

# Enabling Partners, Suppliers, and Customers to Access Applications with Azure Active Directory

## Contents

Solution Overview.....	3
Four Principles for Designing an Identity Solution.....	3
Introducing WoodGrove Groceries – A Case Study .....	4
Azure AD B2B and Azure AD B2C .....	5
Architecture .....	6
Solution Implementation .....	7
Prerequisites .....	7
Tenant Creation .....	7
App Configuration .....	7
Skill-Sets & Roles.....	7
Understanding Policies and the Identity Experience Framework.....	8
Implementing Sign-Up & Sign-In.....	9
Local Identities .....	9
Using Social Identity Providers with Customers .....	9
Using Social Identity Providers for Business Partners .....	11
Enabling Business Customers to Log-in Using their Organizational Identities .....	11
Invitation Based Sign-Up .....	13
Self-Service Sign-Up .....	15
Customizing the Authentication Experience.....	16
Branded Login .....	16
Language and Localization .....	20
Progressive Profiles.....	23
Managing App Access .....	24
Role Based Access Control .....	24
Hybrid App Access.....	24
Conditional Access .....	24
Token and Policy based Access .....	25
Step-Up MFA.....	27
Identity Protection .....	27
Identity Lifecycle Management and Governance .....	27
Terms of Use .....	28
Access Reviews.....	28

Privileged Identity Management .....	28
Pricing.....	29
Solution support and analytics .....	29
Sign-In Reports .....	29
Audit Reports .....	29
Usage Reports .....	30
Getting support from Microsoft .....	31
Additional Resources .....	32

## Solution Overview

Every organization's success, regardless of its size, industry, or compliance and security posture, relies on organizational ability to collaborate with other organizations and connect with customers.

Organizations need an identity solution that is comprehensive, easy, and secure. Azure Active Directory (Azure AD) meets this requirement by providing a single authentication framework that spans the range of users an enterprise interacts with.

This guide details the business value and the mechanics of building an application or web experience that provides a consolidated authentication experience specifically tailored to the contexts of your employees, business partners and suppliers, and customers.

## Four Principles for Designing an Identity Solution

There are four major principles to consider that can guide a successful implementation of an app that interacts with user identities:

- **Usability IS a security feature:** We tend to think that improving security requires a reduction in usability, usually by adding additional security constructs like increasing password complexity. These changes may lead to a user behavior which results in lower security, such as writing down a password on a post-it note. Usability and security don't need to be at odds. Providing an end-user experience that is easy to use can improve security.

For instance, enabling customers to sign-in with their existing social identity providers such as Facebook or Google creates a faster sign-in experience. Users no longer need to remember or write down an additional password. Enabling multi-factor authentication creates an additional layer of security, while only requiring users to enter an easily readable code.

- **Open Standards are Key:** Using open standards across your apps is crucial to ensuring interoperability and staying on top of ever-evolving security standards as new vulnerabilities are identified. You may choose to use business apps in the Azure Marketplace to reduce the number of apps you have to build and manage in-house. Azure AD's app gallery has over half a million apps that your enterprise can choose to use. These apps integrate using standard protocols such as Open ID Connect, OAuth, and SAML.

For legacy line of business apps that you can't easily replace, a good way to move in the direction of standardization is to off-load the core authentication aspects of the app into a cloud identity provider. We will dive deeper into how you can utilize specific solutions like Microsoft's Cloud Application Proxy to achieve this outcome.

- **Identity is a Control Plane:** Using identity as a control plane involves ensuring the right users have access to the right capabilities under the right conditions for the right amount of time. While granting the right users the right set of capabilities or permissions are basic and well-understood requirements from an identity implementation, it is also essential to build in the notion of control based on the right conditions and time.

Conditions can be your email domain, mobile application types, IP address, region, or a determination of whether you're signing in from a corporate managed device or an unmanaged

device. Azure AD Premium uses machine learning and an evaluation engine to determine session risk – high, medium, or low based on the conditions you specify, and then applies policies based on those conditions. For example, if you determine that a user is low risk, they are allowed access. If there is medium risk, you may ask the user to use multi-factor authentication or force a password reset. If it is high risk, you may completely deny them access.

Similarly, you can use the notion of time to exercise control. For instance, you may allow a user to access sensitive resources only for a short window of time after they've authenticated, after which their session is configured to expire, and they must reauthenticate.

- **Design for Privacy and Compliance:** A centralized identity system like Azure AD can also ensure that your architecture's privacy and compliance requirements are easier to manage. Establishing easy ways for users to audit the information you store about them, presenting clear consent screens when storing or accessing information about them, and staying on top of regional and industry-based regulations and privacy laws is also of paramount importance to gaining and retaining your users' trust, while taking proactive measures to keep user data safe and secure.

## Introducing WoodGrove Groceries – A Case Study

To illustrate how each of these principles is adhered to across the different facets of designing your company's digital identity story, we will use 'WoodGrove Groceries,' a fictitious grocery delivery company that is looking to build an app that caters to their employees, local farmers with whom they partner, as well as customers who shop at WoodGrove.

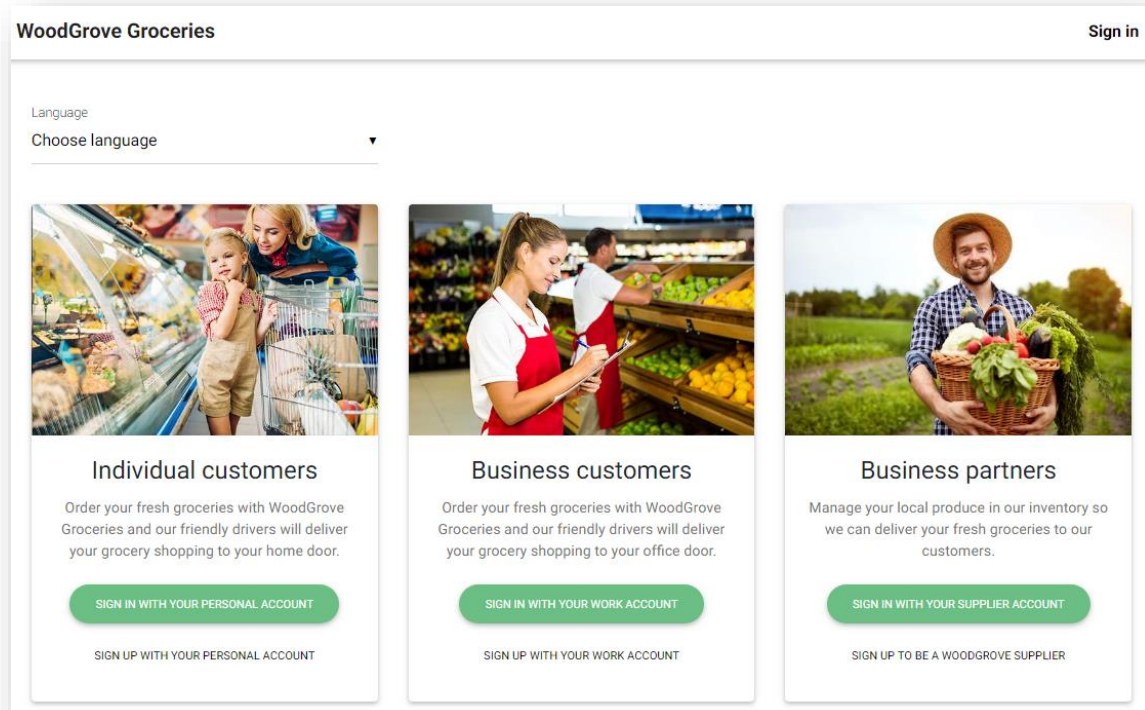


Figure 1 Screenshot of the WoodGrove Groceries app that caters to different user personas

To fulfill their goal, WoodGrove needs to deal with two broad user-bases:

- **Commerce:** The commerce aspect is the interaction with customers. Users might include:
  - **Individual customers**, who can sign-up and buy groceries. They want to sign-in using Google, Facebook, Microsoft accounts, or may choose to create their own username and password.
  - **Business customers (aka organizational customers)**, who can sign-up using their corporate account. They already have an identity in their corporate Azure AD tenant, and it is ideal for WoodGrove and the customer to be able to use it.  
These users can take different actions in the app based on their role. For example, the business customer employee might be a “pantry stocker” who can place orders within a certain budget from a list of pre-approved items. Another employee may be the “pantry manager” who can add new products to the list for stockers to order and can determine the acceptable budget.
- **Collaboration:** The collaboration aspect deals with the interaction of WoodGrove’s own employees, large business partners, and smaller or independent partners. The key personas we’ll focus on here are:
  - **WoodGrove Employees**, who manage the WoodGrove app, approve partner requests and collaborate with partner in SaaS production apps.
  - **Business Partners**, who are distributors, farmers, or manufacturing companies, can sign-in and collaborate with WoodGrove employees and manage the inventory that is available to WoodGrove customers. The larger business partners may wish to use a corporate identity, while the smaller entrepreneurial partners may prefer a social identity such as a Google account.

## Azure AD B2B and Azure AD B2C

We will use Azure AD’s Business-to-Business Collaboration (Azure AD B2B) feature to support these requirements and personas, as well as another product in the Azure AD family called Azure AD Business to Consumer (Azure AD B2C) features.

**Azure AD B2B** enables any organization using Azure AD to collaborate safely and securely with users from any other organization, small or large. Those organizations may or may not have an existing Azure AD tenant and may not even have an IT department.

