

# 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.

**Register an application**

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

iPrint-App ✓

Supported account types

Who can use this application or access this API?

Accounts in this organizational directory only (Micro Focus only - Single tenant)

Accounts in any organizational directory (Any Azure AD directory - Multitenant)

**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*”

Manage + Add a platform

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Web

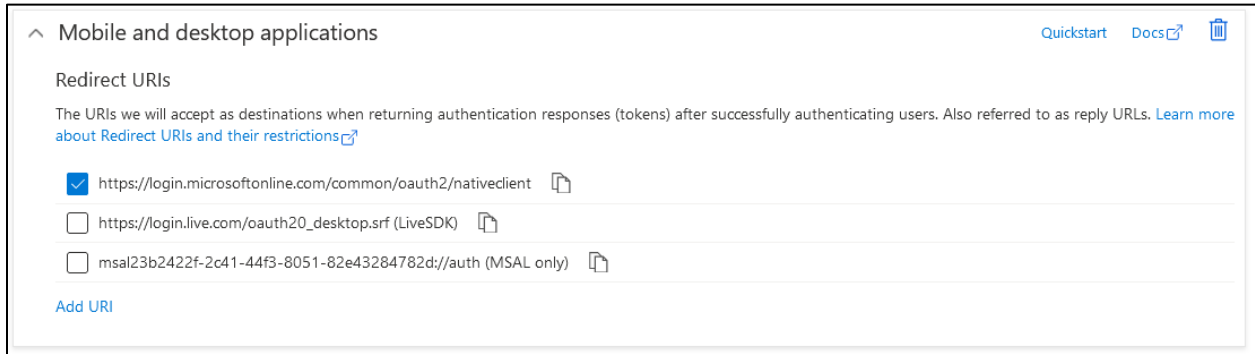
Quickstart Docs

Redirect URIs

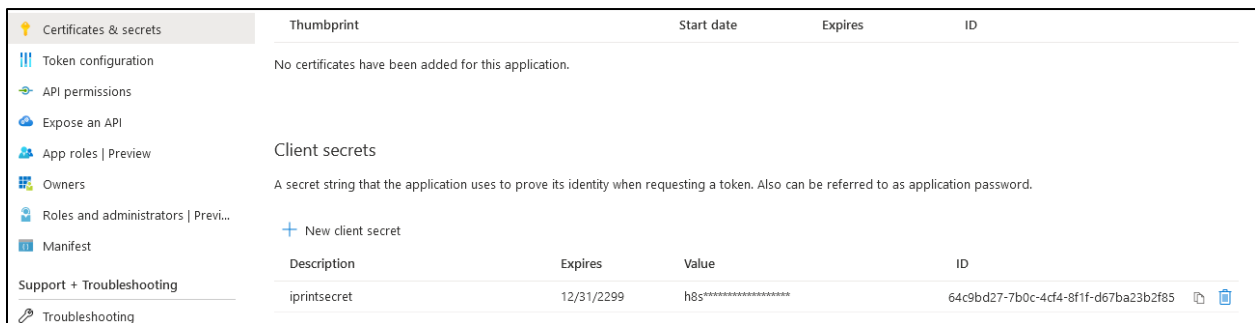
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. Also referred to as reply URLs. [Learn more about Redirect URIs and their restrictions](#)

https://164.99.117.162/iprintauth/aad/login

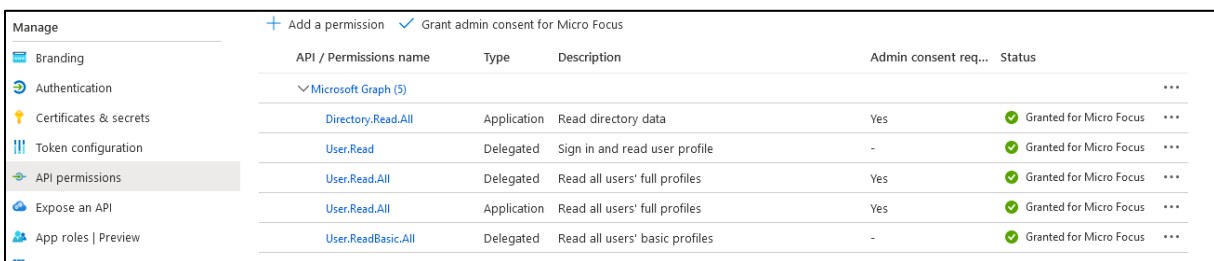
**Step 3:** Select the nativeclient uri under the Mobile and desktop applications of “Authentication Section” as shown below:



