

Azure Active Directory External Identities - Adoption Kit

Version: 3.0

For the latest version, please check <https://aka.ms/aadadoptionkits>

Contents

Azure Active Directory External Identities - Adoption Kit.....	1
Awareness	3
Business Overview.....	3
Pricing and licensing requirements.....	4
Key benefits	4
Announcements.....	4
Training/ learning resources.....	5
Level 100 concepts.....	5
Training.....	5
Videos.....	5
Online courses	6
Whitepaper.....	7
End-user readiness and communication	7
B2B collaboration.....	8
Invitation redemption flow	8
Enable B2B collaboration	8
Manage invitations.....	9
Self-service sign up.....	9
Bulk invite external users	9
Manage access in hybrid organization.....	9
Leave an organization.....	9
Manage authentication.....	9
Federate with identity providers.....	10
One-time passcode authentication (preview)	10
Manage B2B users.....	10
Troubleshoot.....	11
Quickstarts.....	11
B2C integration	12
Quickstarts.....	12
Samples	13

Customer stories/Case studies 14

Support and feedback..... 14

Awareness

This section helps you to analyze the benefits of Azure Active Directory External Identities. You will learn about the ease of use, benefits, pricing, and licensing model. You will also receive up-to-date announcements that discuss ongoing improvements.

