Azure Active Directory Single Sign On (SSO) Configuration

Introduction

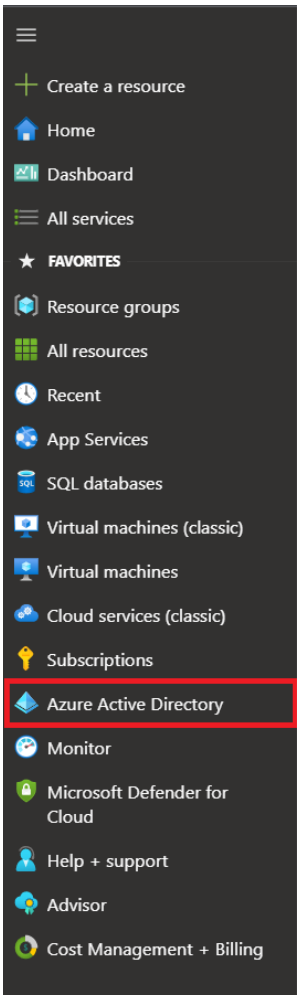
This document will help you register a new application for Azure Active Directory and connect your users with Certainty Software applications.

Register a new application

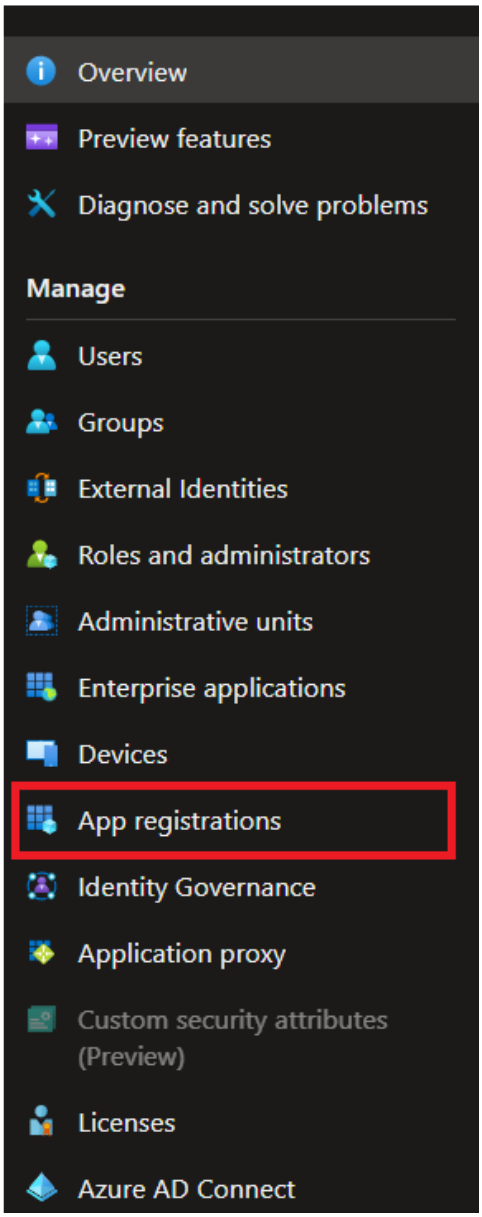
In this section, you will have to register the Certainty authorization server within your Azure Active Directory.

First, go to https://portal.azure.com, your account must have admin rights for managing Azure Active Directory.

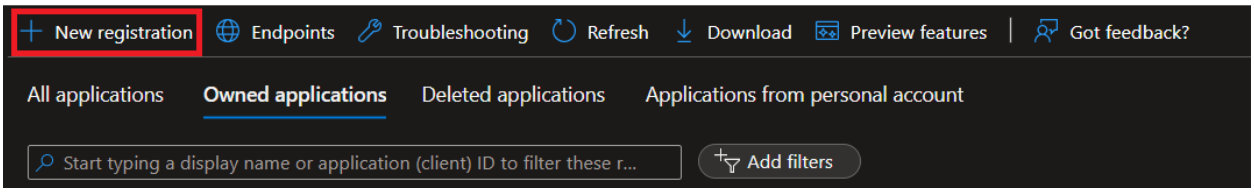
You can access Azure Active Directory from the left menu. Another option is to use the search box, enter 'Azure Active Directory', and select the first result.