**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:

The screenshot shows a configuration form for a new API scope. The fields are as follows:

- Scope name:** user\_impersonation
- Who can consent?:** Admins and users (Admins only is selected)
- Admin consent display name:** user\_obo
- Admin consent description:** Allows application to do OBO
- User consent display name:** e.g. Read your files
- User consent description:** e.g. Allows the app to read your files.
- State:** Enabled

**Step 6:** Configure/Update the highlighted attribute-value pairs in the “Manifest” section:

The screenshot shows the 'Manifest' section in the Azure portal. The JSON configuration is as follows:

```

1  {
2    "id": "2e80162f-8971-4571-b2de-a9082e242b38",
3    "acceptMappedClaims": null,
4    "accessTokenAcceptedVersion": 2,
5    "addIns": [],
6    "allowPublicClient": true,
7    "appId": "23b2422f-2c41-44f3-8051-82e43284782d",
8    "appRoles": [],
9    "oauth2AllowUriPathMatching": false,
10   "createdDateTime": "2020-10-16T07:03:49Z",
11   "disabledByMicrosoftStatus": null,
12   "groupMembershipClaims": "SecurityGroup",
13   "identifierUris": [
14     "api://23b2422f-2c41-44f3-8051-82e43284782d"
15   ],
16   "informationalUrls": {
17     "termsOfService": null,
18     "support": null,
19     "privacy": null

```

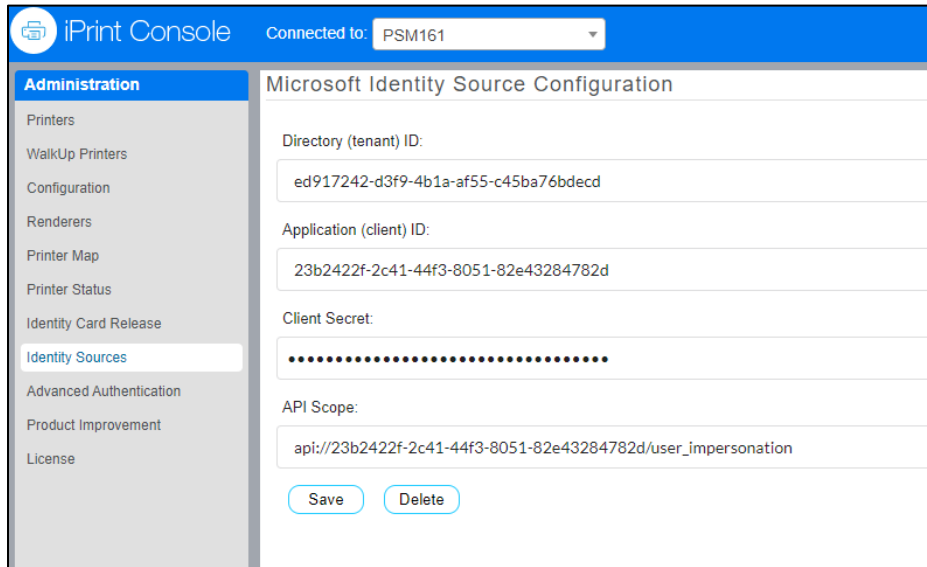
**Step 7:** Capture the following attributes from the application registered (sample values listed below):

- **Directory (tenant) ID:** ed917242-d3f9-4b1a-af55-c45ba76bdecd
- **Application (client) ID:** 23b2422f-2c41-44f3-8051-82e43284782d
- **Client Secret:** a8s\_FBZ11KOiDBFej\_Etr
- **API Scope:** api://23b2422f-2c41-44f3-8051-82e43284782d/user\_impersonation

