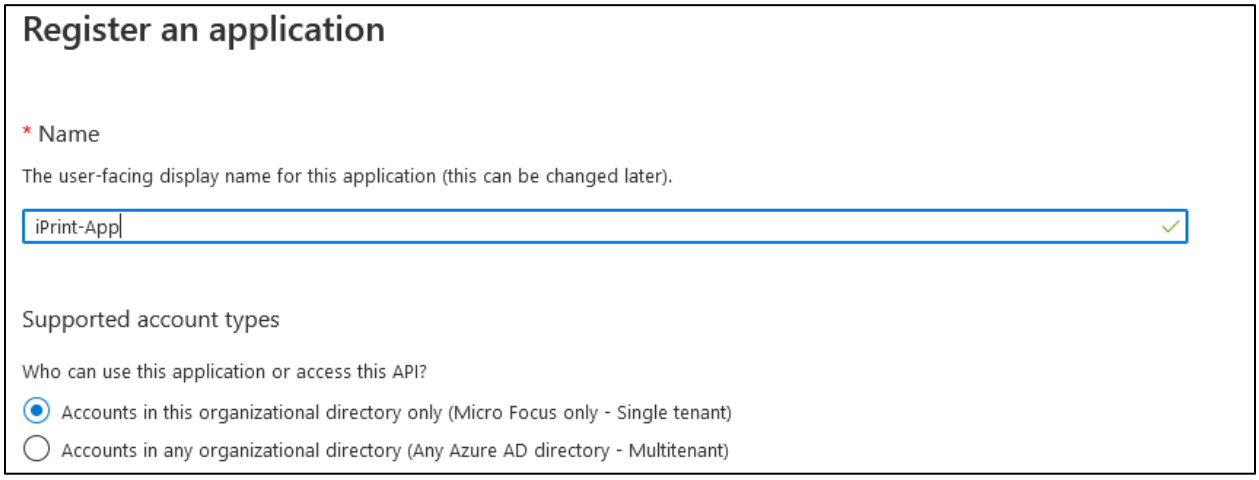
Micro Focus iPrint – Microsoft Azure Active Directory Integration

Overview:

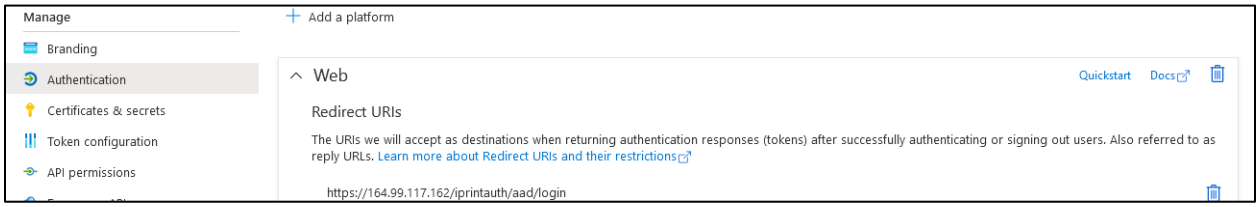
iPrint users can now be authenticated by using Microsoft Identity platform for secure iPrint printers. This functionality is available with Desktop printing, QuickPrint, and Release Portal. The iPrint server performs the authorization of the printers for the users.

Pre-Requisites: Register an Application for iPrint on the Microsoft AzureAD portal using the steps outlined below:

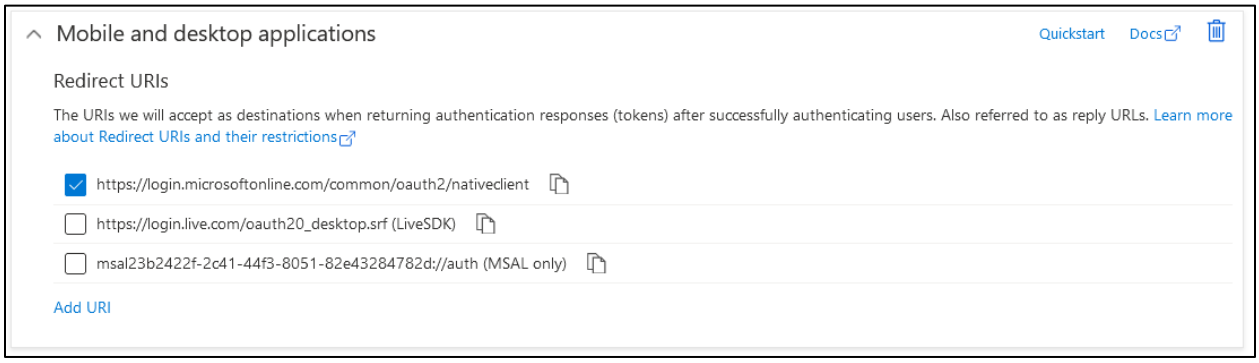
Step 1: Login to the Microsoft AzureAD portal and register an Application for iPrint.