You will be redirected to a new page. To register a new app, click ‘App registration’ under Manage.



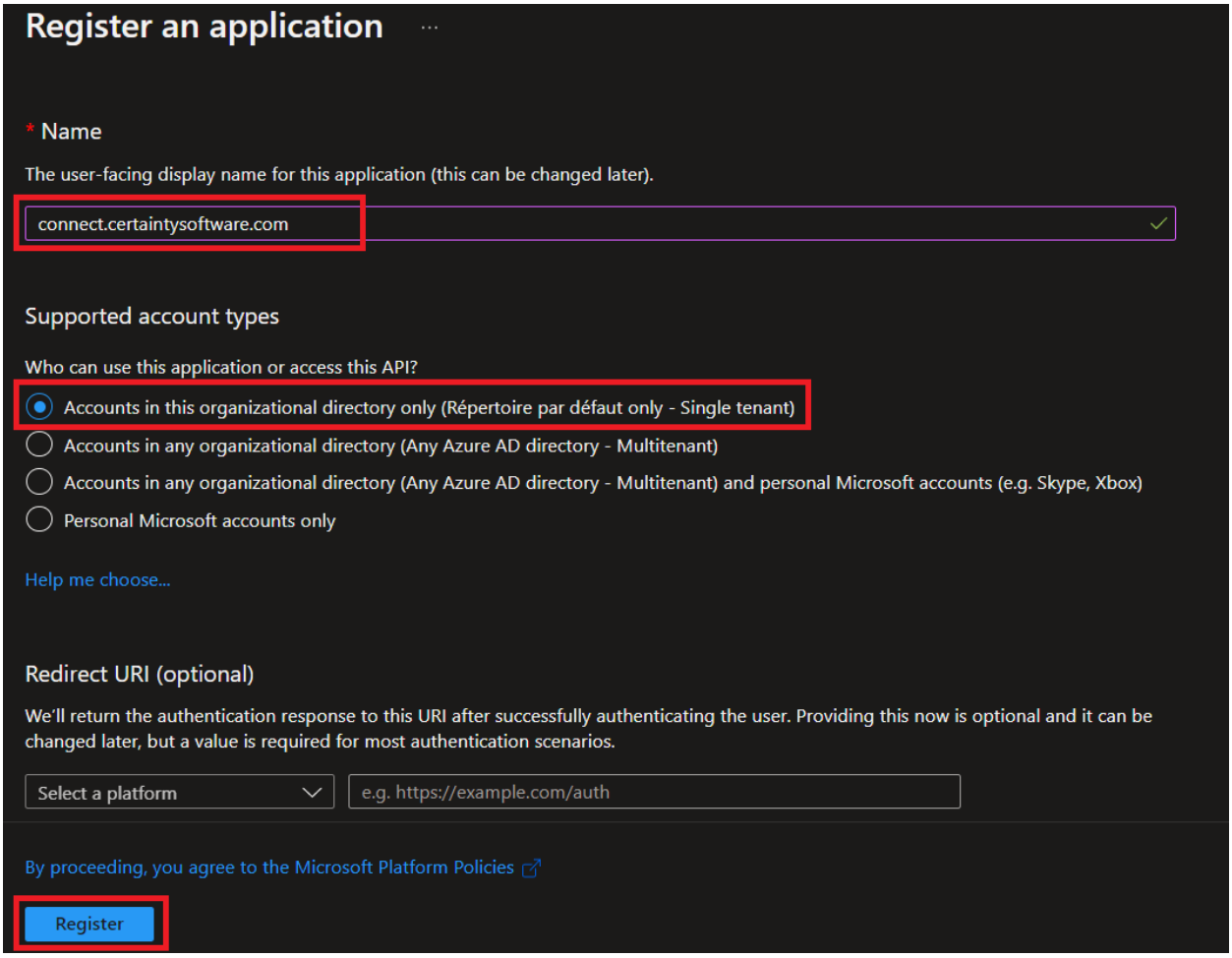
Click the “New registration” button.