Organizations using Azure AD collaboration features can provide access to documents, resources, and applications to their partners, while maintaining complete control over their own corporate data. Developers can use the Azure AD business-to-business APIs to write applications that bring two organizations together more securely. It’s also easy for end users to navigate.

**Azure AD B2C** is a cloud identity service used by governments and enterprises worldwide to provide secure access to their apps for citizens and customers with fully customizable white-labelled signup experiences. Built on Azure Active Directory, which handles billions of authentications per day, the Azure

Azure AD B2C platform is optimized for scale, reliability, and availability for your customer-facing applications. Azure AD B2C manages the federation of user identities, including local accounts, social identity providers, or external Azure AD tenants, and can be configured to allow only the specific providers desired.

## Architecture

To build a digital experience that caters effectively to all these personas, we need to architect a solution that accommodates a variety of different identity providers, security requirements and workflows. Coming back to our WoodGrove Groceries example, below is an architecture that the grocery chain may consider as part of their identity solution design:

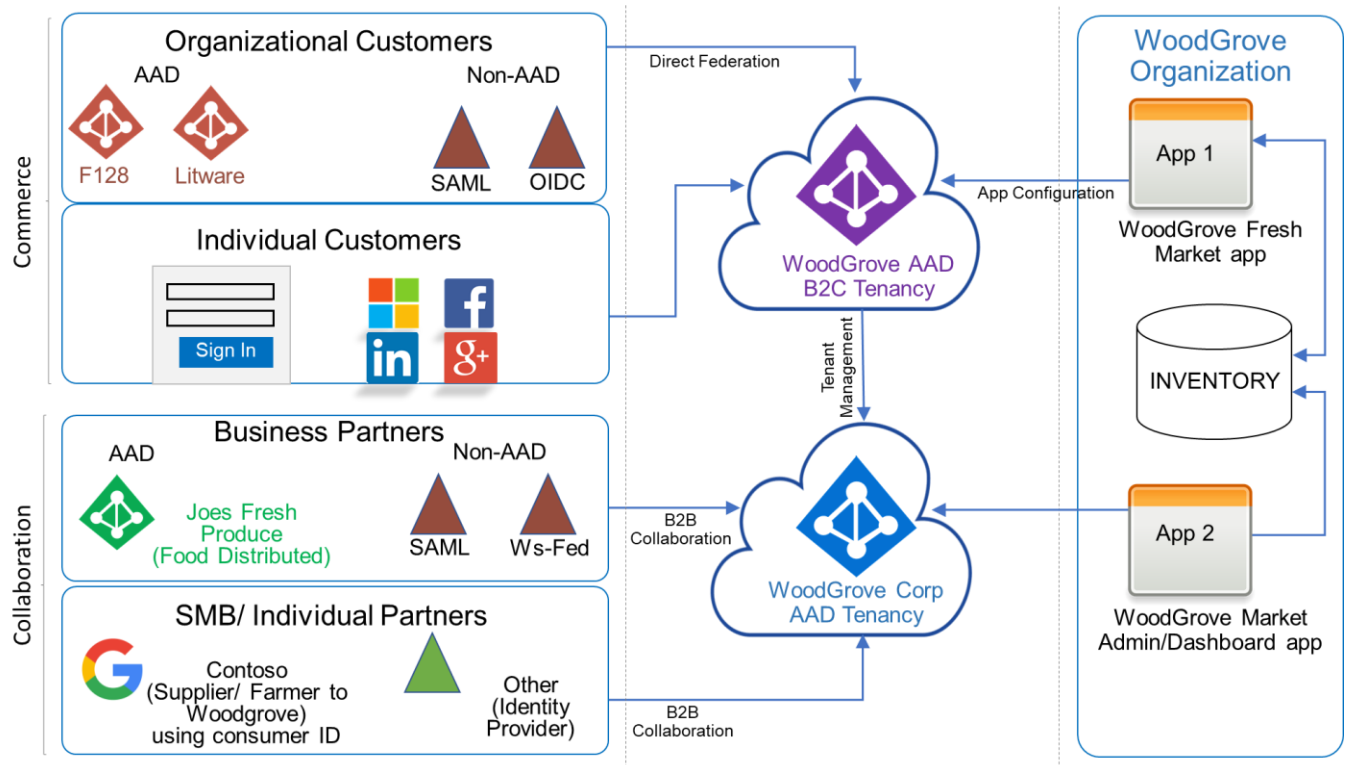


Figure 2 Architecture diagram for the WoodGrove identity deployment

- WoodGrove will stand up two separate Azure AD instances. One is their Corporate Azure AD tenant that will host employee and partner identities, and the other is an Azure AD B2C tenant that hosts individual and organizational customers.
- Organizational customers, such as the two fictitious companies F128 and Litware shown in the diagram, may already host their user identities in Azure AD. Other organizations may run on other identity providers that either use Security Assertion Markup Language (SAML) or OpenID Connect (OIDC). These customers will log into the Azure AD B2C tenant using direct federation using their corporate credentials.
- Individual customers will authenticate against the Azure AD B2C tenant using either a social identity provider or a username and a password they create when they first sign-up for an account with WoodGrove.

- d) Partner Organizations, irrespective of whether they use Azure AD or use another identity provider, can be invited to participate in WoodGrove's corporate tenant using the B2B collaboration workflow that is available in Azure AD.
- e) Small-to-medium business and individual partners can either use a Google account or their existing identity provider to be invited into WoodGrove's Corporate AAD using the B2B collaboration workflow in the same way that larger partner organizations are.
- f) The two apps in this example can authenticate against the two Azure AD tenants and provide access to underlying resources such as their inventory database.

## Solution Implementation

Over the next several sections, we will explain different aspects of the WoodGrove identity architecture and distinguish how the customer and partner interfaces need to be built out depending on whether they are targeted towards 'Commerce' or 'Collaboration' scenarios.

### Prerequisites

#### Tenant Creation

Applicable To:	Collaboration
	Commerce

To implement an identity infrastructure that supports these personas, you will first have to ensure you have an Azure subscription and a tenant in Azure AD.

If you don't already have an Azure AD tenant, you will need to create an Azure Active Directory instance. For more information, please refer to the [Quick Start Guide to Sign Up for Azure AD Premium](#).

You will also need to create an Azure AD B2C tenant. You can get started by referring to our documentation on [Using Azure AD B2C in Four Simple Steps](#).

#### App Configuration

Applicable To:	Collaboration
	Commerce

You will have to register your apps in Azure AD to establish trust between Azure AD and your app. The following links show you how to configure your apps to work with Azure AD B2C and Azure AD B2B:

Registering your Collaboration App with Azure AD: <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-integrating-applications>

Registering and configuring your app with Azure AD B2C: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-app-registration>

#### Skill-Sets & Roles

Applicable To:	Collaboration
	Commerce



Following are some of the skill-sets you might find useful while staffing up for an identity deployment:

Role	Skills/Knowledge Required
<b>Solution Architecture</b>	<ul style="list-style-type: none"><li>• Familiarity with cloud and on-premise identity systems</li><li>• Working knowledge of your existing identity system and the implications of potential migration</li><li>• Understanding of typical stress and load patterns of your user population</li></ul>
<b>Identity Development</b>	Depending on the complexity of your deployment, your developer will need to be proficient in: <ul style="list-style-type: none"><li>• Standards-based authentication protocols (OIDC, OAuth, SAML etc.)</li><li>• REST API development</li><li>• Cloud infrastructure and scaling requirements</li><li>• Basic XML editing</li><li>• Use and possible extension of authentication libraries such as MSAL</li><li>• Proficiency in the programming languages/frameworks used by existing apps</li><li>• Use of Graph APIs and executing scripts to populate or read from user repositories</li><li>• PowerShell scripting to do tenant administration</li></ul>
<b>Design</b>	<ul style="list-style-type: none"><li>• App development for mobile/desktop/web</li><li>• HTML/CSS and JavaScript</li></ul>

## Understanding Policies and the Identity Experience Framework

Applicable To:

Commerce

Policies in Azure AD B2C describe consumer identity experiences, or user journeys, such as sign-up, sign-in, or profile editing. A sign-up policy allows you to control behaviors by configuring the following settings:

- Account types (social accounts such as Facebook and/or local accounts such as email addresses) that consumers can use to sign up for the application
- Attributes (for example, first name, postal code, and shoe size) to be collected from the consumer during sign-up
- Use of Azure Multi-Factor Authentication
- The look and feel of all sign-up/sign in pages
- Information (which manifests as claims in a token) that the application receives when the policy run finishes

You can create these policies either through a user interface in the Azure AD B2C Tenant (built-in policies) or alternatively, you can craft more complex journeys using a declarative XML schema (custom policies). This schema is defined in the Identity Experience Framework that comprises policy parsing rules, as well as the rest of the scaffolding required to enable Azure AD's consumer identity functionality. See below here for more information on the two ways to author policies:

- [Built-in Policies](#)
- [Custom Policies](#)

## Implementing Sign-Up & Sign-In

Customers and partners already have existing identities which may be an organizational account or a social login, such as a Facebook or Twitter account. Allowing customers and partners to use their existing identity provides an easy and secure method of accessing your app. Providing the option of a local account gives customers the ability to create a separate identity that is unique to the WoodGrove app.

### Local Identities

Applicable To:

Commerce

Local Identities refer to the type of account a user can create by providing a user name and password. Often, the user name is the email address of the user. Users may choose to create a new account if they want to create an identity unique to one app, or if they don't have an accepted social identity.

