Introducing Azure Active Directory B2B collaboration

Use cloud power to collaborate with your business partners

Microsoft Corporation

Published: September 2015 (Updated: April 2017)

Version: 1.0

Author: Philippe Beraud (Microsoft France)

Reviewers: Daniel Pasquier (Microsoft France), Arvind Suthar (Microsoft Corporation)

For the latest information on Azure Active Directory, please see

http://azure.microsoft.com/en-us/services/active-directory/

Copyright© 2017 Microsoft Corporation. All rights reserved.

Abstract: Azure AD, the Identity Management as a Service (IDaaS) cloud multi-tenant service with proven ability to handle billions of authentications per day, extends its capabilities with a feature for simply and securely sharing corporate applications with your business partners: Azure AD B2B (business-to-business) collaboration.

This feature helps secure business-to-business collaboration with the partner organizations that you work with every day.It provides simplified management and security for partners and other external users accessing your in-house resources using Azure AD as the control plane. This includes access to popular cloud applications such as Salesforce, Dropbox, Workday, and of course, Office 365 – and all of this is in addition to your mobile, cloud, and on-premises claims-aware corporate applications.Azure AD B2B collaboration is easy to configure and easy to maintain.

This document is intended for IT professionals, system architects, and developers who are interested in understanding how Azure AD B2B collaboration helps supporting your cross-company relationships by enabling partners to selectively access your corporate applications and data using their self-managed identities, and how to leverage the related capabilities.

Table of Content

[Introduction 2](#_Toc480356268)

[Objectives of this paper 6](#_Toc480356269)

[Non-objectives of this paper 6](#_Toc480356270)

[Organization of this paper 7](#_Toc480356271)

[About the audience 7](#_Toc480356272)

[Supporting B2B collaboration scenarios 8](#_Toc480356273)

[Understanding classic partner access models 8](#_Toc480356274)

[Extending Azure AD for external identities 10](#_Toc480356275)

[Understanding Azure AD B2B collaboration partner access model 11](#_Toc480356276)

[Understanding Azure AD B2B collaboration high level workflow 13](#_Toc480356277)

[Comparing B2B collaboration with B2C in Azure AD 13](#_Toc480356278)

[Understanding Azure AD B2B collaboration business model 14](#_Toc480356279)

[Getting Started with Azure AD B2B collaboration 16](#_Toc480356280)

[Fulfilling the pre-requisites for the walkthrough 16](#_Toc480356281)

[Inviting a set of guest users as an administrator (inviter UX) 17](#_Toc480356282)

[Receiving and accepting the invitation as a corporate user (invitee UX) 30](#_Toc480356283)

[Receiving and accepting the invitation as a social ID user (invitee UX) 36](#_Toc480356284)

[Delegating invitations to non-administrators (inviter UX) 43](#_Toc480356285)

[Leveraging multi-factor authentication for guest users 50](#_Toc480356286)

[Customizing onboarding using the Invitation API (inviter UX) 55](#_Toc480356287)

[Viewing and managing the invitees (inviter UX) 56](#_Toc480356288)

[Leveraging auditing and reporting capabilities (inviter UX) 59](#_Toc480356289)

[Appendix A. Building a test lab environment 61](#_Toc480356290)

[Building the test environment for the inviter 61](#_Toc480356291)

[Building the test environment for the Litware369 invitees 75](#_Toc480356292)

[Setting up the test environment for the social ID invitees 78](#_Toc480356293)

# Introduction

Ongoing digital relationships and connectivity with people and things are fundamental to the success of today’s organizations.

Identity is the foundational technology enabling this. Regardless of their size, organizations need a single way to do identity, whether it be for employees, customers, partners or devices. Anything must be able to have a digital relationship - and connect to anything else.

Azure Active Directory (Azure AD) is Microsoft’s vehicle for responding to this requirement by providing Identity Management as-a-Service (IDaaS) capabilities in a cloud or hybrid environment.

By leveraging efficiencies of the cloud and automation to get efficiencies in identity, IDaaS service can:

* Offer in this context all the necessary security and privacy identity capabilities – while maintaining usability.
* Provide a business centric portal for configuring identity services.
* And finally cut costs thanks to superior cloud economics.

These requirements and capabilities will drive almost all organizations to subscribe to identity services that are cheaper, broader in scope, more unifying and more capable than the systems of today.

Because of its enterprise relationships, and its early commitment to build an enterprise grade identity service at cloud scale, Microsoft’s approach to IDaaS is deeply grounded in – and extends – the proven concepts of on-premises Active Directory (AD).

Active Directory (AD) is a Microsoft brand for identity related capabilities. Microsoft has earned widespread adoption of its on-premises identity technology, a suite of capabilities packaged and branded as Windows Server Active Directory (WSAD or simply AD).

In the on-premises world, AD provides a set of identity capabilities. AD is used extensively by governments and enterprises world-wide. AD is widely deployed in the Fortune 1000 and the Global 5000 today as their authoritative identity and access management system as well as in small and medium enterprises and we will not describe it further here. The important new information here is that to meet the requirements of hybrid deployment AD can be extended into public clouds and/or into private clouds.

Azure AD is AD reimagined for the cloud, hardened for the realities and dangers of the cloud environment, and designed to help you solving the new identity and access challenges that come with the shift to a cloud-centric world.

Azure AD is a comprehensive identity and access management cloud solution, utilizing the enterprise-grade quality and proven capabilities of AD on-premises. It combines core directory services, advanced identity governance, security and analytics, and application access management.

Azure AD has been designed to easily extend AD (in whole or in part) into the public Azure cloud[[1]](#footnote-2) as a directory whose content is owned and controlled by the organization providing the information.

**Azure AD is NOT a monolithic directory of information belonging to Microsoft, but rather different directories belonging to and completely controlled by different organizations.** This architecture and commitment is called “multi-tenant[[2]](#footnote-3)” and great care has been provided to insulate tenants (organizations) from each other and from their service operator – Microsoft. Azure AD is a vast network of independent identity systems and directories owned by organizations.

**Azure AD is indeed trusted by millions of organizations serving hundreds of millions of identities for access to Software as a Service (SaaS) applications, including Office 365 and thousands of other partner applications.**

We have indeed re-engineered AD, to support massive scale, devices based on any operating system or architecture, [modern business applications](https://www.microsoft.com/en-us/cloud-platform/mobile-application-development)[[3]](#footnote-4), modern protocols, high availability, and integrated disaster recovery. Azure AD is delivered in a highly-available, fault-tolerant architecture from over 32 regions worldwide.

**Note** The service operates more than 10 million of tenants and actually processes more than 1.3 billion, with a B, authentications every week. Since the release of the service, Azure AD has processed 1 trillion identity authentications. This is a real testament to the level of scale we can handle.

At a high level, Azure AD is a high availability, geo-redundant, multi-tenanted, multi-tiered cloud service that has delivered 99.99% uptime for over a year now. We run it across 32 regions around the world. Azure AD has stateless gateways, front end servers, application servers, and sync servers in all of those data centers. Azure AD also has a distributed data tier that is at the heart of our high availability strategy. Our data tier holds more than 750 million objects.

Since we first talked about it in November 2011, and with such above numbers in the note in mind, Azure AD has shown itself to be a robust identity and access management service for Microsoft cloud services. **No other cloud directory offers this level of enterprise reliability or proven scale.**

Furthermore, last year, Gartner in their Magic Quadrant (MQ) for Identity Management as a Service (IDaaS) has placed Azure AD after its only first year of availability in the “Visionaries” MQ. **Gartner has released their MQ for IDaaS for 2016 and Azure AD Premium has been placed in the “Leaders” quadrant**, and positioned very strongly for our completeness of vision.



**Important note** The above graphic was published by Gartner, Inc. as part of the larger research document - a complimentary access is provided [here](https://info.microsoft.com/EMS-IDaaS-MQ-2016.html)[[4]](#footnote-5)- and should be evaluated in the context of the entire document. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

As Alex Simons, Director of Program Management, Microsoft Identity and Security Services Division, says, “we’re thrilled with the result. It really validates our vision of providing a complete solution for hybrid identity and access for supporting employees, partners and customers all backed by world class security based on Microsoft’s intelligent security graph. This result says a lot about our commitment in the identity and access management space but more importantly about our customers, implementation partners and ISV partners who have worked together with us. They have been awesome about sharing their time and energy every day, to make sure that the products and services we build meet their needs and are helping them position their companies to thrive in the emerging world of cloud and devices.

You might be surprised to know that Microsoft also is the only vendor in the Leader quadrant across Gartner’s Magic Quadrants for IDaaS, Cloud Infrastructure as a Service (IaaS), Server Virtualization, Application Platform as a Service, Cloud Storage Services, and as a leader across the data platform and productivity services. This really shows you why customers are choosing Microsoft across the full spectrum of cloud computing – our services are well integrated and also among the best available in their individual categories.”[[5]](#footnote-6)

Alex Simons adds: “our effort doesn’t stop here. We have a lot of hard work ahead of us and we are planning to deliver more innovative capabilities to further improve our position in the “leaders” quadrant.”[[6]](#footnote-7).

As organizations focus more on their core business, the need to partner with other businesses increases. Organizations need to easily and securely share resources (such as access to corporate applications) with their partners to engage in effective collaboration.

**In this context,** **Azure AD has extended its capabilities with Azure AD B2B (business-to-business) collaboration, a feature of Azure AD now in** [**GA**](https://blogs.technet.microsoft.com/enterprisemobility/2017/04/12/azure-ad-b2b-collaboration-is-generally-available/)**[[7]](#footnote-8) [[8]](#footnote-9).**

**Azure AD B2B collaboration supports your cross-company relationships by enabling partners to selectively access your corporate applications and data using their self-managed identities.**

Azure AD B2B collaboration is:

* **Simple.** Each partner user uses an existing Azure AD account or one that is easily created. You can provide this user with access to your chosen corporate applications. The partner user exists in your Azure AD as an external user, where your IT professionals can provision licenses, assign group membership, and further grant access to corporate applications through the Azure portal or PowerShell just like for users in your organizations.
* **Secure.** Your IT professionals control all access to your corporate applications through your Azure AD. When collaboration is terminated, partner users can be removed from your Azure AD and their access to your applications is immediately revoked.

Azure AD B2B collaboration is a feature that comes with Azure AD. This feature can be used with on the available Azure AD editions, i.e. Azure AD Free, Azure AD Basic, Azure AD Premium P1 and Azure Premium P2, and as part of the [Microsoft Enterprise Mobility + Security (EMS)](https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security)[[9]](#footnote-10) (formerly Enterprise Mobility Suite) E3 respectively E5 offerings, which represents comprehensive and cost effective solutions for enterprise mobility needs.

**Note** For a description of each edition below and a comparison table, see article [Azure Active Directory editions](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-editions)[[10]](#footnote-11). For more information on usage model, see article [Azure Active Directory Pricing](http://www.windowsazure.com/en-us/pricing/details/active-directory/)[[11]](#footnote-12). For information on the usage constraints and other service limits for the Azure AD service per edition, see article [Azure subscription and service limits, quotas, and constraints](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#active-directory-limits)[[12]](#footnote-13).

**Note** For more information on the EMS offerings, see blog post [Introducing Enterprise Mobility + Security](https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security/)[[13]](#footnote-14).

**Note** The EMS offerings are not only available with an [Enterprise Agreement (EA)](http://www.microsoft.com/en-us/Licensing/licensing-programs/enterprise.aspx)[[14]](#footnote-15) but also through the Microsoft’s [Cloud Solution Provider (CSP)](https://partner.microsoft.com/en-us/cloud-solution-provider)[[15]](#footnote-16) and [Open](https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx)[[16]](#footnote-17) programs. For more information, see blog post [Azure AD and Enterprise Mobility Suite now available without an Enterprise Agreement](http://blogs.technet.com/b/ad/archive/2015/03/12/azure-ad-and-enterprise-mobility-suite-now-broadly-available-outside-of-an-enterprise-agreement.aspx)[[17]](#footnote-18).

The partner companies or people who need access to your corporate applications do not need to have Azure AD. Azure AD B2B collaboration provides a simple user signup experience to provide these partners with immediate access to your applications.

## Objectives of this paper

This document is intended as an overview document for discovering and understanding the benefits of the new Azure AD B2B collaboration feature.

**While much of the technology must remain the same, the IDM of employees and IDM of business partners also have different requirements – thus the need for technologies that interact but are honed to specific problems. To master these requirements, Microsoft has worked closely with a number of customers.**

Built on existing Microsoft’s documentation, knowledge base articles, and blog posts, this document provides a complete walkthrough to test, and evaluate Azure AD B2B. It provides additional guidance if any.

**Note** For more information, see articles [Azure Active Directory B2B collaboration frequently-asked questions (FAQ)](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-faq)[[18]](#footnote-19) and [Azure Active Directory B2B collaboration current limitations](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-current-limitations)[[19]](#footnote-20).

## Non-objectives of this paper

This document is not intended as an overview document for the Azure AD offerings but rather focuses on this new collaboration capability.

**Note** For additional information, see article [Getting started with Azure AD](http://msdn.microsoft.com/en-us/library/dn655157.aspx)[[20]](#footnote-21). As well as the whitepapers [Active Directory from the on-premises to the cloud](ttp://www.microsoft.com/en-us/download/details.aspx?id=36391)[[21]](#footnote-22) and [An overview of Azure AD](ttp://www.microsoft.com/en-us/download/details.aspx?id=36391)[[22]](#footnote-23) as part of the same series of documents.

Likewise, it doesn’t provide either in-depth description on how to implement a specific covered feature or capability. Where necessary, it instead refers to more detailed documents, articles, and blog posts that describe a specific feature or capability.

**Note** Please make sure you periodically check the [Azure AD community forum](http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/threads)[[23]](#footnote-24) as well as the [Enterprise Mobility + Security (EMS) Team blog](https://blogs.technet.microsoft.com/enterprisemobility/?product=azure-active-directory)[[24]](#footnote-25) for notification of upcoming enhancement and changes that pertain to Azure AD.

## Organization of this paper

To cover the aforementioned objectives, this document is organized in the following two sections:

* Supporting Business-to-Business collaboration scenarios.
* Getting Started with Azure AD B2B collaboration.

These sections provide the information details necessary to understand the new capabilities introduced in Azure AD for business-to-business (B2B) scenarios, our objectives, and successfully evaluate the available capabilities.

The Appendix A. Building a test lab environment will help you build a suitable test lab environment for such an evaluation.

## About the audience

This document is intended for IT professionals, system architects, and developers who are interested in understanding how Azure AD B2B collaboration help managing partner identities for their B2B relationships and how to leverage the related capabilities.

# Supporting B2B collaboration scenarios

Collaboration between organizations has become essential to the value organizations create. Many organizations take on projects that require partnering with other organizations to spread risk or assemble expertise. Many companies, including Microsoft, have extensive supply chains and partner networks made up of large and small organizations that are essential to delivering customer value.

Identity and access control management is at the core of each and every one these collaborations: you need to give your business partners access to key applications and data, but you also need to make sure these assets don't end up in the hands of the wrong people.

Let’s discuss the partner access model to the applications or other resources you provide.

## Understanding classic partner access models

Traditionally, there have been two ways organizations have tried to solve this problem:

1. Inter-organization federation relationships.
2. Internally managed partner identities.

### Inter-organization federation relationships

Setting up inter-organization federation relationships is the classic approach but has problems:

* Most large organizations do business with many smaller organizations that don't have the expertise and can't afford the (on-premises) identity infrastructure required to setup and manage federation.
* Complexity grows linearly when you have to manage a federation relationship with each partner. Managing thousands of federation relationships becomes untenable.



Beyond the number, this implies from a technical perspective to simultaneously support potentially various federation protocols along with their possible related profiles to accommodate diverse partners’ technical choices and capabilities to interoperate with your own federation infrastructure. Despite SAML 2.0 and WS-Federation are today common standard protocols in this space, the devil is always in the details as one should say… In addition, you have to deals with all the SSL/TLS, signing, and encryption X509 certificates that such solutions leverage. It’s all the more so with the related trust chains.

Once federation finally works with a partner, the federation relationship has to be maintained over the time to ensure a service level agreement (SLA) between your organization and the partner organization (an SLA that has also to be prior defined…) For example, this supposes to monitor the other organization’s metadata if any and to automatically update your own trust definition information to reflect the other organization’s current settings in its configuration. Such an operation allows to adequately in a timely fashion handle any certificate rollover for example.

“*If federation is broken. It's PKI. If it is not PKI, there's a typo. If you typed it correctly (case counts!). It's PKI*”

- Laura E. Hunter

* With federation, you have very limited user level visibility making compliance and audit challenging. The information that is conveyed as claims in the security token issued by the partner organizations is limited by definition to the acceptable size of the security token, potentially as per related specification.

Furthermore, this information also results from a prior business agreement between the two organizations that intend to collaborate, and have to respect and fulfill both the security and the privacy policies of the partner organization before releasing it. It’s thus by definition a tradeoff…

These difficulties lead many organizations to create directories of internally managed partner identities. Let’s consider it.

### Internally managed partner identities

This common practice has also its own security and management concerns:

* When partner accounts are managed by the organization, this is yet another set of usernames and passwords for partner users to remember and yet another set of identities for you to manage (provision, de-provision, reset passwords, etc.).

Beyond the possible need to manage a new directory for that specific purpose, this of course also implies additional processes (sign-up and cleanup at least), cost, and burden on both side. One would say that some well-defined and controlled self-service solutions may contribute to reduce them over the time. This said, these self-service solutions if not already in place have to be de facto designed, implemented and rolled out. All of these lead to additional complexity…

* These accounts in internally managed directories can easily provide too much access and thus put the whole organization at risk. Partner accounts indeed tend not be managed as closely as employee accounts. Therefore, they have become over the time the favored attack vector for hackers:

“*The hackers that carried out the massive data breach at Target Corp. appear to have gained access via a refrigeration contractor in Pittsburgh that connected to the retailer's systems to do electronic billing*.”

– Wall Street Journal

“*Criminals used a third-party vendor's user name and password to enter the perimeter of Home Depot's network.*”

– Home Depot

"*If I want to attack Fort Knox and I know they have locks and guards and strong security, it is easier to attack one of their providers who already have access to the gold.* “

– James Christiansen, VP, Accuvant

Once a partner account managed in the directory is compromised, attackers can move laterally to other accounts in the same identity store. So an exploited partner user puts the whole organization at risk…

* These accounts are disconnected from the partner's identity system, so they are not disabled when partner employees change jobs or are terminated. Access continues long after a partner user has left his organization…

**We believe that the ideal cross-organization identity model is one where each partner has the ability to manage their own employee identities, integrated into their existing IT systems, according to their own corporate security and privacy policies, in a way that works for their business while providing rich cross-organization visibility, and world class compliance and control.**

**And Microsoft is uniquely positioned to help you achieve this ideal.**

## Extending Azure AD for external identities

In addition to managing their employees and mobile workforce access the required SaaS and (cloud-based, hybrid, and on-premises) corporate Line-Of-Business (LOB) applications, Azure AD can help organizations manage their external users, and thus notably share resources with business partners and deliver applications to business.

This is what the new feature Azure AD B2B collaboration should be used for to help secure business-to-business collaboration with the partner organizations that you work with every day.



Azure AD B2B collaboration provides simplified management and security for partners and other external users accessing your in-house resources using Azure AD as the control plane. This includes access to popular SaaS apps such as Office 365, Salesforce, Dropbox, Workday, etc., many Azure services, and other mobile, cloud, and on-premises claims-aware applications.

**Azure AD B2B collaboration is designed to solve the identity management challenges that have emerged, as economic and competitive pressures drive commercial enterprises, to enable cross-organization collaboration wherever and whenever it makes senses for their business and competitively with the ambient credo to “do more with less, with a better agility and time to market”.**

**The end goal aims at enabling organizations of all sizes and in all industries, regardless of their compliance and governance requirements, to work easily and securely with collaborators around the world.**

## Understanding Azure AD B2B collaboration partner access model

Azure AD B2B collaboration is a new set of capabilities that enable simple and secure collaboration with your business partners. Azure AD B2B collaboration is easy to configure with simplified signup for partners of all sizes even if they don’t have their own Azure AD via an email-verified process. It is also easy to maintain with no external directories or per partner federation configurations.

#### Enabling secure partner access to applications

Azure AD B2B collaboration lets you enable access to your corporate resources from partner managed identities as well as social identities in a simpler and more secure manner.

**You can create cross-organizations relationships by inviting and authorizing users from partner organizations – and/or can invite and authorize users with simply a social email address - to access to the authorized corporate line-of-business (LOB) applications and other resources you provide**.

An email-verified process indeed allows your business partners and, more generally speaking, all your guest users who ever they are. You can invite a user with any email address on the planet. Whether the user has an Office365 or on-premises Exchange email address, an outlook.com email address, any social email address (Gmail, Yahoo, etc.), they can seamlessly access the invited organization – and the authorized applications and resources - with inline, lightweight creation of an Azure AD or Microsoft account (MSA):

* An invited user with a corporate email address is homed in an external Azure AD directory and is represented by default as a guest user in the inviting organization. The user signs in with an Azure AD account belonging to his home tenancy. If the external organization that the user belongs to doesn't have an Azure AD directory at the time of invitation, the invited user is created "just in time" in an unmanaged tenant when the user redeems his invitation (see below), after verifying his corporate email address. This is also called a just in time (JIT) tenancy, or sometimes as a viral tenancy.

**Important note** For information on unmanaged tenants and how they can be brought under admin control, see the article [What is Self-Service Signup for Azure?](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-self-service-signup)[[25]](#footnote-26).

* An invited user with a social email address is homed in Microsoft Account and is represented by default as a guest user in the inviting organization. The user signs in with a Microsoft account. As of this writing, the invited user's non-MSA social ID (Gmail, Yahoo, etc.) is created as a Microsoft account just in time during offer redemption (see below). Direct federation with social identity providers will be provided in the future.