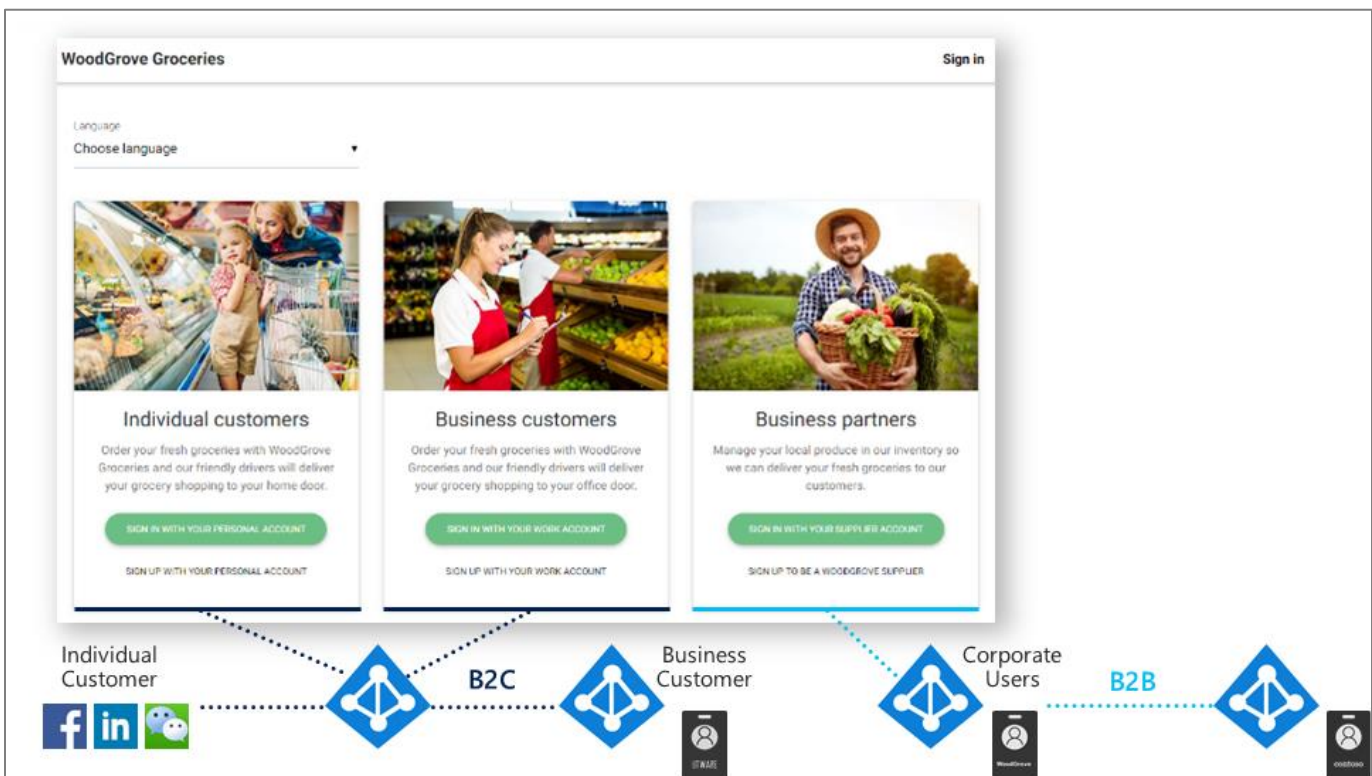
Business Overview

[Azure Active Directory \(Azure AD\) External Identities](#) is a set of capabilities that enables organizations to secure and manage any external user, including customers and partners. These capabilities focus less on a user's relationship to your organization and more on the way an individual wants to sign-in to your applications and resources. The identity provider manages the external user's identity, and you manage access to your apps with Azure AD to keep your resources protected.

The Azure AD supported external identities scenarios are:

- [Azure AD Business-to-Business \(B2B\) collaboration](#). Securely share your company's applications and services with guest users from any other organization, while maintaining control over your own corporate data. A simple invitation and redemption process let partners use their own credentials to access your company's resources.
- [Azure AD Business-to-Consumers \(B2C\) integration](#). An identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single page (SPA), and other applications. You can customize the entire user experience with your brand so that it blends seamlessly with your web and mobile applications.

See this example of [WoodGrove Groceries](#), a live web application created by Microsoft to demonstrate several B2C features. The partner identity is provided by B2B collaboration.



Pricing and licensing requirements

Azure AD External Identities pricing is based on Monthly Active Users (MAU), helping you to reduce costs and forecast with confidence. You can benefit from a free tier and flexible, predictable pricing for external users:

- Your first 50,000 MAUs per month are free for both Premium P1 and Premium P2 features.
- Connect with customers and partners based on the usage and features you need, rather than the licenses you have.
- Pay only for what you use. Forecast with ease as your business and usage scales. Customers are not charged for a MAU's subsequent authentications or for storing inactive users within that calendar month.

For more information, refer to [Azure AD External Identities pricing](#).

Key benefits

Using Azure AD External Identities capabilities provides the following benefits:



Seamless, highly secure access

Connect your users with the apps they need with a seamless experience across cloud, mobile and on-premises apps. You can customize the entire user experience with your brand so that it blends seamlessly with your web and mobile applications.



Comprehensive Identity Protection

Protect user accounts and increase security with conditional access and ongoing threat detection and response. Integrate with external user stores user profile or personal data to satisfy regional or on-premises data storage policies. Facilitate identity verification and proofing with third-party systems.



Efficient management and compliance at scale

Brings all the benefits of Active Directory to application developers that want to bring their apps to consumers. You get the ability to scale as your needs grow, meaning you only pay for what you need. B2C provides multiple options for identity.



Collaborate with any partners

Connect and collaborate with your customers and partners easily and more securely using their identities. You do not need to manage external accounts. You can bring your external partners on board in ways customized to your organization's needs.

Announcements

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to [What's new in Azure AD?](#)

Training/ learning resources

The following resources are a good start to learn about Azure AD External Identities. They include level 100 concepts, videos by our experts, link to online courses, and useful whitepapers for reference.

Level 100 concepts

Microsoft understands that some organizations have unique environment requirements or complexities. If yours is one of these organizations, use these recommendations as a starting point. However, most organizations can implement these recommendations as suggested.

- Find [what is the identity secure score in Azure AD?](#)
- Know the [five steps to securing your identity infrastructure.](#)
- Understand [identity and device access configurations.](#)

To get started with Azure AD External Identities:

- Know [the external identities in Azure AD.](#) Compare B2B and B2C collaboration.
- Learn [what is guest user access in B2B collaboration](#)
- Understand the difference in between [Office 365 external sharing and B2B collaboration](#)
- Know the [limitations of B2B collaboration](#)
- Know the [B2B collaboration FAQs](#)
- Learn [about B2C integration](#)
- Understand how you can [govern access for external users](#)

For more information, deep-dive into [External identities](#) and [B2C documentation](#).

Training

Videos

Video	Description
How to get started with identity security	Learn about identity security, why is it important, and what you can do to get it more secure.
How to improve your identity security posture with Secure Score	Get a walk-through of the identity secure score in the Azure AD portal.
Manage guest organization accounts in My Account	My Account is an online site that lets you manage your work or school account by letting you update your security information, manage your devices and guest organization accounts, and more. Learn how you can manage guest organization accounts in My Account.
User-based security strategy	Learn how to set up the right policies for your users and build your security framework and strategies.
What is Azure AD B2C?	Get an overview of B2C capabilities in Azure AD.

