Azure AD B2C: Woodgrove Demo Guide

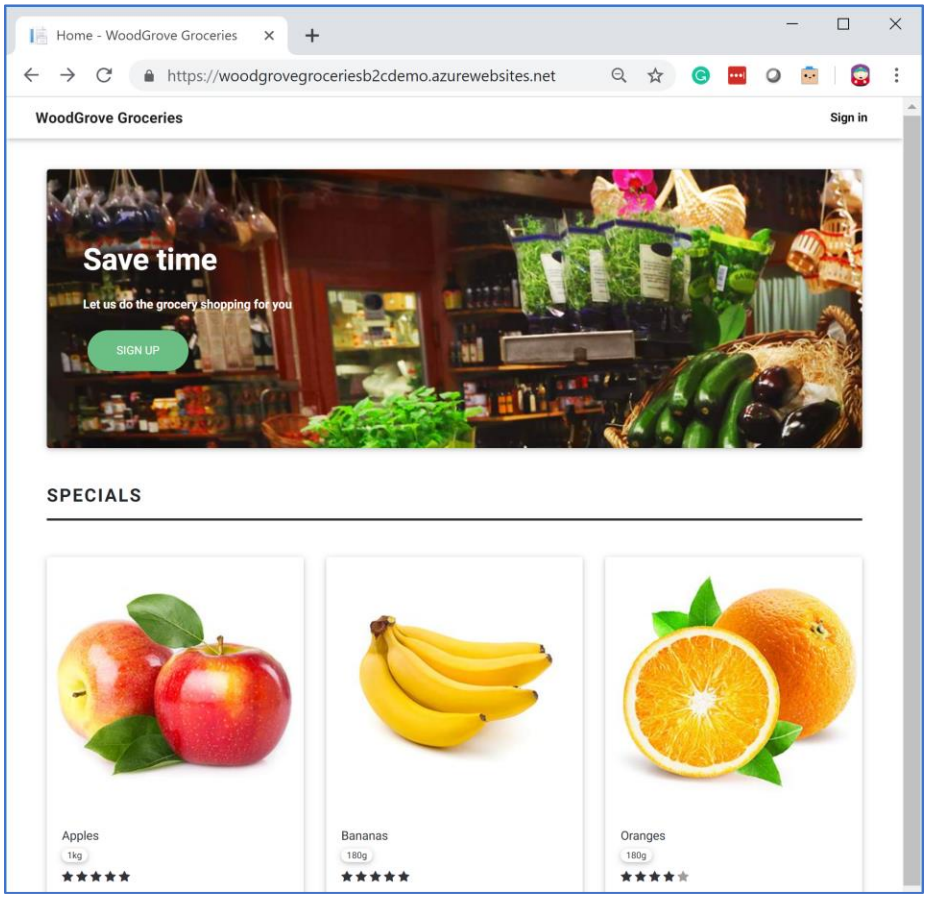
Contents

Introduction

Woodgrove is a fictitious storefront that has been developed to illustrate the various capabilities of the Azure Active Directory B2C platform. Specifically, this portal illustrates how consumer identity (individual customers at Woodgrove), families, and business consumers (corporate buyers) would use a store portal that is powered by Azure AD B2C.

In this document, we will walk you through the different authentication mechanisms used on the Woodgrove web portal, and give you click-through steps on how to use this portal to explore Azure AD's capabilities in scenarios that pertain to external identity management.

