Profile Manager and PTT Pro

Workcloud Communication

Azure AD Integration Guide

MN-004943-01EN Rev A

Copyright

2024/05/08

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

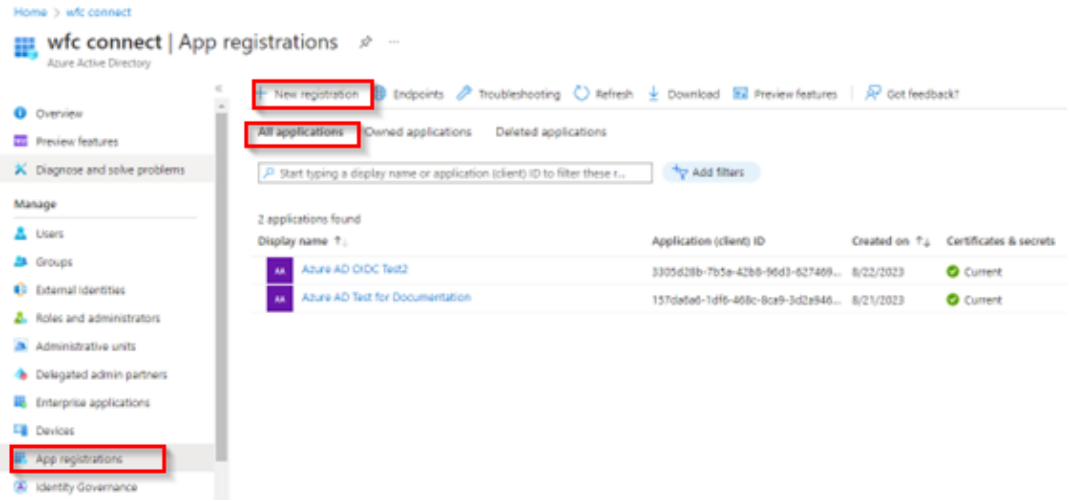
Introduction

This guide describes the steps for an administrator to configure Azure AD, PTT Pro, and Profile Manager to provide authentication, provisioning, and transformation using Azure AD.

Configuring Azure AD

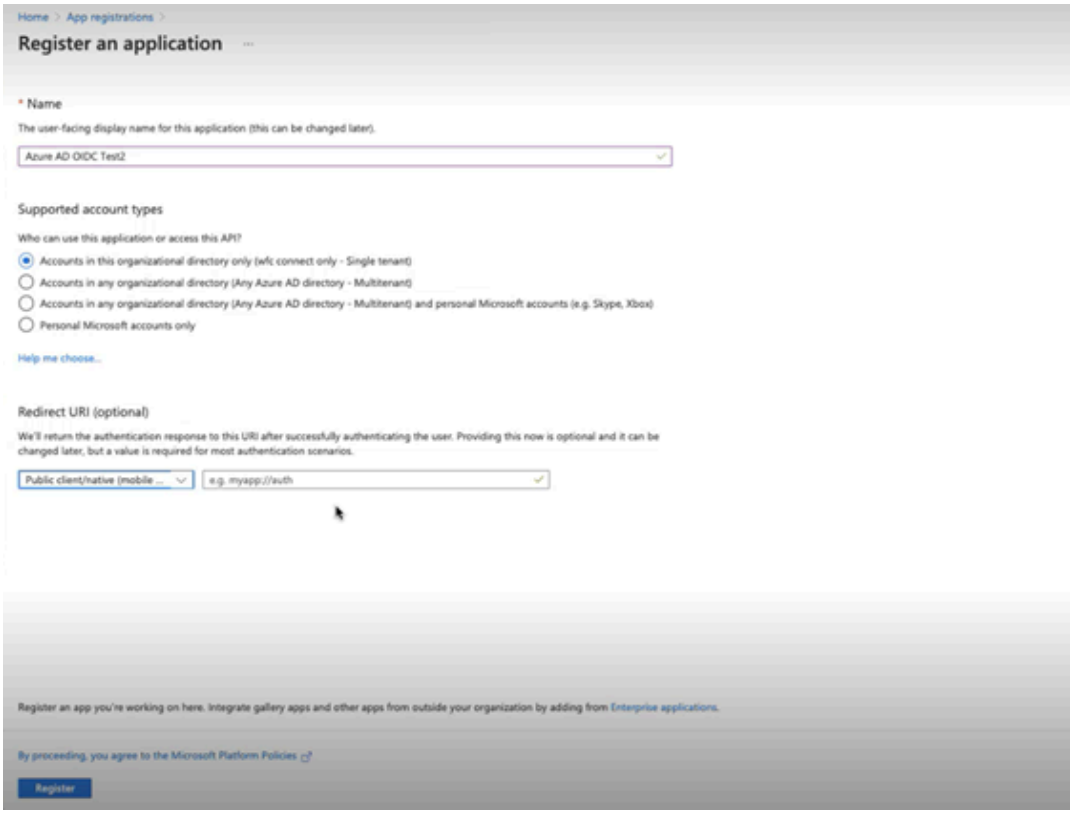
Create a new app registration for Zebra PTT Pro. Create and copy the client secret to configure Zebra PTT Pro.