**Note** Azure AD B2B collaboration provides a smooth path for internally managed partner identities. As such, any internally homed partner identity in the organization's on-premises AD can indeed be easily synced with the organization's Azure AD thanks to the [Azure AD Connect](https://www.microsoft.com/en-us/download/details.aspx?id=47594)[[26]](#footnote-27) tool. Such users can then be manually flagged in the Azure AD directory as guest users (using PowerShell). We will support this being done automatically as part of Future releases of Azure AD Connect might support this being done automatically. This scenario is not further cover in this document.

Likewise, nothing prevents the organization to internally manage in their Azure AD directory partner identities that are flagged as guest users. This scenario is also not further cover in this document.

This email-verified process enables – via PowerShell or API - a bulk invite and authorization of thousands of users at a time from both partner organizations and individuals.

The management burden is reduced as each business partners manage their own accounts while security is increased (see next section).

Complexity is also reduced as each organization federates once with Azure AD and each guest user is represented by a single Azure AD or Microsoft account as stated above. Azure AD creates and allows you to manage the trust relationships in the cloud, freeing you from the complexity of managing and maintaining over the time per-partner federation relationships.

#### Controlling what partners can access

For all guest users with an Azure AD account, security is increased as access is lost when guest users are terminated from their organizations and unintended access is not granted by membership in internal directories. Your business partners use their own login credentials, which frees you from managing user credentials in your directory for users as the join or leave their organization.

Moreover, you control access policies within your organization where you can control and remove the authorization to access your corporate resources separately from the business partner's account lifecycle.

You have the ability to assign all the guest users (whether they have an Azure AD or a Microsoft account) to applications and to add the guest users to suitable security groups. This means for example that you can revoke access to your applications without having to ask the IT department of your business partner to do anything. Furthermore, the above also benefits from the delegation model of Azure AD you may already leverage for your (full-time) employees.

#### Onboarding partners of all sizes, large and small

Azure AD B2B collaboration allows you to setup business-to-business collaboration with partners of all sizes, whether they already use Azure AD or not. For business partners that don't already have Azure AD, and/or for partners with no IT infrastructure at all, Azure AD B2B collaboration has a streamlined signup experience to provide Azure AD or MSA accounts to your business partners as explained above.

Business partners of any size will get and enjoy single sign on (SSO) access to the corporate line-of-business (LOB) applications and other resources you provide.

## Understanding Azure AD B2B collaboration high level workflow

The aforementioned email-verified process is twofold:

1. **Invitation experience.** An administrator of the inviting organization has the ability to invite partners’ users via their email address to the organization’s Azure AD directory, or any group or application.

Once a guest user is added to the directory, a group, or an application, an invitation is created and sent to the invited user (containing an invitation link). As part of the underlying workflow, Azure AD B2B collaboration will creates stub external users in your directory and sends professional, tenant branded email invitations.

1. **Redemption experience.** Each invited guest user will thus receive an email invitation that includes a link to accept the invite. The guest user will have to click that link, signs in and redeems the invitation - the creation of the user entity representing the invited user completes -, and finally have an access granted to the inviting organization’s authorized corporate applications in their context:

As outlined above, for a guest user invited with a corporate email address, if the partner organization doesn’t have any Azure AD tenant, the redeem experience will provision an email verified unmanaged tenant. If the guest user doesn’t exist in the email verified Azure AD tenant, the redeem experience provisions an email verified user.

Conversely, for a guest user invited with a social email address that doesn’t correspond to a Microsoft account (MSA), the redeem experience will invite the guest user to sign-up to a Microsoft account with the same email address that has been used for the email invitation. If the guest user already has such an account with this email address, the user will sign in with this email verified account. As before, the redeem experience then provisions an email verified user for this account.

## Comparing B2B collaboration with B2C in Azure AD

Both the Azure AD B2B collaboration feature and the Azure AD B2C stand-alone offering allow you to work with social identities in Azure AD.

**Note** For more information on Azure AD B2C, see whitepaper [An overview of Azure AD B2C](https://aka.ms/aadpapers)[[27]](#footnote-28) in the same series of papers.

The following table explore how do they compare.

|  |  |
| --- | --- |
| Azure AD B2B collaboration feature | Azure AD B2C stand-alone offering |
| Intended for: Organizations that want to provide access to corporate data, resources and applications to users from any other organization, using any identity of their choice. | Intended for: Customer facing mobile and web apps that target your customers - individual, citizens and institutional or organizational customers (not your employees or external collaborators)– using any identity of their choice |
| Identities supported: Employees with work or school accounts, partners with work or school accounts, or any email address. Soon to support direct federation. | Identities supported: Consumer users with local application accounts (any email address or user name) or any supported social identity with direct federation. |
| Which directory the partner users are in: guest users from the external organization are managed in the same directory as (full-time) employees, but annotated specially. These external users can be managed the same way as (full-time) employees, can be added to the same groups, and so on | Which directory the customer user entities are in: In the application directory. Managed separately from the organization’s (full-time) employee and partner directory (if any). |
| Single sign-on (SSO) to all Azure AD connected apps (including on-premises apps) is supported (for example, Office 365) and other Microsoft and non-Microsoft SaaS apps (like Salesforce, Box, Workday, and so on). | SSO to customer owned apps within the Azure AD B2C tenants is supported. SSO to Office 365 or to other Microsoft and non-Microsoft SaaS apps are NOT supported. |
| Partner lifecycle: Managed by the inviting organization. | Customer lifecycle: Self-serve or managed by the application. |
| Security policy and compliance: Managed by the inviting organization. | Security policy and compliance: Managed by the application. |
| Branding: inviting organization’s brand is used if any. | Branding: Managed by application. Typically tends to be product branded, with the organization fading into the background. |
| More info: [Blog post](https://blogs.technet.microsoft.com/enterprisemobility/2017/02/01/azure-ad-b2b-new-updates-make-cross-business-collab-easy/), [Documentation](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-what-is-azure-ad-b2b) | More info: [Product page](https://azure.microsoft.com/en-us/services/active-directory-b2c/), [Documentation](https://docs.microsoft.com/en-us/azure/active-directory-b2c/) |

**Note** For more information, see article [Compare B2B collaboration and B2C in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-compare-b2c)[[28]](#footnote-29).

## Understanding Azure AD B2B collaboration business model

There is no charge for inviting guest users and assigning them to an application in the organization’s Azure AD directory. Also, up to 10 apps per guest user and 3 basic reports are also free for guest users, since they are part of Azure AD 'Free' tier.

Any paid Azure AD features, extended to guest users via the Azure AD B2B collaboration feature, will need to be licensed with Azure AD paid licenses (Basic, Premium P1, or Premium P2, depending on the features that will be used). The inviting tenant will get 5 guest user rights with each Azure AD paid license. That is, each Azure AD paid license that provides rights to one employee user in a tenant, will now also include rights to 5 guest users invited to the tenant.

**Note** For more information, see article [Azure Active Directory B2B collaboration licensing guidance](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-licensing)[[29]](#footnote-30).

Let’s see in an end-to-end walkthrough how all this works.

# Getting Started with Azure AD B2B collaboration

This walkthrough illustrates how IT professionals and information workers (IW) can work closely with users in any other organization on the planet, provide access to documents, resources and applications, while maintaining complete control over their internal data.

For that purpose, it shows an administrator and a IW using B2B collaboration to invite guest users to access a web application.

Two type of guest user are illustrated:

1. A guest user who already exists in a partner organization’s Azure AD directory,
2. A guest user who has only a Gmail email address.

**Important note** The end-to-end experience may evolve as additional features and other enhancements can be introduced to the service over the time to the service, and more particularly at GA. All screenshots and steps are thus subject to change as the B2B features may evolve until GA. The same considerations apply to the outlined social identity providers that may also update their portal and steps over the time.

## Fulfilling the pre-requisites for the walkthrough

In order to illustrate and test the business-to-business collaboration between an inviting organization and a partner organization, the walkthrough requires two distinct Azure AD directory tenants: one for the inviting organization itself, and another one for its business partner organization.

If you don’t have such directory tenants, Appendix A. provides instructions to create them and setup an appropriate test lab environment. Please refer to this appendix to make sure that your environment reflects the prerequisites.

In terms of scenario for the course of this walkthrough, the Contoso369 organization requires partnering with the Litware369 to assemble expertise, and consequently need to grant an access to some Litware369 users for one of their LOB application. The Contoso369 organization also needs working with some externals experts that only have a social email address.

Contoso369 would like to leverage the new capabilities introduced by Azure AD B2B collaboration. Similarly, Litware369 already benefits from an identity hub in the cloud through their Office 365 subscription, and so, they’re reluctant to invest in any new infrastructure to collaborate with Contoso369.

Consequently, to implement the suggested scenario, we will create or use:

1. **For the inviting organization: the *contoso369.onmicrosoft.com* directory tenant.** **You will have to choose in lieu of a directory name of your choice whose name is currently not in used.**

**Whenever a reference to *contoso369b2c.onmicrosoft.com* is made in a procedure, it has to be replaced by the directory name of your choice to reflect accordingly the change in naming.**

1. **For the business partner organization: The *litware369.onmicrosoft.com* directory tenant.** **You will have to choose in lieu of a directory name of your choice whose name is currently not in used.**

**Whenever a reference to *litware369.onmicrosoft.com* is made in a procedure, it has to be replaced by the directory name of your choice to reflect accordingly the change in naming.**

1. **For the external experts with social IDs: both a *contoso369b2binvitee@gmail.com* Gmail account and a *contoso369b2binvitee@outlook.com* Microsoft account. You will have to create or use two social ID accounts of your choice in lieu of the above ones taken for the illustration.**

**Important note** Unless noticed otherwise, the Free edition of Azure AD is used in the walkthrough for the inviting organization. The Basic or the Premium P1 and P2 editions will offer in this context additional benefit such as extended branding capabilities, as well as conditional access, and group assignment for the applications. If you want to additionally test these capabilities, you can sign-up for an Azure Active Directory Premium P1 [free trial for one month](https://azure.microsoft.com/en-us/trial/get-started-active-directory/)[[30]](#footnote-31). Instructions will be given as part of this walkthrough.

For additional information about how to sign up and start using the Premium P1 or Premium P2 editions, see article [Getting started with Azure Active Directory Premium](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-get-started-premium)[[31]](#footnote-32).

**Important note** A simplified sign-up is provided for invite corporate business partners without Azure AD. This capability is not illustrated as part of this walkthrough.

To simplify the wording as much as possible in the rest of this section, the **inviter** word will refer simultaneously, and depending on the context, to the Contoso369 administrator/information worker/organization/directory tenant that is inviting partner users. Conversely, the **invitee** word will be the Litware 369 or social ID guest user that receives the invitation and must complete the redeem process.

## Inviting a set of guest users as an administrator (inviter UX)

Until recently, the B2B experience was only available in the classic Azure portal at <https://manage.windowsazure.com>.

Azure administrator user experience (UX) enhancements to the B2B experience are now coming to the Azure portal at <https://portal.azure.com> with the ability for administrators to invite guest users to the directory, or any group or application. The next subsections cover each situation.

As a Contoso369 administrator, you will thus use these new capabilities to invite guest users from both the Litware369 organization and social identities.

The above UX enhancements in the Azure portal will enable to seamlessly send email invitations to these corporate and social ID guest users. A corporate guest user will either sign in to an existing Azure AD account, or get a new Azure AD account. Likewise, a social ID guest user will either sign in to an existing Microsoft account, or get a new Microsoft account.

**Note** For more information, see article [How do Azure Active Directory admins add B2B collaboration users?](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-admin-add-users)[[32]](#footnote-33).

### Adding a guest user to the directory

To add a guest user to the directory, proceed with the following steps:

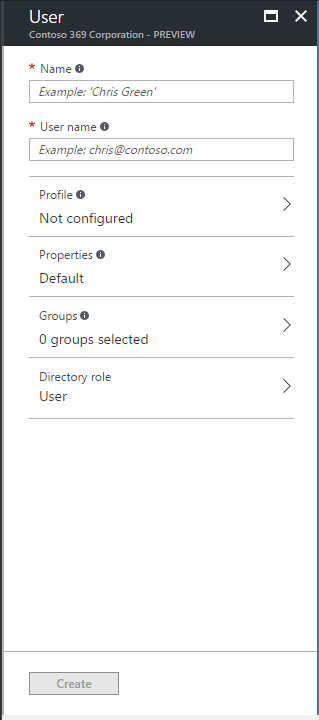
1. Open a browsing session and navigate to the Azure portal at:

<https://portal.azure.com/contoso369.onmicrosoft.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>

1. Sign in to the Azure portal as the Subscription admin user. This is for instance the same Microsoft Account that you used to sign up for Azure as per previous section.
2. Under **MANAGE**, select **Users and groups**. An eponym blade opens.

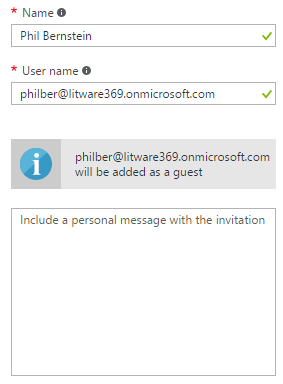
**Note** A blade is one piece of the overall view. You can think of a blade as a window.

1. Under **MANAGE**, select **All users**.
2. Click **+Add** in the upper tray. A **User** blade opens.



1. In **Name**, enter the display name of the guest user, for example “Phil Berstein” in our illustration.
2. In **User name**, enter the (corporate) email address of the guest user, for example “philber@litware369.onmicrosoft.com” in our illustration. This can be any email address as outlined before.

After a few second, an information message should state that the specified email address will be added as guest.



In addition, you can optionally include a personal message with the invitation to the guest user.

1. Click **Create**. A floating notification message should indicate that an invitation is generated. After a second, you should see a successful invitation status.

Et voila! An invitation email from the Microsoft Invitations has been generated and sent to the guest user. This generated email has a unique URL to redeem the invite.

At the same time, the user is added to the organization’s Azure AD directory.

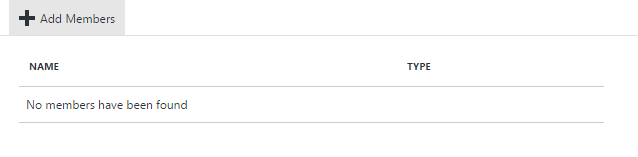
### Adding a guest user to a group

If you followed the instructions provided in the appendix, you were instructed to create a security group named Business Partners. As you might imagine, and as its name might suggest, the purpose of this group aims at containing all the partner users for the design activities in our fictitious company. Such a group can be later leverage in (conditional) access control decisions.

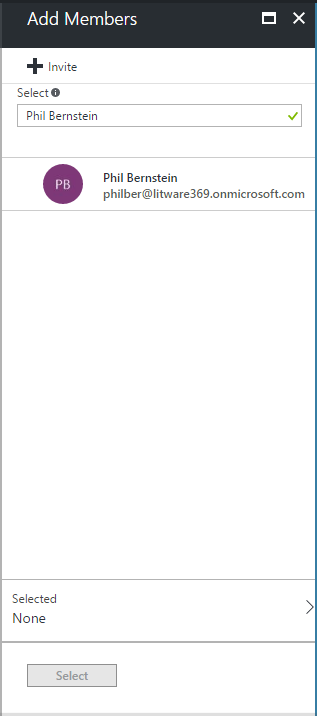
**Note** As mentioned above, the Basic or the Premium P1 and P2 editions offer in this context additional benefit in terms of group assignment to control access. For more information, see article [Managing access to resources with Azure Active Directory groups](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups)[[33]](#footnote-34).

To alternatively add a guest user to the Business Partners group, proceed with the following steps:

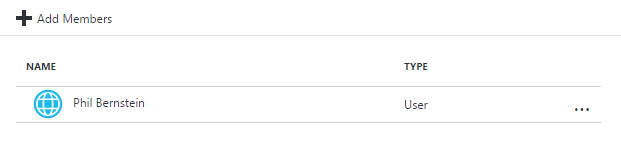
1. Open a browsing session, navigate to the Azure portal at <https://portal.azure.com/>.
2. Sign in to the Azure portal as the Subscription admin user.
3. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
4. Under **MANAGE**, select **Users and groups**. An eponym blade opens.
5. Under **MANAGE**, select **All groups**. A blade opens to list all the existing group.
6. Click to open the **Business Partners** group. An eponym blade opens.
7. Under **MANAGE**, select **Members**. A blade opens to list the members of the group.



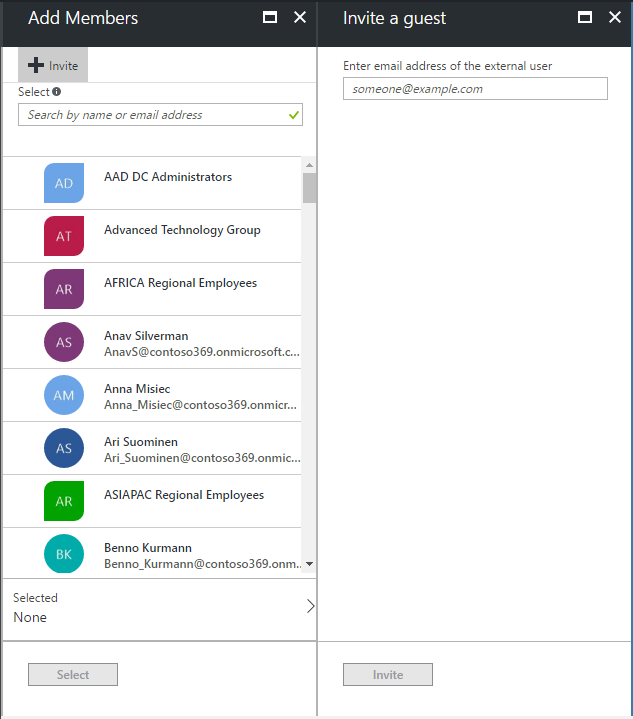
1. Click **+Add Members** in the upper tray. An eponym blade opens.
2. Search for the just added guest user (see previous section): “Phil Berstein”



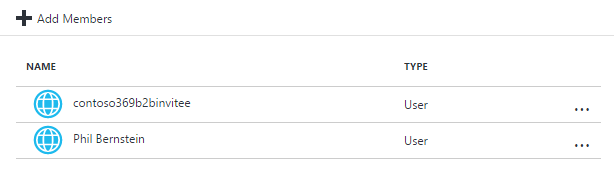
1. Select this account, and then click **Select**.



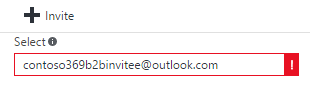
1. Click **+Add Members** again, and then click **+Invite** in the new blade.



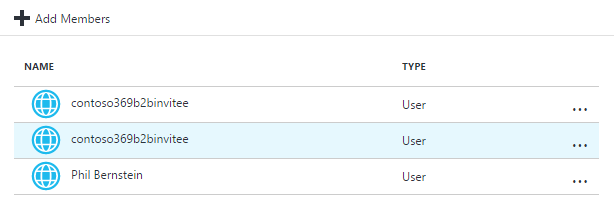
1. Enter the email address of the new guest user, for example in our configuration “contoso369b2binvitee@gmail.com”. This can be any email address as outlined before.
2. Click **Invite**. As before, an invitation is generated and the user is added to the organization’s Azure AD directory. An invitation email from the Microsoft Invitations has been generated and sent to the guest user. This generated email has a unique URL to redeem the invite.
3. Click **Select**. The guest user is added to the group.



1. Click **+ Add Members** again, and then search for “contoso369b2binvitee@outlook.com”. This doesn’t return a result since the user is not in Azure AD yet.



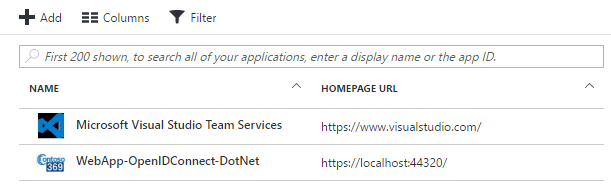
1. Click **+Invite** in the upper tray. An Invite a guest blade opens.
2. Enter the previous email address, i.e. “contoso369b2binvitee@outlook.com” to invite the new guest user. This can be any email address as before.
3. Click **Invite**. The guest user is invited to the organization’s Azure AD directory. As before, an invitation email from the Microsoft Invitations has been generated and sent to the guest user. This generated email has a unique URL to redeem the invite.
4. Click **Select**. The guest user is added to the group.



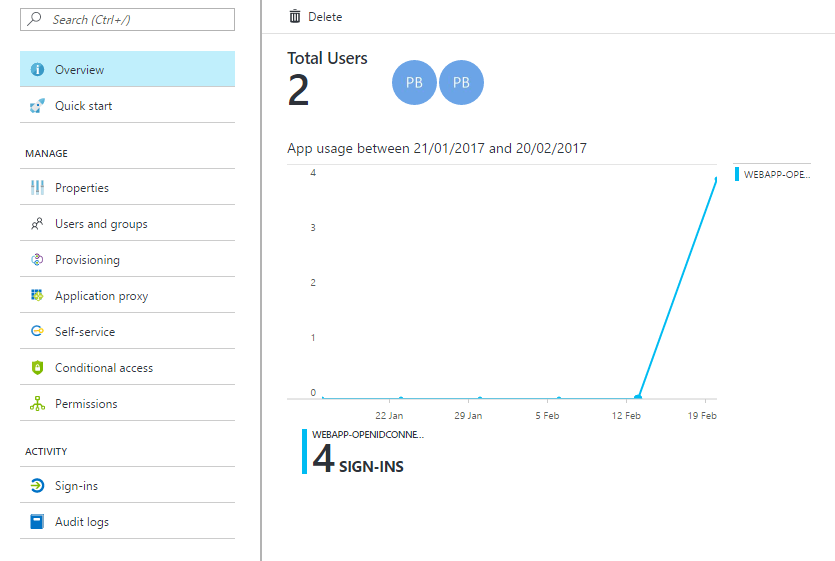
### Adding a guest user to an application

To alternatively add a guest user to an application, proceed with the following steps:

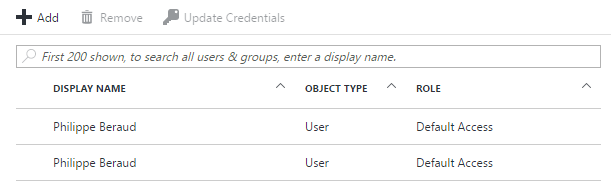
1. Open a browsing session and navigate to the Azure portal at <https://portal.azure.com/>, and then Sign in to the Azure portal as the Subscription admin user.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. Under **MANAGE**, select **Enterprise applications**. An eponym blade opens.
4. Click **All applications**.