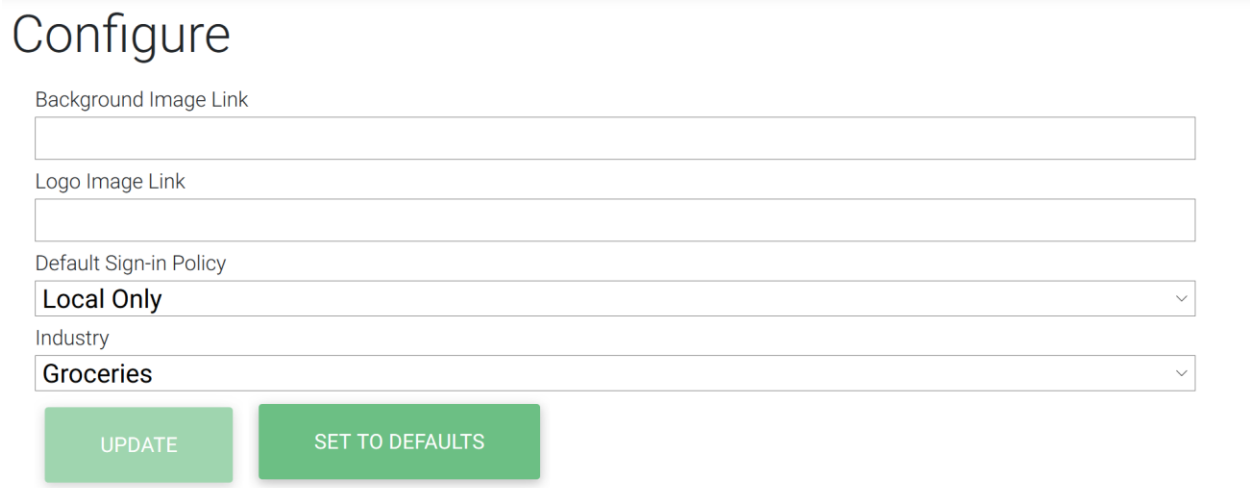
Getting Started



- Go to the Woodgrove web portal: https://aka.ms/CIAMDemo
- In another tab, navigate to the Woodgrove configuration panel: https://aka.ms/CIAMDemoConfig

Using the Configuration Panel

The Configuration Panel allows the person demo-ing Woodgrove to show several different ways in which Azure AD B2C can be customized.



Background Image Link: You can provide a link to any online image file (most standard image file formats are supported) to be used as the background for Azure AD B2C user-journeys. By default, Woodgrove uses stock images that reflect the industry you select on the Configuration Panel.

Logo Image Link: Like the background image, you can provide a link to any online image file to be used as the company logo that will show up in the different Azure AD B2C user-journeys. By default, the portal uses a stock Woodgrove logo.

Default Sign-In Policy: You can select the default sign-up/sign-in policy that you would like to demo. There are several different policies currently available, including policies that show username/password based logins, MFA, password-less auth, TOTP flows and more. We will keep adding further policies here as they are implemented.

Industry: Woodgrove currently supports UI skinning for three different industries: Groceries, Healthcare, Banking. You can choose the industry that most suits your demo.

Important: Note that all configurations that you set from the configuration blade are only valid in the same browser instance. Make sure to hit refresh on the Woodgrove portal to ensure that the Configuration Panel options take effect.

We recommend using Microsoft Edge or Google Chrome for the best experience.

Scenario 1: Signing up (registration) and Signing-In to a Woodgrove Account

In this scenario, we will walk through registering for an account at Woodgrove and how to sign-in after initial registration.

There are several different ways in which you can have your users sign in. For example, you may want your users to sign in with their email address, a username, or just use their phone number instead. Similarly, you may want to ask them for a password, or you might choose to just send them a one-time passcode to their phone and do away with passwords entirely. The following click-steps walk you through a few different options:

1.1 Email ID & Password

This scenario shows you how to set up the demo to enable a conventional sign-up/sign-in using an email address and password ("local accounts" in the Azure AD B2C terminology):

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and click Update.
1. Select 'Sign In with your personal account'.
2. Refresh the web portal tab. Your user will then redirect to the Login page where the user can log in using Email ID & Password.
3. Click 'Sign up now' link from the login screen.
4. The user will then redirect to Sign Up page where the user can register using Email ID & Password.

1.2 Username & Password

Some clients may prefer to use usernames during authentication instead of an email address. These steps show you how to explore a username/password-based authentication experience:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Social & Username - Inline Age Gating' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using a username and password.
5. Click 'Sign up now' link from the login screen.
6. The user will then redirect to Sign Up page where the user can register using a username and password.