1. Log in to the Azure instance and select **Azure Active Directory** > **App Registrations** > **All Registrations**.



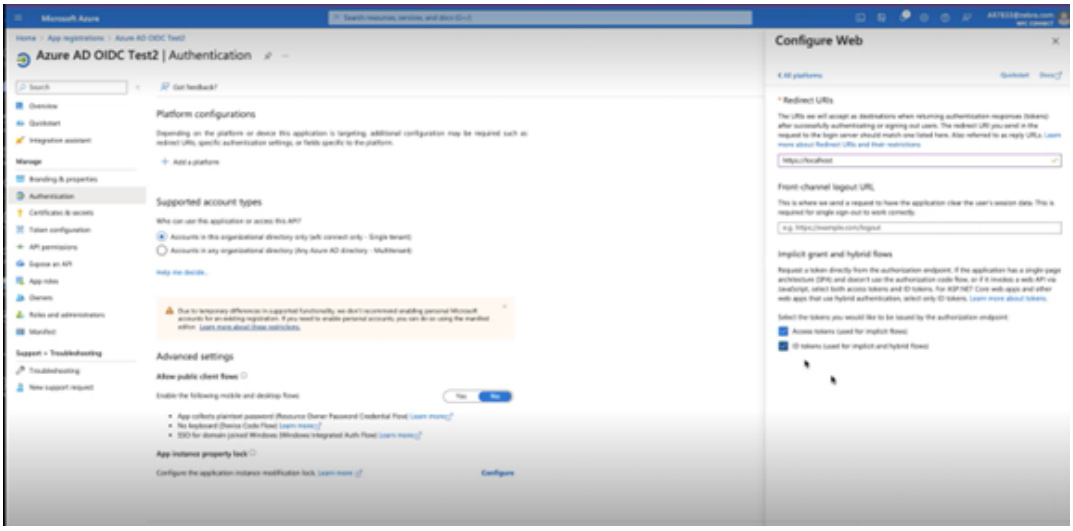
2. Select the **+ New Registration** from the menu to register a new application.

3. Enter the application name and select the first option from **Supported account types** .



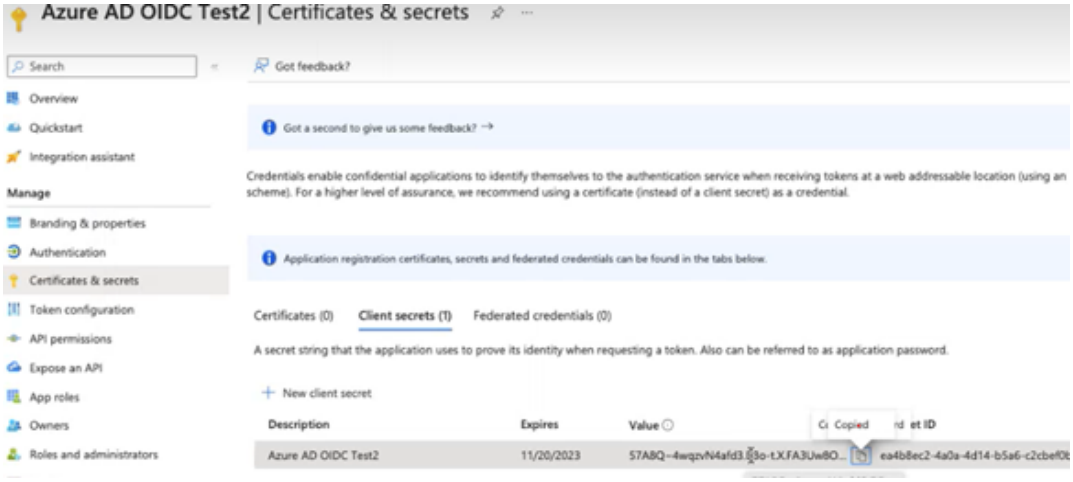
4. Click **Register**.
5. Select the newly created app from the app registrations and navigate to the **Authentication** tab on the right menu.
6. Select the **+ Add** a platform.
7. Click the **Authentication** menu option on the left tab.
8. On the right panel, enter `https://localhost` for the redirect URI. Also, select the bottom two checkboxes shown in the following screenshot.