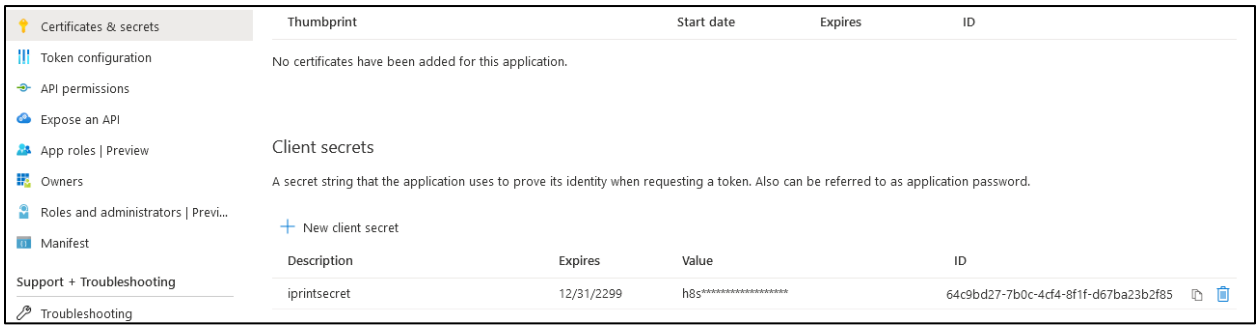
Step 2: Add your server uri in the "Authentication section" in the format of "*https://<ip-address-or-fqdn-of-iPrint-server>//iprintauth/aad/login*"



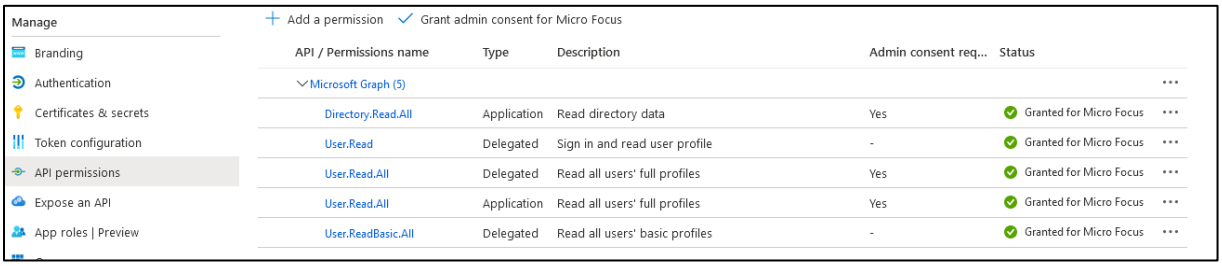
Step 3: Select the nativeclient uri under the Mobile and desktop applications of “Authentication Section” as shown below:



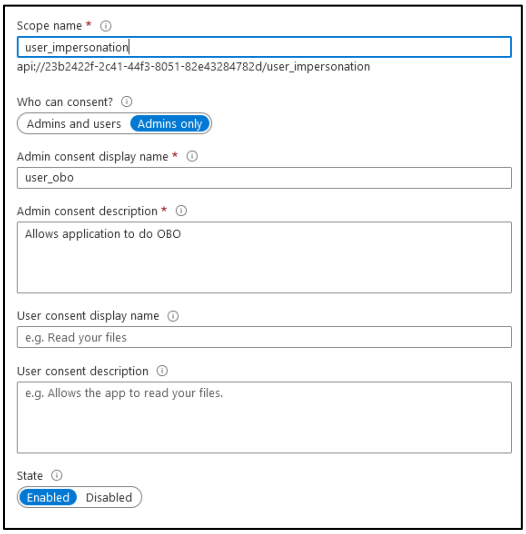
Step 4: Create a new Client Secret in the “Certificates & secrets” section and securely save a copy of it immediately after creation since it would not be readable later on.



