100 XP

Collaborate by using guest accounts and Azure Active Directory B2B

5 minutes

You want the external team to collaborate with the internal developer team in a process that's easy and secure. With Azure Active Directory (Azure AD) business to business (B2B), you can add people from other companies to your Azure AD tenant as guest users.

If your organization has multiple Azure AD tenants, you may also want to use Azure AD B2B to give a user in tenant A access to resources in tenant B. Each Azure AD tenant is distinct and separate from other Azure AD tenants and has its own representation of identities and app registrations.

Guest user access in Azure AD B2B

In any scenario where external users need temporary or restricted access to your organization's resources, give them guest user access. You can grant guest user access with the appropriate restrictions in place, then remove access when the work is done.

You can use the Azure portal to invite B2B collaboration users. Invite guest users to the Azure AD organization, group, or application. After you invite a user, their account is added to Azure AD as a guest account.

The guest can get the invitation through email, or you can share the invitation to an application by using a direct link. The guest then redeems their invitation to access the resources.

By default, users and administrators in Azure AD can invite guest users, but the Global Administrator can limit or disable this ability.

Collaborate with any partner by using their identities

If your organization has to manage the identities of each external guest user who belongs to a given partner organization, it faces increased responsibilities because it has to secure those

identities. There's an increased workload to manage and administer those identities. You also have to sync accounts, manage the lifecycle of each account, and track each individual external account to meet your obligations. Your organization has to follow this procedure for every partner organization with which it wants to collaborate. Also, if something happens to those accounts, your organization is liable.

With Azure Active Directory B2B, you don't have to manage your external users' identities. The partner has the responsibility to manage its own identities. External users continue to use their current identities to collaborate with your organization.

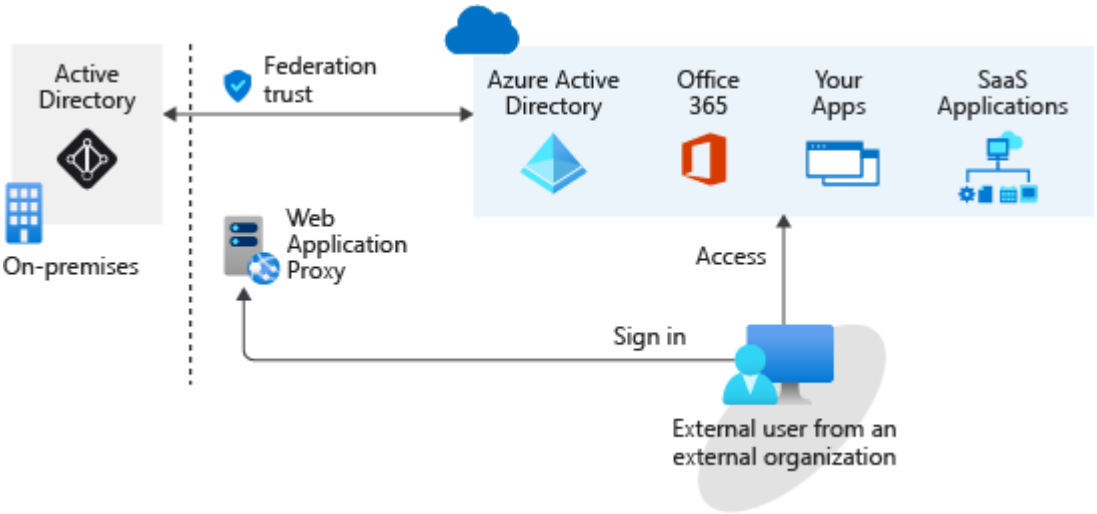
For example, say you work with the external partner Giovanna Carvalho at Proseware. Her organization manages her identity as gcarvalho@proseware.com. You use that identity for the guest account in your organization's Azure AD. After Giovanna redeems the guest account invitation, she uses the same identity (name and password) for the guest account as she does for her organization.

Why use Azure AD B2B instead of federation?

With Azure AD B2B, you don't take on the responsibility of managing and authenticating the credentials and identities of partners. Your partners can collaborate with you even if they don't have an IT department. For example, you can collaborate with a contractor who only has a personal or business email address and no identity management solution managed by an IT department.

Giving access to external users is much easier than in a federation. You don't need an AD administrator to create and manage external user accounts. Any authorized user can invite other users. A line manager could, for example, invite external users to collaborate with their team. When collaboration is no longer needed, you can easily remove these external users.

A federation is more complex. A federation is where you have a trust established with another organization, or a collection of domains, for shared access to a set of resources. You might be using an on-premises identity provider and authorization service like Active Directory Federation Services (AD FS) that has an established trust with Azure AD. To get access to resources, all users have to provide their credentials and successfully authenticate against the AD FS server. If you have someone trying to authenticate outside the internal network, you need to set up a web application proxy. The architecture might look something like the following diagram:



An on-premises federation with Azure AD might be good if your organization wants all authentication to Azure resources to happen in the local environment. Administrators can implement more rigorous levels of access control, but this means that if your local environment is down, users can't access the Azure resources and services they need.

With a B2B collaboration, external teams get the required access to Azure resources and services with the appropriate permissions. There's no need for a federation and trust to be established, and authentication doesn't depend on an on-premises server. Authentication is done directly through Azure. Collaboration becomes simplified, and you don't have to worry about situations where users can't sign in because an on-premises directory isn't available.

Next unit: Exercise - Give guest users access in Azure Active Directory B2B

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