9. In **Advanced settings** , select **allow public client flows**.



10. From the left panel menu, select the **Certificates and Secrets** to add in a client secret. The client's secret expiration should be set to a value agreed upon with the customer.

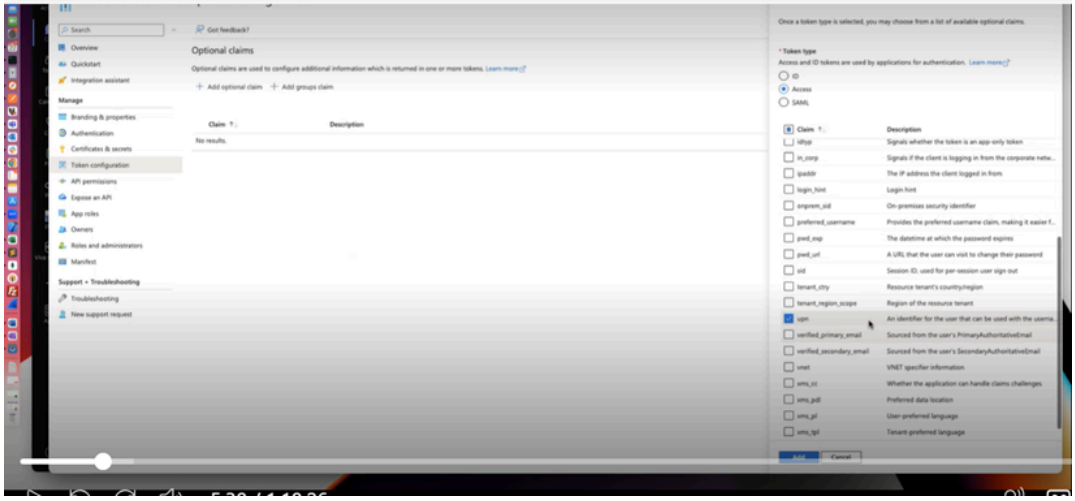
After adding, copying, and saving, the client's secret is important as it cannot be retrieved later.



Configuring the Token

Configure the security tokens so that Zebra PTT Pro users can authenticate.

1. From the **Token configuration** menu, select **Access** from Token type. Enable the **Given Name**, **Family Name**, and **upn** as well as any other attributes the customer may require.



2. From the **Expose an API** menu tab, select **+Add a scope**.

   The **Application ID URI** is automatically populated.