1. Select **WebApp-OpenIDConnect-DotNet**.



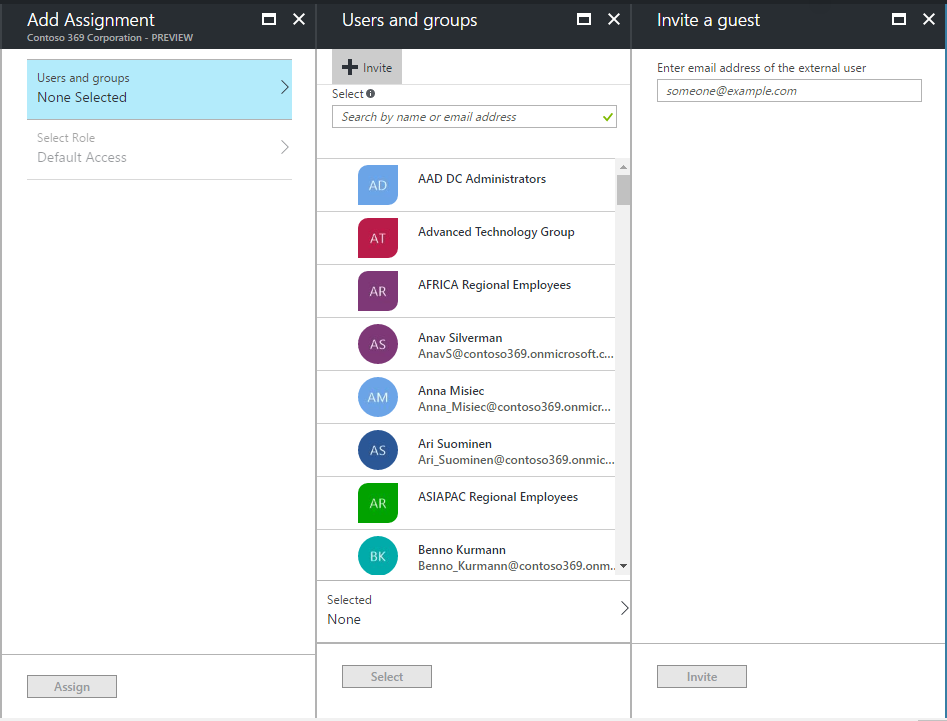
1. Under **MANAGE**, select **Users and groups**. An eponym blade opens.



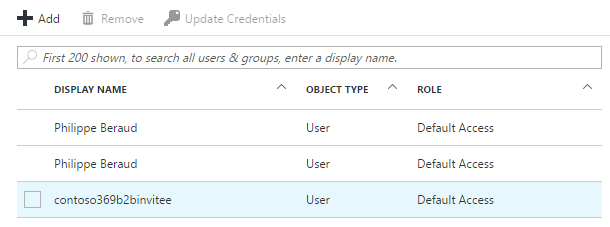
1. Click **+Add** in the upper tray. An **Add Assignment** blade opens.



1. Click **Users and groups**. An eponym blade opens.
2. Click **+Invite** in the upper tray. An **Invite a guest** blade opens.



1. Enter an email address to invite a new guest user. This can be any email address as before, for example “contoso369b2binvitee@gmail.com” in our illustration.
2. Click **Invite**.
3. Click **Select**.
4. Click **Assign**.



1. Repeat above steps 9 to 13 for Phil Berstein (philber@litware369.onmicrosoft.com).

### Bulk inviting guest users with CSV

This section illustrates the Windows PowerShell support for Azure B2B collaboration. Such a support allows an inviter, i.e. a Contoso369 administrator for our illustration, to bulk invite and authorize a set of external users via a comma-separated values (CSV) file.

#### Preparing the CSV file

This CSV file contains information for the invitees.

|  |  |
| --- | --- |
| Field | Description |
| **Name** | Display name for invitee (typically, first and last name) |
| **InvitedUserEmailAddress** | Email address for invitee. This can be any email address. However, DLs are not currently supported. |

At this stage, with the following social guest users created in the appendix:

1. Robert Hatley (contoso369b2binvitee@gmail.com),
2. Alex Schorr (contoso369b2binvitee@outlook.com).

You now have all the required information to define the content of the CSV file.

Create a new CSV file and name it “invitations.csv”. In our illustration, the CSV file looks like the followings, and is saved in C:\Temp.

Name,InvitedUserEmailAddress

Robert Hatley,contoso369b2binvitee@gmail.com

Alex Schorr,contoso369b2binvitee@outlook.com

#### Inviting guest users through PowerShell with the CSV file

To invite guest users through PowerShell with the invitations.csv CSV file, proceed with the following steps:

1. Open an elevated Windows PowerShell or PowerShell Integrated Scripting Environment (ISE) prompt.
2. Import the Azure AD PowerShell V2 module:

PS C:\> Import-Module AzureAdPreview

1. Run the following command to connect to your tenancy

PS C:\> Connect-AzureAd

1. When prompted, sign in as the Subscription admin user.

PS C:\> Connect-AzureAd

Account Environment Tenant

------- ----------- ------

philber@contoso369.onmicrosoft.com AzureCloud 6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1

PS C:\>

1. Run the followings commands in order:

PS C:\> $invitations = import-csv C:\Temp\invitations.csv

PS C:\> $messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo

PS C:\> $messageInfo.customizedMessageBody = “Hi there, Check this out for collaborating with us at Contoso 369”

PS C:\> foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress $email.InvitedUserEmailAddress -InvitedUserDisplayName $email.Name -InviteRedirectUrl "https://myapps.microsoft.com" -InvitedUserMessageInfo $messageInfo -SendInvitationMessage $true}

At this point, thanks to the invitation workflow underneath, an email from the Microsoft Invitations is generated and is sent to the each of the email addresses of invitees you specified in the CSV file. Each generated email has a unique URL to redeem the invite.

This last command produces the following outputs where you can get the Id of each invitee along with the redeem URL for the invitee:

Id : a944337d-3c7d-419d-b380-de36d63694e1

InvitedUserDisplayName : Robert Hatley

InvitedUserEmailAddress : contoso369b2binvitee@gmail.com

SendInvitationMessage : True

InviteRedeemUrl : https://invitations.microsoft.com/redeem/?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&user=a944337d-3c7d-419d-b380-de36d63694e1&ticket=PzunpE%2bXkcxlIkS5BTZ%2bLqvapZP4MTm%2fcdu

Kc6lgjvM%3d&lc=1033&ver=2.0

InviteRedirectUrl : https://myapps.microsoft.com/

InvitedUser : class User {

Id: 87a87b23-6f2b-4d72-ba42-670ab6efba1e

}

InvitedUserMessageInfo : class InvitedUserMessageInfo {

CcRecipients: System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.Recipient]

CustomizedMessageBody: Hi there, Check this out for collaborating with us at Contoso 369

MessageLanguage:

}

InviteduserType : Guest

Status : PendingAcceptance

Id : 03ed7b35-8503-4ee4-8898-0797e0997b24

InvitedUserDisplayName : Alex Schorr

InvitedUserEmailAddress : contoso369b2binvitee@outlook.com

SendInvitationMessage : True

InviteRedeemUrl : https://invitations.microsoft.com/redeem/?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&user=03ed7b35-8503-4ee4-8898-0797e0997b24&ticket=7NKu5pgc4s2q25mn3A7rSlh%2b6eVrAHmLe4mpCOD

E0vA%3d&lc=1033&ver=2.0

InviteRedirectUrl : https://myapps.microsoft.com/

InvitedUser : class User {

Id: c09fe798-1cf9-4441-b27e-f3ba63becaea

}

InvitedUserMessageInfo : class InvitedUserMessageInfo {

CcRecipients: System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.Recipient]

CustomizedMessageBody: Hi there, Check this out for collaborating with us at Contoso 369

MessageLanguage:

}

InviteduserType : Guest

Status : PendingAcceptance

**Note** For more information, see article [Azure Active Directory B2B collaboration code and PowerShell samples](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-code-samples)[[34]](#footnote-35).

To alternatively add guest users to a group, proceed with the following steps:

1. Repeat above steps 1 to 4 but for the last command, set the parameter SendInvitationMessage to $false as follows:

PS C:\> foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress $email.InvitedUserEmailAddress -InvitedUserDisplayName $email.Name -InviteRedirectUrl "https://myapps.microsoft.com" -InvitedUserMessageInfo $messageInfo -SendInvitationMessage $false}

1. Add the users to the intended group(s) via the Azure portal or PowerShell.
2. Rerun the command by now setting the parameter SendInvitationMessage to $true as follows:

PS C:\> foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress $email.InvitedUserEmailAddress -InvitedUserDisplayName $email.Name -InviteRedirectUrl "https://myapps.microsoft.com" -InvitedUserMessageInfo $messageInfo -SendInvitationMessage $true}

At this point, and as before, thanks to the invitation workflow underneath, an email from the Microsoft Invitations is now generated and is sent to the each of the email addresses of invitees you specified.

### Adding a guest user to a role

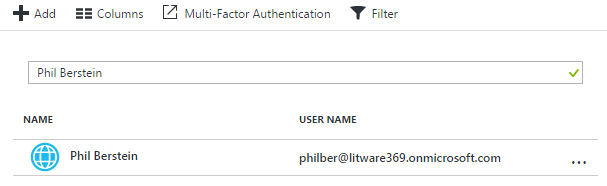
By default, guest users are added as guest users to the organization’s directory and guest permissions in the directory are also restricted by default.

This said, you may need to grant some specific guest users more privileges. Azure AD B2B collaboration allows to add guest users to any given role based on your organization's needs: **User** vs. **Global administrator** vs. **Limited administrator**.

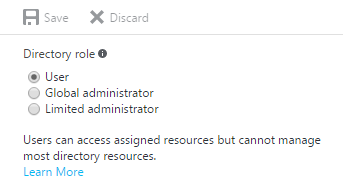
**Note** For more information, see article [Adding an Azure Active Directory B2B collaboration user to a role](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-add-guest-to-role)[[35]](#footnote-36).

To grant a guest user a specific role, proceed with the following steps:

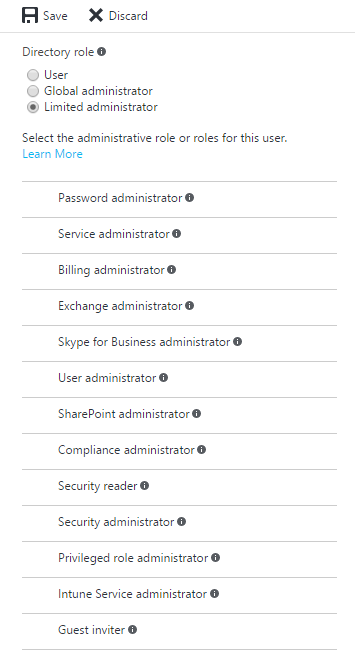
1. Open a browsing session and navigate to the Azure portal at <https://portal.azure.com/>, and then Sign in to the Azure portal as the Subscription admin user.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. Under **MANAGE**, select **Users and groups**, and then **All users**.
4. Search the guest user, for example Phil Berstein.



1. Select the user.
2. Under **MANAGE**, click **Directory role**.



1. Select **Limited administrator** as an illustration.



As illustrated, this role provides you with a great granularity.

1. Select all needed roles. One should note that the **Guest inviter** role has access to invite guest user.

**This role thus allows to control who can invite through policies and delegate invitations to users in the allowed roles to invite. This represent an important new way to delegate guest user invitations.**

As an illustration, if you grant the above **Guest inviter** role to Phil Berstein, and provided that Phil belongs to a role that has enumeration privileges in the Litware 369 organizations Azure AD directory, from which he is adding users, the invited users will be added into the Contoso 369 organization without needing invitations.

**Note** For more information, see article [Add B2B collaboration users without an invitation](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-add-user-without-invite)[[36]](#footnote-37).

1. Click **Save**.

### Customizing invitation email with branding

You can benefit from a professional, tenant branded invitation email for the invitation and redemption experience.

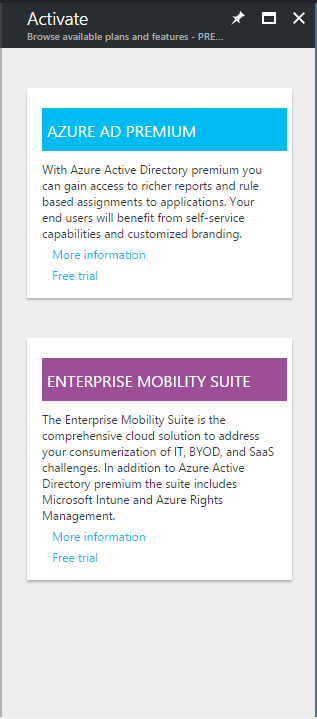
For that purpose, the invitation emails use the company branding that you can set up for your Azure AD directory. This feature enables you to customize the text and the graphics your users see when they sign in to your Azure AD.

**This feature requires an Azure AD Basic**, **Premium P1 or Premium P2 subscription.**

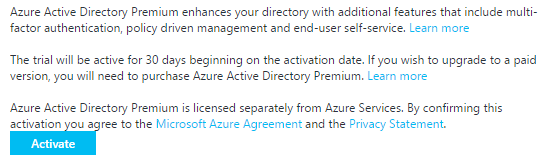
**Note** If you have You have a Basic or a Premium license assigned, you will indeed be able to customize how the sign-in page and the Access Panel – see later in this document - will appear to both users within the organization and guest users. More specifically, you can brand these pages to include your company’s logo and customize other on-screen elements. For more information, see articles [Add company branding to your Sign In and Access Panel pages](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-company-branding)[[37]](#footnote-38) and [Improving the branding logic of Azure AD login pages](https://blogs.technet.microsoft.com/enterprisemobility/2017/04/07/improving-the-branding-logic-of-azure-ad-login-pages/)[[38]](#footnote-39).

To benefit from a 30-days free Azure AD Premium P2 trial, proceed with the following steps:

1. Back to the directory blade in the Azure portal, click **Company branding**.
2. Click **Get a free Premium trial to use this feature**. An **Active** blade opens.



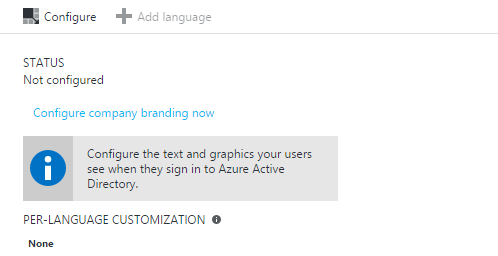
1. For the sake of this walkthrough, click **Free trial** under **AZURE AD PREMIUM**. A new blade opens.



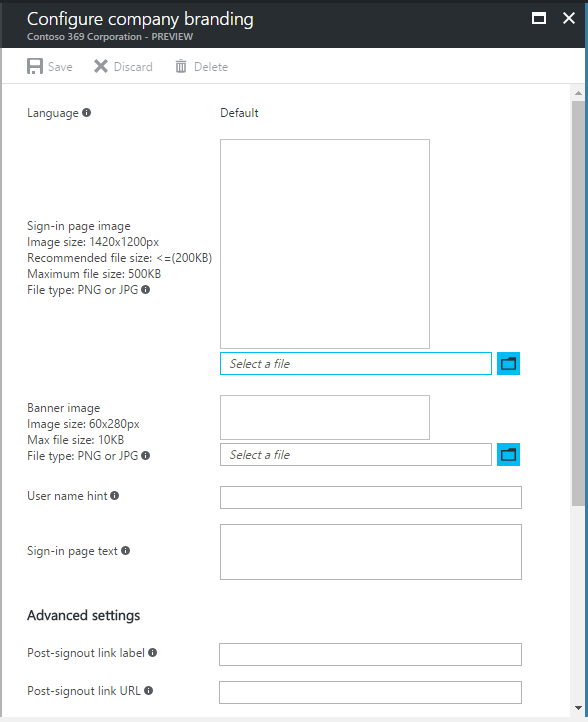
1. Click **Activate**. A floating notification tile should indicate the successful activation of the 30-days trial.

To configure the company branding, proceed with the following steps:

1. Back to the directory blade in the Azure portal, click **Company branding** again. An eponym blade opens.



1. Click **Configure company branding now**. An **Active** blade opens.



1. Configure the various customization settings to accommodate your own needs. See the article [Add company branding to your Sign In and Access Panel pages](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-company-branding)[[39]](#footnote-40) for the details on how to configure them.
2. Click **Save**, and then close the blade.

**Let’s consider the user experience from the invitee perspective: corporate user vs. social ID user.**

## Receiving and accepting the invitation as a corporate user (invitee UX)

You will now be in this section an invitee, and for example Phil Berstein, an employee of the Litware369 organization. As stated above, you now should have received the invitation mail from the Microsoft Invitations on behalf of the Contoso 369 organization.

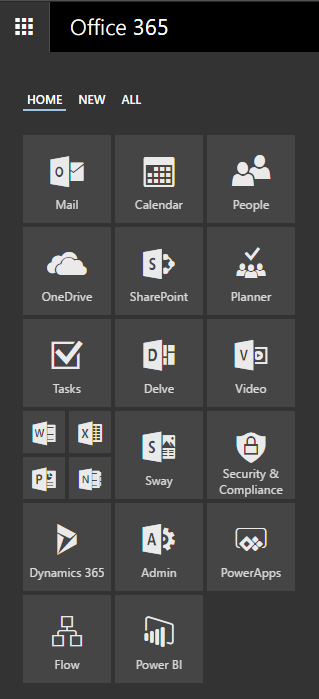
**Note** For more information, see article [Azure Active Directory B2B collaboration invitation redemption](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-redemption-experience)[[40]](#footnote-41).

**Let’s see how the redeem workflow works.**

### Receiving the invitation email

To receive and accept the invitation, proceed with the following steps:

1. Open your mailbox. In our illustration, we use an Office 365 subscription. In this context, open a browsing session and navigate to the Office portal at <https://portal.office.com>. to access your mail box
   1. Sign-in with Phil Berstein as suggested above.
   2. Open the apps launcher in the top left corner.



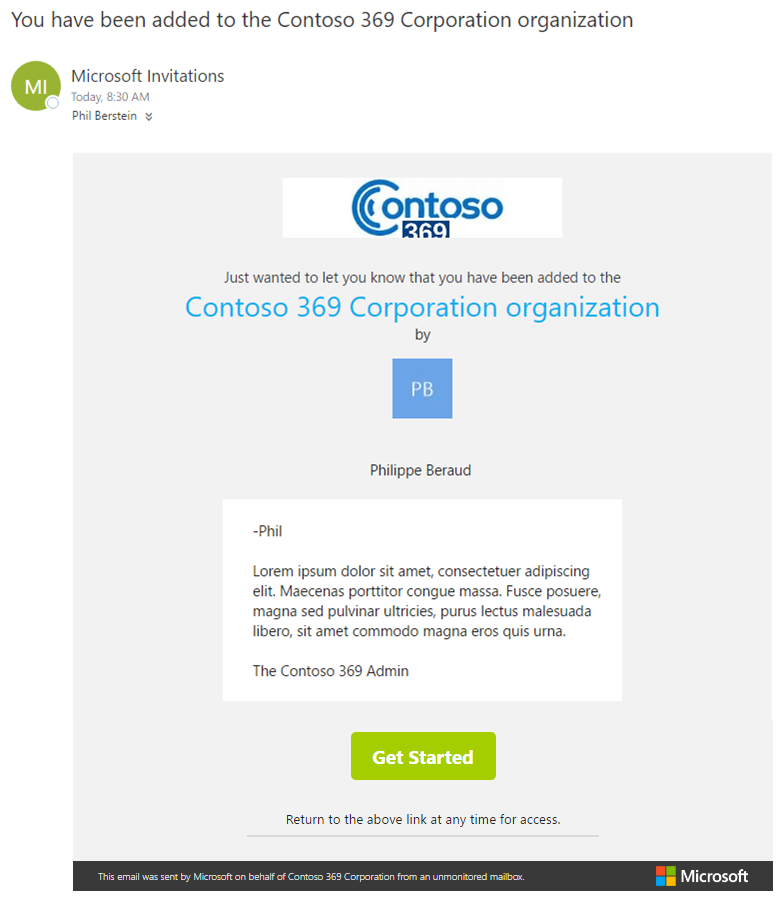
* 1. Select **Mail**.

You can alternatively navigate to:

<https://outlook.office365.com/owa/?realm=litware369.onmicrosoft.com>

and sign in.

1. Open the mail received from Microsoft Invitations. The content of the email will look similar to what's shown hereafter.



This invitation mail includes the inviter name. In addition, it can be branded with the tenant company branding of the inviter (as illustrated here).

**Note** For more information, see article [The elements of the B2B collaboration invitation email](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email)[[41]](#footnote-42).