In the “Register an application” form, enter “connect.certaintysoftware.com”.

In the supported account types, select “Account in this organizational directory only” if you have one tenant. If you have multiple tenants, you can select the second option ‘Accounts in any organizational directory’.

For this document, we will use the first option.

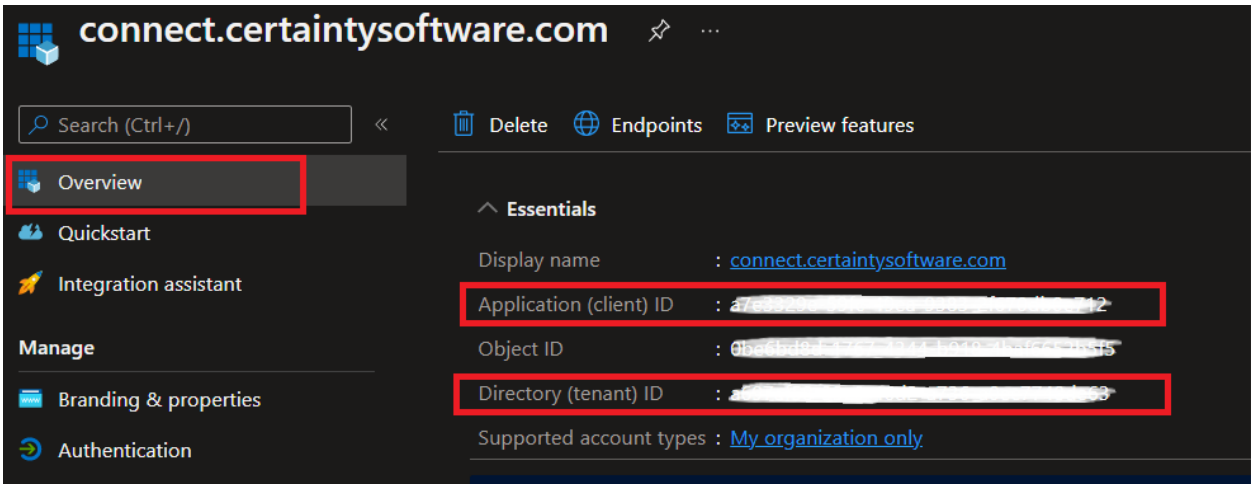


Click the “Register” button.

Redirect URI (optional) will be configured later in this document.

Please note your application (client) ID and Directory (tenant) ID. You will have to share both with the Certainty Software Team to log into the portal and mobile app.

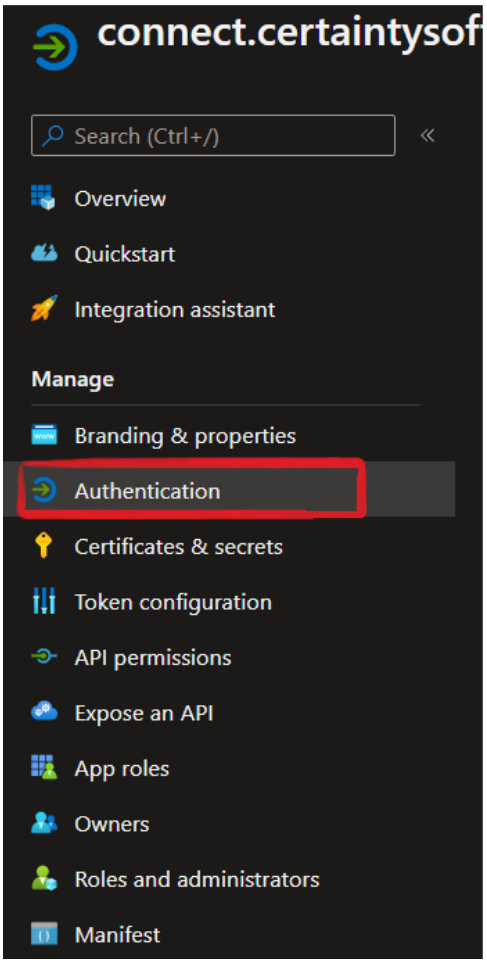
The application ID will also be used when running the PowerShell script for adding job title in the list of claims.