Local accounts are fully supported for consumer workflows. Users can create an account in a self-service manner, including verifying the email address they provide. A self-service password reset flow can be provided to users that need to reset their password.

To learn how to create a local account-based user experience for your customers, click here:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-policies>

Note: At this time, you cannot invite collaboration users to create their own usernames and passwords. They will have to use a social identity or more commonly, their organizational identities as discussed in the section below.

### Using Social Identity Providers with Customers

Applicable To:

Commerce

Supporting social identity providers lets your customers select the sign-in option that is best for them, providing an easy, user-focused experience.

- Using a social provider saves your customer from having to remember another set of credentials, making their sign-up and sign-in process less cumbersome.
- Consolidating all their login experiences with one social provider means a customer can grant or revoke access to the apps they use by logging into a centralized app permissions experience that each of these social identity providers offers.

The following are several social identity providers that are supported out of the box for consumer experiences, along with guidance and samples on how to incorporate each one into your app: [Microsoft Account](#), [Facebook](#), [Google](#), [Amazon](#), [LinkedIn](#), [Twitter](#), [GitHub](#), [Weibo](#), [QQ](#), [WeChat](#)

In the likely event that a social identity provider does not collect or provide you with all the necessary attributes you want to obtain, you can also collect the additional data by defining a custom data collection screen within the sign-up flow after the user has finished signing up using their social identity of choice. This ensures that your application can expect a consistent set of attributes from every user, no matter what the source of the customer's identity is.

During the sign-in process for an individual consumer in the WoodGrove app, the user is sent to an authentication endpoint. The user then selects the identity provider they wish to use. If the user selects a social identity provider, they will be directed to the social provider's authentication page, and upon successfully logging in, may be asked to consent to sharing a specific set of datapoints with your company.

Once the user has given consent to the social identity provider, the provider redirects to the AAD B2C authentication endpoint. Depending on your policy configuration, Azure AD B2C can store the information it received from the external identity provider, or alternatively, pass it on to the app without storing it at all. If there are other attributes you need to get from the user, you can also customize the policy to query the user for additional data before completing their registration. The user will be prompted for any additional requirements as defined by the policy. Once they have completed the sign-in process, they are returned to the app with the claims defined by the policy.

Here is an example of an Azure AD B2C token that is returned to an app after the user has logged in with a Google account. This token format is consistent, irrespective of the provider your user signed in with.

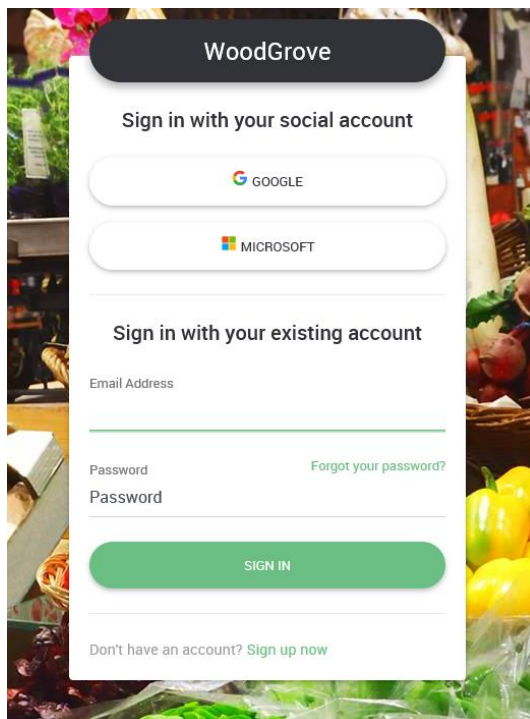


Figure 3 Example of social identity providers in WoodGrove's shopping app

```
{
  "exp": 1138397431,
  "nbf": 1138394931,
  "ver": "1.0",
  "iss": "https://login.microsoftonline.com/23c3a30d-d3db-429d-82f6-ed2538d45256/v2.0/",
  "sub": "84d5754c-4282-46df-a1af-1c01efab0dc9",
  "aud": "b7fde2f2-2c30-17c8-bcbc-57184b72ec68",
  "nonce": "defaultNonce",
  "iat": 1125394031,
  "auth time": 1138394031,
  "name": "User",
  "idp": "google.com",
  "new_user": true,
  "emails": [ "{user-email}@gmail.com" ],
  "tfp": "B2C_1A_sign_up_sign_in_personal"
}
```

Note: Most social identity providers only provide a small subset of users' data to apps that authenticate through them, typically just the email address or a name. You can explicitly request further scopes from the identity provider by using [custom policy flows](#).

#### Using Social Identity Providers for Business Partners

Applicable To:

Collaboration

Smaller partners who don't have a full identity solution in-house may also want to log in using a social identity. At this time, Microsoft Account accounts are supported for collaboration workflows, with other providers being onboarded over time. For more information on how to invite partners to collaborate using social identities, click here: <https://aka.ms/b2b-google-federation>.

#### Enabling Business Customers to Log-in Using their Organizational Identities

Applicable To:

Commerce

Using an identity provider that your business customer owns has several advantages:

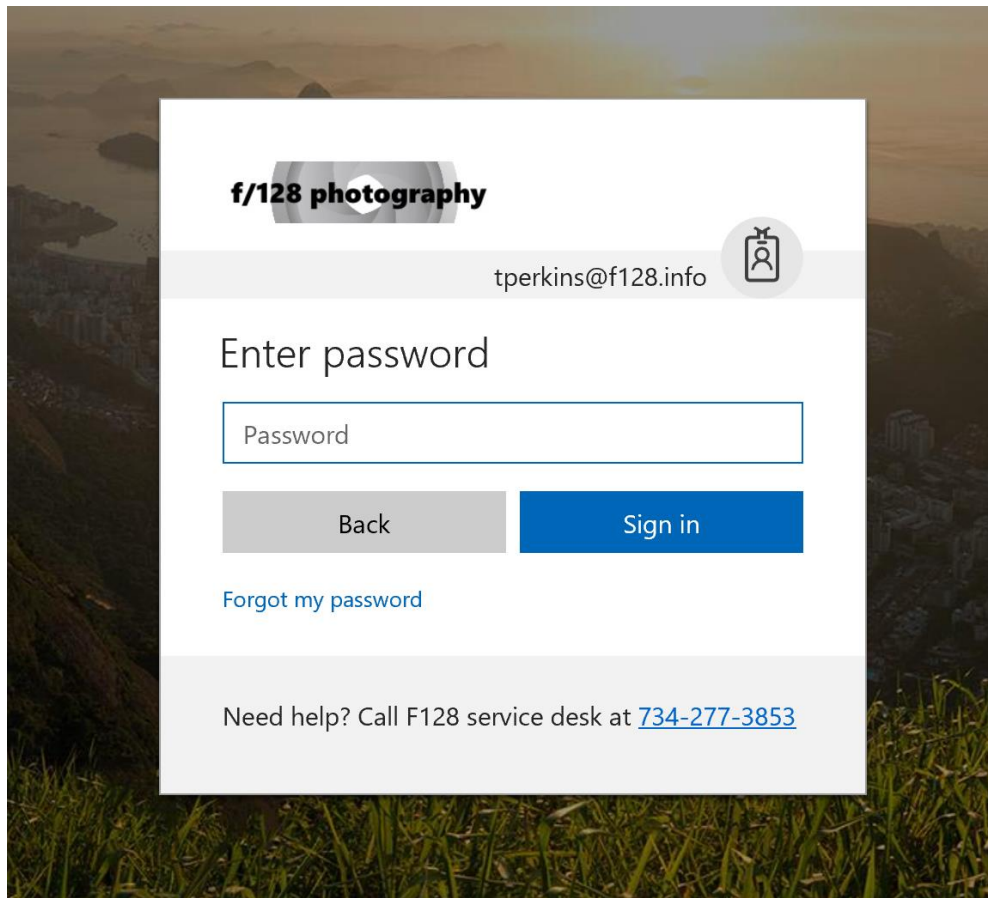
- The customer's IT department manages individual users. This is more secure, as it ensures only users who are still employees at the customer's company have access to your portal.
- Individual users can see their own company's branding on the authentication page, which lets them know they're logging in to a trusted portal/experience.

Azure AD B2C allows you to configure federated authentication through any identity provider that uses a standards compliant protocol. Click here for examples on how to integrate custom identity providers:

- [Integrating an OAuth2/OIDC Provider](#)
- [Integrating a SAML Provider](#)

As a special case of the examples above, you can integrate federated authentication into your commerce app by your business customers if they happen to be using Azure AD as their identity system.

This can be orchestrated by crafting an Azure AD B2C policy that uses Azure AD as the only available Identity Provider in a log-in journey. A policy can allow every Azure AD tenant or may provide a list of Azure AD tenants that are allowed or blocked. During the sign-in process for a business customer, the application sends the user to the authentication endpoint of the Azure AD B2C tenant. Since Azure AD is the only available identity provider defined in this example, the user is immediately redirected to the common Azure AD authentication endpoint. If the user is not already authenticated, they will need to sign-in.