1.3 Phone Number & Password

A primary phone number is usually a lot easier for users to remember than email addresses or usernames. There is a growing trend towards also allowing users to use their phone numbers for login. Try out these steps to understand how to use phone numbers in place of usernames in Azure AD B2C:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Social & Phone' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using their phone number and password.
5. Click 'Sign up now' link from the login screen.
6. The user will then redirect to Sign Up page where the user can register using their phone number and password.

1.4 Phone Number & One-Time Passcodes (OTP)

We can also go one step further and do away entirely with passwords. This is accomplished by asking the user to enter their phone number that they've registered with you, and then sending them a one-time passcode via SMS instead of having them enter a password. To read more about the benefits of going passwordless, click here: https://www.microsoft.com/en-us/security/technology/identity-access-management/passwordless

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Phone based OTP' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using a phone number and OTP.
5. Select 'Sign Up with your personal account' from here.
6. The user will then redirect to Sign Up page where the user can register using a phone number and OTP.

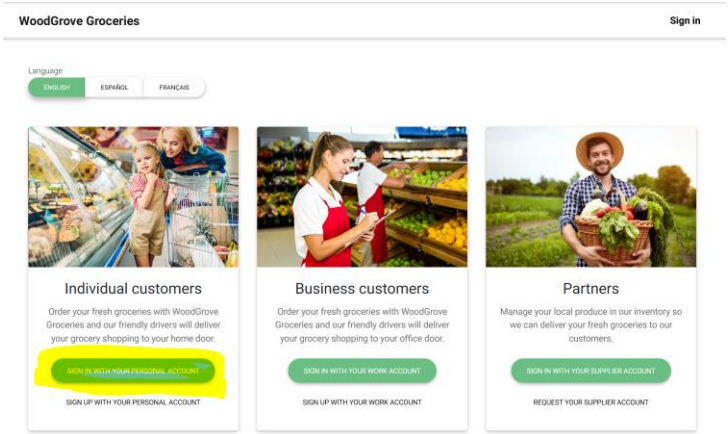
Scenario 2: Bring Your Own Social Identity

For an industry like grocery/retail, there are a few advantages in having your users log in using Facebook, Google, LinkedIn or other social network credentials.

- **Better User Profiling:** If a user signs up using a social identity, this allows Woodgrove to also ask their user if they can obtain further information about their social media profiles to help target your product offerings to them. Additionally, many users will have a concurrent Google/Facebook session running in their browser.
- **Single Sign On:** By logging in with one of their social providers, these users can enjoy the benefits of single-sign-on. This means that if they're already logged in to their social media provider in that browser, they won't need to re-enter their credentials when they browse to the grocery store. Less friction, more shopping!
- **Single Point of Access Management:** For a customer at Woodgrove, signing into a number of websites using the same social media credentials also allows the shopper to review and revoke access to the apps that they interacted with from one central portal. For instance, Facebook has an 'Apps' portal that users can go to that lists out the different apps that are authenticating using Facebook, as well as what user attributes those apps have access to. A user can review this list periodically and decide whether one or more of those apps need to be removed from their list of approved apps.

Following are the click-steps for how to demo social identity integration:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local & Social' and Update.
3. Select **'Sign In with your personal account'** in the Woodgrove Demo app screen



4. The user will then redirect to the Login page where the user can select any of the social providers listed in this demo (Google, Microsoft, and Facebook).
5. The user will then redirect to social provider's login screen
6. During the login, note that we collect a few more pieces of additional information from the user, that weren't available from their social identity provider before redirecting them back to the application after login.
7. Note: If a user is already signed-in to the social provider, they'll be automatically returned to the Woodgrove site without being prompted for credentials.