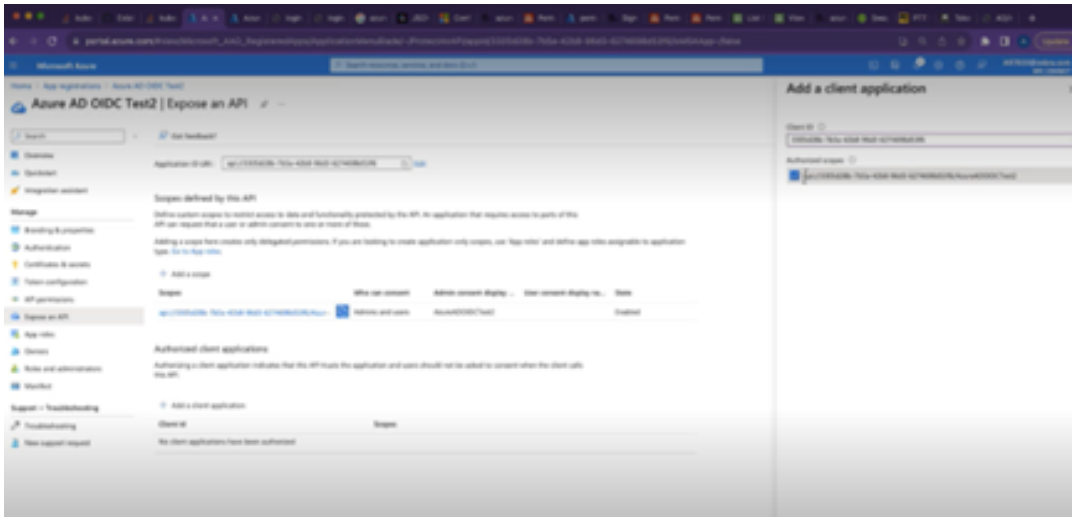
3. Enter the **scope name**, **Admin consent name,** , and **description**.

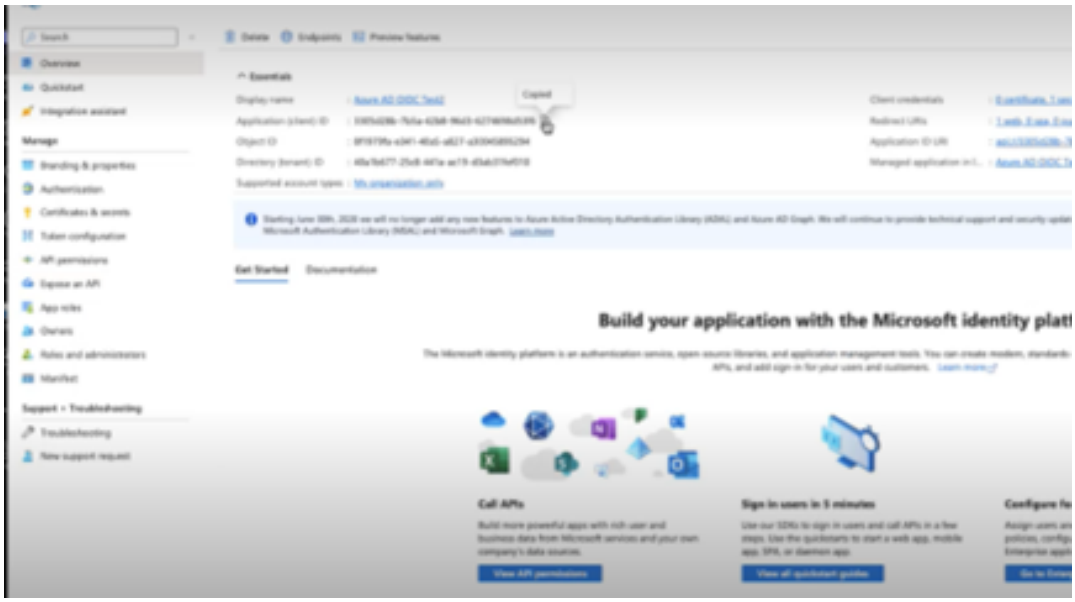
4. From **Who can consent**, select **Admins** and **users**.

5. When done, select **add scope**.

6. After the scope has been added, select the **Add a client application**. Add the client ID and select the Authorized scopes. The client ID can be found on the overview page of the Azure instance.

7. Add the **client ID**, and select the **Authorized scopes**. The client ID can be found on the overview page of the Azure instance.





PTT Pro Setup

When PTT Pro is deployed, Zebra requires the following information to configure the PTT Pro Server and Profile Manager for the customer.

- PTT Pro configuration elements:
  - OAuth URL
  - Access URL
  - OAuth Token

The configuration elements are available through the Well-Known URL.

NOTE:

- To support the shared-device model, the serial numbers of each device must be entered into the PTT Pro Server.
- The PTT Pro Server can support a mix of OAuth and Activation Code device users.
- Each device user must have an OAuth user name to authenticate to the Azure AD.

