Microsoft Azure AD Configuration Guide

**Introduction**

Use this guide along with the Data Tab Configuration guide to configure a Microsoft Azure AD-integrated SecureAuth IdP realm.

**Prerequisites**

1. Have Azure AD and access to the admin console
2. Create or designate an existing administrator service account with read and optional write access for SecureAuth IdP
3. Create a **Native Client Application** on Azure AD (see Azure AD Configuration Steps below)

**Azure AD Configuration Steps**

Microsoft Azure enables use of the old and new portal

Follow the necessary instructions based on the portal in use for Microsoft Azure (New or Old)

**Azure New Portal**

**App Registrations**

1. Log on Microsoft Azure, and select **Azure Active Directory** from the left-side menu
2. Select **App registrations**
3. Click **Add**
4. Provide a friendly **Name** for the new application
5. Select **Native** from the **Application Type** dropdown
6. Set the **Redirect URI** to the Fully Qualified Domain Name (FQDN) of the SecureAuth IdP appliance, followed by the realm with which Azure AD is integrated, e.g. `https://idp.company.com/secureauth2`
7. Click **Create**

**New App**
8. Once the new application is created, select it from the **App registrations** panel, and copy the **Application ID**, which is used in the SecureAuth IdP configuration steps.

9. Click **Settings** and then **Required permissions**
10. Under **Required permissions** click **Windows Azure Active Directory**

11. Under **Enable Access**, delegate permissions to be granted, and then click **Save**

12. Under **Required permissions** click **Grant Permissions**

---

**Domain Names**

13. Select **Domain names** from the **Azure Active Directory** menu options

14. Copy the `.onmicrosoft.com` domain name, which is used in the SecureAuth IdP configuration steps

---

**Azure Old Portal**
1. Log into the Azure AD admin console, and select Active Directory from the left-side menu.

2. Select the directory to use for the integration.
3. Under **Applications**, click **Add** at the bottom to create a new native client application.

### New Native Client Application

4. Select **Add an application my organization is developing**

5. Provide a **Name** for the new application, and select **Native Client Application**

6. Complete the creation steps
What do you want to do?

- Add an application my organization is developing
- Add an application from the gallery
ADD APPLICATION

Tell us about your application

NAME
New App

Type

- WEB APPLICATION AND/OR WEB API
- NATIVE CLIENT APPLICATION
7. Once the new native client application is created, open the New App.

8. Under Update Your Code, locate the Client ID, which is used in the SecureAuth IdP Configuration Steps.
9. Back in the directory, under Domains, locate the onmicrosoft.com Domain Name of directory for the integration, which is used in the SecureAuth IdP Configuration Steps.
1. In the **Membership Connection Settings**, select **Microsoft Azure AD** from the **Data Store** dropdown

2. Provide the **Username** and **Password** of the administrator service account

3. Set the **Tenant Domain** to the `.onmicrosoft.com Domain Name` of the Azure directory (step 10 (new) / step 9 (old) above)

4. Set the **Client ID** to the **Application ID** (new) / **Client ID** (old) of the new native client application (step 8 above)

5. Provide a list of **Allowed Groups** and / or **Denied Groups** (comma delimited) to restrict access to the realm (if any)

6. Click **Test Connection** to ensure that the connection is active

Click **Save** once the configurations have been completed and before leaving the **Data** page to avoid losing changes

Refer to **Data Tab Configuration** to complete the configuration steps