Scenario 3: Collecting Multi-Factor Authentication (MFA) Information During Sign Up

When a user signs up, you may want to force them to also provide a way for you to enforce a second or third factor of authentication, such as an authenticator app or a one-time passcode to a mobile device. While this makes the sign-up slightly more cumbersome for the user, it adds a significant layer of security to their profile. To learn more about the benefits of using MFA, take a look at our online documentation: How it works: Azure Multi-Factor Authentication. The following demo shows you the same sign-up experience you tried in Scenario 1, but with MFA collection enforced.

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using their email ID and password.
5. Click 'Sign up now' link from the login screen.
6. The user will then redirect to the Sign Up page where the user can register using email ID and password.
7. Sign up will be followed by MFA where the user must verify their phone number. The user will be logged in after successful MFA.

Scenario 4: Progressive Profiling and Profile Completion Percentage

Progressive profile building is the notion that you don't ask a user signing up for your service for a lot of information about them during sign-up, but instead make the sign-up itself lightweight. On subsequent logins, you may choose to ask them one additional question that helps complete their profile. Some apps and sites incentivize their user by offering them discounts for completing their profile. Other portals such as LinkedIn may 'game-ify' profile completion by showing the user what percentage of their profile is complete, and describe the advantages of having a fully completed profile.

The following demo shows you configure a progressive profile building user flow in Azure AD B2C, and how a 'percentage complete' tracker might work for a Woodgrove user.

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. Click 'Sign up now' link from the login screen.

6. The user will then redirect to Sign Up page where the user can register using Email ID & Password.
7. Sign up will be followed by MFA where the user must verify their Phone Number and the user will be logged in after successful MFA.
8. After login, go to the right top corner of the application and click on the logged in username displayed. The user will get to see the profile completion percentage in the pop-up displayed.
9. After that, each time when the user logs in, the user will see progressive profile pages that ask them to provide additional profile details such as allergy information, and their consent to share allergy details. These details are used to calculate a profile completion percentage.

Scenario 5: Age Gating

Age gating in Azure Active Directory (Azure AD) B2C enables you to identify minors that want to use your application. You can choose to block the minor from signing into the application. Users can also go back to the application and identify their age group and their parental consent status. Azure AD B2C can block minors without parental consent. Azure AD B2C can also be set up to allow the application to decide what to do with minors.

After you enable age gating in your user flow, users are asked when they were born and what country/region they live in. If a user signs in that hasn't previously entered the information, they'll need to enter it the next time they sign in. The rules are applied every time a user signs in. For more information on Age Gating, look up our online documentation: Enable Age Gating in Azure Active Directory B2C.

The Woodgrove demo shows you two different ways in which to enforce Age Gating – In-line Age Gating, in which a user is asked to enter their age information during signup, and secondly, as a 'Pre-Check' where the user is asked to provide age info before we ask the user to provide any information about them whatsoever.

5.1 In line with Sign Up

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Social & Username - Inline Age Gating' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Username & Password. The user will not be permitted to log in if the user's age falls under the age limit.
5. Click 'Sign up now' link from the login screen.
6. The user will then redirect to Sign Up page where the user can register using Username & Password along with birth and country details. The user will not be permitted to sign up if the user's age falls under the age limit.

5.2 Pre check before Sign Up

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Social & Username - With Pre Age Gating' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Username & Password.
5. Click 'Sign up now' link from the login screen.

6. The user will then redirect to a Pre-Sign-Up page where user can enter birth and country details. The user will not be permitted to access sign up page if the user's age falls under the age limit.

Scenario 6: Inviting External Users

You may be familiar with a sign-up flow where a friend, coworker or family member initiates a sign-up request for you to a service. In this scenario, we show you how a family member might invite others in their family to a family or team account. Presumably, the parents or a corporate plan administrator would need to authorize and provide credit card confirmation to ship an order, while other users have a limited set of actions they can perform on the site. The invited member gets an email asking them to register with Woodgrove and become a part of a certain group. Follow the steps below to try this piece of functionality out:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Invitation Flow' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. Click 'Sign up now' link from the login screen.
6. The user will then redirect to Sign Up page where the user can register using Email ID & Password.
7. After Sign Up, the user will be navigated to the invitation page where the user can invite external users by providing their Email ID.
8. The external users will be receiving the invitation via email and they can accept the invitation by clicking the link present in the Email which will take them to the application's accept invitation page.