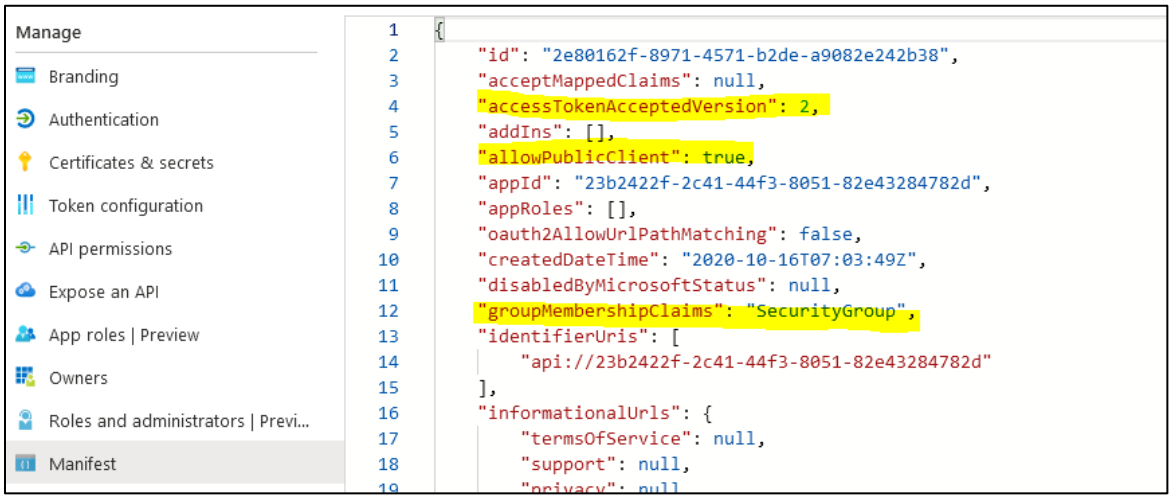
Step 5: Configure the API permissions as listed below and “Grant Admin Consent” for all the permissions in the “API Permission” section.



Step 5: Configure the API Scope in the "Expose an API" section by adding a new scope with the following details:



Step 6: Configure/Update the highlighted attribute-value pairs in the "Manifest" section:



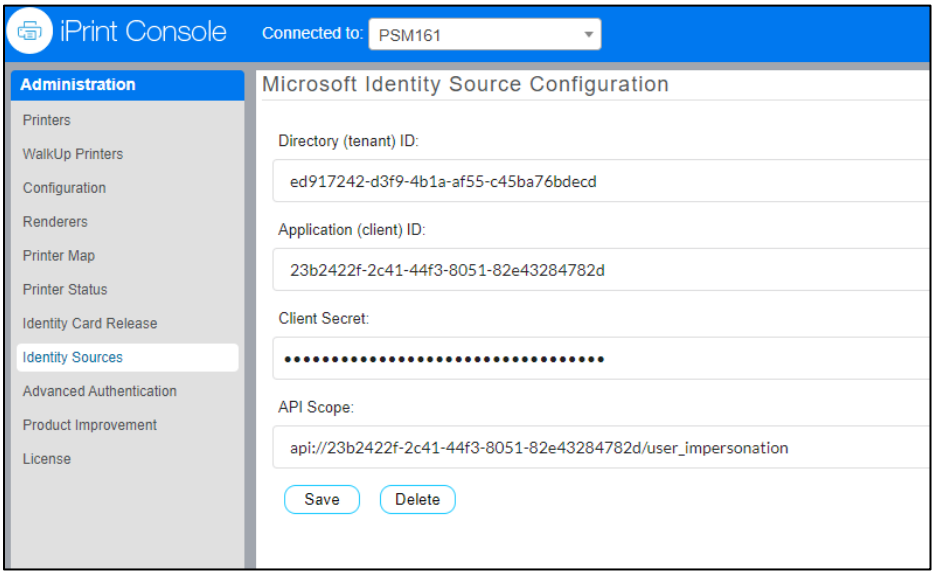
Step 7: Capture the following attributes from the application registered (sample values listed below):