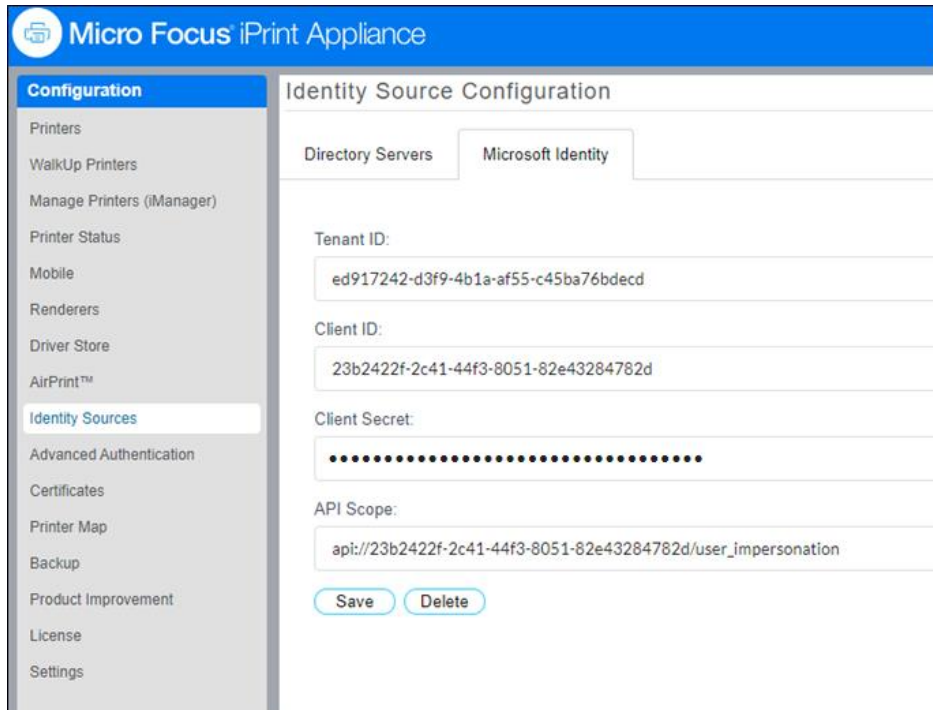
**Step 8:** Create a Group by name “IPRINT\_ACCESS\_GROUP” and add the required AzureAD Users / Groups as members.

## iPrint Server Configuration:

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



The screenshot shows the iPrint Console interface. The top header is blue with the iPrint logo and the text "iPrint Console". To the right of the header, it says "Connected to: PSM161" with a dropdown arrow. On the left, there is a navigation menu under the heading "Administration". The menu items are: Printers, WalkUp Printers, Configuration, Renderers, Printer Map, Printer Status, Identity Card Release, Identity Sources (highlighted in blue), Advanced Authentication, Product Improvement, and License. The main content area is titled "Microsoft Identity Source Configuration". It contains four input fields: "Directory (tenant) ID:" with the value "ed917242-d3f9-4b1a-af55-c45ba76bdecd"; "Application (client) ID:" with the value "23b2422f-2c41-44f3-8051-82e43284782d"; "Client Secret:" with a masked value of 15 dots; and "API Scope:" with the value "api://23b2422f-2c41-44f3-8051-82e43284782d/user\_impersonation". At the bottom of the form are two buttons: "Save" and "Delete".