*Figure 4 Federated authentication allows the end-user to see their own corporation's branding while logging in*

Just like any OAuth-based external identity provider, the customer's corporate Azure AD tenant gets consent that the user wishes to share information with your Azure AD B2C tenant before logging them in and sharing their information with Azure AD B2C:

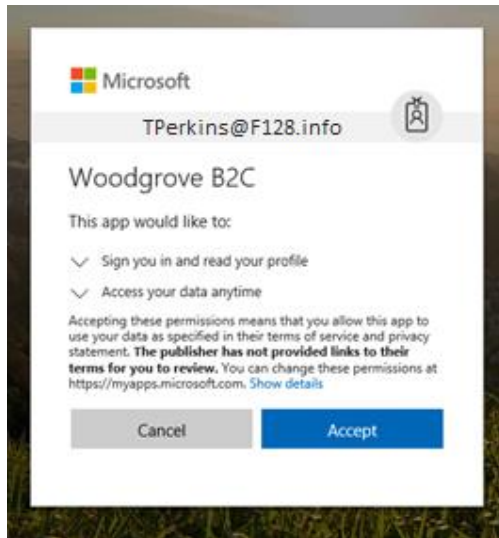


Figure 5 OAuth Permission flow before sharing user information

To learn more about how to configure Azure AD B2C to enable organizational login from other companies using Azure AD, see: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-setup-oidc-azure-active-directory>.

## Invitation Based Sign-Up

Applicable To:

Collaboration

Sharing appropriate resources with business partners in a secure and reliable fashion is a common collaboration requirement. Azure AD B2B allows you to invite users from other companies into your directory, where you can assign permissions to your resources for them to access. The partner company still manages the identities of their employees, removing the requirement for your company to do so. This can be done in two main ways, either using the Azure Portal, or via an automated method.

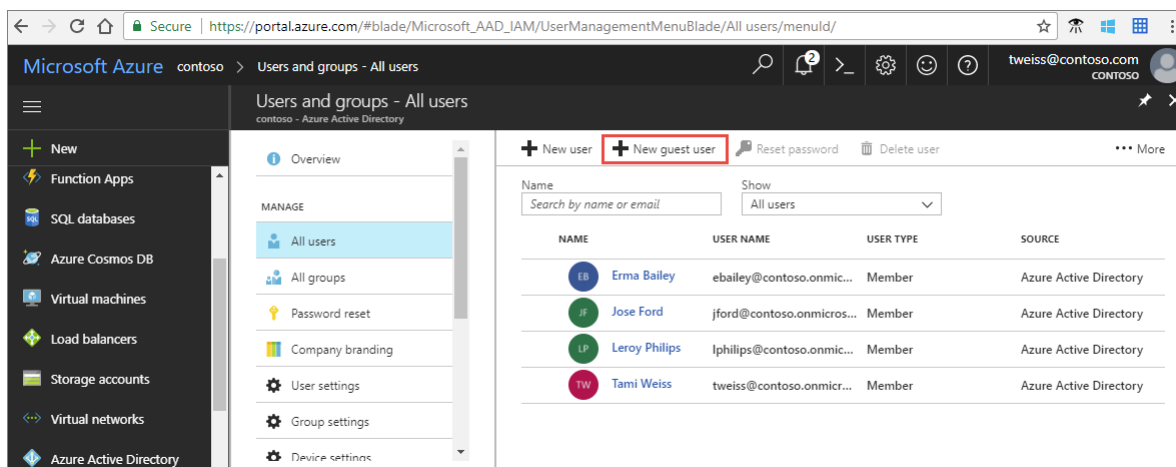


Figure 6 Inviting a collaboration user directly from the Azure Portal using Azure Active Directory

The first way to invite an employee of a partner organization to your company Azure AD tenant is by using the Azure Portal. An administrator of your Azure AD tenant uses the “New Guest user” button and

fills in the email and invitation message to send. An email is sent to the selected user, and the invited collaborator can sign in with an identity of their choice. If the user doesn't have a Microsoft account or an Azure AD account, then one is created for them seamlessly at the time of the invitation redemption. For more information on how to trigger a B2B invitation as an administrator from the Azure Portal, please refer to the following documentation: [Azure AD B2B – Add Users as an Administrator](#)

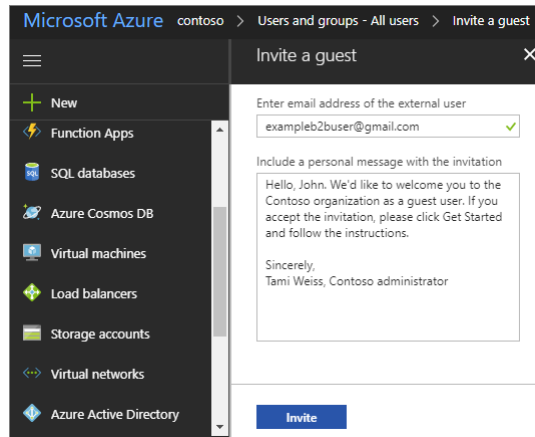


Figure 7 Email generated as part of inviting a guest to your corporate tenant

The second method to send an Azure AD B2B invitation is by utilizing the Graph API. This allows any properly configured app to create an invitation that is sent to the user. This can be added in an application that allows certain employees to send invitations to partners.

When an invitation is sent, an inactive user entry is created so that roles and licenses can be assigned to a user before the user redeems the invitation.



Figure 8 Sample invitation email sent to a guest user of a corporate tenant

This email contains a link which takes the user to a Microsoft sign-in page where they are prompted to sign in with an existing Microsoft account or to create a new Microsoft account. The user is shown a consent screen, indicating that the WoodGrove Azure AD tenant will be able to sign the user in and read their profile information. Once the partner accepts the consent, they have been added to WoodGrove Groceries Azure AD directory as a guest user. Now that the user has been added to the WoodGrove AAD directory, WoodGrove employees can share documents with the partner, and the partner can log into designated apps.

Once the partner user has accepted the invitation, resource owners in your company may share documents, applications and resources, while maintaining complete control over your corporate data.

### Self-Service Sign-Up

Applicable To: Collaboration

Another method is creating a self-service registration portal where partners can register themselves.

Going back to the WoodGrove Groceries scenario, a self-service portal has been established for use by WoodGrove Groceries partners. When a business partner uses the sign-up link for partners on the login screen, they are taken to a self-service registration page. This allows them to enter their e-mail address and other relevant information.

The screenshot shows a web portal titled "Woodgrove Guest Enrollment". At the top, there is a dark navigation bar with links for "Woodgrove", "Sign Up", "About", "Contact", and "Admin Sign In". The main content area has a light gray background. On the left, there are four labeled input fields: "Email Address" (containing "user@company.domain"), "First Name" (containing "Employee"), "Last Name" (containing "Partner"), and "Request Comment" (containing "I need to work with inventory for Partner Corp"). Below these fields is a blue "Request Access" button. On the right, there is a light gray box containing the text "Hi there, welcome to the B2B guest enrollment".

Figure 9 Example of a self-service sign-up portal for collaborators



Woodgrove
Sign Up
About
Contact
Admin
employee@woodgrove.company
Sign out

Pending Guest Requests

Save

Refresh

Approve all

	RequestID	Email Address	Request Comment	Status	Notes
<div>Approve</div> <div>Deny</div> <div>Pending</div>	7b31a757-b8e3-4dc2-81ab-0e3956f2963d	user@company.domain	I need to work with inventory for Partner Corp		

Figure 10 Admin experience for a self-service collaborator enrollment app

This self-service portal is configured to automatically allow entry to employees from known partner organizations. However, an independent partner that signs up will require a WoodGrove employee to approve their partner request. The application makes a call to the Graph API to create the partner invitation. This call creates a user object in the WoodGrove AD tenant, with an indication that an invitation is pending. An email is then sent to the address the partner signed up with.

Here's an example of how to set up a self-service portal for collaboration:

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/self-service-portal>

## Customizing the Authentication Experience

Provide a visual security indication by customizing the app login interface that you present users. It ensures that the user sees a page that is familiar to them, whether it is related to your app or to the user's identity provider.

### Branded Login

Providing a consistent login experience across your apps and websites through branding and visuals builds trust with users by reducing confusion and preventing disparate authentication experiences.

Following are a few approaches to branding the login experience:

#### Built-in Company Branding

Applicable To:

Collaboration

Commerce

If you are using Azure AD Premium, you can use its Company Branding feature for out-of-the-box authentication experiences customized with your company's name, logo, color scheme and more.