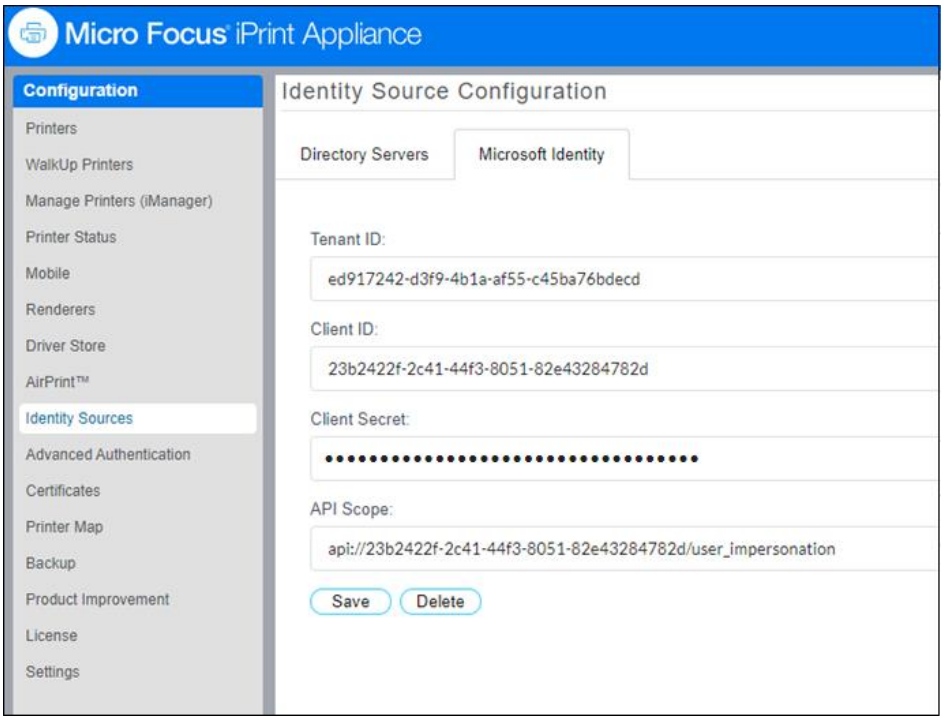
- **Directory (tenant) ID:** ed917242-d3f9-4b1a-af55-c45ba76bdecd
- **Application (client) ID:** 23b2422f-2c41-44f3-8051-82e43284782d
- **Client Secret:** a8s_FBZI1KOiDBFej_Etr
- **API Scope**: api://23b2422f-2c41-44f3-8051-82e43284782d/user_impersonation

Step 8: Create a Group by name "**IPRINT_ACCESS_GROUP**" and add the required AzureAD Users / Groups as members.

iPrint Server Configuration:

Configure the AzureAD Application details (from Step 7) on iPrint Advanced / iPrint Appliance using the Management Console:

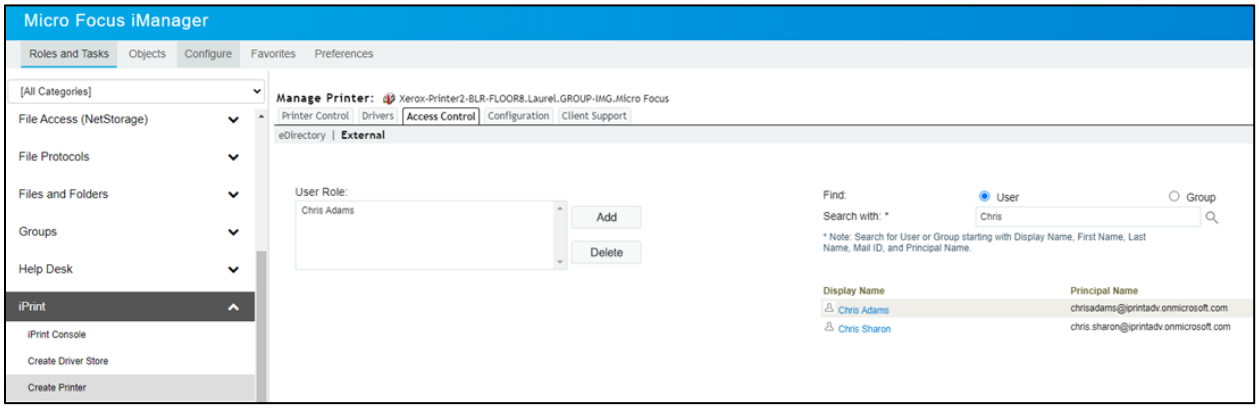




Configuring Printer ACLs:

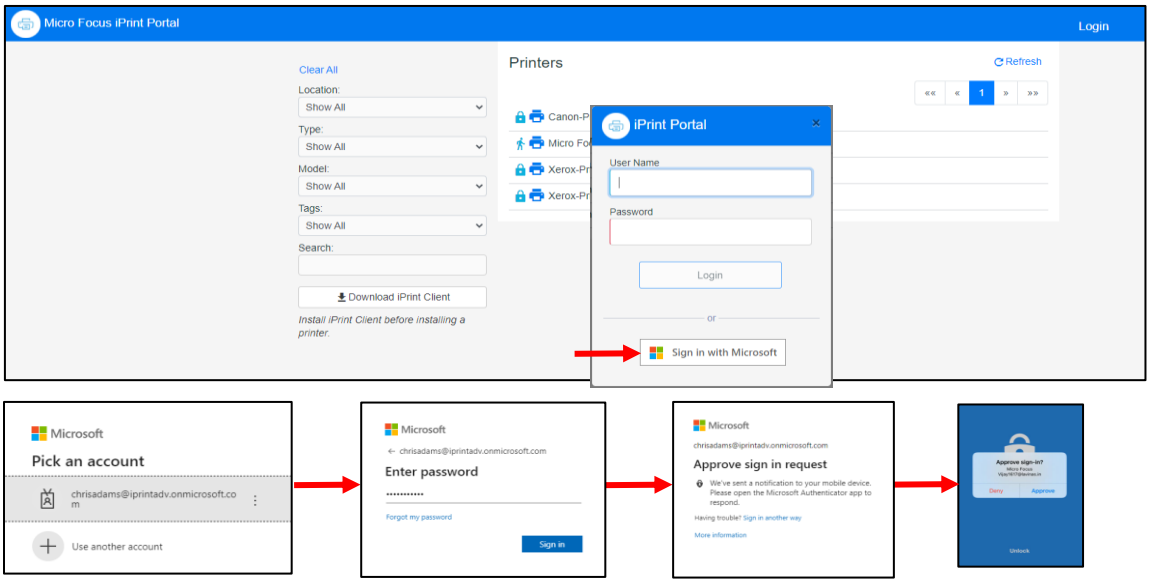
Create a new Secure Printer or Configure an existing with the required ACLs by adding the AzureAD users or groups using iManager:

i. Navigate to the iPrint section of iManager and “Manage Printer”.
ii. Select a Secure Printer and navigate to Access Control tab.
iii. Click External tab and click Add.
iv. Select the “User” option and enter the search criteria, for instance, the first name of the user.
v. Once the user(s) is displayed in the search results, click on the user’s hyperlink.
vi. Add the required user(s) and/or group(s) and save the changes to the Printer ACL using OK/Apply.



