Modern ways for external collaboration – Azure AD B2B
Summary

Collaboration with external partners is becoming increasingly important for companies. Global enterprise supply chains are more agile than ever before and require frequent information exchange between different parties. This brings additional collaboration needs for most global enterprises. Managing external partner accounts is always challenging for enterprise IT departments. IT admins need to create identities for each external partner and manage them in their active directory.

Today, with Azure AD B2B, organizations can work with any other organization easily and securely without having to create and manage new identities for their partners.

Our whitepaper explains how organizations can benefit from Azure AD B2B and simplify their IT operations, reduce costs (by managing fewer identities and paying less for licenses), and improve their security posture.

The document also highlights several scenarios in which various Azure services such as conditional access, identity protection and multi-factor authentication (MFA) are integrated with Azure AD B2B.
What is the current problem with external collaboration?

No matter how big or small, regardless of industry and irrespective of their compliance and security posture, every organization must collaborate with other organizations to succeed in their business. Today, this is done in expensive, time-consuming and often insecure ways.

- External Identities must be created by IT for each partner, and there is no seamless integration between companies.
- Each collaboration requires different identities and credentials.
- Each identity causes additional license costs.
- Instead of using IT tools, organizations often follow simple and insecure ways, bypassing the steps required to manage external identities lifecycle.

Recent pandemic (Covid-19) situations have increased the demand for remote working and external collaboration (according to Microsoft, the number of active B2B collaboration users increased by 65% in March 2020).

According to the recent data breach report by Verizon, 37% of data breaches are due to stolen or lost credentials. With hacking attacks, identity causes account for over 80% of all breaches.
How can Azure AD B2B help?

Azure AD B2B brings a variety of benefits to external collaboration between companies. Here are the most important business reasons to use Azure AD B2B:

• **Easy and secure collaboration**: It is intuitive for the end user. There are no external partner requirements. When collaboration with your partners is over, partner users can be easily removed from your Azure tenant and their access to your applications is revoked immediately. Additional Azure AD security features such as identity protection, conditional access policies and multi-factor authentication (MFA) can be easily extended to partner collaboration.

• **Enhanced IT governance**: Azure AD B2B provides end-to-end lifecycle management of external identities. This helps organizations build a strong governance structure. Additional Azure capabilities (e.g. identity protection, entitlement management) can be extended with Azure AD B2B to enhance governance capabilities.

• **Reduced IT operational costs**: There is no longer a need to create identities, manage passwords and fulfill complex configuration requirements for external identities. By using Azure AD B2B, these IT operations and all related costs can be handed off to external partners. In addition, business users can handle the invitation of partner identities (only for organizations approved by IT) without IT effort, enabling seamless collaboration between business and IT.

• **Lower license costs**: Azure AD B2B offers free licenses at a 1:5 ratio for Azure AD paid services. In the new Microsoft licensing model (MAU*), the first 50,000 AD users even receive a P2 license at no cost. The details are explained in the licensing section of the document.

You can find the complete list of Azure AD B2B benefits in the slides below.
What is Azure AD B2B?

Azure AD B2B:

Azure AD B2B collaboration is an Azure AD service that enables organizations to share their company’s applications and services with external partners via an invitation process. External users are invited to consume company resources through this secure invitation process. This enables secure collaboration with external partners, even if they do not have Azure AD or an IT department.

How does it work?

1. An invitation URL is sent to the partner by email or direct link
2. The guest user must click the URL and sign in with their identity
3. When guest users access the resources for the first time, they are prompted to accept Microsoft’s privacy policy (Terms of use) and consent for the collaborating organization to access and process your data. The terms of use can also be configured to include the company’s privacy policy
4. If a direct link is used, the guest user will be redirected to their home tenant for the authentication
5. After login and authentication, the guest user can access the resource
Top 4 use cases where Azure AD B2B can help in your organization

1. **Collaborating with partners who have their own Azure AD identity:** The partner’s Azure AD identity is invited to join your company resources.