Video	Description
How to configure basic policies in Azure AD B2C?	Learn how to configure basic policies for B2C.
Advanced use cases with Azure AD B2C	Learn about the advanced use cases of B2C in Azure AD.
What is Azure AD B2B collaboration?	Get an overview of B2B collaboration, learn about its capabilities, and key scenarios, and understand the business value of this feature.
How to manage B2B identities	Learn how you can manage external users and their access in Azure AD.
Azure AD B2B authentication and federation	Learn about the key scenarios that are supported with B2B collaboration and how they can be deployed in the Azure AD portal.

Online courses

Refer to the following courses on Azure AD External Identities collaboration at pluralsight.com:

Course	Description
Design Identity Management in Microsoft Azure	<p>Learn to use Azure AD to enable a highly secure identity that can be leveraged across your organization's services and applications provided externally.</p> <p>Refer to Azure AD Overview module to learn about Azure AD B2B collaboration.</p>
Design Authentication for Microsoft Azure	<p>Learn to leverage Azure AD to solve all your cloud authentication requirements.</p> <p>Refer to Authentication Requirements for Different Scenarios module.</p>
Azure-tutorials: Implement-B2B-collaboration	Learn how to integrate Azure AD with existing directories, configure the application access panel, and implement Active Directory for B2C and B2B.

Whitepaper

Whitepaper	Description
Distribute Power BI content to external guest users using Azure Active Directory B2B	This is a technical whitepaper outlining how to distribute content to users outside the organization using the integration of Azure AD B2B.
Azure AD Customer and Partner Identity Management	Explore common use cases for external identities. Learn about unlocking business value by empowering digital relationships with your customers and partners.
Modernize customer and partner relationships for CMOs, CHROs, COOs	Learn how Microsoft Azure AD External Identities can help business leaders execute on their marketing, operational, communications, and workforce goals.
Secure your customer-facing apps	Learn why IT leaders must keep security top-of-mind for consumer-facing apps.

End-user readiness and communication

This section provides customizable posters and email templates to roll out Azure AD B2B collaboration to your guest users.

Invitation emails are a critical component to bring partners on board as B2B collaboration users in Azure AD. You can use them to increase the recipient's trust. You can add legitimacy and social proof to the email to make sure the recipient feels comfortable with selecting the **Get Started** button. Refer to [The elements of the B2B collaboration invitation email - Azure Active Directory](#).