The invitation email contains a **Get Started** button with redeem URL that you can use at any time:

<https://invitations.microsoft.com/redeem/>

?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1

&user=6c4be36a-3b36-4c6a-874e-28fabc09a04d

&ticket=%2fY3EL%2b42Chj4ujA%2b2xxJnn4lfpddNzAwvhg4JND%2fjc4%3d

&lc=1033

&ver=2.0

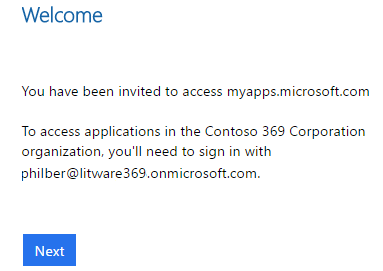
### Accepting the invitation

To accept this invitation, proceed with the following steps:

1. Click **Get Started** in the previous invitation email:

<https://invitations.microsoft.com/redeem/?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&user=6c4be36a-3b36-4c6a-874e-28fabc09a04d&ticket=%2fY3EL%2b42Chj4ujA%2b2xxJnn4lfpddNzAwvhg4JND%2fjc4%3d&lc=1033&ver=2.0>

The redeem URL opens a new tab in the web browser and navigates to the Azure B2B collaboration redeem portal for the inviter. The invitation accept landing page should be displayed.

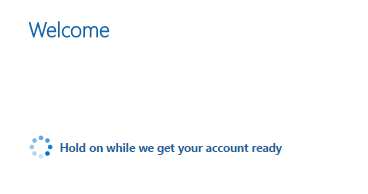


**Note** The invitation accept landing page can be branded with the tenant branding of the inviter. This requires a Basic, a Premium P1 or a Premium P2 edition of Azure AD.

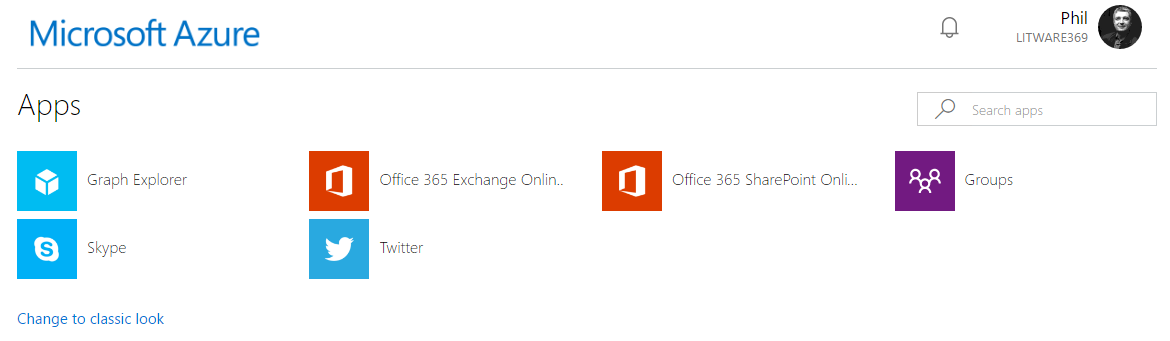
Beyond the invitee’s email address, the above invitation accept landing page provides some context for the invitee on how to accept the invitation. It indicates that after completing the sign-in, the user you will be redirected to the Access Panel:

<https://myapps.microsoft.com/?tenantid=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&login_hint=philber@litware369.onmicrosoft.com>

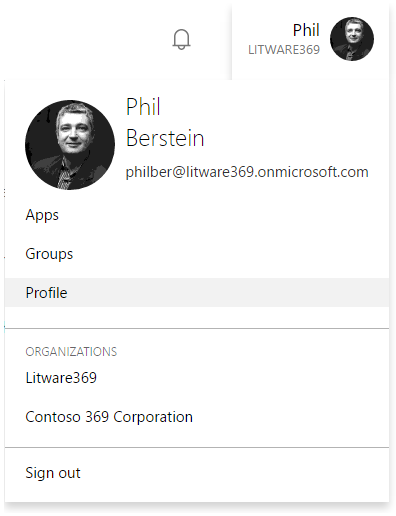
1. Click **Next**. The account is getting ready.



1. After some redirections in the browser address bar, the invitee is now finally redirected to the Access Panel. By default, the Access Panel list all the applications the user has access to in their home’s organization, e.g. the Litware 369 organization.



1. The Access Panel also allows the guest user to view and launch assigned applications in their inviting organization’s directory. The guest user simply needs to change the directory. Click the user’s picture in the upper right corner.



1. Select **Contoso 369 Corporation**. The invitee is redirected to the Access Panel for the Contoso 369 directory.

If you’re curious about the OpenID Connect id\_token security token that carry the user’s claims, you can grab it in the “identity dance” with the [Fiddler](http://www.telerik.com/fiddler)[[42]](#footnote-43) tool. Following is an illustration in this context:

id\_token=

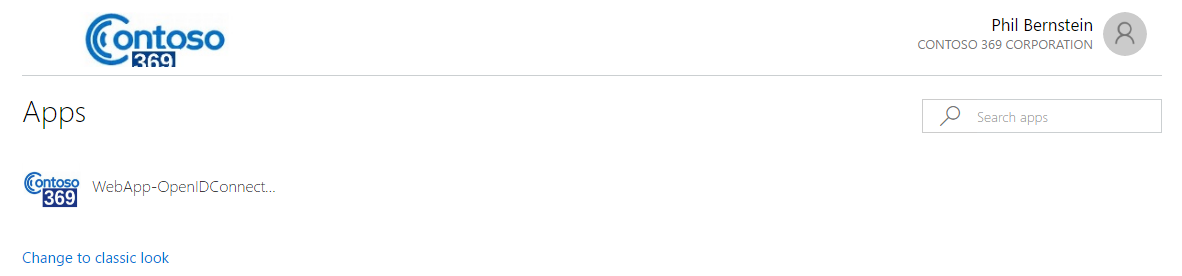
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Il9VZ3FYR190TUxkdVNKMVQ4Y2FIeFU3Y090YyIsImtpZCI6Il9VZ3FYR190TUxkdVNKMVQ4Y2FIeFU3Y090YyJ9..EWACOslSdLJdgFSt\_9\_6ZMGe7yLdGt-wadIWQ92o\_FYi1DASqALW5bPywmnvO-t1r86I4iZhJtcZyhH7\_TONx\_j9ZYbxOyxAErUeb-T0LQ6rHX23O58C0LKTKD6BIVJ-tnepmWXGotKOl6b5pm3lnIjsJHWEwgvACsqVywH-lqk-jZytZr09tD8UL27HTqHtW0Uof1l0c20d99Zqnup\_VKOPvyCOabvdc-sd5lBN1aQrK3hI6-N27-p7qy2sMhzGGwrWqX4\_OslOfFN1aiBYHh\_bUSzSzi-M3vt8mLu1c9\_KgTWAYHSkES3B6ZpaivGrfpRjU75Ft\_4AQoFkTonCeA

Decoding the URLBase64 id\_token from the response yields the following claims decoded in JSON:

**Note** Since the JWT tokens issued by Azure AD are signed but not encrypted, you can easily inspect the content of such a token for debugging purposes. There are several tools available to do so such as the [JWT Decoder](http://calebb.net/)[[43]](#footnote-44) or [JWT.io](https://jwt.io/)[[44]](#footnote-45).



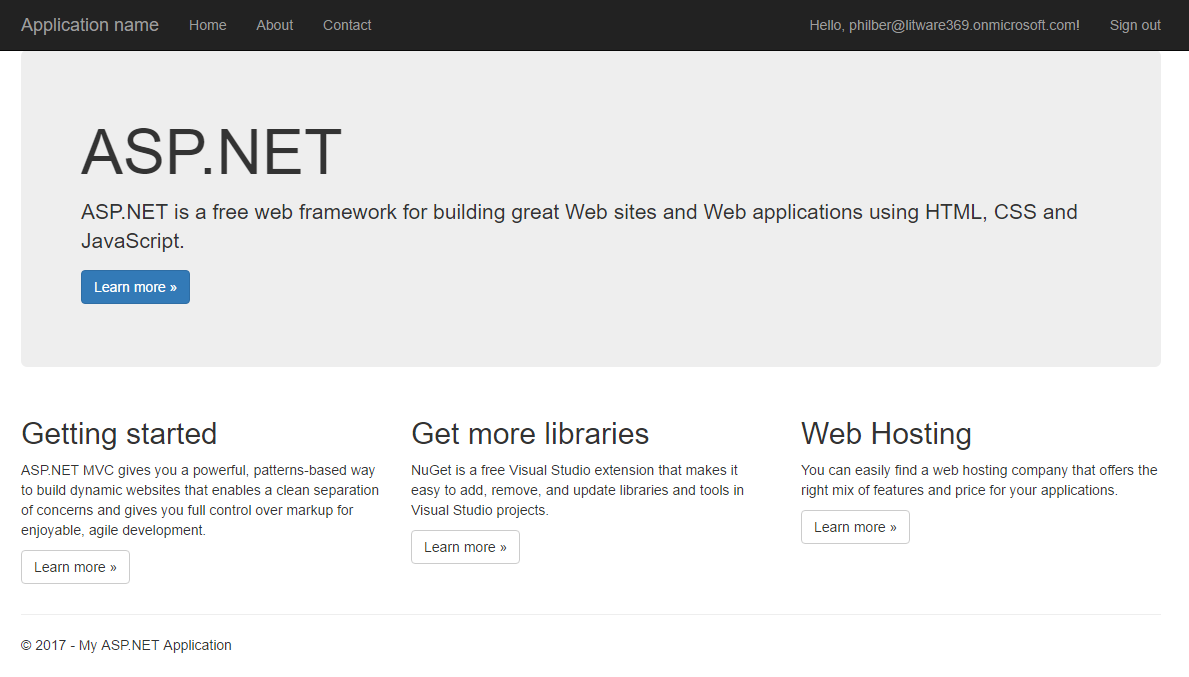
Back to the Access Panel, the sample application WebApp-OpenIDConnect-DotNet should now appear here.



1. Click **WebApp-OpenIDConnect-DotNet**. You will be redirected to the sample application.

**Note** In our illustration, you should run the sample application from the Visual Studio prior clicking to the above icon.

1. Click **Sign in**. You’re authenticated as philber@litware369.onmicrosoft.com.



1. Et voila!

**Note** Since the major mobile platforms don't support the browser plugins as notably used by the Access Panel (e.g. the password-based single sign-on browser plugins), a "My Apps" mobile application is also available to help users access their apps on their mobile devices. The "My Apps" application is optimized for your mobile device and supports all of the features of the Access Panel. You will have the exact same user experience.

"My Apps" is available as of today for both the iOS and Android platforms. My Apps for Android works on any device running Android version 4.1 or higher, and is available in the [Google Play store](https://play.google.com/store/apps/details?id=com.microsoft.myapps)[[45]](#footnote-46). My Apps for iOS is supported on any iPhone or iPad running iOS version 8.0 and up, and is available in the [Apple App Store](https://itunes.apple.com/us/app/my-apps-windows-azure-active/id824048653?mt=8)[[46]](#footnote-47).

## Receiving and accepting the invitation as a social ID user (invitee UX)

As you already know, Azure AD B2B collaboration provides you with ability to invite a user with any email address on the planet. For the sake of the walkthrough, both the UXs with a Gmail and a Microsoft accounts are covered to illustrate the two-possible user experience (UX) at the time of this writing.

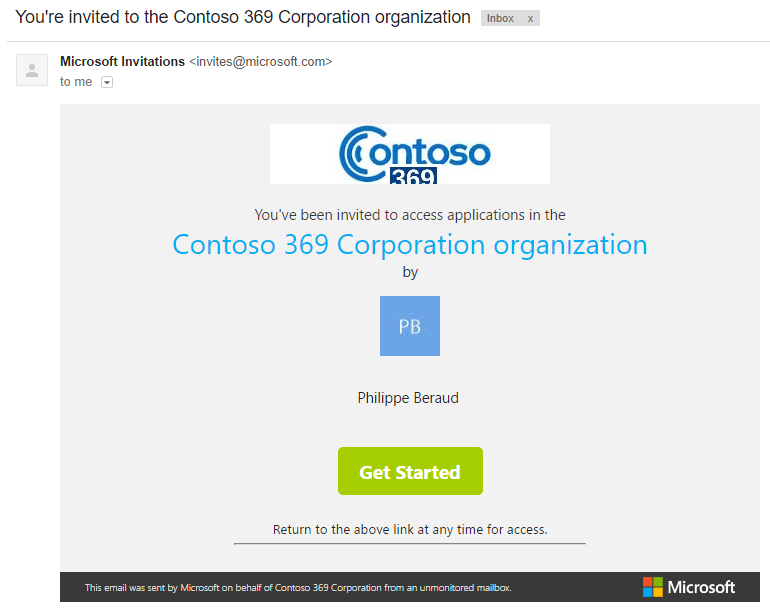
**Note** For more information, see article [Azure Active Directory B2B collaboration invitation redemption](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-redemption-experience)[[47]](#footnote-48).

Let’s start with the Gmail account.

### Receiving the invitation email for the Gmail account

To receive and accept the invitation for the Gmail social ID account, proceed with the following steps:

1. Open your Gmail mailbox. Open a browsing session and navigate to <https://mail.google.com/> to access your mail box
2. Sign-in as contoso369b2binvitee@gmail.com.
3. Open the mail received from Microsoft Invitations. The content of the email will look similar to what's shown hereafter.



As before, this invitation mail includes the inviter name. It can be also additionally branded with the tenant company branding of the inviter (as illustrated here).

**Note** For more information, see article [The elements of the B2B collaboration invitation email](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email)[[48]](#footnote-49).

Likewise, the invitation email contains a **Get Started** button with redeem URL that you can use at any time:

<https://invitations.microsoft.com/redeem/>

?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1

&user=755de4cb-3fd8-4fb6-8a45-83cb0cc5712a

&ticket=vAjJoQsseyI4UarYYFv3K3LcM2z3wZqUuCaoIPcXxvs%3d

&lc=1033

&ver=2.0

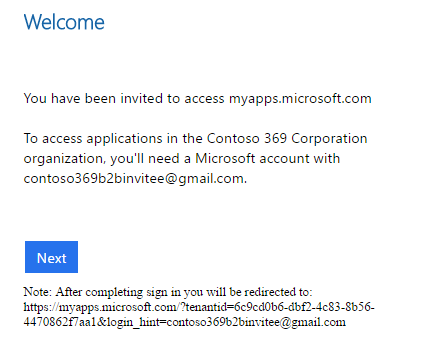
### Accepting the invitation for the Gmail account

To accept this invitation, proceed with the following steps:

1. Click **Get Started** in the invitation email:

https://invitations.microsoft.com/redeem/?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&user=755de4cb-3fd8-4fb6-8a45-83cb0cc5712a&ticket=vAjJoQsseyI4UarYYFv3K3LcM2z3wZqUuCaoIPcXxvs%3d&lc=1033&ver=2.0

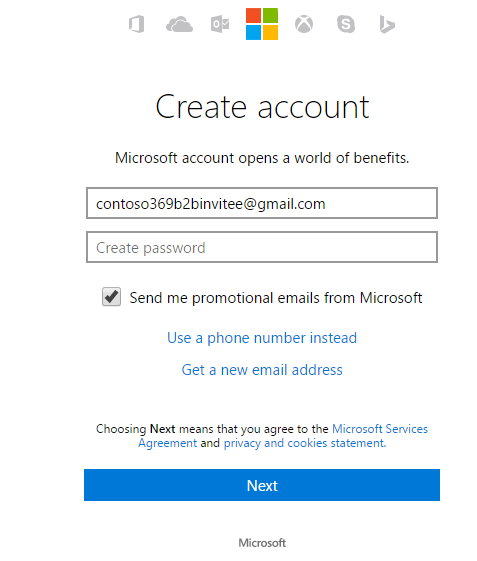
The redeem URL opens a new tab in the web browser and navigates to the Azure B2B collaboration redeem portal for the inviter. The invitation accept landing page should be displayed.



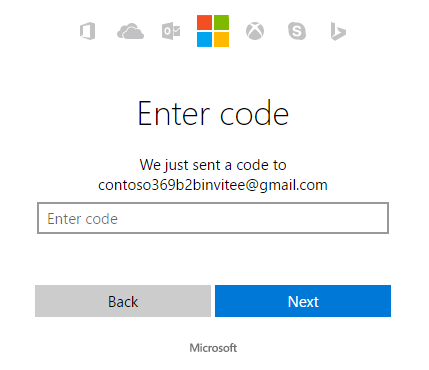
**Note** The invitation accept landing page can be branded with the tenant branding of the inviter. This requires a Basic, a Premium P1 or a Premium P2 edition of Azure AD.

Beyond the invitee’s email address, the above invitation accept landing page provides some context for the invitee on how to accept the invitation: as stated, a Microsoft account with [contoso369b2binvitee@gmail.com](mailto:contoso369b2binvitee@gmail.com) as the ID is needed. At this time of this writing, no direct federation with Google accounts is available as already mentioned.

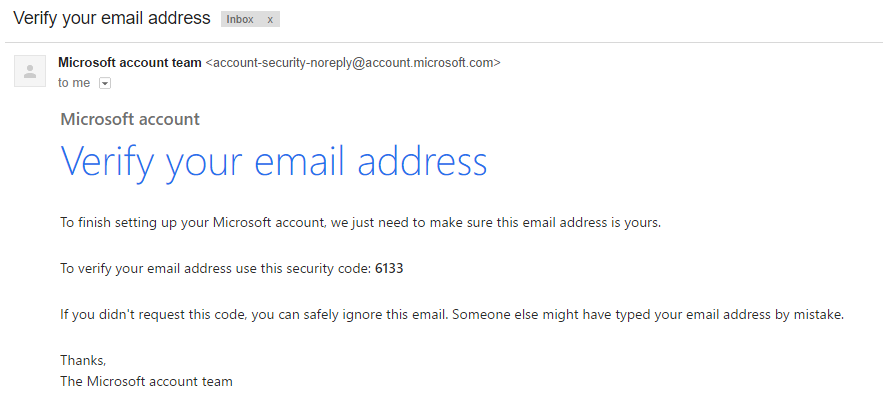
1. Click **Next**. As expected, you’re now invited to create a Microsoft account.



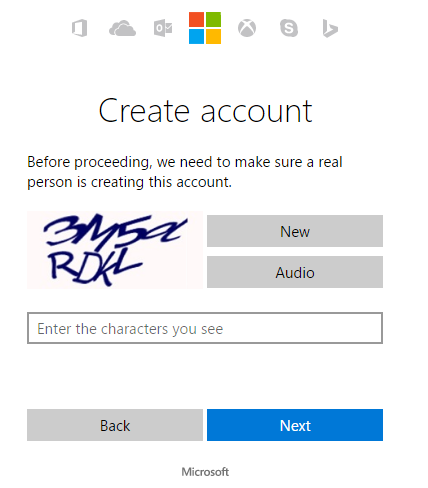
1. Specify a password for this Microsoft account, for example “Pass@word1!?” in our illustration.
2. Click **Next**.



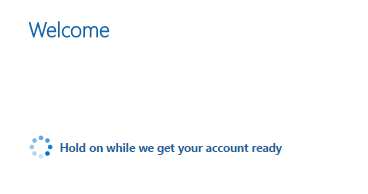
1. Check your Gmail mailbox for the code send by the Microsoft account team.



1. Back to the **Microsoft account** tab in the web browser, enter the received code, here 6133, and then click **Next**.



1. Enter the characters you see in the Captcha, and then click **Next**. The account is getting ready.

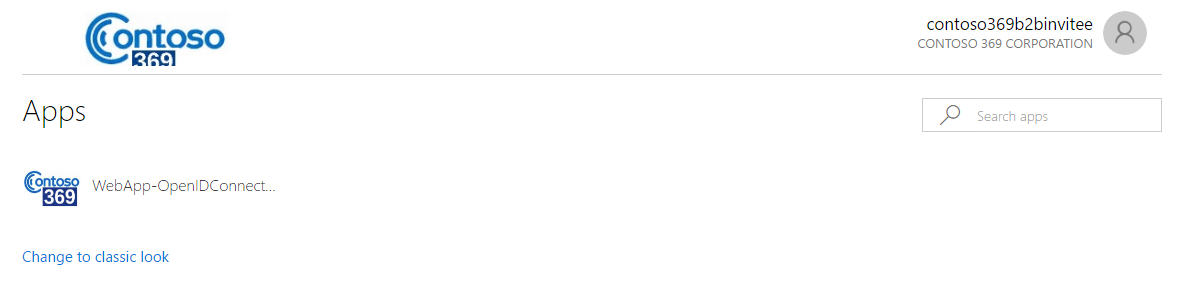


1. The invitee is now finally redirected to the Access Panel:

<https://myapps.microsoft.com/?tenantid=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&login_hint=contoso369b2binvitee@gmail.com>

**Note** Logging in after creating a new guest account in Azure AD may fail occasionally, but will work on a retry (hitting F5 at invite acceptance screen).