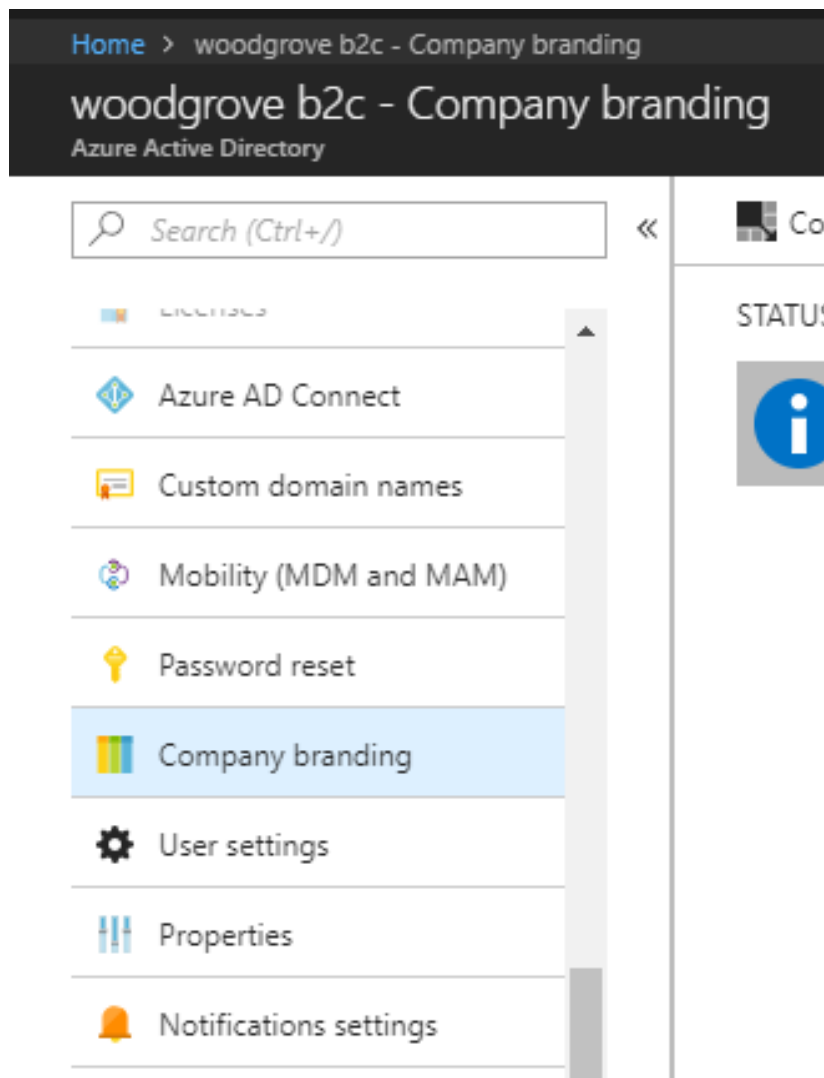


Figure 11 Configuring Company Branding in Azure AD

For more information on how to configure Company Branding, click here:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding>

Note that if you are allowing a user to login using their own corporation's federated identity provider, the user will be presented with their own company's branding if that company also uses Azure AD.

#### Full Branding

Applicable To:

Commerce

Throughout authentication, users expect to see a familiar branded experience that reflects the design, look and feel of the app or site they're attempting to authenticate against. Azure AD B2C allows for customization of every page customers interact with when signing in, editing their profile, changing their password or any other interaction handled by Azure AD B2C.

Out of the box, Azure AD B2C provides a neutral login experience which is useful for quick proof of concept implementations, or when you haven't yet finalized your user experience.

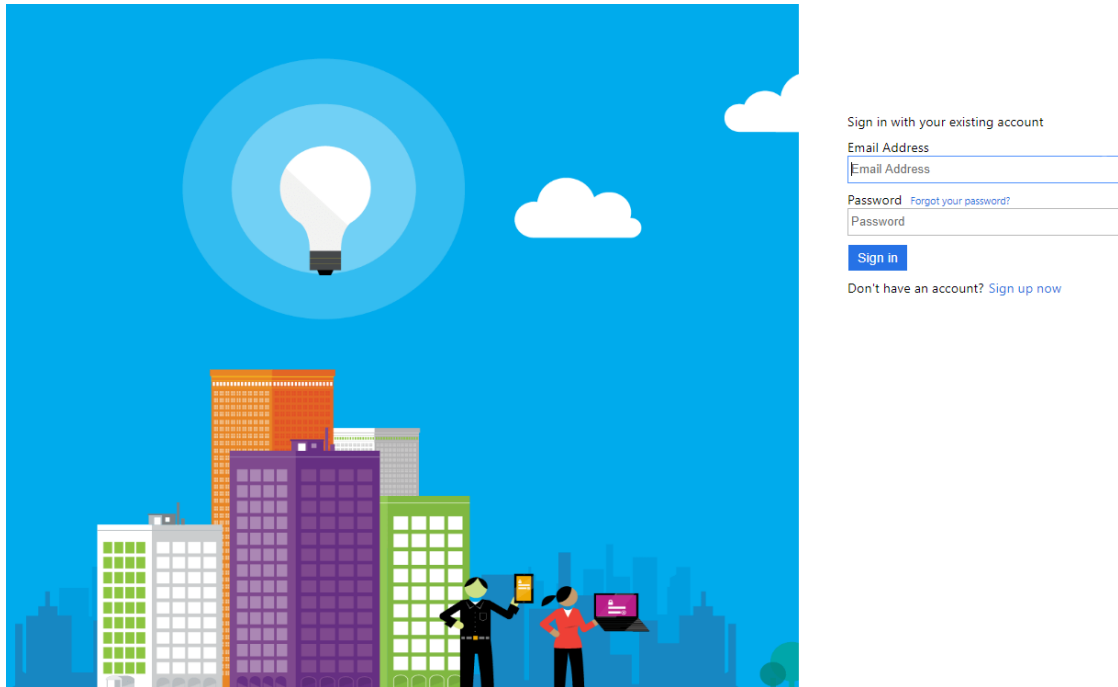


Figure 12 Built-In Azure AD B2C Sign-Up/Sign-In user interface

However, you can build custom UI experiences while defining policies. Azure AD B2C runs code in your customer's web-view and uses an approach called [Cross-Origin Resource Sharing \(CORS\)](#) to render your customized user experience. At run-time, the Azure AD B2C engine loads your HTML and CSS content from a CORS-enabled URL that you specify. This allows you to keep updating the look and feel of your authentication experience to reflect different marketing campaigns and seasonal changes without updating the app itself.

In the Azure Portal, selecting the "Page UI customization" section while creating a policy will allow you to define the location of the content you wish to use.

Figure 13 Portal configuration of built-in sign-up/sign-in policies in Azure AD B2C

```
<!DOCTYPE html>
<html>
  <head>
    <title>!Add your title here!</title>
  </head>
  <body>
    <!-- Leave this element empty because Azure AD
    B2C will insert content here. -->
    <div id="api"></div>
  </body>
</html>
```

As you are designing the customized page, you define a special div element that will be filled with the elements needed to create the page. The page may contain styles and link to other resources such as CSS or images. The elements inserted by Azure AD B2C can be styled using CSS or in-line styles defined within the page. The use of JavaScript for customization is currently blocked for security reasons but will be available using a custom domain or the domain b2clogin.com in late 2019.

This is an illustration of how the Azure AD B2C engine merges in the sign-in elements to a customized HTML/CSS experience you have designed:

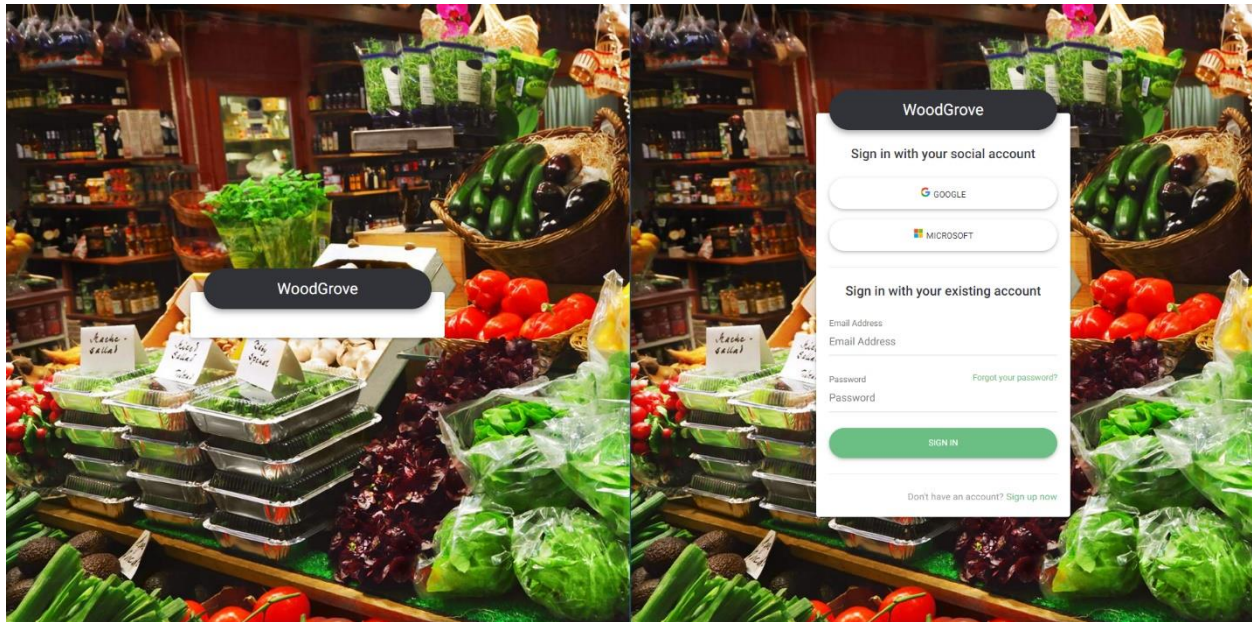


Figure 14 The image on the left shows the plain HTML without Azure AD B2C elements merged in. The image on the right shows Azure AD B2C elements merged in at run-time

Customized pages don't have to be static. The server hosting the content can change the background, styles, or any other parameters of the page that is served based on your own criteria. In addition, using a custom policy allows Azure AD B2C to send parameters to the server hosting the content to dynamically change the content based on the parameters supplied. For an example of how to do this, reference: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-ui-customization-custom-dynamic>

More information about UI customization in custom policies, including information about hosting pages on an Azure blob storage account, as well as a description of the elements that Azure AD B2C inserts into customized pages, is available here: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-ui-customization-custom>

### Language and Localization

Enhance the user experience by customizing the language and visual cues provided to your user during an authentication flow based on their own language and region. In addition to a few localization options available in all Azure AD tenants by default, you can also do highly customized language modifications for certain commerce scenarios.