Finding a Well-Known URL

Customers may know their well-known URL. The construction of a well-known URL is typical; for example `https://login.microsoftonline.com//.well-known/openid-configuration`, although there can be some differences. In this URL, the <Tenant-ID> is used as a placeholder for the actual Tenant ID.

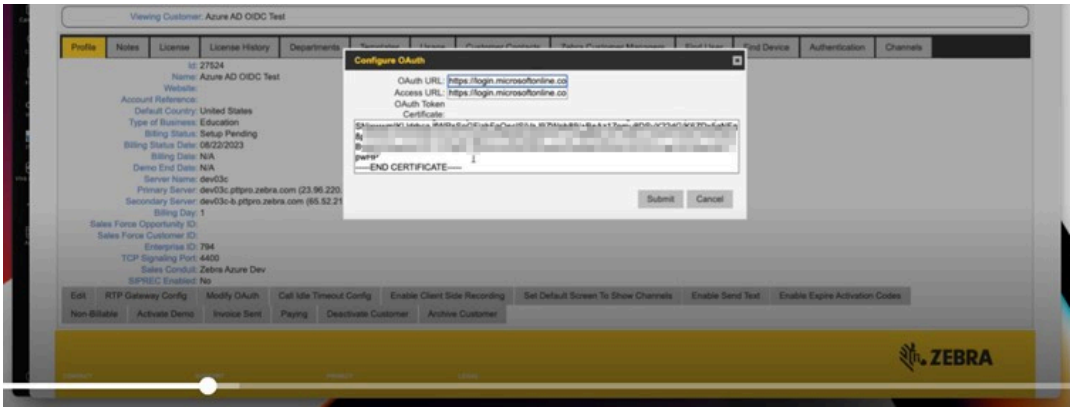
About the Well-Known URL for Azure AD

The Well-Known URL concept was created to provide a publicly available central location for server and metadata resources. It provides publicly available information about a site. A Well-Known URL defines a sign-in flow that enables a client application to authenticate a user and obtain information (or claims) about that user, such as the user name, email, etc. Identifying URLs, encryption schemes, and other information useful in establishing server-to-server communications is useful.

Configuring the PTT Pro Server and Clients

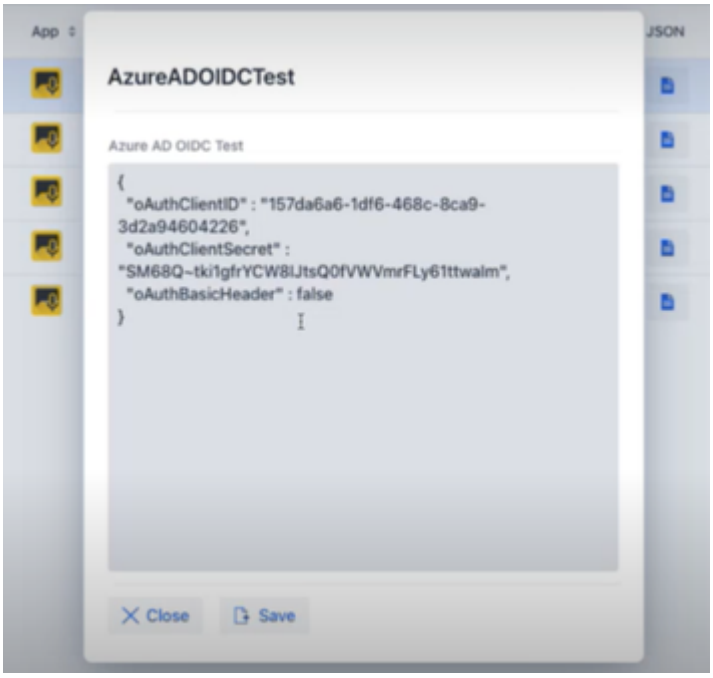
Configure the PTT Pro Server with the OAuth parameters to support authentication with the Azure AD.

On the PTT Pro server, the **OAuth URL**, **Access URL** and **Certificates** must be configured.