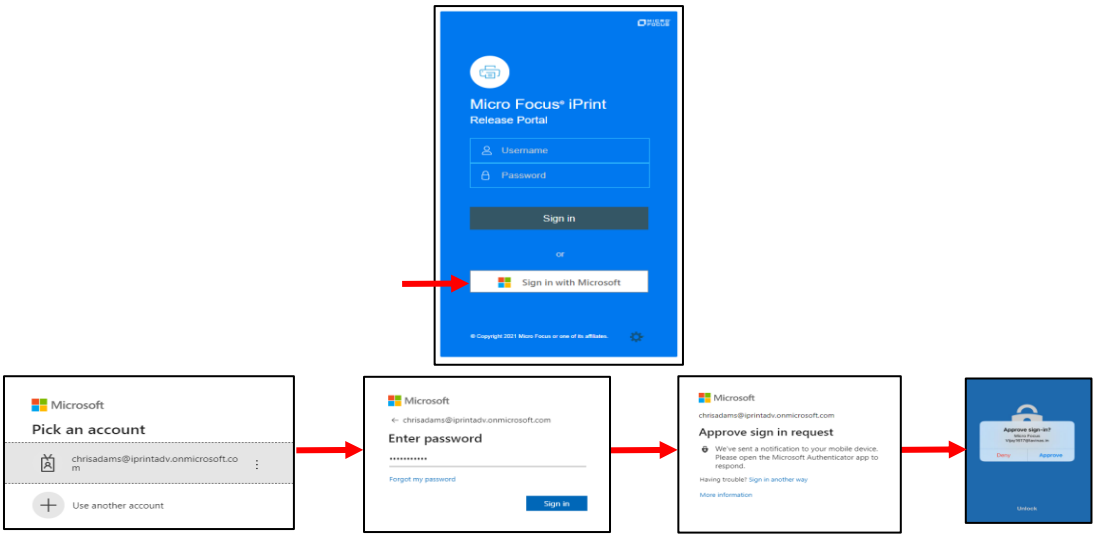
Print Operations Using Print Portal:

Login to the Print Portal using the AzureAD user and submit a Quick Print job to the authorized secure printer.



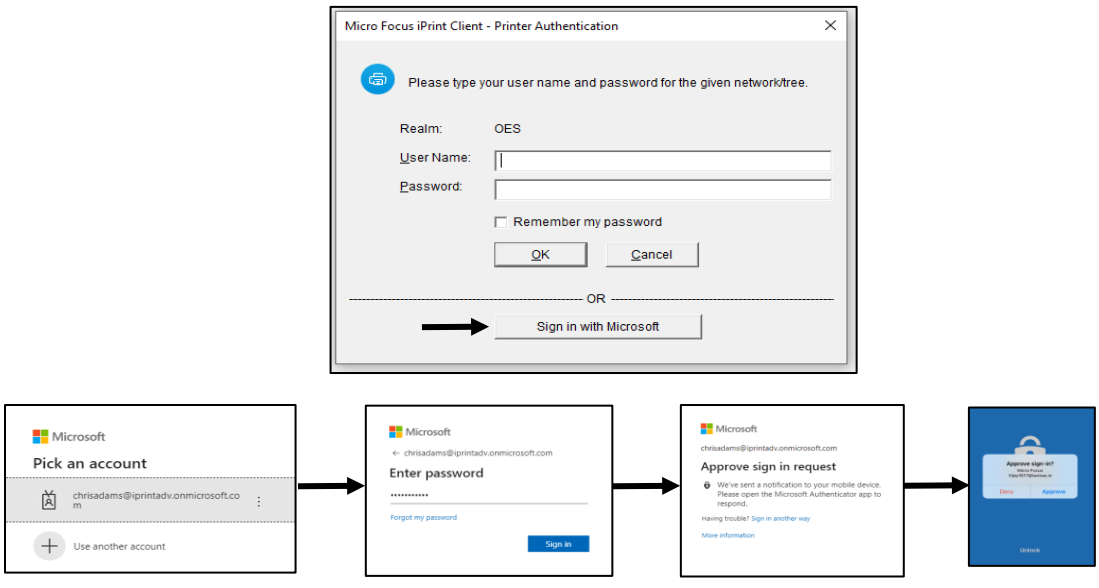
Print Operations using Release Portal:

Login to the Release Portal using the AzureAD user and release an existing Print job in the queue to an authorized secure printer.



Printer Installation and Print Operations Using Windows Desktop Client:

Login to the Print Portal using the AzureAD user and select a secure printer for installation. “Sign in with Microsoft” and provide the AzureAD user credentials while installing the printer.



Printer Installation and Print Operations Using Windows iPrint Lite Client:

Right click on a supported file in the File Explorer and click on iPrint option. “Sign in with Microsoft” and provide the AzureAD user credentials for submitting the print jobs to the authorized printer(s).