Scenario 7: Linking Your Account to a Social Account

In Scenario 2, we discussed the advantages of having a user sign-up using a social account. Azure AD B2C also allows you to link your store shopping account with a social account such as Facebook or GoogleID, so that you can log in with either your social credentials or the store account credentials you set up. The following demo shows you how to set up an account-linking user flow:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. After login, go to the right top corner of the application and click on the logged in user name displayed. A pop-up will be shown, select the 'Link Your Social Account' option from the pop-up and It will take the user to the Social Providers listing page.
6. The user can choose any social provider (Only Facebook for now) from there and it will take the user to the selected social provider's login screen.
7. After Login, the social account will be linked to the existing local account. After that, the user will be able to use the application by using both local and social accounts.

Scenario 8: Edit Profile

A common requirement for most consumer users who sign up for a service, is the ability to change different attributes in their user profile. For instance, they may have moved and need to change their mailing address or may want to update their profile picture. The following demo shows you how an Edit Profile user flow works in Azure AD B2C.

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. After login, go to the right top corner of the application and click on the logged in username displayed. A pop-up will be shown, select 'EDIT PROFILE' option from the pop-up and It will take the user to the profile edit page.

Scenario 9: Delete Your User Account

An important part of ensuring your portal is GDPR compliant is to provide the user with the ability to delete their user profile that they have created with you. Azure AD B2C allows you to create a user flow that lets user delete their accounts. To understand more about Azure AD's default data retention and deletion policies, refer to our online documentation: How To Delete an Azure AD User. The following steps show you a standard user-initiated account deletion:

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. After login, go to the right top corner of the application and click on the logged in username displayed. A pop-up will be shown, select 'FORGET ME' option from the pop-up and It will delete the logged in user and sign out the user from the application.

By default, this user flow implements a soft-delete. A user who is softly deleted can be restored for up to 30 days post deletion. You can also configure scripts to support instant permanent deletion, although that is out of the scope of this demo.

Scenario 10: Self-Service for Forgot Username/Password

Every good authentication platform should have a way for a user to reset their password. Ideally, you should also be able to let a user change their username. Allowing a user to self-service on this scenario will greatly decrease support calls to your helpdesk. This scenario shows you a demo of how a user can change both their username and password using a B2C user flow.

1. Go to the configuration page
2. Set Default Sign-in Policy as 'Social & Username - Inline Age Gating' and Update
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Username & Password

5. Click 'Forgot your username?' link from the login screen
6. The user will then redirect to Forgot Username page where the user is requested to enter the details to find the Username. If found, the Username will be sent to the registered Email ID.

Scenario 11: Up-leveling a User's Authentication Based On What They're Trying to Access

There may be certain parts of your site that require you to ensure that your user has a higher level of access. For instance, on the Woodgrove grocery site, the grocery store may choose to just have a basic login be adequate for a user to look at product prices, and to add groceries to their cart. But they may want a user to go through a multi-factor authentication step when they're checking out and using their credit card to confirm a purchase. In this scenario, we mock up the experience of a checkout by requiring a user to complete an MFA instead of actually putting in credit card information to complete a transaction.

1. Go to the configuration page.
2. Set Default Sign-in Policy as 'Local Only' and Update.
3. Select 'Sign In with your personal account'.
4. The user will then redirect to the Login page where the user can log in using Email ID & Password.
5. After login, add some products to cart and click 'Complete Purchase' button from Cart Page.
6. It will take the user to Multi-Factor Authentication (MFA) where the user must verify their Phone Number and purchase will be completed after successful MFA.

Conclusion

Hope you've enjoyed trying out the Woodgrove Demo. For more information on how you can get help with developing on Azure AD B2C, visit our online documentation at Support and Help Options for developers. If you have feedback about the product, or this demo, please mail us at <>