Remember to Copy the Application (client) ID. It will be used later.

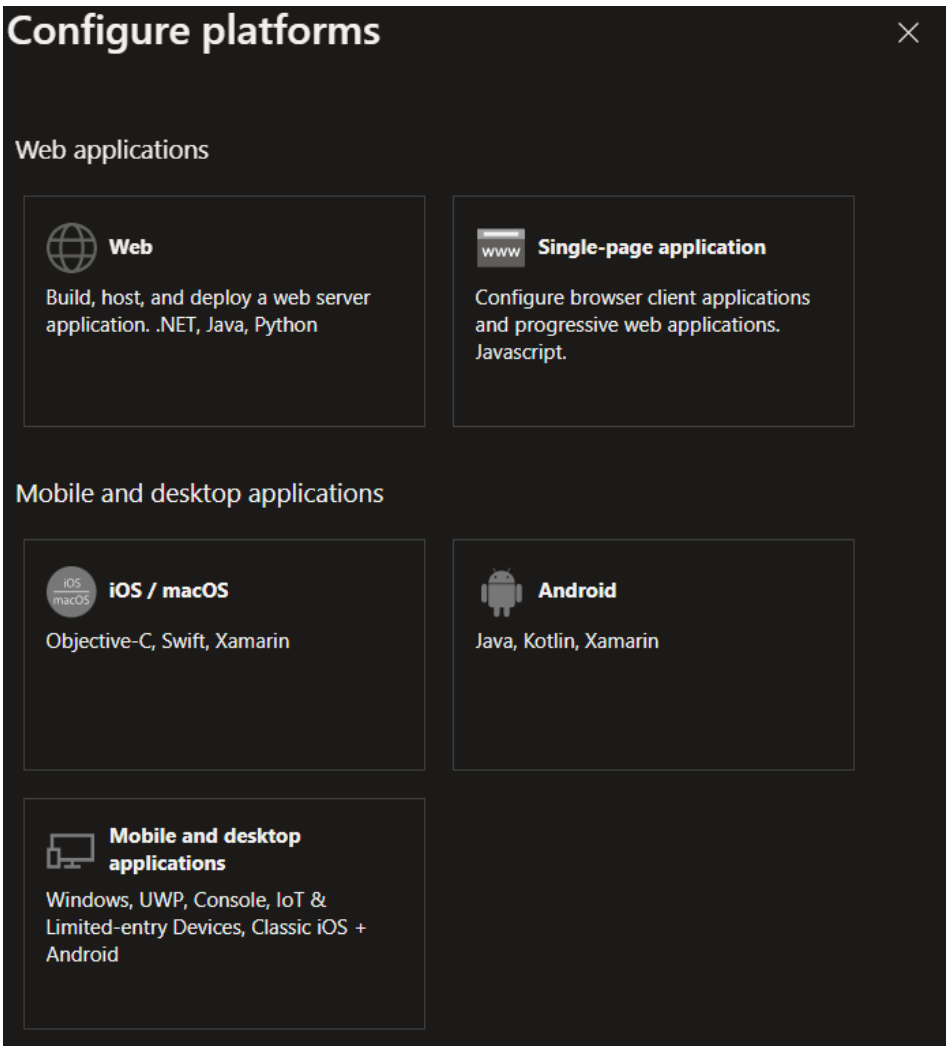
Authentication

To manage redirect URIs, logout URIs, and flows, click the “Authentication” link in the “Manage” section.