#### Default Localization

Applicable To:	Collaboration
	Commerce

By default, Azure AD uses the following priority order for rendering language and locale to users:

- 1) The user's preferred language/locale setting if they already have an account in Azure AD and have made an explicit choice.
- 2) The default language/locale settings of the home or corporate tenant of the user

- 3) The default language/locale settings of the external company's tenant that is inviting a user to collaborate with them.

Additionally, in collaboration scenarios only, an administrator can also use the Invitation Manager API to specify the language of an invitation mail that is sent to an external user. This will override any settings in 1-3 above. For information on how to configure the Invitation Manager API, click here:

[https://blogs.msdn.microsoft.com/premier\\_developer/2017/09/29/getting-started-with-the-azure-ad-b2b-invite-api/](https://blogs.msdn.microsoft.com/premier_developer/2017/09/29/getting-started-with-the-azure-ad-b2b-invite-api/)

### App & Policy Localization

Applicable To:

Commerce

Azure AD B2C accommodates different languages to suit your users' needs and simplify the sign-in experience. Out of the box, Azure AD B2C provides translation for 36 languages. You can provide your own translations for any language you want to support or override the default translations to better fit the voice of your app.

NAME	LOCALE	DEFAULT	ENABLED
বাংলা (ভারত)	bn-IN		
čeština	cs		
dansk	da		
Deutsch	de		
Ελληνικά	el		
English	en	✓	✓
español	es		✓
suomi	fi		
français	fr		✓
ગુજરાતી	gu		
हिंदी	hi		
hrvatski	hr		
magyar	hu		
italiano	it		
日本語	ja		
ಕನ್ನಡ	kn		

Figure 15 Language customization using built-in policy configuration

For built-in policies, the language customization tab in your Azure AD B2C policy configuration enables you to turn on support for any of the provided languages, or to add your own languages or updated translations. To learn more about how to do language customization using built-in policies, see: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-language-customization>.

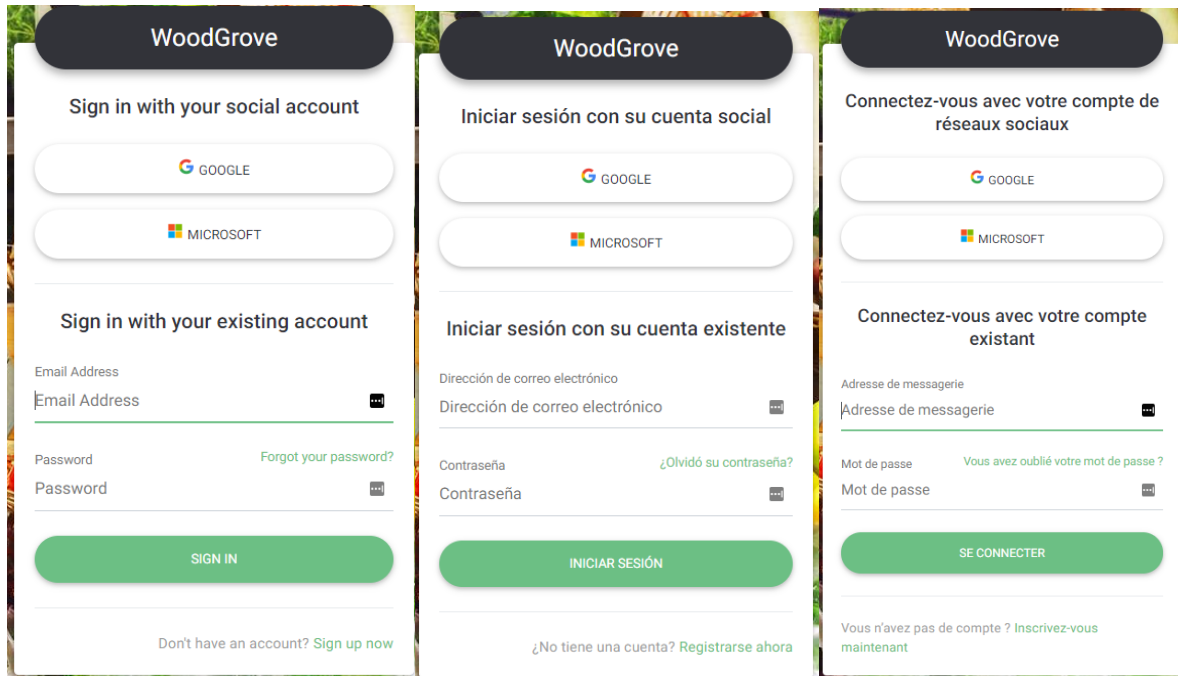


Figure 16 Localization of an Azure AD B2C policy in different languages

The same functionality is also available through custom policies. For a complete walkthrough on how to localize your experience using custom policies, please refer to the following tutorial: [Language Customization in Custom Policies](#)

**WoodGrove**

Email Address  
Email Address

SEND VERIFICATION CODE

New Password  
New Password

Confirm New Password  
Confirm New Password

Display Name  
Display Name

☐ I agree to the WoodGrove terms of service

Country/Region  
Country/Region

Postal Code  
Postal Code

CREATE

CANCEL

WoodGrove terms of service  
The standard Lorem Ipsum passage, used since the 1500s  
"Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do

## Progressive Profiles

Applicable To:

Commerce

When providing a sign-up experience for a user, there is a trade-off between collecting all the information necessary for your business versus the time it takes for a user to sign-up. In trying to collect too much information, the user may get frustrated and leave without signing up.

Progressive profiles resolve this issue by ensuring that your user data collection is compliant with the General Data Population Regulation (GDPR) requirements.

In a progressive profile experience, the user is asked only for the information that is necessary for you to authenticate them into your app.

An example of using progress profiles to prevent minors from accessing your application may look like this: When starting the sign-up process, the user is asked for their country of residence and their date of birth. Based on this data, the policy determines if the user is a minor and the user sign-up flow can be immediately blocked.

Alternatively, the policy can return a JSON response to the application indicating the user didn't meet the age requirements. In either case, the user's profile has not been created in Azure AD B2C and has no identity token or claims.

Figure 17 Collecting only core attributes during initial sign-up

If the policy is configured to return JSON data, the application can then take specific actions to show the user a different experience, or to start a process for parental consent.

Using progressive profiles to reduce sign-up friction may look somewhat different. The sign-up flow may just ask for a display name and to agree to the terms of service. The user would be allowed to access the application with the limited profile they have. The next time the user signs in, the policy would request any additional information that is needed from the user. These may be optional pieces of data or may be required for specific application functionality. If the user hasn't supplied the necessary information, they can be directed to a profile-edit flow that allows them to provide the necessary data. When using this approach, the application must properly handle situations where the user claims it receives from Azure AD B2C don't contain all the information that a fully completed profile may contain.



## Managing App Access

Setting up the right processes for managing app access across your user base will help reduce the overhead of manually onboarding users every time a new app is rolled out. The following strategies and corresponding functionality available in Azure AD for you to efficiently manage user app access.

### Role Based Access Control

Applicable To:

Collaboration

Role-based access control (RBAC) allows better security management for large organizations and for small or medium businesses working with external collaborators, vendors, or freelancers. These users may need access to specific resources in your environment but not necessarily to the entire infrastructure or any billing-related scopes.

RBAC can be assigned in Azure AD in four different ways:

- **Direct assignment:** Users can be assigned directly to a resource by the owner of that resource.
- **Group membership:** A group can be assigned to a resource by the resource owner, and by doing so, granting the members of that group access to the resource. Membership of the group can then be managed by the owner of the group.
- **Rule-based:** The resource owner can use a rule to express which users should be assigned access to a resource.
- **External authority:** The access to a resource is derived from an external source; for example, a group that is synchronized from an authoritative source such as an on-premises directory or a SaaS app such as WorkDay. The resource owner assigns the group access to the resource, and the external source manages the members of the group.

More granular RBAC capabilities are in development and are expected to be available as a feature in Azure AD in the future. For more information on access management for business collaborators, see: <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups>

### Hybrid App Access

Applicable To:

Collaboration

A hybrid organization has apps both on-premises and in the cloud. Azure AD enables you to grant users access to both cloud and on-prem apps so that they can use the same sign-in credentials for both environments. This can be done regardless of whether you manage external partner accounts locally in your on-premises identity system or as external accounts as Azure AD B2B users.

To learn more about how to configure external collaborators to use the same credentials across your on-premise and cloud apps, see: [Azure Active Directory B2B collaboration for hybrid organizations](#).

### Conditional Access

Applicable To:

Collaboration

With Azure AD B2B collaboration, organizations can enforce multi-factor authentication (MFA) policies for B2B users. These policies can be enforced at the tenant, app, or individual user level, the same way

that they are enabled for full-time employees and members of the organization. MFA policies are enforced at the resource organization.

In the WoodGrove grocery example, the administrator at WoodGrove can invite an employee at F128, one of their suppliers, to collaborate with them. If one of WoodGrove's apps requires its users to complete an MFA, the F128 employee will also need to complete the same MFA. It is worth noting that since WoodGrove has required the MFA, it will need to ensure they have enough Azure AD Premium licenses to cover the invited user's use of MFA.

For more information on how to configure conditional access for your collaborators, click here:

<https://docs.microsoft.com/en-us/azure/active-directory/b2b/conditional-access>

#### Token and Policy based Access



One of the key constructs you will need to support in an app which hosts multiple personas is the ability to provide different users with different levels of functionality based on their identity. While there isn't native support for Role Based Access Control in Azure AD B2C, this kind of separation can be created using different policies for each persona. Your app can then provide different levels of access to the user based on the claims contained in their token.