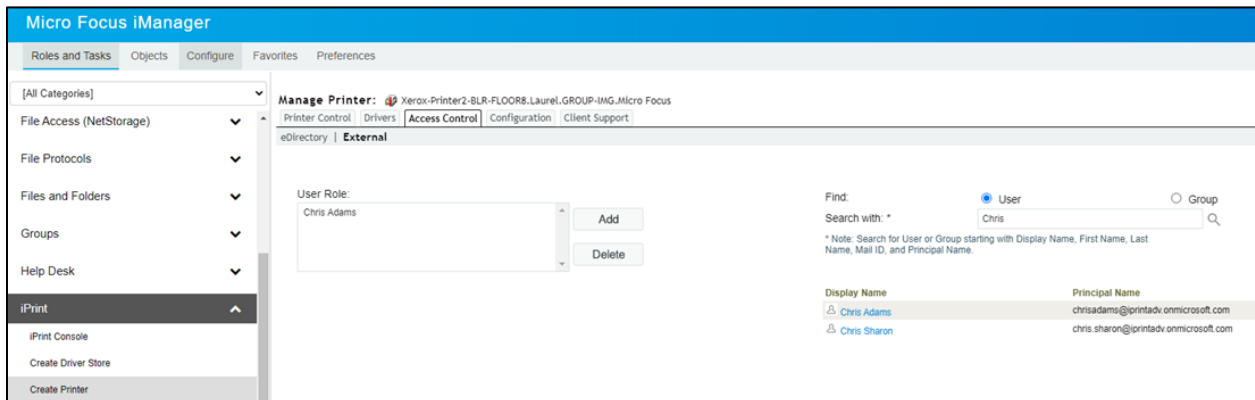


The screenshot shows the Micro Focus iPrint Appliance interface. The top header is blue with the Micro Focus logo and the text "Micro Focus iPrint Appliance". On the left, there is a navigation menu under the heading "Configuration". The menu items are: Printers, WalkUp Printers, Manage Printers (iManager), Printer Status, Mobile, Renderers, Driver Store, AirPrint™, Identity Sources (highlighted in blue), Advanced Authentication, Certificates, Printer Map, Backup, Product Improvement, License, and Settings. The main content area is titled "Identity Source Configuration". It has two tabs: "Directory Servers" and "Microsoft Identity" (selected). Below the tabs are four input fields: "Tenant ID:" with the value "ed917242-d3f9-4b1a-af55-c45ba76bdecd"; "Client ID:" with the value "23b2422f-2c41-44f3-8051-82e43284782d"; "Client Secret:" with a masked value of 15 dots; and "API Scope:" with the value "api://23b2422f-2c41-44f3-8051-82e43284782d/user\_impersonation". At the bottom of the form are two buttons: "Save" and "Delete".

## Configuring Printer ACLs:

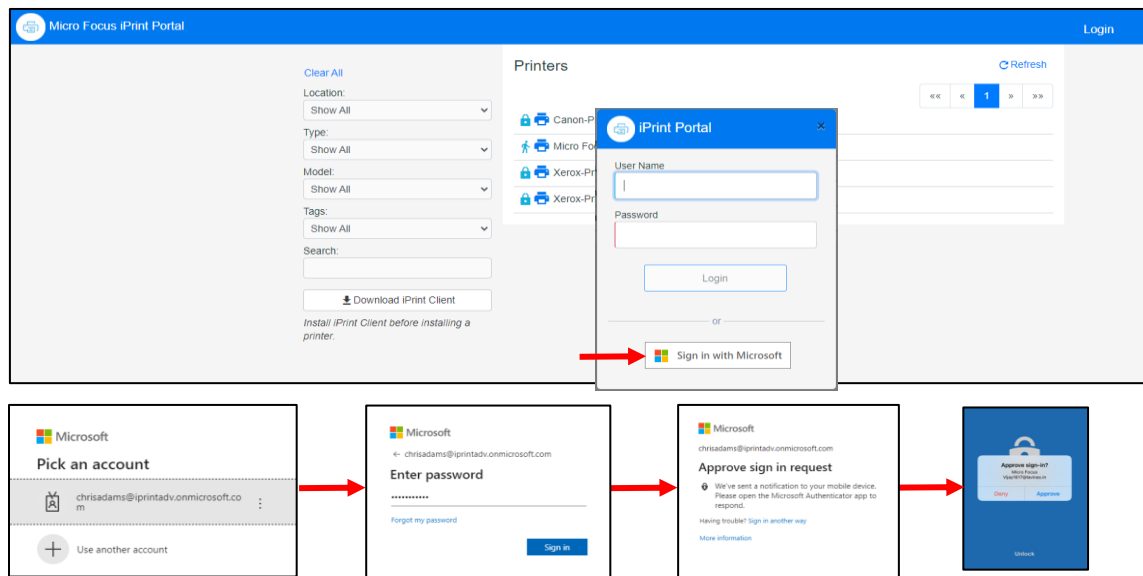
Create a new Secure Printer or Configure an existing with the required ACLs by adding the AzureAD users or groups using iManager:

- 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.