Platform configurations

Click the “Add a platform” button and select “Web”.



Enter https://connect.certaintysoftware.com/[CLIENT_INSTANCE]/signin-oidc in the redirect URI of the application and click “Configure”.

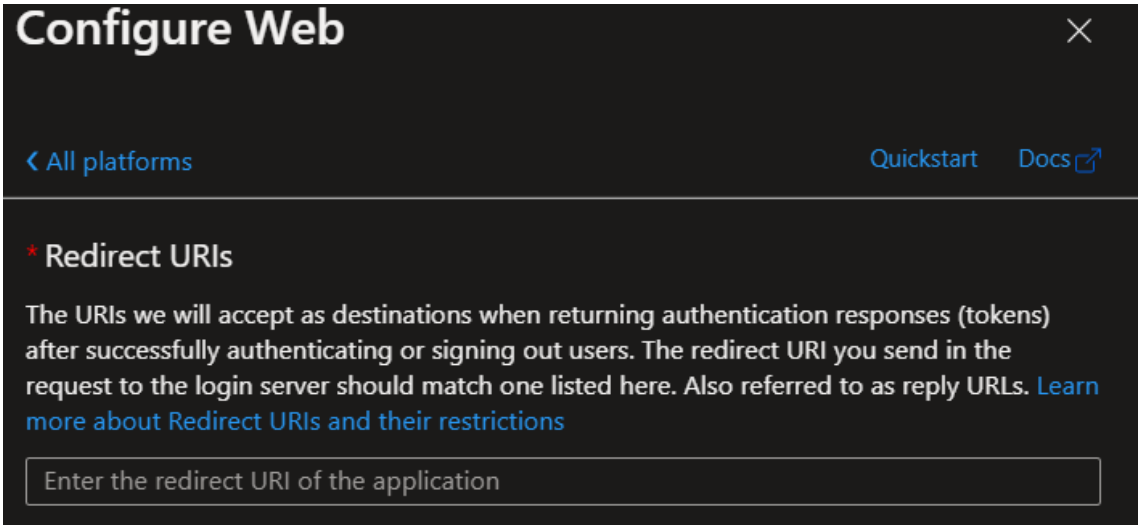
The client instance should be the subdomain used with your Certainty Software applications.

For example:

