

[Previous](#)

Unit 4 of 11 ▾

[Next](#) >

✓ 100 XP



Describe Azure external identities

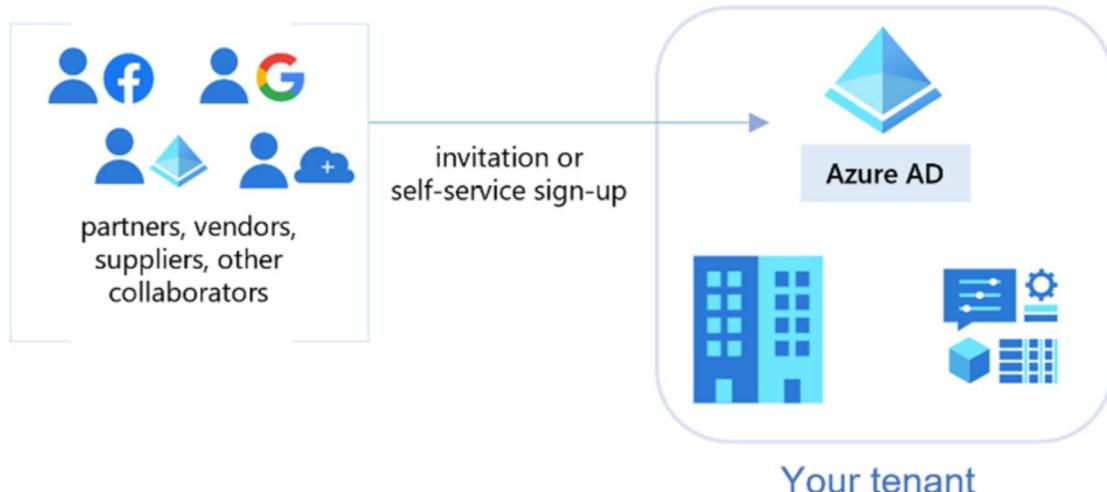
3 minutes

An external identity is a person, device, service, etc. that is outside your organization. Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization. If you want to collaborate with partners, distributors, suppliers, or vendors, you can share your resources and define how your internal users can access external organizations. If you're a developer creating consumer-facing apps, you can manage your customers' identity experiences.

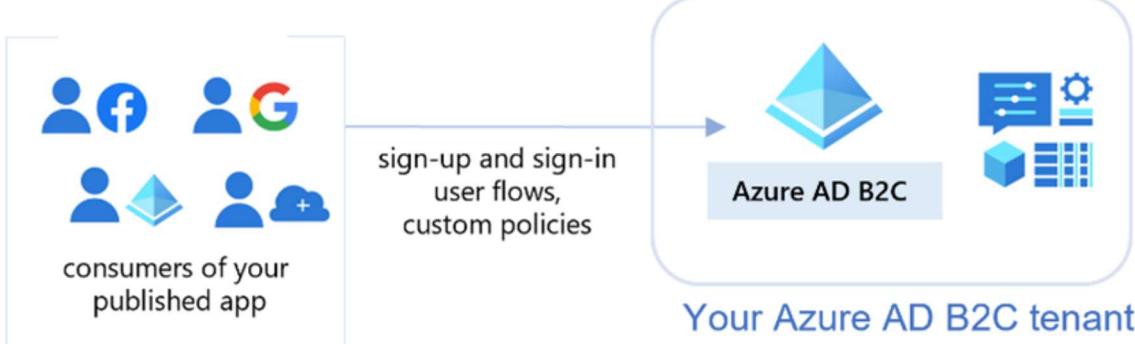
External identities may sound similar to single sign-on. With External Identities, external users can "bring their own identities." Whether they have a corporate or government-issued digital identity, or an unmanaged social identity like Google or Facebook, they can use their own credentials to sign in. The external user's identity provider manages their identity, and you manage access to your apps with Azure AD or Azure AD B2C to keep your resources protected.

Azure AD External Identities

B2B collaboration



Azure AD B2C



The following capabilities make up External Identities:

- **Business to business (B2B) collaboration** - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.
- **B2B direct connect** - Establish a mutual, two-way trust with another Azure AD organization for seamless collaboration. B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams. B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.

- **Azure AD business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

Depending on how you want to interact with external organizations and the types of resources you need to share, you can use a combination of these capabilities.

With Azure Active Directory (Azure AD), you can easily enable collaboration across organizational boundaries by using the Azure AD B2B feature. Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.

You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Azure AD. When an access review is finished, you can then make changes and remove access for guests who no longer need it.

Next unit: Describe Azure conditional access

[Continue >](#)