2. **Collaborating with partners who do not have an Azure AD identity but do have an on-premise identity:** In this case, the home organization configures direct federation (using SAML or WS federation) between the partner organization before providing external identities.

3. **Collaborating with partners who only have email - email one-time passcode:** In this scenario, the external partner only has a valid email and authentication takes place with a one-time email passcode.

4. **Collaborating with partners who have only social identities such as Google and Facebook:** Here, the partner is instructed to create a Microsoft identity as part of the invitation process. Simple pre-configuration for Facebook and Google identities is required.

---

Azure AD B2B use cases

Azure AD B2B can be deployed in all types of business regardless of their size. Below we highlight the top use cases of Azure AD B2B.
1. Can be compared to domain/forest trust on-premise AD
2. The home organization user creates an invitation by entering the partner company user either in Azure AD B2B or directly in the application such as Microsoft Teams
3. The invitation background service validates the invitation (whether it is from allowed domains, if the user has already been created, etc.)
4. After validation, the invitation service creates the user object in the home company Azure tenant and marks the status of the object as pending until the provisioning flow is complete
5. The partner company user receives an email from the invitation service containing the access link to the invited application or directory

Note
Can be compared with Domain/Forest Trust On-premise AD
5. Once the partner company user accesses the link on the email, the Azure AD authentication service recognizes that there is a user in the home company tenant (in pending status) that belongs to the partner company and forwards the authentication request accordingly.

6. The partner company user is authenticated against its own Azure AD tenant + multi-factor authentication (MFA) and conditional access can be enforced to provide additional security.

7. Then the partner user must give consent to share their information with the home company (this step is required when the user first accesses the resources).

8. Once consent is received, the Azure AD B2B invitation service finalizes the flow, the user account is no longer in pending status and, after this step, the guest user can access the resources within the home company.

Example scenario:
A project manager in the home company invites a user from the partner company to collaborate in Microsoft Teams. The partner company does not require support from its IT department. The project manager at the home company can invite the partner directly via Microsoft Teams.
Use case 2:
The partner has on-premise but no Azure AD identity

5. When the partner clicks on the link, the invitation request is sent to the partner company’s ADFS because the email belongs to a different domain and is configured with a different federation service. The user enters their credentials, and ADFS sends an authentication response back to Azure AD. If the credentials are correct, Azure AD validates the authentication + multi-factor authentication (MFA) and conditional access “policies” can be enforced to provide additional security

6. Then the partner user must give consent to share their information with the home company (this step is required when the user first accesses the resources)

7. Once consent is received, the Azure AD B2B invitation service finalizes the flow, the user account is no longer in pending status and, after this step, the guest user can access the on-premise application within the home company

Example scenario:
The home company invites an external corporate agency to use an on-premise application. Note: Additional configuration (e.g. Azure App Proxy, MCAS) may be required to provide access to the on-premise application.
5. In this step, the Azure authentication service generates a one-time email passcode and sends it to the partner’s email address.

6. The partner validates the authentication by entering the one-time passcode.

+ multi-factor authentication (MFA) and conditional access can be enforced to provide additional security.

7. Then the partner user must give consent to share their information with the home company (this step is required when the user first accesses the resources).

8. Once consent is received, the Azure AD B2B invitation service finalizes the flow, the user account is no longer in pending status and, after this step, the guest user can access the resources within the home company.

**Example scenario:**
The home company invites an external consultant to consume reports in Power BI. The consultant can use the reports after accepting the invitation and authenticating with a one-time passcode.
5. When the partner clicks on the link, since the email address belongs to Gmail, it is directed to Google Social IdP via OAuth for authentication. The user enters their Gmail username and password and is authenticated with Google IdP. 

+ Multi-factor authentication (MFA) and conditional access can be enforced to provide additional security.

6. Next, partner users must give consent to share their information with the home company (this step is required when the user first accesses the resources).

7. Once consent is received, the Azure AD B2B invitation service finalizes the flow, the user account is no longer in pending status and, after this step, the guest user can access the resources within the home company.