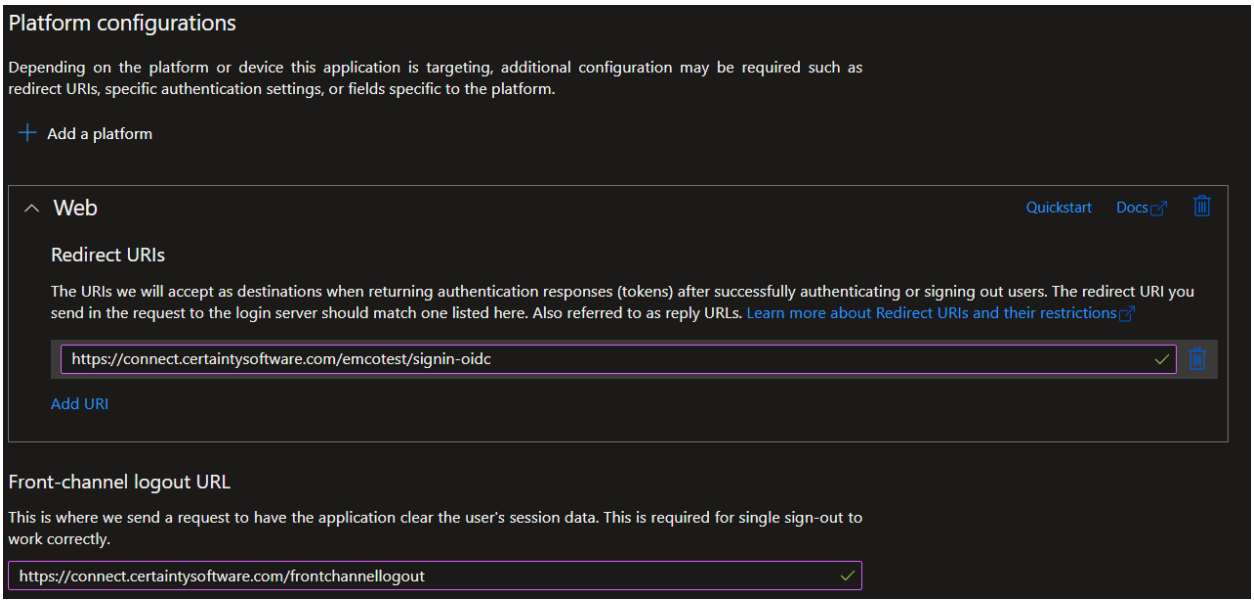
https://demo.certaintysoftware.com

https://demo.checkitsoftware.com

The CLIENT_INSTANCE is demo.

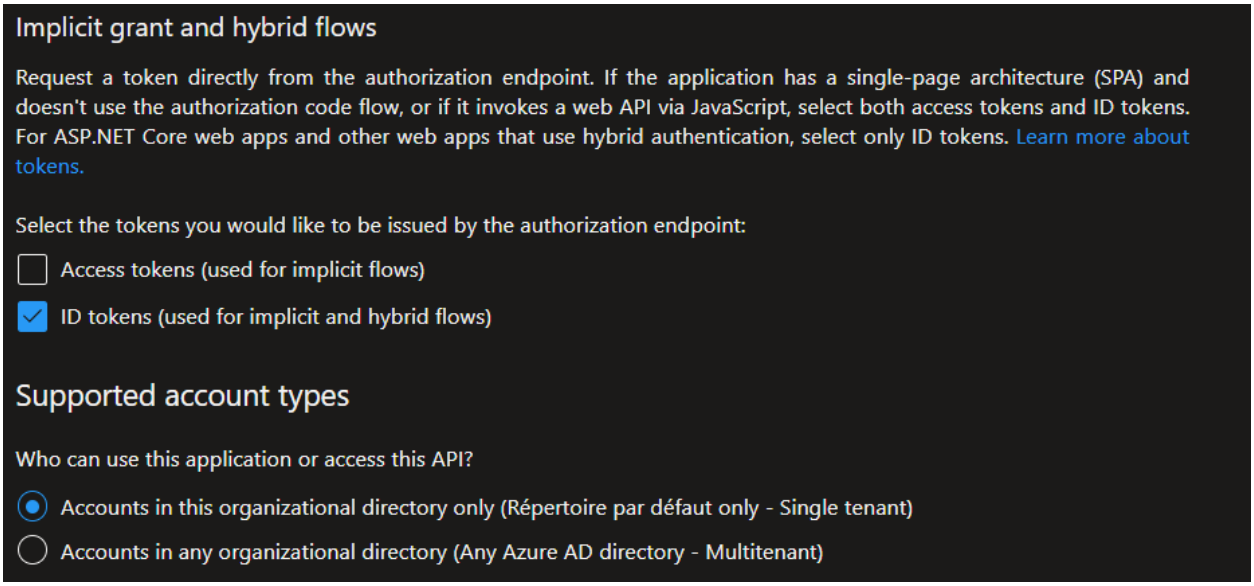


In the “Front-channel logout URL”, enter: https://connect.certaintysoftware.com/frontchannellogout.



Implicit grant and hybrid flows

In the “Implicit grant and hybrid flows”, select “ID tokens (used for implicit and hybrid flows)”.



The ID Token will be sent to the Certainty Authorization Server, it will include some information about the connected user, such as full name, email address, job title, etc.

In the supported account types, leave the first option selected (if you selected multitenant in the register an application form, the second option will be selected).

To validate your changes, click “Save”.