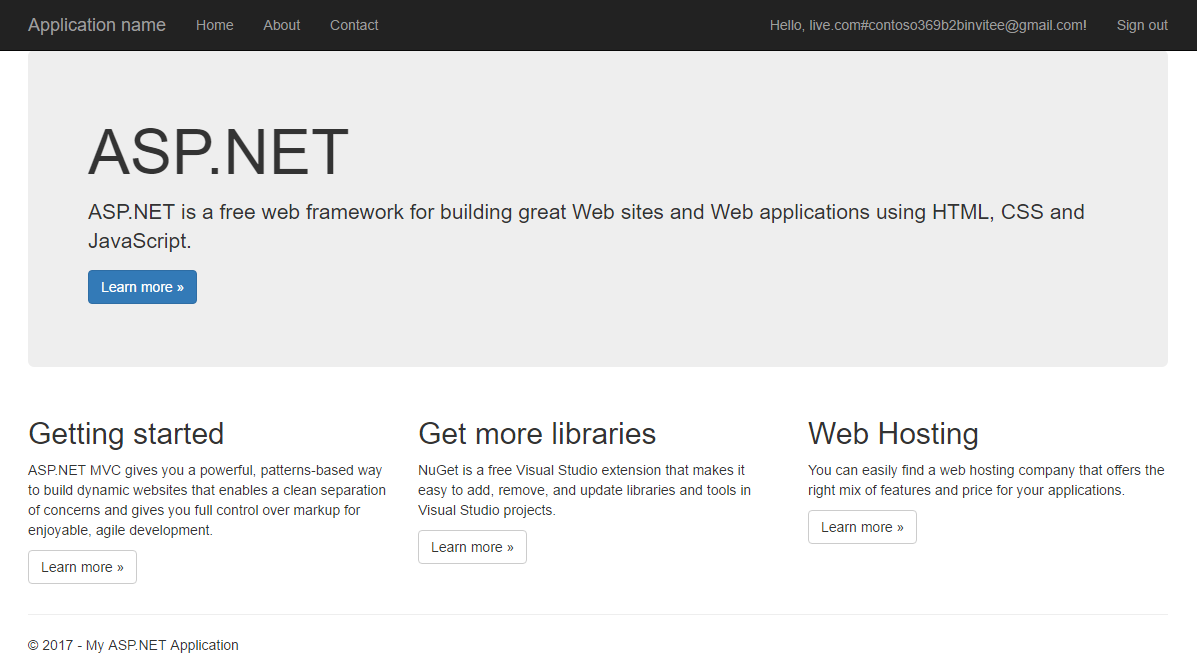
The sample application WebApp-OpenIDConnect-DotNet should appear here.



1. Click **WebApp-OpenIDConnect-DotNet**. The invitee is redirected to the sample application.

**Note** In our illustration, you should run the sample application from the Visual Studio prior clicking to the above icon.

1. Click **Sign in**. You’re authenticated as live.com#contoso369b2binvitee@gmail.com.



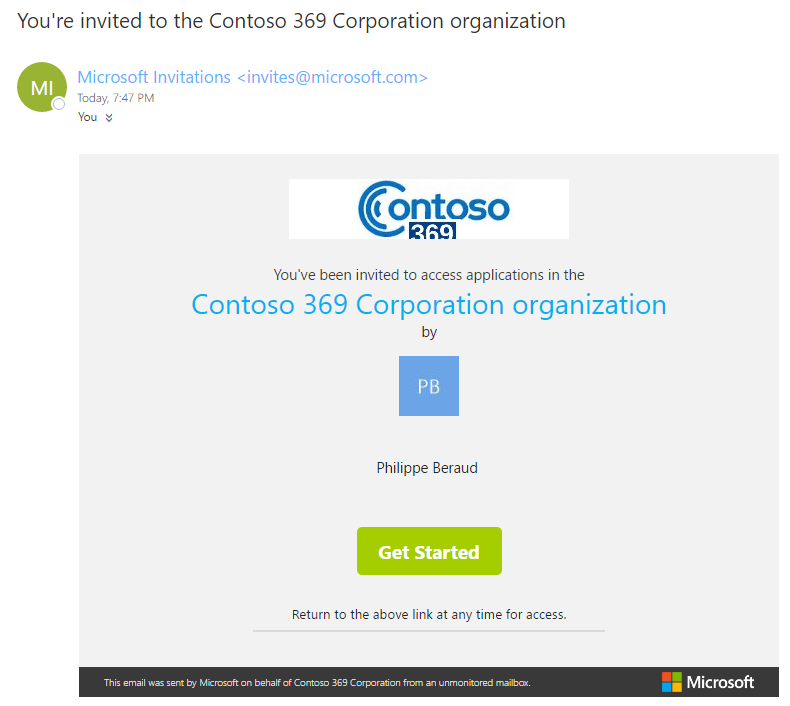
1. Et voila!

Let’s switch to the Microsoft account.

### Receiving the invitation email for the Microsoft account

To receive and accept the invitation for the Microsoft account, proceed with the following steps:

1. Open your Outlook.com mailbox. Open a browsing session and navigate to <https://outlook.live.com/owa/> to access your mail box
2. Sign-in as contoso369b2binvitee@outlook.com.
3. Open the mail received from Microsoft Invitations. The content of the email will look similar to what's shown hereafter.



As already mentioned, this invitation mail includes the inviter name. It can be also additionally branded with the tenant company branding of the inviter (as illustrated here).

**Note** For more information, see article [The elements of the B2B collaboration invitation email](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email)[[49]](#footnote-50).

The invitation email contains a **Get Started** button with redeem URL that you can use at any time:

<https://invitations.microsoft.com/redeem/>

?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1

&user=e395f7fb-7d3f-412e-9948-2906ace5bf5b

&ticket=z7dPQ9YWDOM%2bgMsO8WmZdfGwe1ucSIgCxMOmDAhRC%2fM%3d

&lc=1033

&ver=2.0

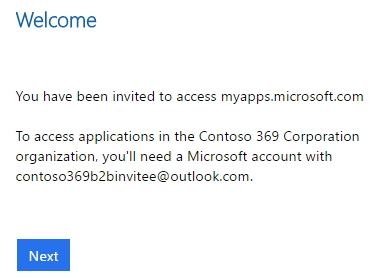
### Accepting the invitation for the Microsoft account

To accept this invitation, proceed with the following steps:

1. Click **Get Started** in the invitation email:

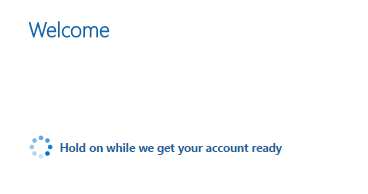
<https://invitations.microsoft.com/redeem/?tenant=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&user=e395f7fb-7d3f-412e-9948-2906ace5bf5b&ticket=z7dPQ9YWDOM%2bgMsO8WmZdfGwe1ucSIgCxMOmDAhRC%2fM%3d&lc=1033&ver=2.0>

The redeem URL opens a new tab in the web browser and navigates to the Azure B2B collaboration redeem portal for the inviter. The invitation accept landing page should be displayed.



Beyond the invitee’s email address, the above invitation accept landing page provides some context for the invitee on how to accept the invitation: as stated, a Microsoft account with [contoso369b2binvitee@outlook.com](mailto:contoso369b2binvitee@outlook.com) as the ID is needed.

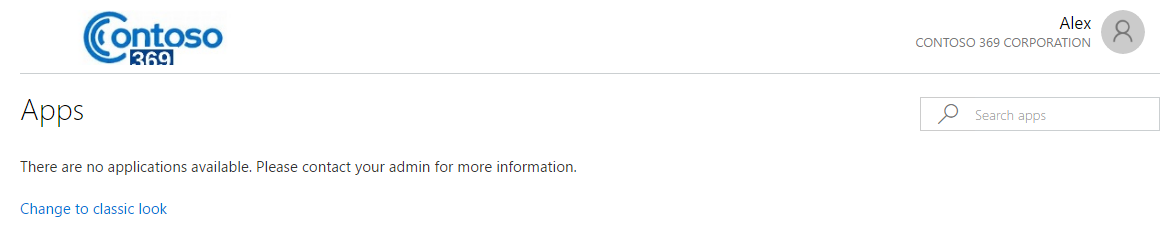
1. Click **Next**. The account is getting ready.



1. The invitee is now redirected to the Access Panel:

<https://myapps.microsoft.com/?tenantid=6c9cd0b6-dbf2-4c83-8b56-4470862f7aa1&login_hint=contoso369b2binvitee@outlook.com>

At this stage, the sample application WebApp-OpenIDConnect-DotNet isn’t listed since Alex Darrow hasn’t been assigned to the application so far. This is the purpose of the next section to illustrate another facet of Azure AD B2B collaboration.



## Delegating invitations to non-administrators (inviter UX)

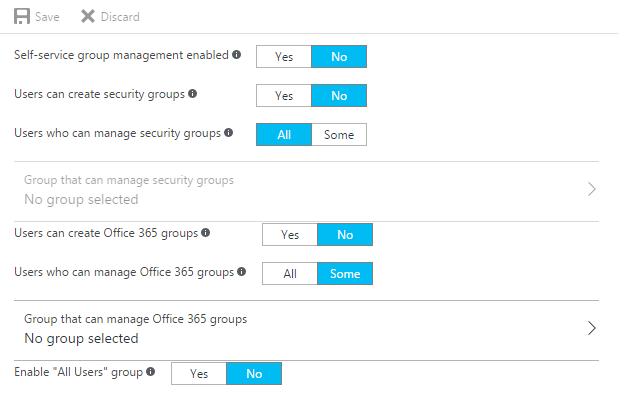
We will now illustrate the Azure AD B2B collaboration self-service invitation capabilities for information workers (IW) in the Access Panel, and more especially the ability for Information workers to invite guest users to any self-service group or application that they manage.

**Note** For more information, see article [How do information workers add B2B collaboration users to Azure Active Directory?](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-iw-add-users)[[50]](#footnote-51).

### Enabling self-service group management

To enable self-service group management, proceed with the following steps:

1. Open a browsing session, navigate to the Azure portal at <https://portal.azure.com/>, and then signs in with your administrative credentials.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. Under **MANAGE**, select **Users and groups**. A new blade opens.
4. Under **MANAGE**, select **Group settings**. The blade expands to display all the settings.

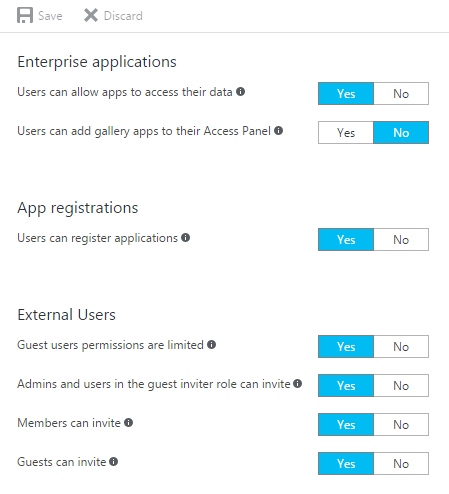


1. Click **YES** next to **Self-service group management enabled** to enable self-service group management for users through the Access Panel.
2. Click **Save**.

### Controlling who can invite

To control who can invite, proceed with the following steps:

1. Back to the directory blade, click **User setting**. A **Group** blade opens.



By default, all users, including the guest users, can invite.

1. The invitation policy can be set to one of the followings:
   1. Turn invitations off: **Admins and user in the guest inviter role can invite** set to **No**, **Members can invite** set to **No**, and **Guest can invite** set to **No**.
   2. Only global administrators and limited administrators with the Guest Inviter role can invite: **Admins and user in the guest inviter role can invite** set to **Yes**, **Members can invite** set to **No**, and **Guest can invite** set to **No**.
   3. Global administrators, Limited administrators with the Guest Inviter role, and members can invite: **Admins and user in the guest inviter role can invite** set to **Yes**, **Members can invite** set to **Yes**, and **Guest can invite** set to **No**.
   4. All users, including the guest users, can invite (default): **Admins and user in the guest inviter role can invite** set to **Yes**, **Members can invite** set to **Yes**, and **Guest can invite** set to **Yes**.

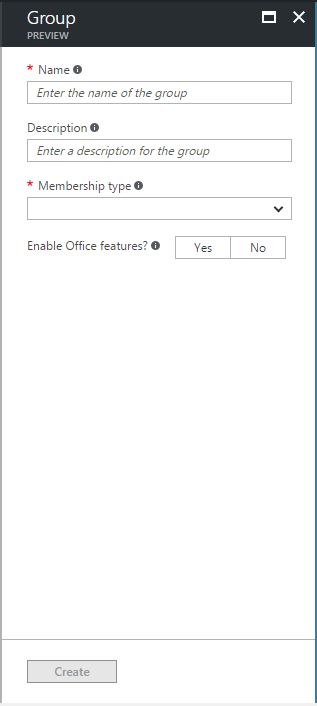
Leave the default setting and select **Discard**.

**Note** For more information, see article [Delegate invitations for Azure Active Directory B2B collaboration](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations)[[51]](#footnote-52).

### Creating an “Assigned” group for access to the app

To create an “Assigned” group for access to the app, proceed with the following steps:

1. Back to the directory blade, click **Add a group** under **Quick tasks**. A **Group** blade opens.

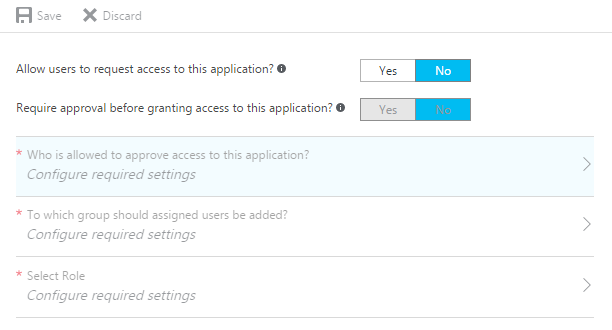


1. In **Name** and **Description**, type “Self-service App Access for WebApp-OpenIDConnect-DotNet App”.
2. In **Membership type**, select **Assigned**. As of this writing, guest users cannot be added to a dynamic group (or to a group that is synced with the on-premises organization’s AD).
3. In **Enable Office features**, select **No**.
4. Click **Create**. A floating notification tile should indicate the successful creation of the group.

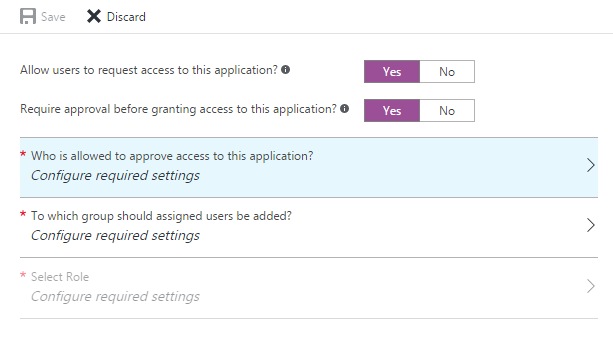
### Assigning the self-service group for access to the app

To assign the self-service group for access to the app, proceed with the following steps:

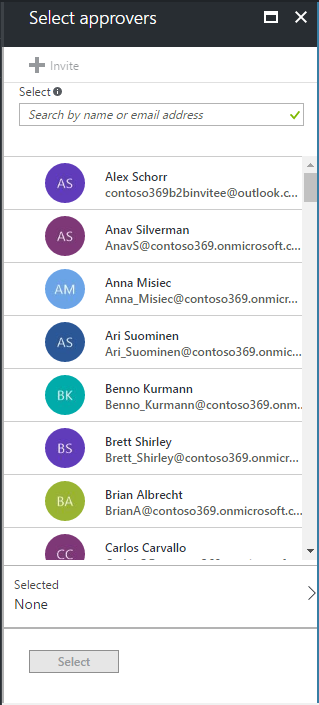
1. Back to the directory blade, select **Enterprise applications** under **MANAGE**. An eponym blade opens.
2. Select **All application**, and then select **WebApp-OpenIDConnect-DotNet**.
3. Under **MANAGE**, select **Self-service**. An eponym blade opens.



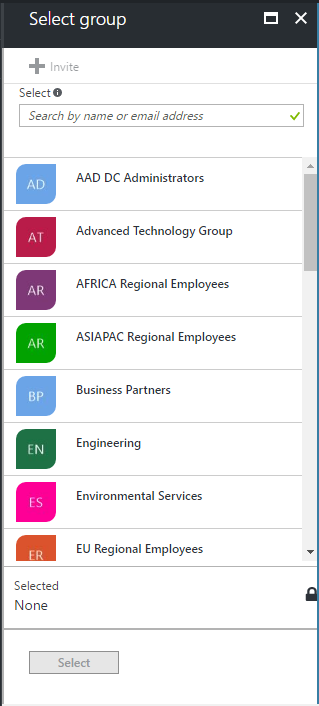
1. Select **Yes** next to **Allow user to request access to this application**.
2. Select **Yes** next to **Require approval before granting access to this application**.



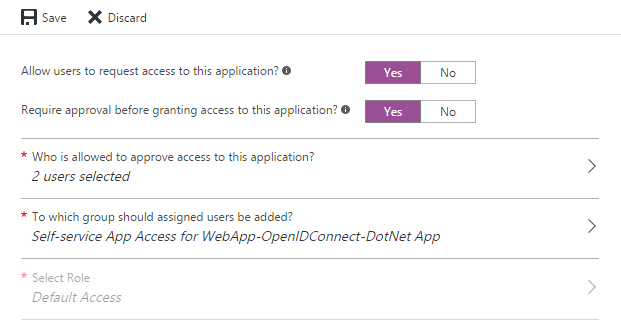
1. Select **Who is allowed to approve access to this application?** A **Select approvers** blade opens.



1. Select one or multiples IW accounts to whom you’d like to delegate this capability. (You can alternatively use your own admin account.).
2. Click **Select**.
3. Select **To which group should assigned users be added?** A **Select group** blade opens.



1. Search the previously created group “Self-service App Access for WebApp-OpenIDConnect-DotNet App”, select it, and then click **Select**.

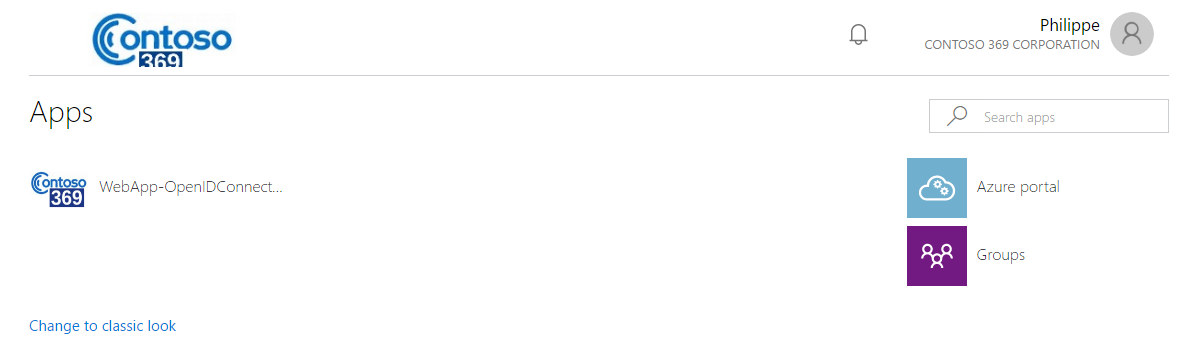


1. Click **Save**.

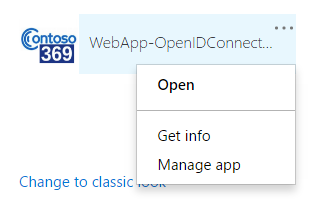
### Adding guest users to the app

To add a guest user to the app, proceed with the following steps:

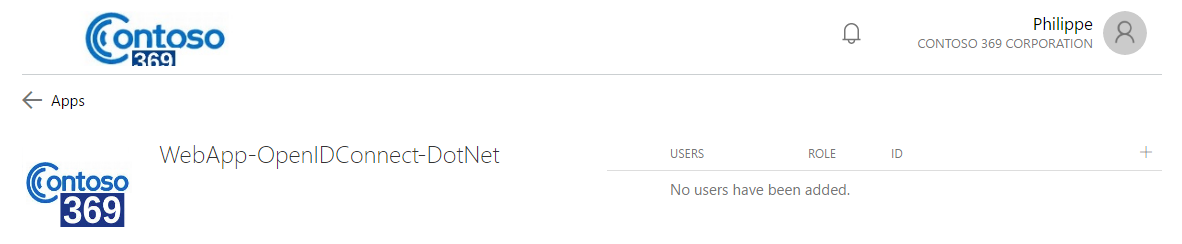
1. Open a browsing session and navigate to the Access Panel at <https://myapps.microsoft.com>, and then signs in with your information worker (IW) credentials.



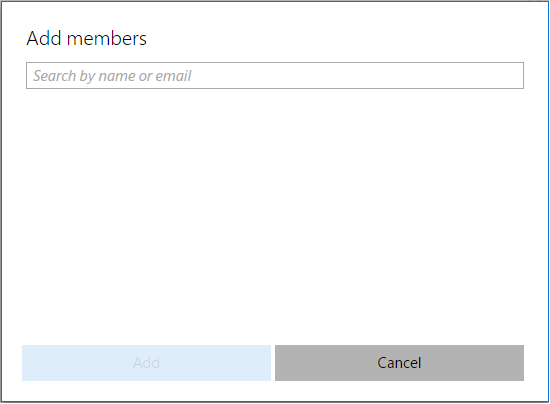
1. Right-click **WebApp-OpenIDConnect-DotNet**.



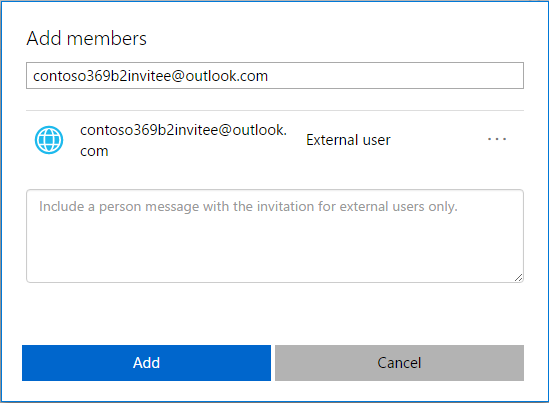
1. Select **Manage app**.



