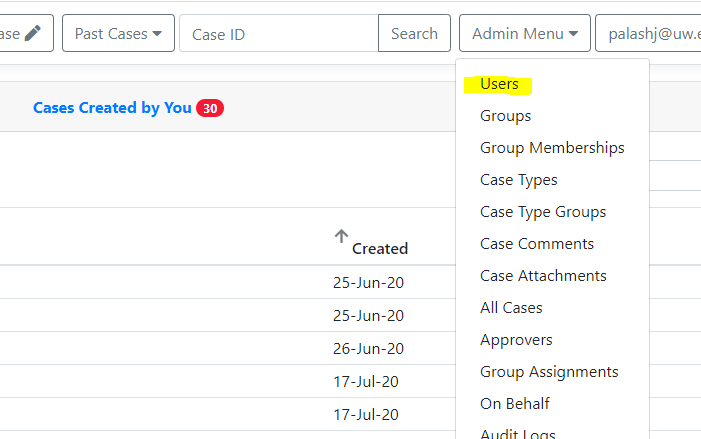
How this works at the backend?

Whenever a user logs in, or visits homepage of Resolve, their group membership claims are retrieved from Azure AD and mapped/synced to the local database. So, if a user belongs to 3 groups relevant to Resolve, which are already added to LocalGroup entity and Azure AD for Resolve enterprise app, the group membership will show up automatically under *‘Group Memberships’* menu for the admins. If the user is removed from one of the groups at a later point in time, the group membership at Resolve would also change, once the user logs in or visits the homepage again. In conclusion, before an admin sends an invite to a new user to login to Resolve, the user ideally should be added to all relevant groups beforehand.

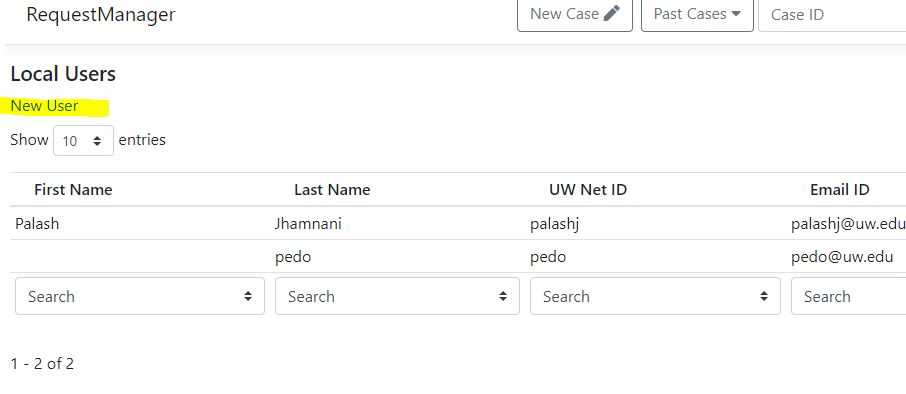
## Sign up by admin

Second way to add a user for the workflows to begin is through an admin. An admin can follow below steps to add a user:

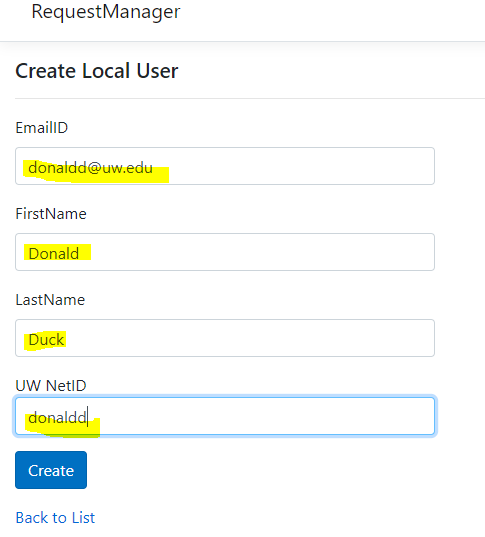
Step 1: Login as an Admin and go to “Users” section



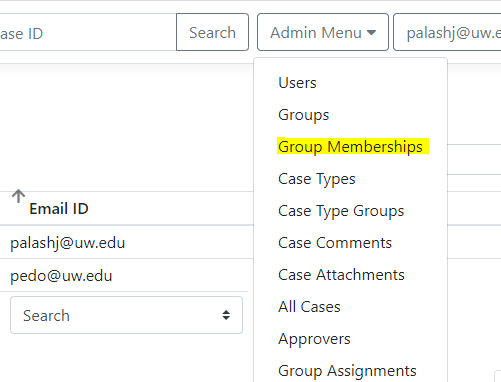
Step 2: Create new user



Step 3: Fill all 4 values are shown and hit create



Step 4: Then go to “Group Memberships”



Step 5: Manually add memberships for the new user for existing groups on Resolve. Keep in mind that the user must belong to those groups on <https://groups.uw.edu/>, otherwise the memberships will be deleted when the user logs in to Resolve.