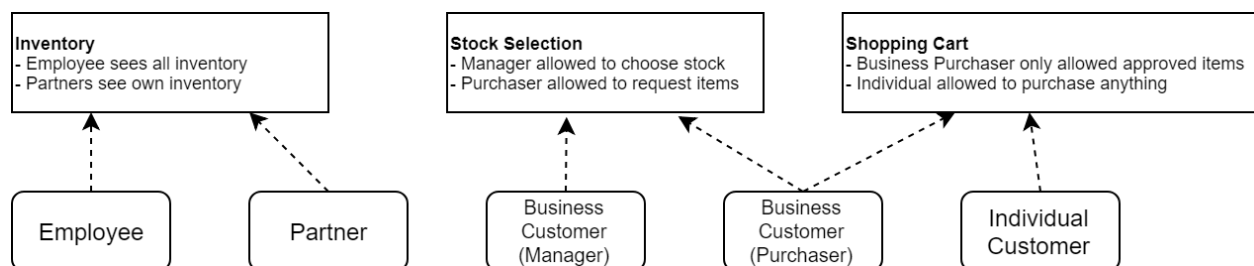


Figure 18 Assigning permissions based on user roles

Let's look at the WoodGrove shopping app again. In this app, the employees may see more restricted types of information, such as inventory levels across all products. Partners may also see inventory but are restricted to just the items that they are providing. Special types of customers may require a differing experience as well. In dealing with business customers, one member of the business can purchase inventory from a pre-selected list, and another person is responsible for determining what items are on the list. Individual customers might be able to buy anything available without restrictions.

This access control can be implemented using a few different approaches:

1. **Different policies for each persona.** The policy used to sign the user in dictates the content of the token issued by Azure AD B2C. Your app can pivot off the policy name itself which is dictated by the “tfp” claim, or alternatively, one policy may have some number of claims that are not available when logging in through another policy instead.

**Example token for individual**

```
{
  "name": "User",
  "idp": "google.com",
  "emails": [ "{user-email}@gmail.com" ],
  "tfp": "B2C_1A_sign_up_sign_in_personal"
}
```

**Example token for business manager**

If the tfp claim identifies the user as having authenticated with the B2C\_1A\_sign\_up\_sign\_in\_personal policy, it provides the user with the individual customer experience. If the user signed in with the B2C\_1A\_sign\_up\_sign\_in\_work policy, the app presents the experience meant for business users.

2. **Different Claim Values Based on the User’s Role.** In this example, a new custom attribute called business\_customer\_role has been created. Every business user is further classified as a purchaser or a manager. The app looks up the value of this claim to decide if the business user can only make purchases from a limited approved set of products, or if they have more purchasing privileges.

**Example token for business manager**

```
{
  "name": "User",
  "idp": "https://sts.windows.net/businesscustomer...",
  "emails": [ "{user-email}@businesscustomer.domain" ],
  "business_customer_role": "manager",
  "tfp": "B2C_1A_sign_up_sign_in_work"
}
```

**Example token for business stocker**

To learn more about how to create and manage custom attributes for your users, please refer to the documentation: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-custom-attr>

## Step-Up MFA

Applicable To:	Collaboration
	Commerce

Even if a user has already logged in, you may choose to have certain parts of your app require a higher level of proofing to grant access. This can be done by placing a multi-factor authentication policy in front of sensitive parts of your app such as an administration portal. See <https://aka.ms/StepUpAUTH> for sample policies illustrating this.

## Identity Protection

Applicable To:	Collaboration
	Commerce

Azure Active Directory Identity Protection is a feature of the Azure AD Premium 2 (P2) edition that enables you to:

- Detect potential vulnerabilities affecting your organization's identities
- Configure automated responses to detected suspicious actions that are related to your organization's identities
- Investigate suspicious incidents and take appropriate action to resolve them

These features provide protection for both employee and partner accounts. Additional information can be found here: [Azure Active Directory Identity Protection](#).

The typical access patterns expected of employee or partner accounts rarely apply to consumer accounts, which have a limited access scope. Azure AD B2C provides protection against denial of service and password attacks for your apps that use consumer accounts. Additional details are available here: [Azure Active Directory B2C: Threat management](#).

## Identity Lifecycle Management and Governance

Organizations want to minimize the number of employees, collaborators and end-users who have access to secure information or resources to reduce the chance of a malicious user getting access, or an authorized user inadvertently impacting a sensitive resource. However, users still need to carry out privileged operations in Azure AD, Azure, Office 365, or SaaS apps.

For commerce scenarios, the customer chooses when to sign up or sign in to your app, and similarly, also decides when they no longer want to interact with your app by deleting their account with you.

However, in collaboration scenarios, the end-user is typically not the person who chooses the levels of access they have to a partner's resources. This is instead governed by their own employer's administrators, based on factors such as whether the employee is still with the company or is working on the same project. While your relationship with the business collaborator may last for a long time, the individuals performing actions on behalf of the business may change.

In the following sections, we will explore the tools in Azure AD that enable you to manage external users' access to your corporate resources. Additionally, for a full video walk-through of governance and lifecycle management capabilities for managing external users, click here: [Azure AD B2B User Lifecycle Management](#)

## Terms of Use

Applicable To:

Collaboration

Commerce

During the initial account sign-in experience for both partner and consumer accounts, a description of the terms of use for your app can be provided. The specific messaging that you provide may be different for partner accounts versus consumer accounts.

You will want the users to agree to the terms of use when they initially sign-up to use your app. For regular sign-in events, the users should not need to accept the terms of use unless they have changed since the last acceptance. Additionally, you want to be able to know who has accepted the terms of use, which version, and when that acceptance occurred.

Azure Active Directory provides these abilities for employee, partner, and consumer accounts.

For additional information related to partner and employee accounts: [Azure Active Directory Terms of use feature](#).

For additional information related to consumer accounts: [Manage user access in Azure AD B2C - Capture terms of use agreement](#).

## Access Reviews

Applicable To:

Collaboration

Access Review is a capability of Azure AD that helps you decide if an employee or a guest you invited to collaborate with you in the past still requires access to your resources. Doing periodic access reviews ensures your users don't retain unnecessary permissions. With Access Reviews, you can:

- Conduct access reviews of guests' access to applications and group memberships, using the insights that are provided to efficiently decide whether guests should have continued access.
- Recertify employee access to applications and group memberships with access reviews.
- Collect access review controls into programs that are relevant for your organization to track reviews for compliance or risk-sensitive applications.
- Recertify the role assignment of administrative users who are assigned to Azure AD roles such as Global Administrator, or Azure subscription roles. This capability is included in Azure AD Privileged Identity Management.

For more information on how to configure Access Reviews, click here: [Azure AD Access Reviews](#)

## Privileged Identity Management

Applicable To:

Collaboration

Privileged Identity Management (PIM) is another core aspect of ensuring your employees and guests are only given the level of access they need, for the duration of time that they need it. This feature allows you to maintain tighter control of your users' permissions and privileges with capabilities such as being able to audit and view reports on the list of users who have privileged roles, Just-In-Time elevation of access for users, getting real-time alerts about changes in administrator assignments, and more.

For more information on PIM, click here: [What is Privileged Identity Management?](#)

## Pricing

Three separate components are combined to create this solution. Azure Active Directory is the source of employee identity. Azure AD B2B integrates with Azure Active Directory to allow guest users access to your company's resources. Azure AD B2C is a separate tenant that stores customer identity.

The following are links to pricing information for the components required for this solution:

- [Azure AD B2C Pricing](#)
- [Azure AD Pricing, including B2B usage](#)
- [Azure Pricing Calculator](#) (for Azure App Services, Storage or other helper components)

## Solution support and analytics

Comprehensive telemetry and analytics are essential to ensure your users can access your apps and services without issue, and can help you identify potential security, scaling, and usability issues proactively. The following are some of the built-in reports and reporting interfaces you can use to assess the health of your overall identity solution.