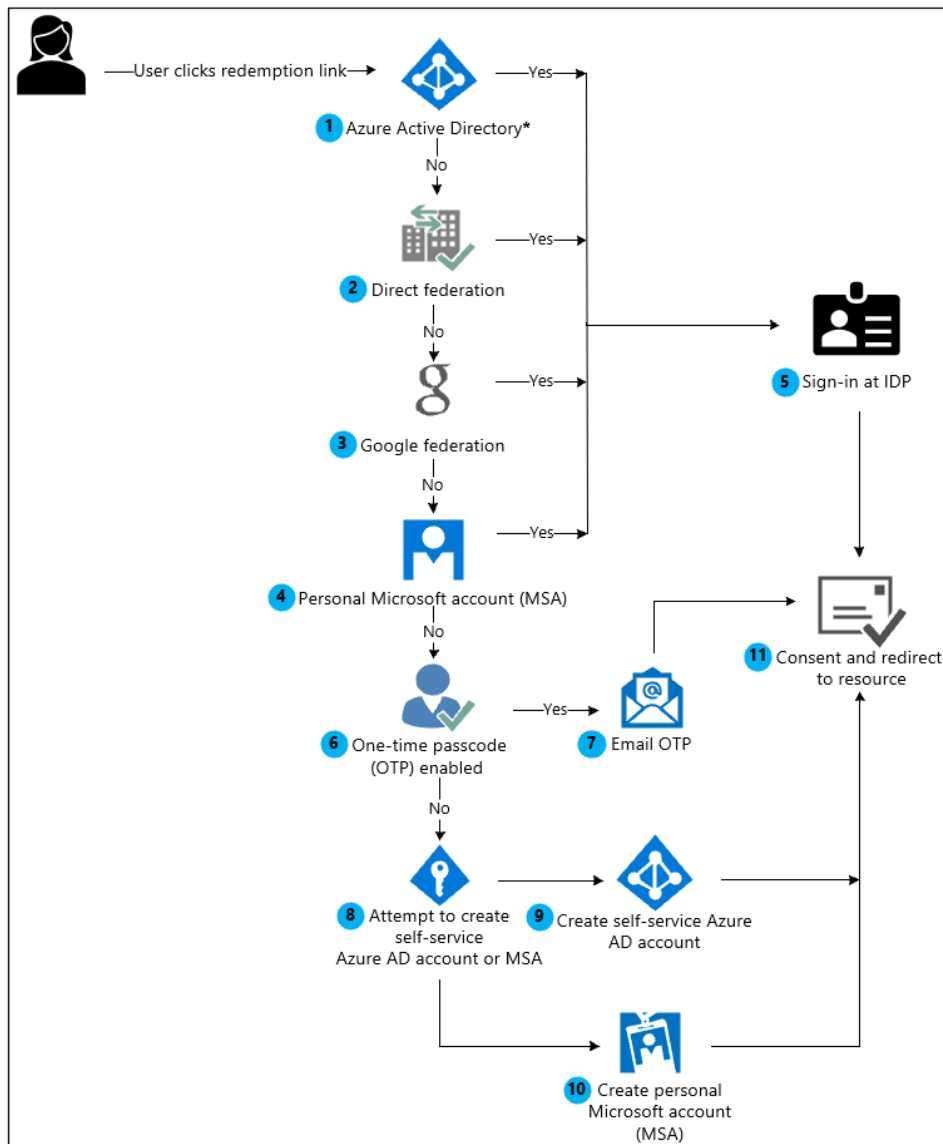
B2B collaboration

In this section, learn to configure and manage Azure AD B2B collaboration for your organization. You can also refer to some quickstarts and troubleshoot common issues.

Invite external users into your own tenant as "guest" users that you can assign permissions to (for authorization) while allowing them to use their existing credentials (for authentication).

Invitation redemption flow

Understand the [redemption flow and consent experience for the user](#) to follow the ways guest users can access your resources (email or direct link) and the consent process they will encounter.



Enable B2B collaboration

Make sure your organization's external collaboration settings are configured such that you can invite guests. To view and set these policies, see [Enable B2B external collaboration and manage who can invite guests](#).

Before you progress, we recommend that you visit these [Azure AD B2B best practices and recommendations](#).

Manage invitations

Extend invite to the B2B users. Refer to the links below:

Link	Description
Admins adding B2B users	Add guest users to the directory, group, or to an application. The invited user's account is added to Azure AD. The guest user must then redeem their invitation to access resources.
Information workers adding B2B users	After a guest user has been added to the directory in Azure AD, an application owner can send the guest user a direct link to the app they want to share.
Invite internal users to B2B	The distributors, suppliers, vendors, and other guest users may have internal credentials for them. Add the guest users with these credentials.
Allow or block invitations to B2B users from specific organizations	Use an allow or a deny list to allow or block invitations to B2B users from specific organizations.
Azure Active Directory B2B collaboration API and customization	Use the API to customize the invitation process

Self-service sign up

As an alternative to sending invitations directly to individuals, you can allow external users to [sign up for specific applications themselves](#).

Bulk invite external users

You can [bulk-invite external users to an organization from email addresses](#) that you have stored in a .CSV file.

Manage access in hybrid organization

[Give your external partners access to apps and resources in a hybrid configuration](#) where you have both on-premises and cloud-based resources.

Leave an organization

An [Azure AD B2B guest user can decide to leave an organization at any time](#) if they no longer need to use apps from that organization or maintain any association.