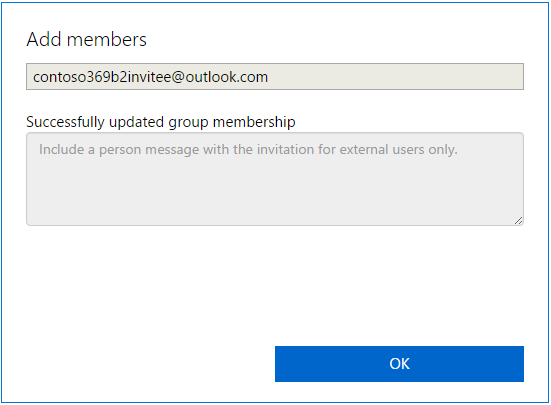
1. Click +next to **ID** in the **USERS** table header. An **Add members** dialog opens.



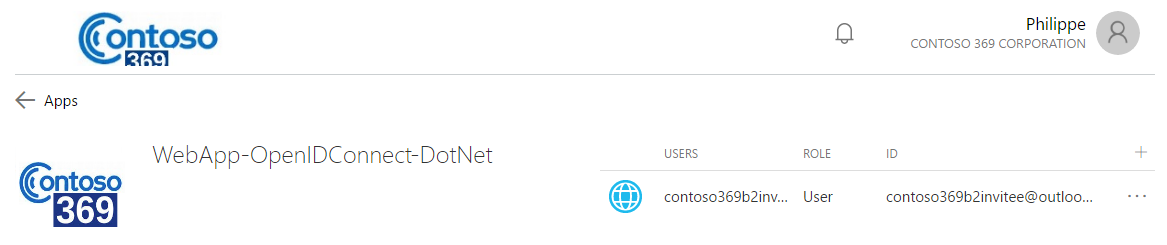
1. Enter “Alex Schorr” or “contoso369b2binvitee@outlook.com”.



1. Click **Add**.



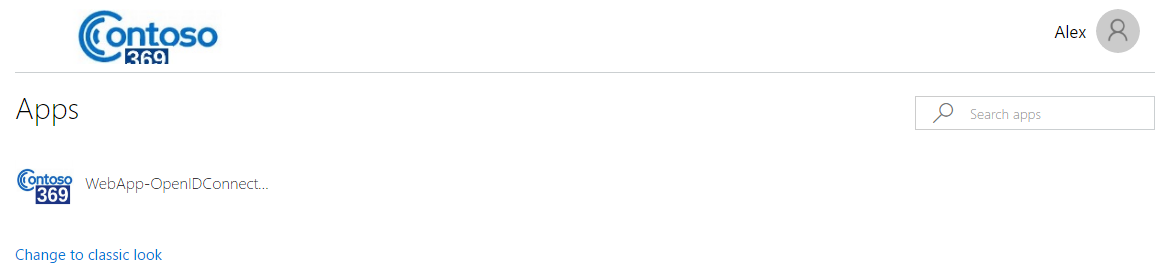
1. Click **OK**.



### Accessing the assigned app

To access the assigned app, proceed with the following steps:

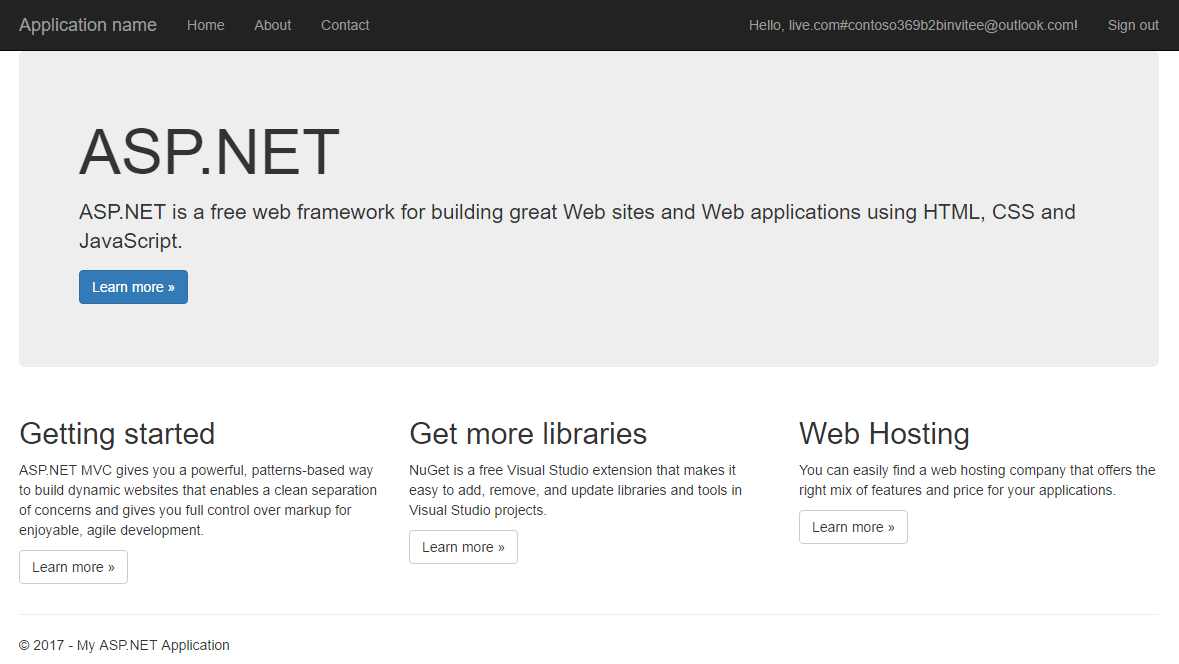
1. Open a browsing session and navigate to the Access Panel at <https://myapps.microsoft.com>, and then signs in as Alex Schorr (contoso369b2binvitee@outlook.com).



1. Click **WebApp-OpenIDConnect-DotNet**. You will be redirected to the sample application.

**Note** In our illustration, you should run the sample application from the Visual Studio prior clicking to the above icon.

1. Click **Sign in**. You’re authenticated as live.com#contoso369b2binvitee@outlook.com.



1. Et voila!

## Leveraging multi-factor authentication for guest users

As the title states, let’s illustrate how to leverage multi-factor authentication (MFA) for guest users in the inviting organization, here the Contoso369 organization.

**Note** For more information, see article [Multi-factor authentication for Azure Active Directory B2B collaboration users](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-mfa-instructions)[[52]](#footnote-53).

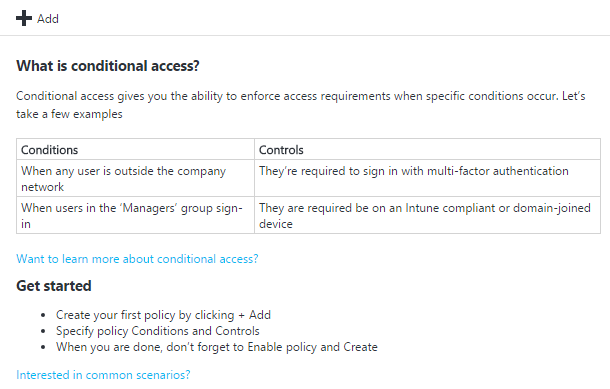
### Setting up conditional access (inviter UX)

**Conditional access requires the Azure AD Premium P1 or P2 editions.**

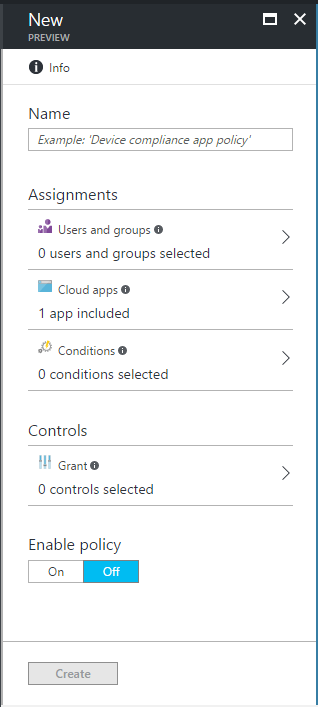
If you’ve followed the steps of this walkthrough in order, a 30-days trial period has already been activated for the company branding (see section § Customizing invitation email with branding.)

To set up conditional access, proceed with the following steps:

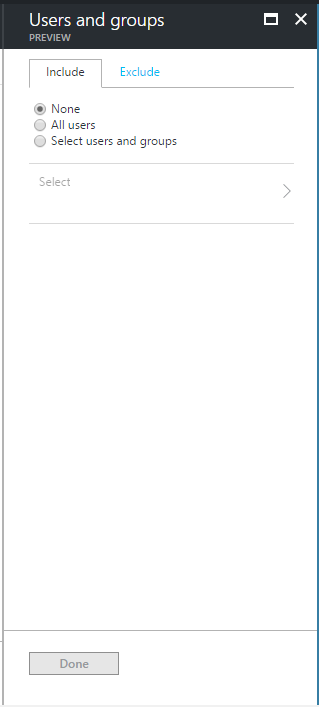
1. Open a browsing session, navigate to the Azure portal at <https://portal.azure.com/>, and then signs in with your administrative credentials.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. select **Enterprise applications** under **MANAGE**. An eponym blade opens.
4. Select **All application**, and then select **WebApp-OpenIDConnect-DotNet**.
5. Under **MANAGE**, select **Conditional access**. An eponym blade opens.



1. Click **+ Add**. A new blade opens.

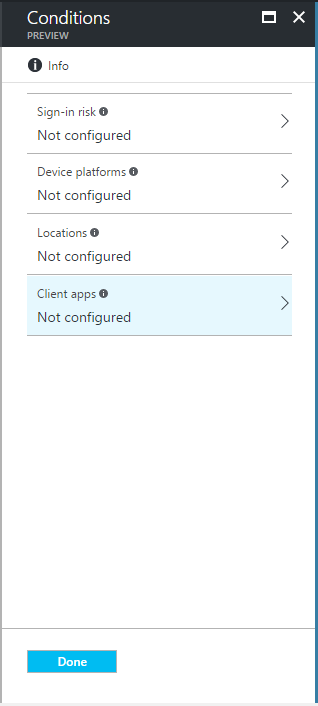


1. In **Name**, enter a policy name, for example “MFA policy”.
2. Under **Assignments**, select **Users and groups**. A new blade opens.

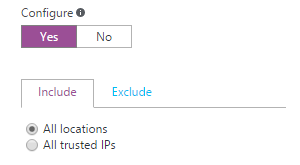


* 1. Click **Select users and groups**.
  2. Click **Select**. In the **Select** blade, search **Business Partners**., select it, and then click **Select**.
  3. Click **Done**.

1. Choose a condition to enforce. Select **Conditions**. A new blade opens.

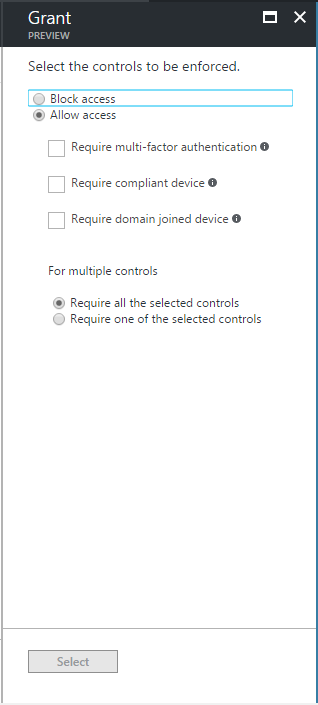


* 1. Select **Locations**. An eponym blade opens.
  2. Select **Yes** next to **Configure**.
  3. Leave **All locations** selected.



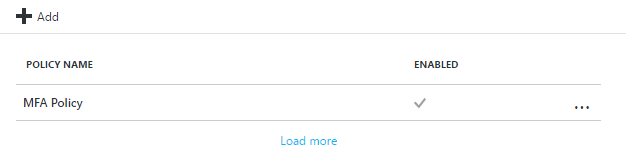
* 1. Click **Done** twice.

1. Under **Controls**, select **Grant**. A new blade opens.



* 1. Leave **Allow Access** selected.
  2. Check **Require multi-factor authentication**.
  3. Click **Select**.

1. Under **Enable policy**, click **On**.
2. Click **Create**.

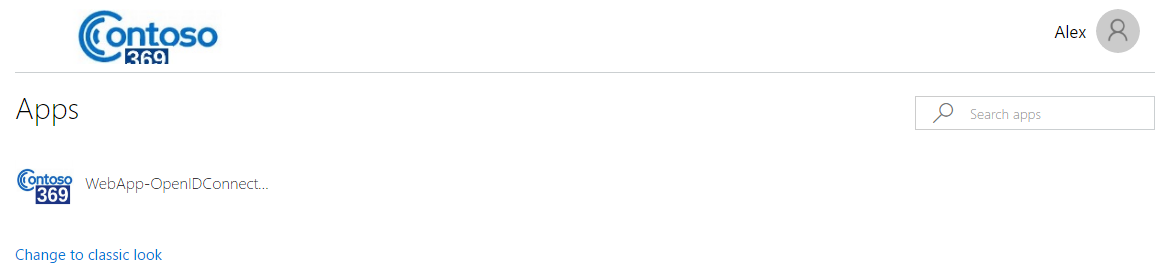


### Receiving and accepting the invitation with MFA redemption (invitee UX)

Compared to the UX outlined in sections § Receiving and accepting the invitation as a corporate user (invitee UX) and § Receiving and accepting the invitation as a social ID user (invitee UX), the only difference resides when the guest user click the sample application WebApp-OpenIDConnect-DotNet in the Access Panel.

To illustrate the experience, proceed with the following steps:

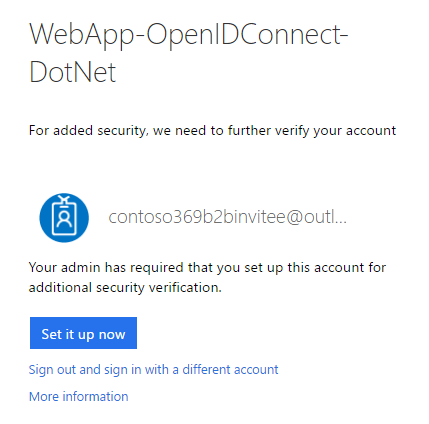
1. Open a browsing session and navigate to the Access Panel at <https://myapps.microsoft.com>, and then signs in as Alex Schorr (contoso369b2binvitee@outlook.com).



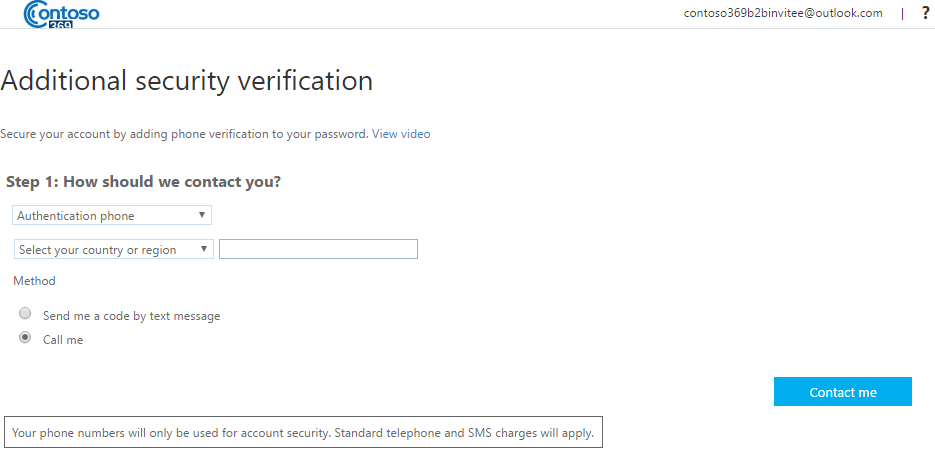
1. Click **WebApp-OpenIDConnect-DotNet**. You will be redirected to the sample application.

**Note** In our illustration, you should run the sample application from the Visual Studio prior clicking to the above icon.

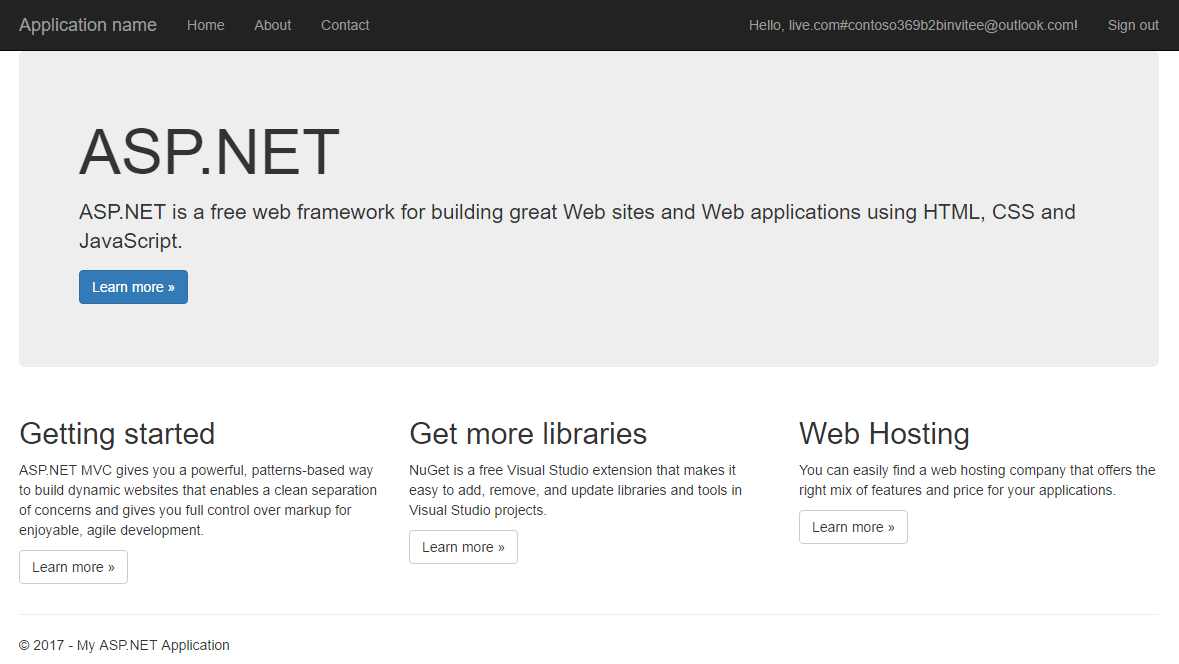
1. Click **Sign in**. You’re now invited to setup the multi-factor authentication as per above MFA policy.



1. Click **Set it up now**.



1. Select your country and enter your phone number, and then click **Contact me**.
2. Answer the call and press #. After a successful verification, click **Done**. You’re authenticated as live.com#contoso369b2binvitee@outlook.com.



1. Et voila!

## Customizing onboarding using the Invitation API (inviter UX)

Developers can use the Invitation REST API to write applications that bring two organizations together in a secure way but is seamless to information workers (IW) and is intuitive for them to navigate.

This API currently in beta is documented at <https://graph.microsoft.io/en-us/docs/api-reference/beta/resources/invitation>. It allows to send request to the invitation manager, and this add guest user in the directory in a similar way on what has been previously illustrated with PowerShell for bulk invites, see section § Bulk inviting guest users with CSV. The API enables to fully customize the invitation and onboarding workflows.

Following is an example of such a request:

POST https://graph.microsoft.com/beta/invitations

Content-type: application/json

Content-length: 551

{

"invitedUserDisplayName": "Rober Hatley"  
 "invitedUserEmailAddress": "contoso369b2Binvitee@gmail.com"  
 "inviteRedirectUrl": "https://myapps.microsoft.com/"  
 "sendInvitationMessage": true  
 "customizedMessageBody": "Hello Robert, let’s collaborate together!"

}

**Note** For more information, see articles [Azure Active Directory B2B collaboration code and PowerShell samples](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-code-samples)[[53]](#footnote-54) and [Azure Active Directory B2B collaboration API and customization](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-api)[[54]](#footnote-55). The former provides a sample code that illustrates how to call the above invitation API in "app-only" mode.

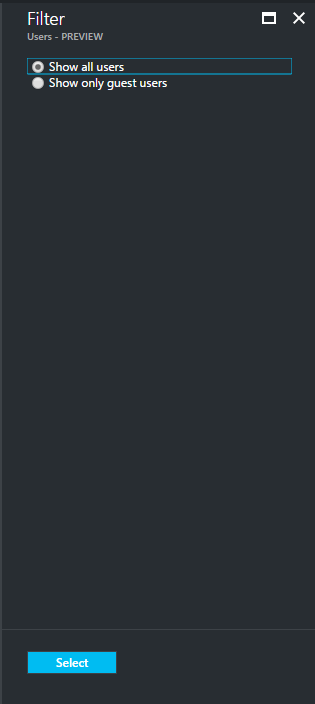
## Viewing and managing the invitees (inviter UX)

To complete this walkthrough, let’s see how guest users can be viewed and managed with the inviting organization’s Azure AD directory.

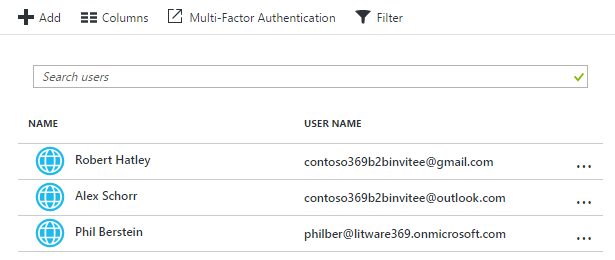
### Viewing the guest users

To view and manage the guest users, proceed with the following steps:

1. Open a browsing session and navigate to the Azure portal at <https://portal.azure.com/>, and then Sign in to the Azure portal as the Subscription admin user.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. Under **MANAGE**, select **Users and groups**, and then **All users**.
4. Click **Filter**.



1. Select **Show only guest users**, and then click **Select** to see all the guest user accounts added to the directory.



These guest user accounts are accounts where the userType attribute is set to **Guest**. This attribute indicates the relationship of the user with the organization’s Azure AD directory. (An employee of the organization is set to **Member**.)

