External Identities is a new public preview feature of Azure AD which allows external users to authenticate with a non-Microsoft account such as their Google or Facebook identity.  This has been available in Azure AD B2C for some time, but that solution is really targetted at highly customised applications with potentially millions of users.  External Identities opens up that idea to you ordinary Azure AD tenant so that any SAML or WS-Fed IdP can be used.  You are essentially federating Azure AD with the external IdP, not a million miles off in construct to how you might federate your Active Directory Domain Services domains to trust others.

In this blog, I will go through the admin process of enabling this for Google, then demonstrate the user experience when using Microsoft Teams.  I will create a second and third blog on External Identities covering the process for Facebook then a custom IdP.

Prerequisite: Google Web App Client ID and Secret

1. You’ll need a **Google API client ID** and **secret** before we can do anything in Azure AD.  Visit [console.developers.google.com](https://console.developers.google.com/) with a Google account and create a **project**.  It’s recommended you use a shared account for your tenant’s administration rather than a personal one and give the project a name distinguishable for future reference.

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

2. You are redirected into your project, and from here navigate to **APIs & Services** > **OAuth consent screen** and choose a **User Type** of **External**, then click**create**.

Graphical user interface, application

Description automatically generated

3. You only need to fill out the **Application name** and **Authorised domains** on the following screen.  The application name can be anything but the domain must be **microsoftonline.com**.  You may also want to review the **token grant rate** which by default allows for 10,000/day.  Save the settings once filled in.

Graphical user interface, text, application, email

Description automatically generated

4. Navigate to **Credentials** on the left-hand pane then **+ Create Credentials**.  We want to create an **OAuth client ID**.

Graphical user interface, application

Description automatically generated

5.  On the client ID page, our **application type** is going to be a **web application** and we need to add in the following **authorised redirect URIs**then choose **create**.  Note you easily copy your AAD tenant ID from the **Overview**page of Azure AD in the Azure portal ([aad.portal.azure.com/#blade/Microsoft\_AAD\_IAM/ActiveDirectoryMenuBlade/Overview](https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview))

* https://login.microsoftonline.com
* https://login.microsoftonline.com/te/your-AAD-tenant-ID/oauth2/authresp

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

7. You’ll be presented with the **client ID** (ending **apps.googleusercontent.com**) and **secret**(password).  Save these as you’ll need them to configure Azure AD.  You can retrieve them later from the Google APIs console just by going back into the web application we created.

Graphical user interface, text, application, email

Description automatically generated

Configure Azure AD

1. In Azure Active Directory, navigate to **External Identities**> **All identity providers**> **+ Google**  ([aad.portal.azure.com/#blade/Microsoft\_AAD\_IAM/CompanyRelationshipsMenuBlade/IdentityProviders](https://aad.portal.azure.com/#blade/Microsoft_AAD_IAM/CompanyRelationshipsMenuBlade/IdentityProviders))

Graphical user interface, application

Description automatically generated

2. Enter the **client ID**and **secret** you created earlier and choose to **save**.  This adds Google as a social identity provider.  You can remove it, if required later, from this same page and clicking **…**

Graphical user interface, application

Description automatically generated

Graphical user interface, application

Description automatically generated

User Experience

So what benefit does this bring to the external user?  I’ll demonstrate this using Microsoft Teams.

Firstly, let’s go through the experience of an **unsupported** external identity: a Yahoo Mail user has been invited to join a Team.  This uses Azure B2B to create a guest user account for the user.

The user follows the invitation email link and they are prompted to create a **Microsoft account** (this is Microsoft’s consumer account; not an Azure AD account) via [signup.live.com](https://signup.live.com/), assuming they do not already have one.  They can use the original email address (i.e. they don’t need to make one ending in yourdomain.com or microsoft.com), but need to provide a password and details such as their country/region and birthday.  Then they need to verify the account with a code sent to their email address.  They will probably need to go through a captcha too, then approve the app permissions.  Finally, they’ll get in.

Graphical user interface, application, Teams

Description automatically generated Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated Waterfall chart

Description automatically generated with low confidence

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

In Azure AD, an administrator can see the user as a **guest**.

Graphical user interface, text, application, email

Description automatically generated

Now the **supported** external identity: a Google user has been invited after you followed the earlier steps to add Google as an Azure AD supported External Identity social identity provider.

The user follows the invitation email link and they are prompted to log in.  The link in the email to **Open Microsoft Teams** points originally to **login.microsoftonline.com** but as the invite was sent to a Google user, it redirects to**accounts.google.com** for authentication.  They need to give the app permissions, then they’re in.

Graphical user interface, application, Teams

Description automatically generated Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application, Teams

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

How much easier was that!?

In Azure AD, the user is a guest, and note that the **source** is Google, rather than the **Microsoft Account** our Yahoo user had to create.

Graphical user interface, text, application, email

Description automatically generated

As the user experience for account creation improves and improves in consumer applications, we must continue to improve it for business applications that use Azure AD too.  External Identities give you the same authenticated user security as guest accounts but without the overhead of an additional account for that guest to manage.