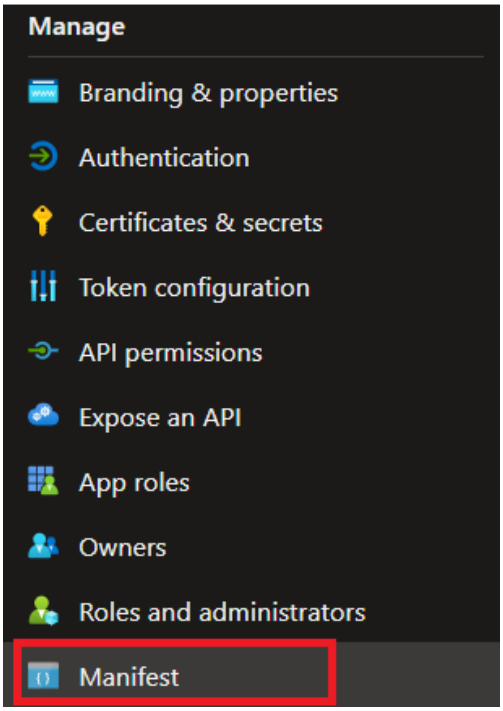
Manifest file

This step is only required if user provisioning is activated when using SSO.

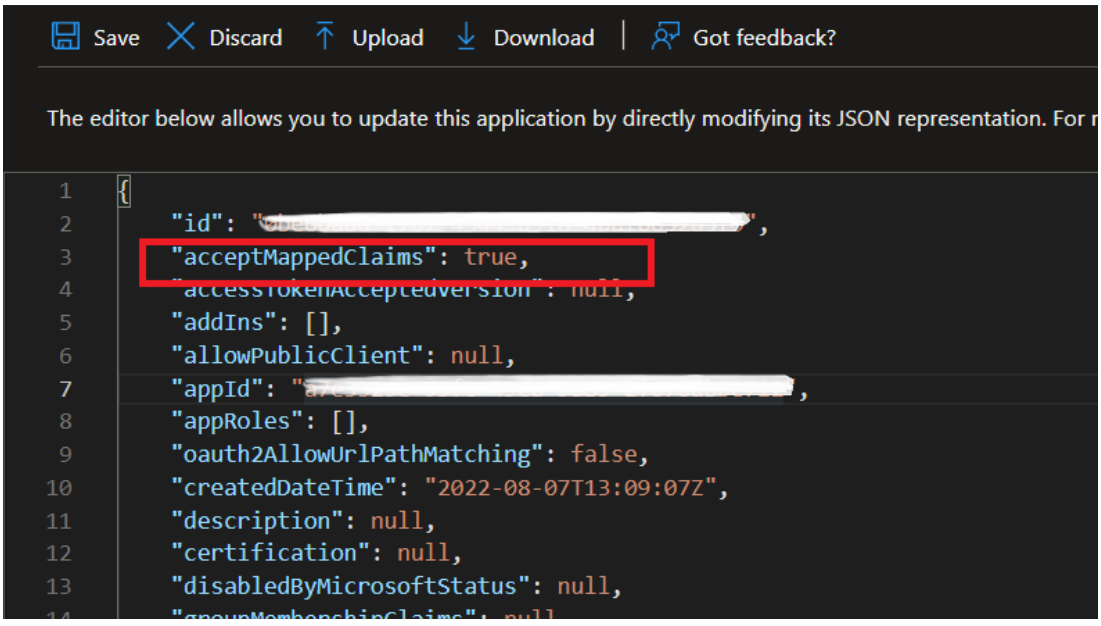
User provisioning allows assigning certain roles and role groups based on the “Job Title” setup for users in Azure. Certainty Software can require a mapping document to initialize automatic provisioning.

Clients can also request assigning sites automatically based on specific user property on Azure.

The last step is to update the “Manifest” file, to access the online editor, click “Manifest” under “Manage”.



In row #3, you will find acceptMappedClaims property that has the value “null”. Change it to ‘true’ and click the “Save” button.



Registering an application is now complete.

Adding Job Title and Department claims

By default, the job title and department are not included in the ID token sent to the authorization server. In this section, you will add the user's job title and their department so Certainty systems can assign roles based on job titles using a predefined mapping.