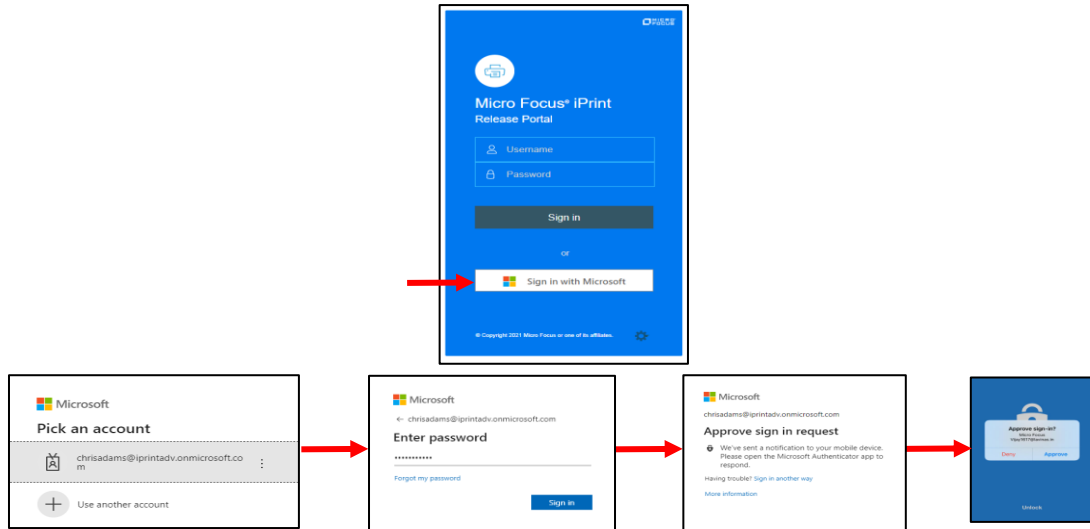
## Print Operations Using Print Portal:

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



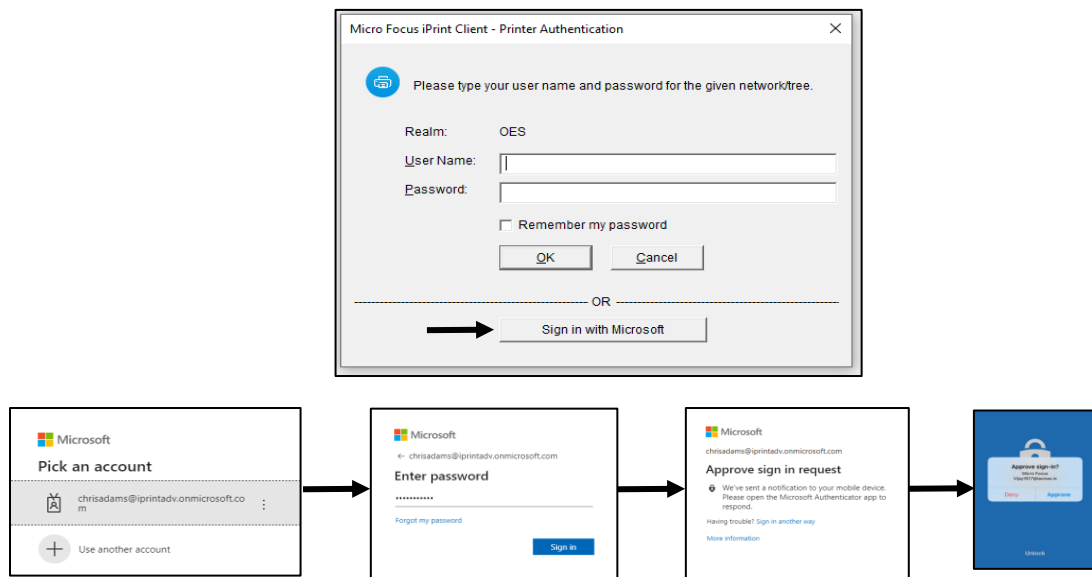
## Print Operations using Release Portal:

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).