As outlined before, such an account corresponds to the following situations:

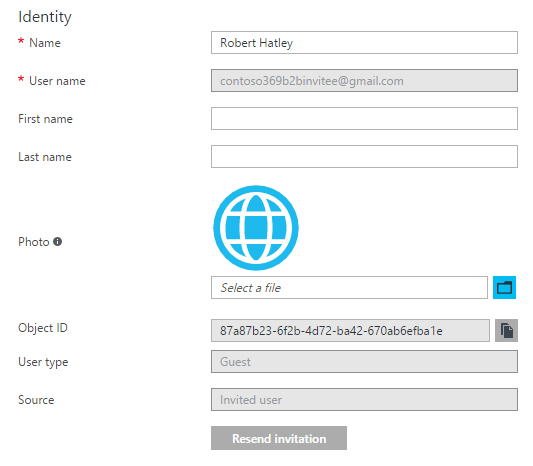
1. An account homed in another Azure AD directory and represented as a guest user in the organization’s Azure AD directory. This situation is illustrated with Phil Berstein.
2. An account homed in Microsoft Account (MSA) and represented as a guest user in the organization’s Azure AD directory. This situation is illustrated with Robert Hatley and Alex Schorr.

- and additionally -

1. An account (already) homed in the organization's on-premises AD, synced with the organization's Azure AD directory and where the userType attribute is manually set to Guest. This situation of an internally managed partner identity for some specific reasons is not illustrated in this document.
2. An account homed in organization's Azure AD directory where the userType attribute is set to Guest, and with credentials managed by directly the organization. This situation of an internally managed partner identity for some specific reasons is not illustrated in this document.

The Source attribute indicates how the user sign ins. Not yet redeemed invitees are flagged as **Invited User** while redeemed invitees are listed as **External Active Directory** (situation 1 above), **Microsoft Account** (situation 2 above), **Windows Server AD** (situation 3 above), or **Azure Active Directory** (situation 4 above).

1. Beyond the above considerations, you can manage the user, like any other (member) user in the directory, and for example extend the user information with the available attributes. Azure AD also enables to add custom attributes.
2. Finally, for not yet redeemed invitees for any reason, you can resend the invitation from the guest users’ profile.
   1. Select a guest user, for example **Robert Hatley**.
   2. Under **MANAGE**, select **Profile**.



* 1. Click **Resend invitation**.

**Note** For more information, see article [Properties of an Azure Active Directory B2B collaboration user](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-user-properties)[[55]](#footnote-56).

### Hardening the All Users dynamic group

The **All users** dynamic group allows the directory’s administrators to enable a group containing all users in the tenant with a single click. (This group can be enabled in **Group settings** in the **Users and groups**.)

By default, this group includes all users in the directory, including members and guests.

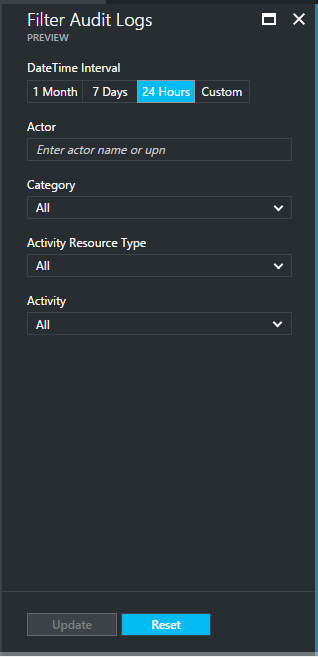
It can be hardened as per article [Dynamic groups and Azure Active Directory B2B collaboration](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-dynamic-groups)[[56]](#footnote-57) so that group, so that it only contains user account where the userType attribute is not equal to **Guest**.

## Leveraging auditing and reporting capabilities (inviter UX)

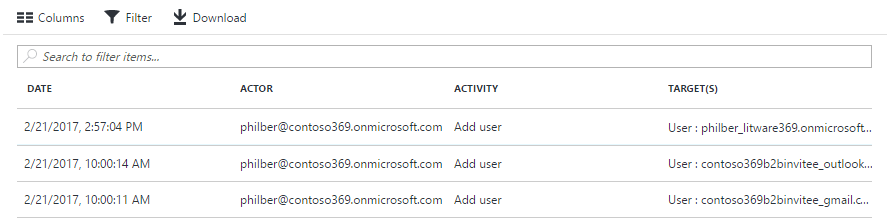
With Azure AD, you can get access to a standard set of activity reports giving you visibility into which users have been added, which are using which applications, when they were using and where they are using them from.

To view the activity, proceed with the following steps:

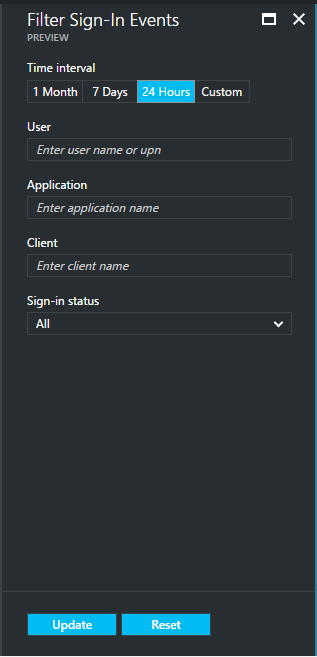
1. Open a browsing session and navigate to the Azure portal at <https://portal.azure.com/>, and then Sign in to the Azure portal as the Subscription admin user.
2. Select **Azure Active Directory** from the left navigation (favorites) pane. The directory blade opens.
3. Under **ACTIVITY**, select **Audit logs**. An eponym blade opens.
4. Click **Filter**. A new blade opens.



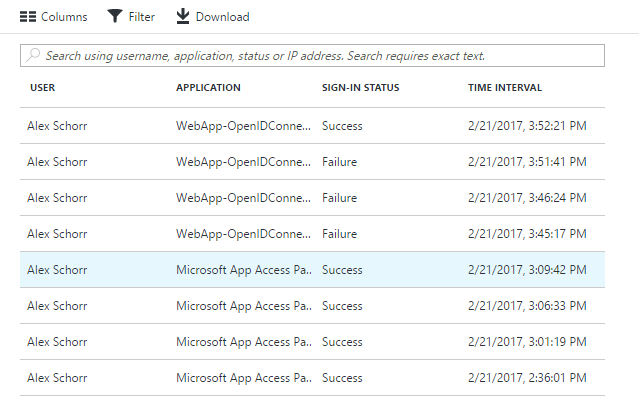
* 1. In **DateTime Interval**, select **24 hours**.
  2. In **Activity**, select **Add user**.
  3. Click **Update**.



1. Click **Download** to export the report as a CSV file.
2. Back in the directory’s blade, now select **Sign-ins** under **ACTIVITY**.



* 1. In **DateTime Interval**, select **24 hours**.
  2. In **User**, type “Alex Schorr”.
  3. Click **Update**.



1. Click **Download** to export the report as a CSV file.

**This concludes the Azure AD B2B collaboration overview.**

# Appendix A. Building a test lab environment

As its title suggests, this section guides you through a set of instructions required to build a representative test lab environment that will be used in the section Getting Started with Azure AD B2B collaboration to configure, test, and evaluate the new capabilities introduced by the Azure AD B2B collaboration feature.

Since we’d like to test a business-to-business collaboration between an inviting organization and a partner organization as well as social identities that will receive the invitations. So, for the corporate part, the suitable test environment is twofold: on one hand, the one for the inviting organization, and on the other hand, the one for business partner organization that will collaborate with the inviting organization.

Two additional social identities will be also created to illustrate the ability to work with any email address.

To simplify the wording as much as possible in the rest of this section, the **inviter** word simultaneously, and depending on the context, will refer to the administrator/organization/directory tenant that is inviting partner users. Conversely, the **invitee** word will be the guest user that receives the invitation and must complete the redeem process whether they are user from a partner organization or individual users that are referenced with their social identities.

The next three sections cover the specifics of both inviter and invitee environments and social identities (Gmail and Microsoft) that will allow to test the scenarios that pertains to Azure AD B2B collaboration from both perspectives.

## Building the test environment for the inviter

### Creating an Azure AD directory

The B2C collaboration feature can be turned on in your existing directories, if you have any. You can thus re-use one of your existing organizational tenants, rather than creating a new directory to try out the Azure AD B2B collaboration features.

An Azure AD directories can be created through an Azure Subscription. This subscription is only needed to access the classic Azure portal at <https://manage.windowsazure.com>.

If you do not already have an Azure account, you can sign up for a [free one-month trial](http://azure.microsoft.com/en-us/pricing/free-trial/)[[57]](#footnote-58).

**Note** If you have an MSDN Subscription, see article [Azure benefit for MSDN subscribers](http://azure.microsoft.com/en-us/pricing/member-offers/msdn-benefits-details/)[[58]](#footnote-59).

**If you don’t have any directory at this time, please follow the instructions in the next section, otherwise skip this section.**

To create a new Azure AD directory, proceed with the following steps:

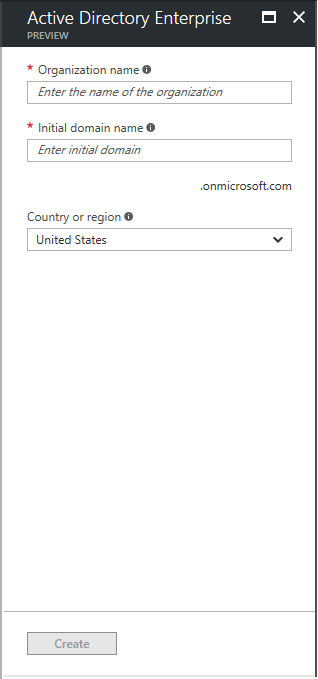
1. Open a browsing session and navigate to the Azure portal at <https://portal.azure.com/>.
2. Sign in to the Azure portal as the Subscription admin user. This is for instance the same Microsoft Account that you used to sign up for Azure as per previous section.
3. Click **New** on the left pane. An eponym blade opens.

**Note** A blade is one piece of the overall view. You can think of a blade as a window.

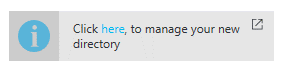
1. Select **Security + Identity**.



1. Select **Azure Active Directory**. An eponym blade opens.

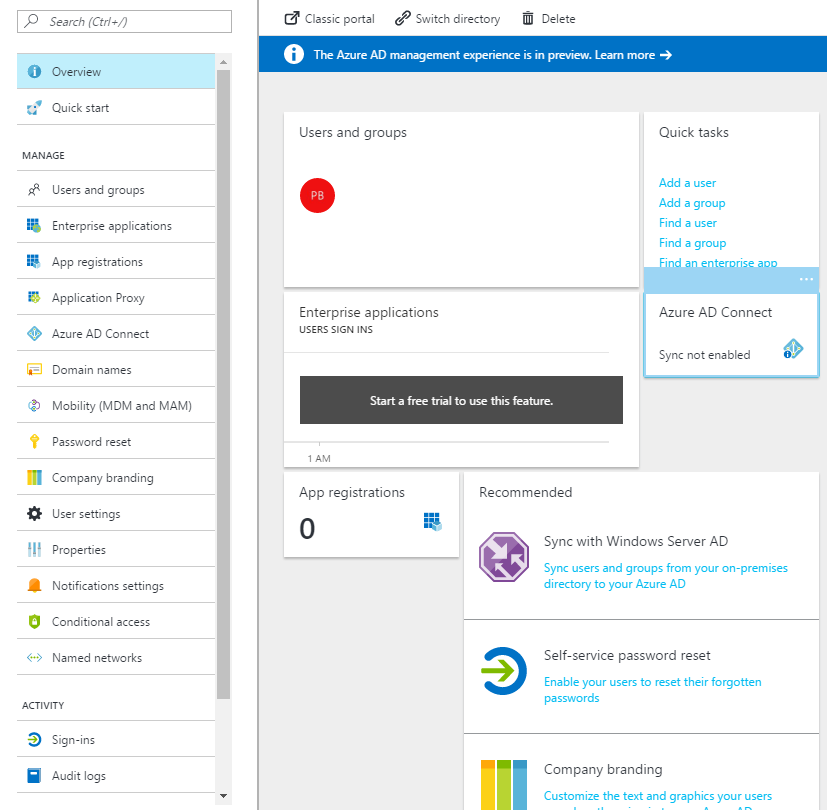


1. Configure the basic properties for your new directory, i.e. its name, default domain name, and the country or region as follows:
   1. In **Organization name**, choose a name for the directory (that will help distinguish it from your other directories in your Azure subscription), for example in our illustration “Contoso 369 Corporation”.
   2. In **initial domain name**, choose a default domain name which you can use to bootstrap usage of this directory, for example “contoso369.onmicrosoft.com”.
   3. In **Country or region**, choose a country or region for your directory. This setting is used by Azure AD to determine the datacenter region(s) for your directory. It cannot be changed later.
2. Click **Create**.



1. Once the creation of the directory completes, click the link in the added tile in the blade to start managing the newly created directory. You’re redirected to:

<https://portal.azure.com/contoso369.onmicrosoft.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>



Your user account is included in that new directory, and you're assigned to the global administrator role. (Other administrators can be added later as required.)

This enables you to manage the directory you created without signing in as a different user of that directory.

**For the course of this walkthrough, we’ve created the *contoso369.onmicrosoft.com* B2C directory.** **You will have to choose in lieu of a B2C directory name of your choice whose name is currently not in used.**

**Whenever a reference to *contoso369.onmicrosoft.com* is made in a procedure, it has to be replaced by the B2C directory name of your choice to reflect accordingly the change in naming.**

### Creating a Business Partners group

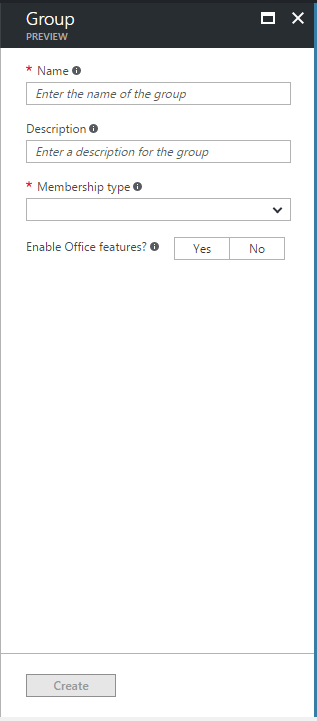
A group is a collection of users and groups that can be managed as a single unit. Users and groups that belong to a particular group are referred to as group members.

As with Active Directory on-premises, using groups in Azure AD can simplify administration by assigning a common set of permissions and rights to many accounts at once, rather than assigning permissions and rights to each account individually. (Groups can be created directly on Azure AD – as illustrated here - or originated from the on-premises AD that is synced to Azure AD.)

**Note** For more information, see the article [Managing access to resources with Azure Active Directory groups](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups)[[59]](#footnote-60).

To create a Business Partners group, proceed with the following steps:

1. While still in the directory blade in the Azure portal, click **Add a group** under **Quick tasks**. A **Group** blade opens.



1. In **Name**, type "Business Partners".
2. In **Membership** **type**, select **Assigned**.
3. Select **No** next to **Enable Office feature**.
4. Click **Create**. A notification tile should indicate the successful creation of the group.

### Installing Azure AD PowerShell V2

The Azure AD PowerShell V2 module provides a set of cmdlets specifically designed for Azure AD tenant-based administration. So, thanks to a PowerShell interface, you can administer your Azure AD tenant using Windows PowerShell and you can complete common configuration tasks and manage your organization data.

**Note** For more information, see article [Azure Active Directory V2 PowerShell module](https://docs.microsoft.com/en-us/powershell/azuread/v2/azureactivedirectory)[[60]](#footnote-61). Each Azure AD cmdlet has required and optional arguments, called parameters, that identify which objects to act on or control how the cmdlet performs its task. For more information about an Azure AD cmdlet, at the Windows PowerShell command prompt, type “Get-help” and the name of the cmdlet.

**Important note**TheActive Directory V2 PowerShell module currently in public preview (e.g. version 2.0.0.110 as of this writing) progressively replaces the [Azure AD PowerShell V1](http://connect.microsoft.com/site1164/Downloads/DownloadDetails.aspx?DownloadID=59185)[[61]](#footnote-62) module (e.g. version 1.1.166.0 as of this writing). For more information, see blog post [In case you missed it: #AzureAD PowerShell v2.0 is now in public preview!](https://blogs.technet.microsoft.com/enterprisemobility/2016/10/13/in-case-you-missed-it-azuread-powershell-v2-0-is-now-in-public-preview/)[[62]](#footnote-63) and eponym article [Azure Active Directory V2 PowerShell module](https://docs.microsoft.com/en-us/powershell/azuread/v2/azureactivedirectory)[[63]](#footnote-64).

The preferred way to install Azure AD PowerShell V2 is to use PowerShell Gallery. You can get it from here: <https://www.powershellgallery.com/packages/AzureADPreview>

**Note** Installing items from the PowerShell Gallery requires the latest version of the PowerShellGet module, which is available in Windows 10, in Windows Management Framework (WMF) 5.0, or in the MSI-based installer (for PowerShell 3 and 4). If the PowerShellGet module is not already available in your current configuration, it is available at <https://www.powershellgallery.com>. For more information, see <https://msdn.microsoft.com/powershell/gallery/readme>.

Administrative privileges are needed on the local computer in order to install this module.

To install the latest Azure AD PowerShell V2 module from the PowerShell Gallery, proceed with the following steps:

1. Open an elevated Windows PowerShell or PowerShell Integrated Scripting Environment (ISE) prompt.
2. Run the following command to install Azure AD PowerShell V2:

PS C:\> Install-Module -Name AzureADPreview

1. When prompted, press Y to confirm the installation.

### Configuring a sample “LOB” application

Since the purpose of the end-to-end walkthrough consists in granting an access to a web app for invited and authorized external user, we consequently need an app.

As stated before, Azure AD B2B collaboration includes access to popular SaaS applications such as Salesforce, Dropbox, Workday, and of course, Office 365 – and all of this is in addition to mobile, cloud, and on-premises claims-aware applications.

**Note** For more information, see article [Configure SaaS apps for B2B collaboration](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-configure-saas-apps)[[64]](#footnote-65).

For the sake of the walkthrough, we are going to use on a local machine a sample claims-aware application. The following sections will guide you on how to add, configure, and run a sample application on your favorite platform and IDE.

If you don’t have an IDE to configure, build, and run the sample, you can refer to the next section for instructions to install Visual Studio Community 2015 is a free, fully-featured, and extensible IDE for creating modern applications for Windows, Android, and iOS, as well as web applications and APIs, and cloud services.

Otherwise, you can skip this section.

#### Installing Visual Studio Community 2015

To install Visual Studio Community 2015, proceed with the following steps:

1. Open a browsing session and navigate to <https://www.visualstudio.com/vs/community/>.
2. Click **Download Community 2015**.
3. Click **Save** to download the setup file (vs\_community\_EN\_\_1511326103.1482352600.exe file).
4. Click **Run**, and follow the instructions to setup the environment.

#### Getting a sample application from the GitHub

Microsoft provides a full suite of sample applications and documentation on GitHub at <https://github.com/azure-samples?query=active-directory> to help you get started with learning Azure AD. This includes tutorials for native clients such as Windows, Windows Phone, iOS, OSX, Android, and Linux.

The page <https://azure.microsoft.com/en-us/resources/samples/?service=active-directory> links you to these code samples that show you how it's done and code snippets that you can use in your applications. On the code sample page on GitHub, you'll find detailed read-me topics that help with requirements, installation and set-up. And the code is commented to help you understand the critical sections.

**Note** To understand the basic scenario for each sample type, see article [Authentication Scenarios for Azure AD](https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios)[[65]](#footnote-66).

For the purpose of this walkthrough, we are going to use the active-directory-dotnet-webapp-openidconnect quick start sample that demonstrate how to write a web application the directs the user’s browser to sign them in to Azure AD.

As the name of the sample application suggest, this sample shows how to build a .Net MVC web application that uses the OpenID Connect standard protocol to sign-in users an Azure AD tenant.

The code for this sample application is maintained on GitHub: [active-directory-dotnet-webapp-openidconnect](https://github.com/Azure-Samples/active-directory-dotnet-webapp-openidconnect)*[[66]](#footnote-67)*.

However, for the sake of brevity, we will use an almost completed version for this sample application.

To get this almost completed sample application, proceed with the following steps:

1. Download the [active-directory-dotnet-webapp-openidconnect-complete.zip](https://github.com/Azure-Samples/active-directory-dotnet-webapp-openidconnect/archive/master.zip)[[67]](#footnote-68) file from GitHub and save it to your computer if you haven’t done so already.
2. Click **Save** and save it on your computer.
3. Extract the active-directory-dotnet-webapp-openidconnect-complete.zipfile.

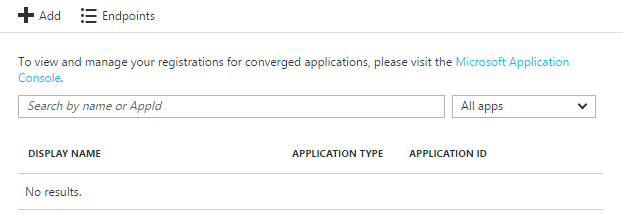
#### Adding the sample application in the Azure AD directory

To add the sample application in the Azure AD directory, proceed with the following steps:

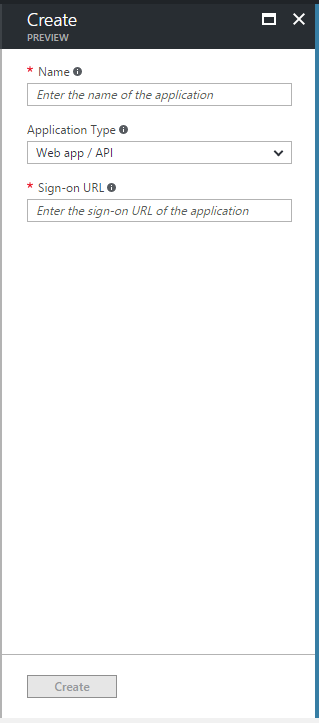
1. Open a browsing session and navigate to:

<https://portal.azure.com/contoso369.onmicrosoft.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>

1. Sign into the Azure portal as the administrator of the directory to configure.
2. Under **Manage**, select **App registrations**.