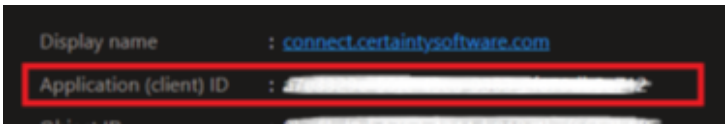
To add the job title in the list of claims, you will have to create a new Azure AD Policy.

For that, you will need to run the PowerShell script below (this script can be saved on local hard drive for easy access).

Please select the object below, copy and then paste it to a folder for the file to be available.

add_job_title_and_de
partment_policy_to_az

Once stored locally, open the script with a notepad and change the Application ID variable with the one found in the overview page of app registration.



We are using Version 3 of the script; it adds both job title and department claims to the ID Token. The job title will be mapped in the Certainty app to the role group and department to the site.

Before running the script, you must change the Application ID, you can get the ID from the App registration overview page, and you can also change the policy name to whatever you want.

```
$claimsMappingPolicy = [ordered]@{
  "ClaimsMappingPolicy" = [ordered]@{
    "Version" = 1
    "IncludeBasicClaimSet" = $true
    "ClaimsSchema" = @(
      [ordered]@{
        "Source" = "user"
        "ID" = "JobTitle"
        "JwtClaimType" = "job_title"
      },
       [ordered]@{
```

```
            "Source" = "user"
            "ID" = "Department"
            "JwtClaimType" = "department"
        }
    )
  }
}


$appID = "[YOUR_APPLICATION_ID8GOES_HERE]"
$policyName = "JobTitleClaimMappingPolicy"

$sp = Get-AzureADServicePrincipal -Filter "servicePrincipalNames/any(n: n eq '$appID')"

$existingPolicies = Get-AzureADServicePrincipalPolicy -Id $sp.ObjectId `
                | Where-Object { $_.Type -eq "ClaimsMappingPolicy" }
if ($existingPolicies) {
  $existingPolicies | Remove-AzureADPolicy
}

$policyDefinition = $claimsMappingPolicy | ConvertTo-Json -Depth 99 -Compress
$policy = New-AzureADPolicy -Type "ClaimsMappingPolicy" -DisplayName $policyName -
Definition $policyDefinition

Add-AzureADServicePrincipalPolicy -Id $sp.ObjectId -RefObjectId $policy.Id
Write-Output ("New claims mapping policy '{0}' set for app '{1}'." -f $policy.DisplayName,
$sp.DisplayName)
```

In order to run this PowerShell script, you will have to connect to your Azure Active Directory in a terminal. Use the terminal window at the bottom of “Windows PowerShell ISE” that runs in admin mode.

```
PS C:\> AzureADPreview\Connect-AzureAD
```

IF YOU GET AN ERROR:

If the above does not work and you receive an error such as:

```
Get-AzureADServicePrincipal : The term ‘Get-AzureADServicePrincipal’ is not recognized
as the name of a cmdlet, function, script file, or operable program. Check the spelling of
the name, or if a path was included, verify that the path is correct and try again.
```

Run this command in the terminal:

```
PS C:\> Install-Module AzureADPreview
```

You may be asked to install a nugget. If so, click “yes for all” when prompted and then Import.

```
PS C:\> Import-Module AzureeADPreview
```

Try now to run this command:

```
C:\> Get-AzureADPolicy
```

This command allows you to enter your username (email) and password.

Once connected, go the script directory and run the ps1 file. Or just click > (Run) in PowerShell ISE.

```
C:\> cd c:\script_folder
C:\script_folder> .\ add_job_title_and_department_policy_to_azure_ad_v3.ps1
```

To check if the policy has been created, run the script below:

```
C:\> Get-AzureADPolicy
```

Please remember to forward the Application (Client ID) and Directory (Tenant) ID to Certainty Software.

If you need any help, don’t hesitate to contact us directly at support@certaintysoftware.com