

Trigger an Azure Function with Easy auth or AAD auth enabled

Last updated by | Ranjith Katukojwala | Mar 7, 2023 at 11:35 AM PST

Contents

- [Issue](#)
- [Cause](#)
- [Resolution](#)

Issue

The customer wants to trigger an Azure Function from Data Factory but it fails when AAD Auth/ Easy Auth is enabled on Azure Function

Cause

When AAD auth is enabled on the Function app, only user/groups who are part of the AAD auth has permission to trigger the app.

Resolution

1. Verify if the AAD auth is setup in Azure Function with the below details • The Issue URL is in the form "<https://sts.windows.net/<Tenant-ID>/>" • Under allowed token the Function app URL is listed <https://<functionAppName>.azurewebsites.net> • In the function app, set the Authorization level to Anonymous because we have configured AAD auth.



Active Directory Authentication

These settings allow users to sign in with Azure Active Directory. Click here to learn more. [Learn more](#)

Management mode ⓘ

Off Express **Advanced**

Client ID

e63[REDACTED]

Issuer Url ⓘ

[https://sts.windows.net/\[REDACTED\]/](https://sts.windows.net/[REDACTED]/)

Show Secret

Allowed Token Audiences


[https://\[REDACTED\].azurewebsites.net](https://[REDACTED].azurewebsites.net)

2. Navigate to Azure Active Directory in the portal -> App registrations -> search for your function app name with the filter All applications -> Search and open the APP used in Function -> App roles | Preview -> Create app role -> create the role like below -> Apply.


Edit app role




 Delete

Display name * 


Function App

Allowed member types * 


- ☐ Users/Groups
- ☒ Applications
- ☐ Both (Users/Groups + Applications)

Value * 

Function.Test

Description * 

123

Do you want to enable this app role? 



Apply

Cancel

3. Navigate to the Overview page of the App -> click the Managed application in the local directory

Dashboard > Microsoft > ADF-FunctionApp-AADAuth

Search (Ctrl+J) Delete Endpoints Preview features

Overview

Quickstart Integration assistant

Manage Branding Authentication

Essentials

Display name : ADF-FunctionApp-AADAuth

Application (client) ID : [REDACTED]

Directory (tenant) ID : [REDACTED]

Object ID : [REDACTED]

Supported account types : My organization only

Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : https://[REDACTED].azurewebsites.net

Managed application in local directory : ADF-FunctionApp-AADAuth

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide updates to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

In the Properties, -> set User assignment required? to Yes.

ADF-FunctionApp-AADAuth | Properties

Enterprise Application

Save Discard Delete Got feedback?

Overview

Deployment Plan

Manage

Properties

Owners

Roles and administrators (Preview)

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Enabled for users to sign-in? Yes No

Name * ADF-FunctionApp-AADAuth

Homepage URL https://[REDACTED].adf-test-app.azurewebsites.net

Logo AD

Select a file

Application ID [REDACTED]

Object ID [REDACTED]

User assignment required? Yes No

Visible to users? Yes No

4. Use the PowerShell commands below to give the app role to your MSI(managed identity), replace the <datafactory-name> and <aad-appName>. Make sure you have installed the AzureAD PowerShell module and have enough permission to assign the app role.

```
Connect-AzureAD
$MSI = Get-AzureADServicePrincipal -Filter "displayName eq '<datafactory-name>'"
$funapp = Get-AzureADServicePrincipal -Filter "displayName eq '<aad-appName>'"
$PermissionName = "Function.Test" (Note - The permission value here should be the same value you add/create)
$approle = $funapp.AppRoles | Where-Object {$_.Value -eq $PermissionName}
New-AzureADServiceAppRoleAssignment -ObjectId $MSI.ObjectId -PrincipalId $MSI.ObjectId -ResourceId $funapp.ObjectId
```

5. (Optional) to verify if the above commands created the correct permission, Navigate to the Overview page of the App -> click Managed application in the local directory - > In the Users and groups there will be an entry with your Data Factory Name and Object Type "ServicePrincipal".
6. Navigate to Data Factory, create a pipeline with web activity: -
 - URL: Default URL from function in form
`https://<functionAppName>.azurewebsites.net/api/<triggerName/FunctionName>`
 - Drop down Advance and choose "MSI" for Authentication.
 - Add Resource value as `https://<functionAppName>.azurewebsites.net`
 - Debug / Trigger (after publishing) pipeline.

How good have you found this content?