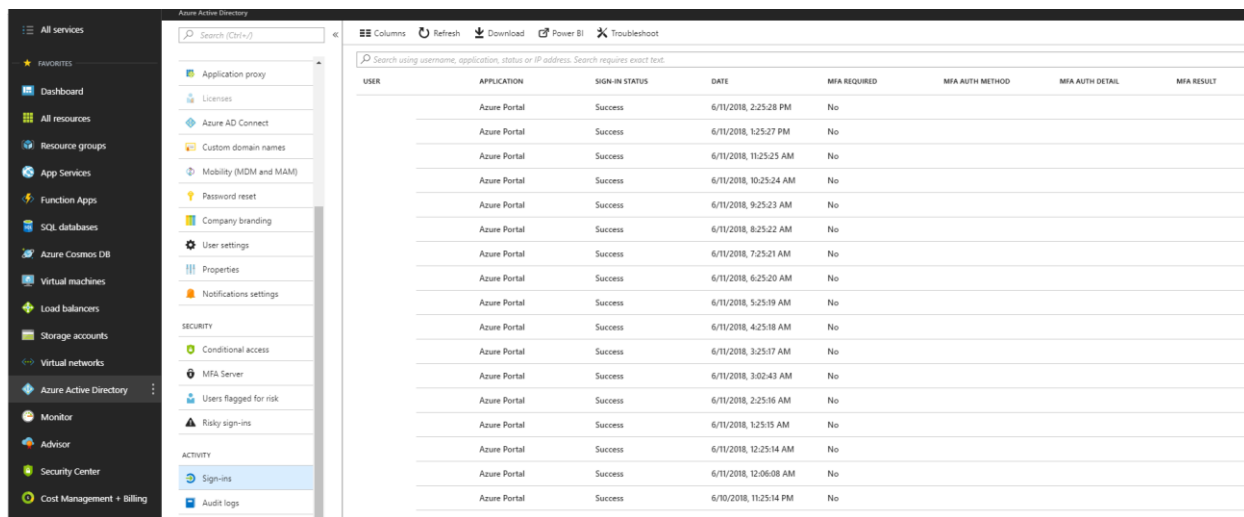
### Sign-In Reports

Applicable To:

Collaboration

Commerce

Sign-in reports provide a record of each sign-in on an Azure AD tenant. You can view these reports in the Azure portal (Azure Active Directory > Activity > Sign-ins)



USER	APPLICATION	SIGN-IN STATUS	DATE	MFA REQUIRED	MFA AUTH METHOD	MFA AUTH DETAIL	MFA RESULT
	Azure Portal	Success	6/11/2018, 2:25:28 PM	No			
	Azure Portal	Success	6/11/2018, 1:25:27 PM	No			
	Azure Portal	Success	6/11/2018, 11:25:25 AM	No			
	Azure Portal	Success	6/11/2018, 10:25:24 AM	No			
	Azure Portal	Success	6/11/2018, 9:25:23 AM	No			
	Azure Portal	Success	6/11/2018, 8:25:22 AM	No			
	Azure Portal	Success	6/11/2018, 7:25:21 AM	No			
	Azure Portal	Success	6/11/2018, 6:25:20 AM	No			
	Azure Portal	Success	6/11/2018, 5:25:19 AM	No			
	Azure Portal	Success	6/11/2018, 4:25:18 AM	No			
	Azure Portal	Success	6/11/2018, 3:25:17 AM	No			
	Azure Portal	Success	6/11/2018, 3:02:43 AM	No			
	Azure Portal	Success	6/11/2018, 2:25:16 AM	No			
	Azure Portal	Success	6/11/2018, 1:25:15 AM	No			
	Azure Portal	Success	6/11/2018, 12:25:14 AM	No			
	Azure Portal	Success	6/11/2018, 12:06:08 AM	No			
	Azure Portal	Success	6/10/2018, 11:25:14 PM	No			

Figure 19 Built-in sign-in reports

### Audit Reports

Applicable To:

Collaboration

Commerce

Azure AD generates audit logs containing activity information about resources, issued tokens, and administrator access. Audit reports on both admin and app activity are available in the Azure portal

(Azure Active Directory > Activity > Audit logs). For Azure AD B2C, audit reports also contain rich data about authentication, and email and MFA activity by end-users. For more information about the data available via audit reports for Azure AD B2C, click here: <https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-audit-logs>

DATE	TARGET(S)	INITIATED BY (ACTOR)	ACTIVITY
6/10/2018, 10:21:09 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 10:19:37 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 10:19:36 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:28:02 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:27:04 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:23:25 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:20:58 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:18:16 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:18:15 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:17:16 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:15:50 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:12:55 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 5:12:55 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 4:52:15 PM	User : bf2d	9775393	Issue an id_token to the application
6/10/2018, 4:50:15 PM	User : bf2d	9775393	Issue an id_token to the application

Figure 20 Built-in admin audit logs

## Usage Reports

Applicable To:

Commerce

Azure AD provides authentication reports based on user sign-in and Azure Multi-Factor Authentication for end users of your application family across identity providers. When you know the number of users registered in the tenant, the providers they used to register, and the number of authentications by type, you can answer questions like:

- How many users from each type of identity provider (for example, a Microsoft or LinkedIn account) have registered in the last 10 days?
- How many authentications using Multi-Factor Authentication have completed successfully in the last month?
- How many sign-in-based authentications were completed this month? Per day? Per application?
- How can I estimate the expected monthly cost of my Azure AD B2C tenant activity?

Usage reports are only available via the Usage Reporting API and are not available via the Azure portal. They include number of users, number of logins, and volume of MFA.

For more information on how to use Azure AD B2C's reporting API to generate usage reports, see: [Azure AD B2C Reporting API](#).

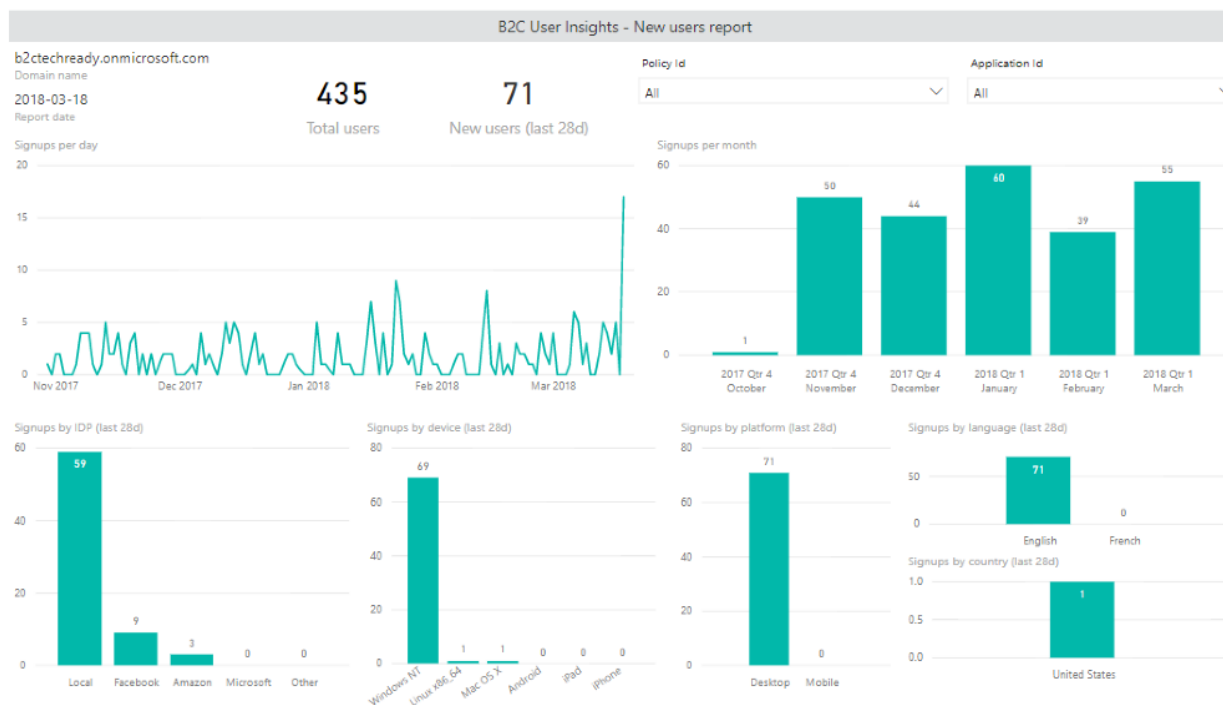


Figure 21 A Power BI dashboard generated using data from B2C's Reporting API

## Getting support from Microsoft

**Azure Support:** Depending on your Enterprise Agreement with Microsoft, you can call Microsoft Support and open a ticket for any issue related to your Azure Identity deployment. For more information on how to get in touch with Microsoft Support, please visit our Azure support portal:

<https://azure.microsoft.com/en-us/support>

**FastTrack:** If you have purchased Enterprise Mobility and Security (EMS) licenses or Azure AD Premium licenses, you may be eligible to receive deployment assistance from the FastTrack program. For more information on how to engage with FastTrack, please refer to our documentation on the [FastTrack Center Eligibility Benefit for Enterprise Mobility and Security](#)

**Engage the Product Engineering Team:** If you are working on a major customer deployment with millions of users, you can work with your Microsoft account team or your Cloud Solutions Architect to decide if the project's deployment complexity warrants working directly with the Azure Identity Product Engineering team.

**EMS Blog:** Subscribe to the [EMS Blog](#) to stay up to date with all the latest product announcements, deep dives, and roadmap information provided directly by the Identity engineering team. You can also post comments and get feedback from the engineering group.

**Azure Active Directory Public Forums:** Azure AD also has several closely monitored channels available to the public. Here are some useful links:

- Stack Overflow using the tag ['azure-ad-b2c'](#)
- [UserVoice](#) to submit or vote on new feature requests in Azure AD B2C



- Microsoft Azure on Reddit: <https://www.reddit.com/r/AZURE/>
- [MSDN Forum for Azure AD](#)

#### Code Samples on GitHub:

- [Azure AD B2C](#)
- [Azure AD B2B](#)

## Additional Resources

- Gaining Expertise with Azure AD B2C: A Course for Developers: <https://aka.ms/LearnAADB2C>
- WoodGrove B2C/B2B App Referred to in this document: <http://aka.ms/externaliddemo>
- Product Demos for B2B from Ignite 2017: <https://youtu.be/jgdxtBk8vDI>
- Azure AD B2B Product Documentation: <https://aka.ms/aadb2b>
- Azure AD B2C Product Documentation: <https://aka.ms/aadb2c>

© 2018 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes

It is understood and agreed to that project plan may provide certain information that is and must be kept confidential. To ensure the protection of such information you should not disclose any part of this plan to anyone unless required to do so by law.