If the user runs the PTT Pro without Profile Manager, the Client ID and Client secret must be configured within the PTT Pro clients. The Client ID and the Client secret are provided with a PVM token that the user can scan when launching PTT Pro. The components needed for basic configuration are:

- oAuthClientID
- oAuthClientSecret
- oAuthBasicHeader



Configuring Profile Manager to Support Azure AD

The Profile Manager configuration requires five elements; each element can be derived from the Well-Known URL based on the Azure Configuration or the Token Certificate.

Enter each of the elements in the **OAuth Details** screen, as shown in the following example:

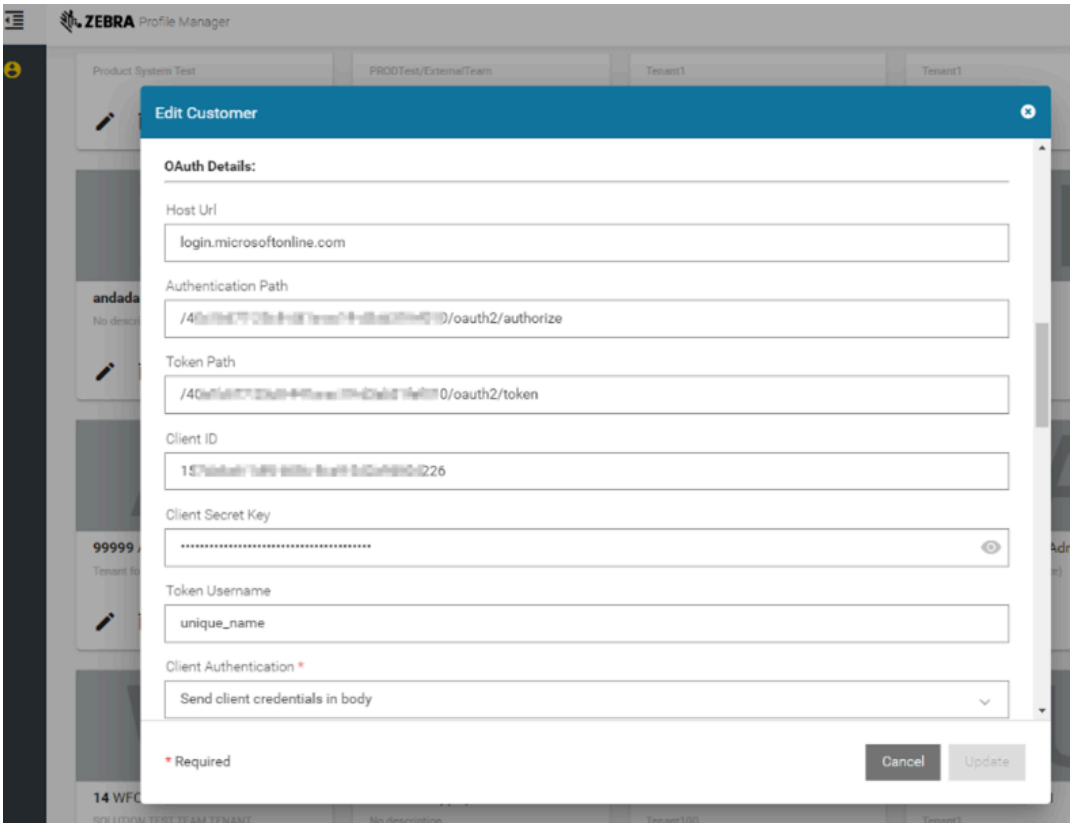


Table 1 Fields Description Details

Name	Description
Host URL	This is the customer domain. The Host URL is the prefix for the Authentication and Token Path, https is assumed and automatically added by the system.
Authentication Path	The Authentication Path is appended to the authorization_endpoint as captured in the JSON response from the Well-Known URL.
Token Path	The token path is appended to the token_endpoint as captured in the JSON response from the Well-Known URL.
Client ID	and the Application ID from Azure AD.
Client Secret Key	.
Token Username	The Token Name can be determined by using the JWT.IO website to examine the access token retrieved by Postman.
Client Authentication	Send client credentials in the body.

Revision History

Version	Date	Description
MN-004943-01EN	05/08/2024	First version.