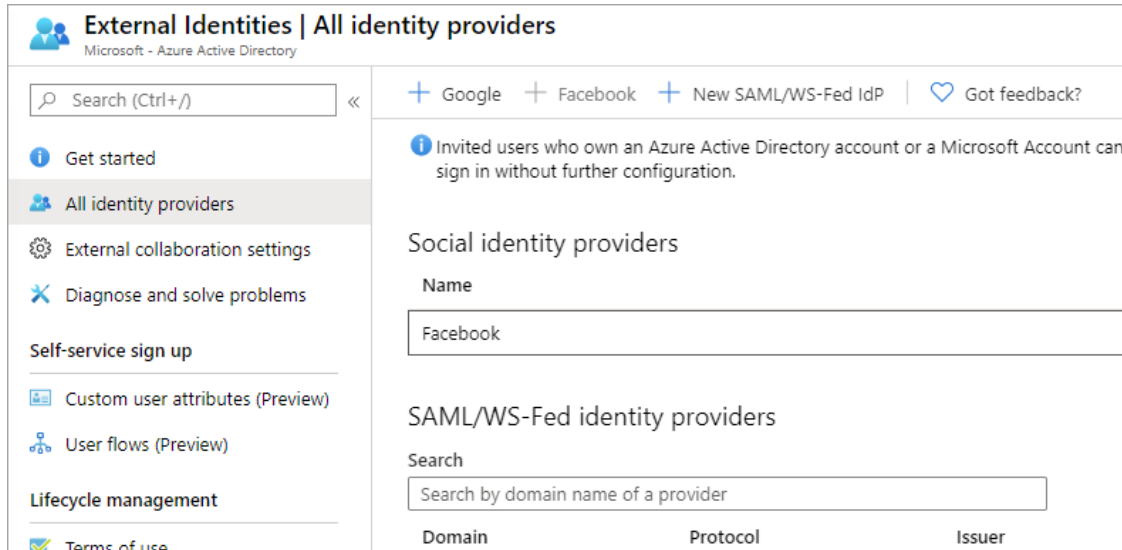
Manage authentication

You can securely authenticate the guests using their preferred identity providers or enable one-time passcode authentication (OTP).

Federate with identity providers

Whenever possible, [federate directly with identity providers](#) to allow invited users to sign in to your shared apps and resources without having to create Microsoft Accounts (MSAs) or Azure AD accounts.

You can enable users to sign in with various identity providers- [Google](#), [Facebook](#) or [direct federation with Active Directory Federation Services \(AD FS\) and third-party providers](#). See example: [Direct federation with AD FS \(preview\)](#)



One-time passcode authentication (preview)

In case the B2B guest user cannot authenticate with any of the above identity providers, you [can enable one-time passcode authentication for the user](#).

Manage B2B users

Know the [properties and states of the B2B guest user object](#) (UserType = Guest) before and after invitation redemption. Refer to the links below:

Link	Description
Add a B2B user to a role	Grant permissions to users from partner organizations in your Azure AD tenant
Create dynamic groups for B2B users	Create a group with rules for complex attributes. Members can be automatically added to or removed from a security group based on their attributes.
B2B collaboration for integrated SaaS apps	Configure SaaS apps for B2B collaboration
Conditional Access for B2B collaboration users	With B2B collaboration, organizations can enforce Multi-Factor Authentication 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.
Manage access for external users	Use Azure AD Entitlement Management for B2B guest user sign-up and manage their access to resources

[Manage guest access with Azure AD access reviews](#)

Ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access.

[Auditing and reporting a B2B collaboration user](#)

You can use access reviews to periodically verify whether guest users still need access to your resources. The Azure AD audit logs provide records of system and user activities, including activities initiated by guest users.

Troubleshoot

Resolve common problems with Azure AD B2B. See [Troubleshoot Azure AD B2B collaboration](#) issues.

Quickstarts

Follow the step-by-step guidance to:

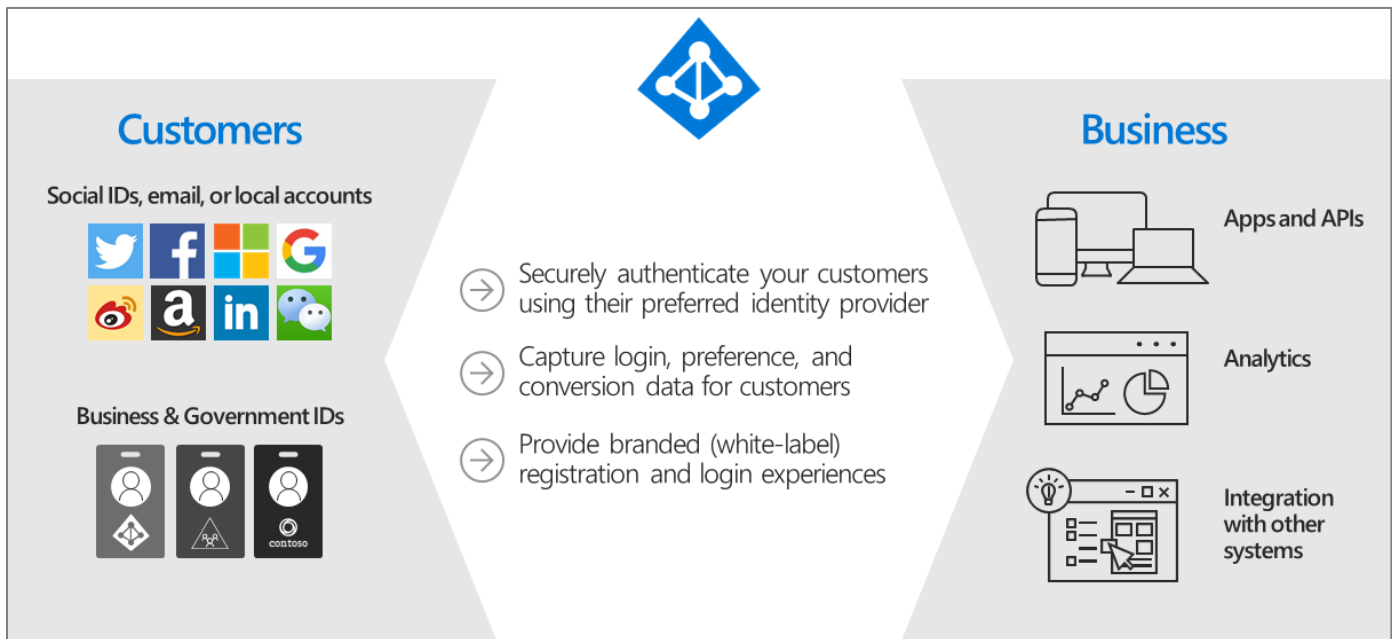
- [Use PowerShell to bulk invite Azure AD B2B collaboration users](#)
- [Bulk invite Azure AD B2B collaboration users](#)
- [Enforce Multi-Factor Authentication for B2B guest users](#)
- [Add a guest user with PowerShell](#)
- [Add guest users to your directory in the Azure portal](#)

B2C integration

In this section, learn to implement Azure AD B2C in your organization. Follow best practices and recommendations and refer to QuickStart links for step-by-step guidance.

Set up business-to-customer identity as a service. Your customers can use their preferred social, enterprise, or local account identities to get single sign-on (SSO) access to your applications and APIs. Customize and control how customers sign up, sign in, and manage their profiles when using your applications.

Understand the primary resources you work with in the service, its features, and how these enable you to provide a fully custom identity experience for your customers in your applications. See [Technical and feature overview of Azure AD B2C](#).



Visit the [best practices and recommendations](#) to cover some of the primary aspects of integrating Azure AD B2C into existing or new application environments.

Quickstarts

Follow the step-by-step guidance to:

1. [Create an Azure AD B2C tenant](#)
2. [Register a web application](#)
3. [Create user flows](#)
4. [Add identity providers to your applications](#)
5. [Customize the interface of user experiences](#)
6. Authenticate the users
 - o [Enable authentication in a web application](#)
 - o [Authenticate users in a native desktop client](#)
 - o [Enable authentication in a single-page application](#)
 - o [Enable authentication in a Python web application](#)
7. Grant API access
 - o [Grant access to an ASP.NET web API](#)
 - o [Grant access to a Node.js web API from a desktop app](#)

- [Protect and grant access to a Node.js web API from a single-page application](#)

For more information, deep-dive into the [How-to guides to implement B2C](#) and [References](#).

Samples

Refer to [sample codes for applications](#) including iOS, Android, .NET and Node.js.

Customer stories/Case studies

Discover how most organizations are coming together using Azure AD External Identities capabilities. The following featured stories demonstrate this scenario:



[Intralox used Azure AD B2C to build a secure, self-service portal that customers can access with their own corporate identities.](#) Intralox wanted to give customers easy access to the tool, while protecting its intellectual property. The manufacturer deployed Azure AD B2C and integrated it with Microsoft Dynamics 365 to validate and authenticate users. Customers sign in using their own work credentials, so accessing the tool is simple and secure.



[Singapore Airlines transforms customer loyalty with blockchain on Azure.](#) It uses Azure AD B2C to govern access, safeguard data across the shared network, and provide a solution that works with all of the partners' existing systems and databases.

To learn more about customer and partner experiences on Azure AD External Identities capabilities, visit - [See the amazing things people are doing with Azure.](#)

Support and feedback

How can we improve Azure AD External Identities capabilities? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our [Technical Community](#), a platform to Microsoft Azure AD users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try [StackOverflow](#) or visit the MSDN [Azure AD forums](#).

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - [feedback.azure.com](#).