Example scenario:
A finance manager in the home company invites an external accountant to collaborate on Dynamics 365. He/she can do this directly from Dynamics 365 by clicking “Invite external accountant”.

Prerequisite
The home company IT administrator must first configure Gmail as a social identity provider in their tenant.
Key benefits of Azure AD B2B at a glance

Secure

• Provide access to partner accounts via a secure and compliant invitation process
• Eliminate the risk of lost or orphan credentials
• Ensure consent from external partners (agreement to terms of use) to access your company resources. Enterprises can also integrate their information security policies in the consent approval and therefore check the audit log of reports of terms of use in the Azure portal

Easy integration with Azure functionalities

• Leverage integrated Azure functionalities such as MFA, conditional access, self-service password reset (SSPR) to improve the security posture
• Azure identity protection and Azure audit logs make it very easy to create user risk and logon policies, and take action to mitigate security risks and monitor security and compliance breaches

Licensing advantage

• Use Azure AD B2B collaboration feature without any additional licensing cost (each employee can invite up to 5 guests at no additional cost)
• The first 50,000 MAUs are free for both P1 and P2 licenses

Simplify identity lifecycle management

• Leaving identity management to external partners allows you to focus on different collaboration scenarios
• Reduce IT operations (no IT involvement for external account creation)

Seamless user experience

• Share Office 365, OneDrive documents, apps with external partners or invite them to Teams meetings quickly and easily via Azure AD B2B
• Users only need the invitation link to access shared resources
• Single sign-on to on-premise applications
Licensing requirements for Azure AD B2B

With Azure AD B2B collaboration, companies can invite up to five guest users for each Azure AD edition license they have for an employee or non-guest user. The following table explains the current and new licensing models:

<table>
<thead>
<tr>
<th>Licensing model</th>
<th>Benefits</th>
<th>Example scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:5 ratio</td>
<td>• Free based on the 1:5 ratio for Azure AD paid services</td>
<td>• For example, a company has 100 guest users who all require MFA. In this case, 20 Azure premium P1 licenses are required.</td>
</tr>
<tr>
<td></td>
<td>• Use of free Azure AD features with no additional licensing requirements</td>
<td></td>
</tr>
<tr>
<td>Microsoft External Identity Licensing</td>
<td>• The first 50,000 MAUs are free for both P1 and P2 licenses</td>
<td>• With this license model, companies do not need to purchase additional licenses for their guest users, as the first 50,000 users do not require a license</td>
</tr>
<tr>
<td>based on MAU*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*MAU: monthly active users
What are the next steps after Azure AD B2B

- Explore the **self-service sign-up user flow** feature in Azure AD B2B. Self-service sign-up is a public preview feature of the Azure active directory. A self-service sign-up user flow creates a sign-up experience for your external users through the application you want to share. You can integrate your custom flows with the Azure AD B2B scenarios shown in this document to collect additional information from your external partners during the sign-up process. Check [here for details and examples](#).

- If you have already implemented Azure AD B2B and secured your identities, it is time to leverage **entitlement management**: Entitlement management is an Azure governance feature that allows you to manage access requests from your external partners via the creation of access packages and catalogs. Additionally, you can use delegation to ensure seamless business involvement.
  - **Tip:** You can consume this service for your first 50,000 monthly active users for free. For details, see [licensing details](#).

- Detect and manage identity related risks and vulnerabilities via **Identity Protection**
  - **Tip:** You can consume this service for your first 50,000 monthly active users for free. For details, see [licensing details](#).
About Avanade
Avanade is the leading provider of innovative digital and cloud-enabling services, business solutions and design-led experiences, delivered through the power of people and the Microsoft ecosystem. Avanade, which is majority-owned by Accenture, was founded in 2000 by Accenture LLP and Microsoft Corporation and has 38,000 employees in 25 countries.

Visit us at www.avanade.com

© 2021 Avanade Inc. All rights reserved. The Avanade name and logo are registered trademarks in the U.S. and other countries. Other brand and product names are trademarks of their respective owners.