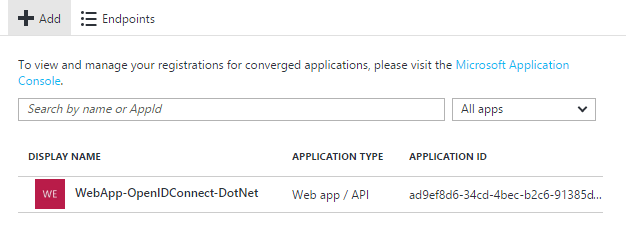
1. Click **+ Add**. A **Create** blade opens.



1. In **Name**, specify a name for the web application, for example “WebApp-OpenIDConnect-DotNet” to reflect the name of this sample’s project. This used as human-readable moniker to refer to the application.
2. In **Application type**, leave **Web app / API** selected.
3. In **Sign-on URL**, enter the base URL for the sample, which is by default “https://localhost:44320/”.
4. Click **Create**. A floating notification tile should indicate that the application has been successfully created.



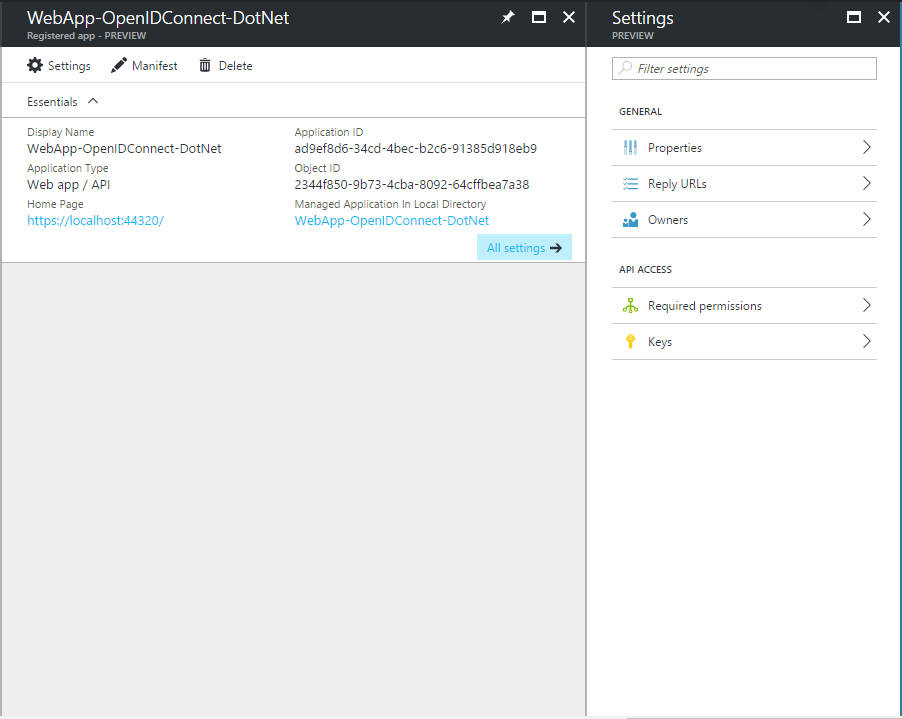
1. After a successful creation of the app, the app is now listed.



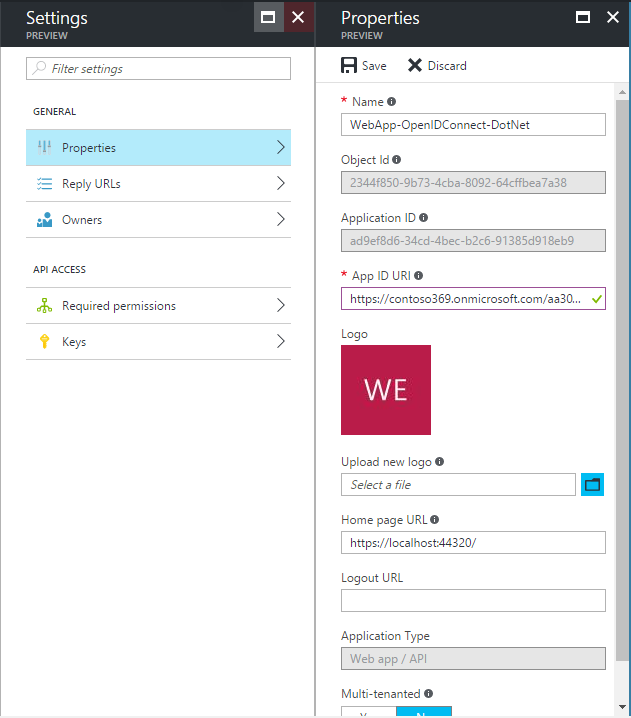
All done! Before moving on to the next step, you need to find the Client ID of your sample application.

To get the Client ID of your sample application, proceed with the following steps:

1. While still in the previous blade, click the newly created app. A related blade opens.



1. Under **GENRAL**, click **Properties**.



1. Copy the **Application ID** value to the clipboard: ad9ef8d6-34cd-4bec-b2c6-91385d918eb9. Note this value.

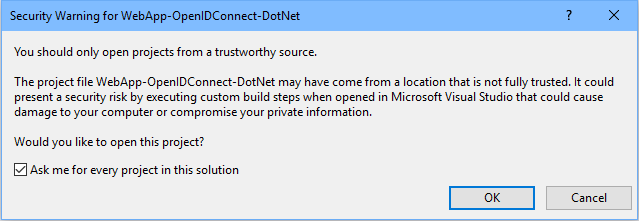
#### Updating the sample application

We will now configure the sample to use the contoso369.onmicrosoft.com directory tenant where it has been registered.

The OpenID Connect OWIN middleware (Microsoft.Owin.Security.OpenIdConnect) enables the sample application to seamlessly use OpenID Connect for authentication. This middleware is available as [NuGet package](http://www.nuget.org/packages/Microsoft.Owin.Security.WsFederation/)[[68]](#footnote-69) for the Visual Studio development environment.

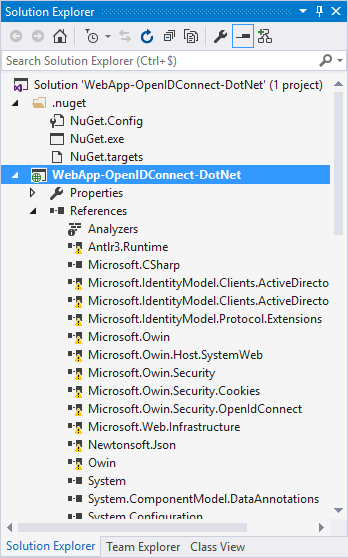
To configure the sample application, proceed with the following steps:

1. Open the solution in Visual Studio Community 2015.
   1. Click **File** | **Open** | **Project/Solution**
   2. Navigate to the extracted complete.zip file
   3. Open the WebApp-OpenIDConnect-DotNet.sln solution file. A **Security Warning** dialog may open up.

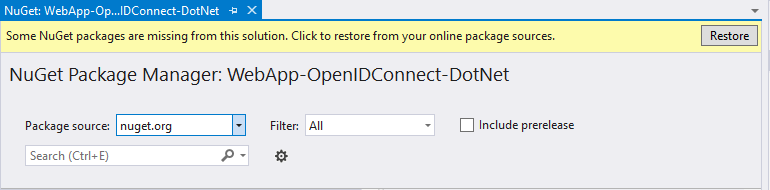


* 1. In this eventuality, uncheck **Ask me for every project** in the solution and click **OK**.

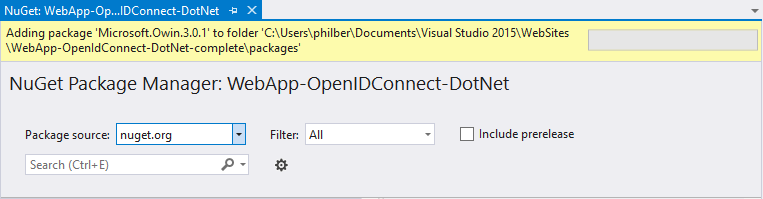
1. Open the **Solution Explorer** if it’s not already the case.



1. The **References** section of the WebApp-OpenIDConnect-DotNet shows a series of unresolved references with an exclamation mark.
2. Under **WebApp-OpenIDConnect-DotNet**, right-click **References**, and then select **Manage NuGet Packages...** to (try to) resolve them. A **NuGet** window opens and is docked as a tabbed document.



1. Click **Restore**. The missing NuGet packages are then downloaded to resolve the above unresolved references.



1. Back to the **Solution Explorer** window, select **WebApp-OpenIDConnect-DotNet**.
2. Open the web.config file in the root folder of the project.

<?xml version="1.0" encoding="utf-8"?>

<!--

For more information on how to configure your ASP.NET application, please visit

http://go.microsoft.com/fwlink/?LinkId=301880

-->

<configuration>

<appSettings>

<add key="webpages:Version" value="3.0.0.0" />

<add key="webpages:Enabled" value="false" />

<add key="ClientValidationEnabled" value="true" />

<add key="UnobtrusiveJavaScriptEnabled" value="true" />

<add key="ida:ClientId" value="[Enter client ID as obtained from Azure Portal,

e.g. 82692da5-a86f-44c9-9d53-2f88d52b478b]" />

<add key="ida:Tenant" value="[Enter tenant name, e.g. contoso.onmicrosoft.com]" />

<add key="ida:AADInstance" value="https://login.microsoftonline.com/{0}" />

<add key="ida:PostLogoutRedirectUri" value="https://localhost:44320/" />

</appSettings>

…

</configuration>

1. In web.config, Find the app key ‘ida:ClientId’ and replace the value with the **Application ID** value you copied from the Azure portal: “ad9ef8d6-34cd-4bec-b2c6-91385d918eb9”.
2. Find ‘ida:Tenant’ and replace the value with your directory tenant name, for example in our configuration “contoso369.onmicrosoft.com”.
3. If you changed the base URL of the sample, find the app key ‘ida:PostLogoutRedirectUri’ and replace the value with the new base URL of the sample. Otherwise, leave it unchanged.

<?xml version="1.0" encoding="utf-8"?>

<!--

For more information on how to configure your ASP.NET application, please visit

http://go.microsoft.com/fwlink/?LinkId=301880

-->

<configuration>

<appSettings>

<add key="webpages:Version" value="3.0.0.0" />

<add key="webpages:Enabled" value="false" />

<add key="ClientValidationEnabled" value="true" />

<add key="UnobtrusiveJavaScriptEnabled" value="true" />

<add key="ida:ClientId" value="ad9ef8d6-34cd-4bec-b2c6-91385d918eb9" />

<add key="ida:Tenant" value="contoso369.onmicrosoft.com" />

<add key="ida:AADInstance" value="https://login.microsoftonline.com/{0}" />

<add key="ida:PostLogoutRedirectUri" value="https://localhost:44320/" />

</appSettings>

…

</configuration>

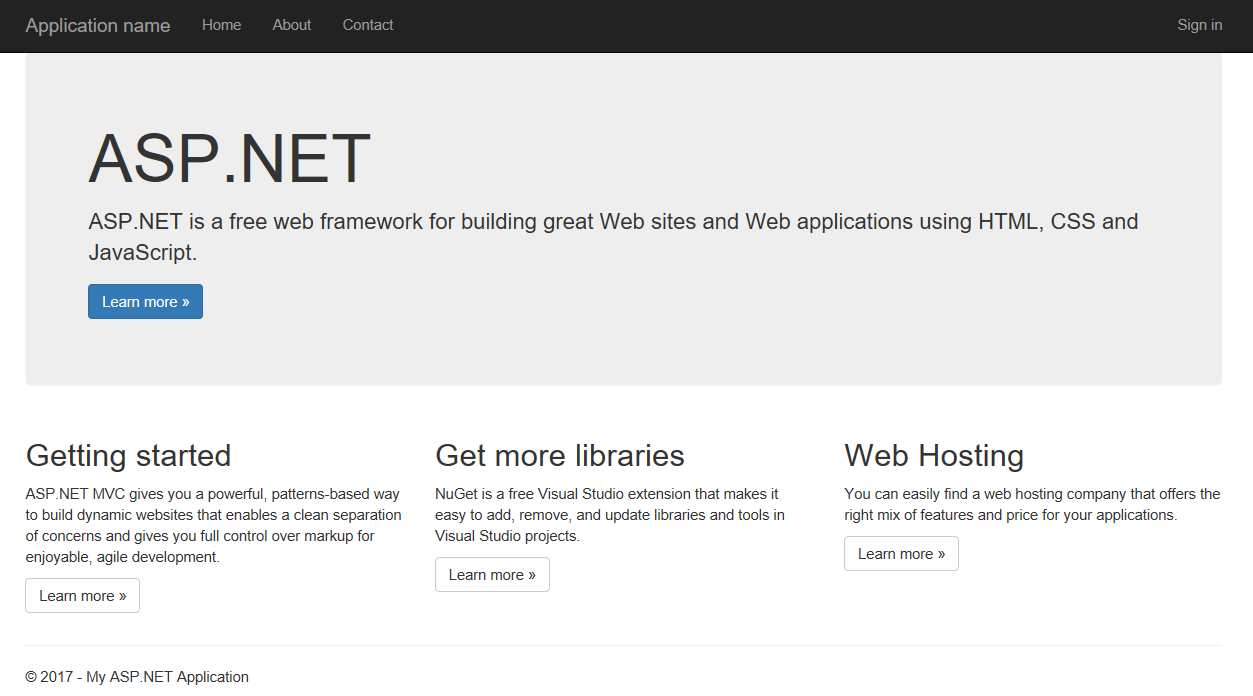
1. Save the file. Click **FILE** | **Save All**.

#### Running the sample application

You are almost done using the sample application with Azure AD B2B collaboration.

To run the sample application, proceed with the following steps:

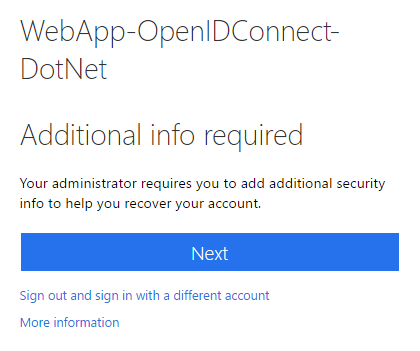
1. Clean the Visual Studio solution. Click **BUILD** | **Clean Solution**.
2. Rebuild the Visual Studio solution. Click **BUILD** | **Rebuild Solution**.
3. Run the sample application. Press F5 to run the solution.



1. Click **Sign in** in the upper right corner. You should be redirected to Azure AD to sign in.

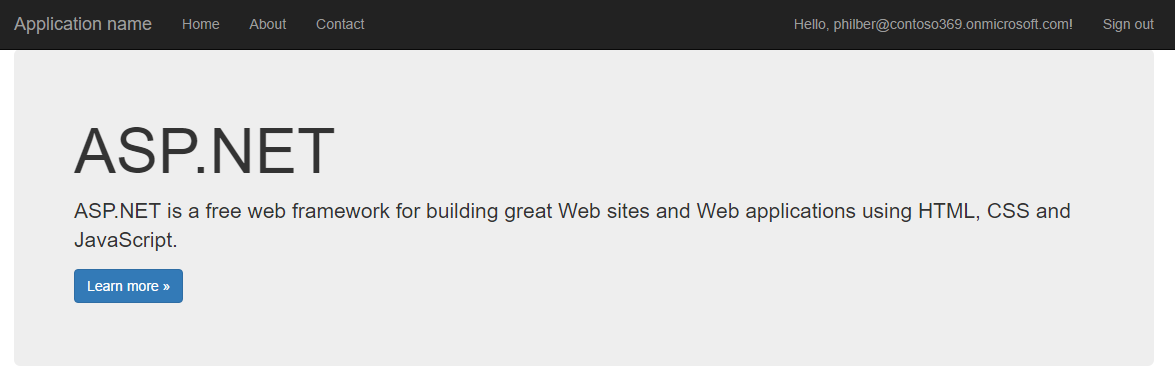
### 

1. Sign in as the Subscription admin user. This is for instance an admin user that you’ve created later.
2. Enter your credentials and click **Sign in**.
   1. Depending on the configuration of your directory, you may be asked to specify additional information so that you can later recover your account if needed.



* 1. If prompted, click **Next**, and then provide the configurated additional information.

1. Et voila!



#### Finalizing the configuration of the sample application (Optional)

To finalize the configuration of your sample application, proceed with the following steps:

1. Open a browsing session and navigate to:

<https://portal.azure.com/contoso369.onmicrosoft.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Overview>

1. Sign into the Azure portal as the administrator of the directory to configure.
2. Under **Manage**, select **App registrations**.
3. Click **WebApp-OpenIDConnect-DotNet**.
4. Under **GENRAL**, click **Properties**.
5. Upload a logo for the application. In **Upload new logo**, point the logo file that meets the displayed requirements.



1. Click **Save**.

The sample application is ready to be used by external user thanks to Azure AD B2B collaboration. For the moment, the configuration required for your organization to invite external users is completed.

Let’s deal with the second part of the test environment.

## Building the test environment for the Litware369 invitees

As mentioned earlier, for business partners with valid business email addresses who don't already have Azure AD, Azure B2B collaboration provides a streamlined self-service sign-up experience to provide Azure AD accounts to these guest users. An unmanaged tenant will be created for that purpose.

**Important note** For information on unmanaged tenants and how they can be brought under admin control, see the article [What is Self-Service Signup for Azure?](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-self-service-signup)[[69]](#footnote-70).

This experience isn’t illustrated in this walkthrough since it requires the invitees to have a valid business email address to be in a position to receive email invitations.

Having such an address imposes the setup an entire mail environment with suitable records in a public DNS registrar, etc.

If you have such an email address, you can ignore the rest of this section and use it to receive an invitation.

**For the sake of brevity, this walkthrough rather supposes that you have an Office 365 subscription in place. If you don’t have any subscription, the next section provides you with instructions to provisioning one for the walkthrough.**

### Provisioning an Office 365 subscription

To sign up to a free 30-day Microsoft Office 365 Enterprise E3 trial, follow the instructions at <https://go.microsoft.com/fwlink/p/?LinkID=403802&culture=en-US&country=US>.

**For the course of this walkthrough, we’ve provisioned an Office 365 Enterprise (E3) tenant: *litware369.onmicrosoft.com*.** **You will have to choose in lieu of it a directory tenant name of your choice whose name is currently not in use.**

**Whenever a reference to *litware369.onmicrosoft.com* is made in a procedure, it has been replaced by the directory tenant name of your choice to reflect accordingly the change in naming.**

### Creating mailbox enabled test users

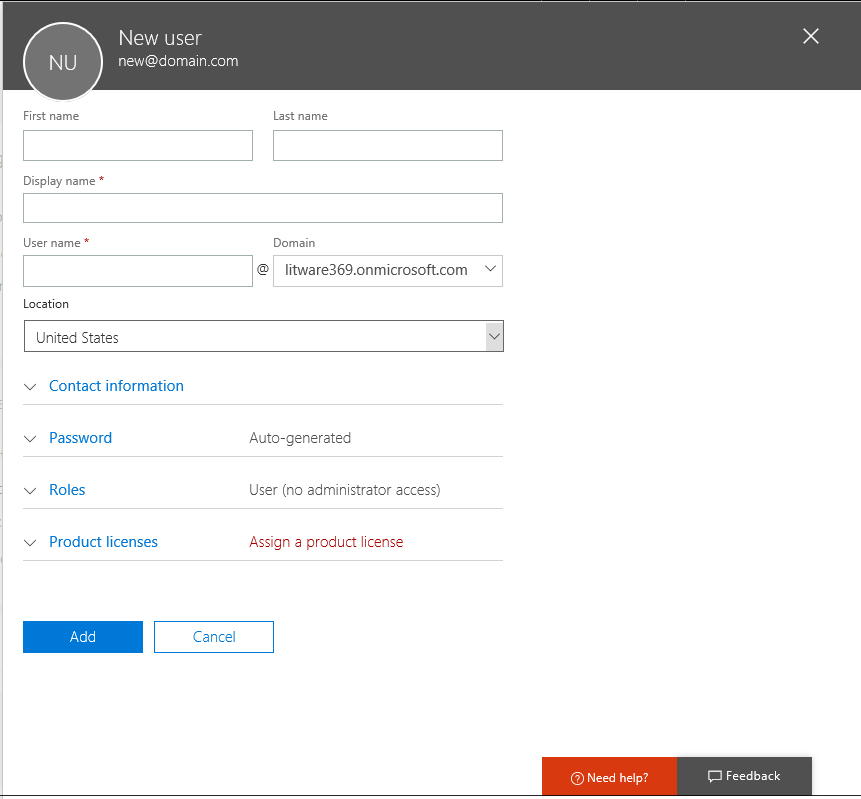
For the purpose of the walkthrough, you will need to create one mailbox enabled test user: Phil Berstein (philber@litware369.onmicrosoft.com),

Since only one user is to be created, you will create the user manually from the Office 365 admin center.

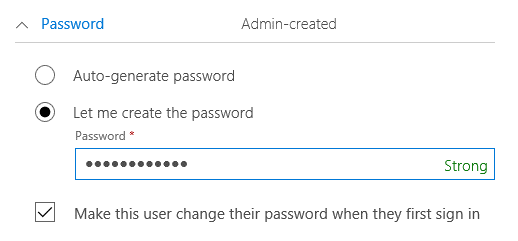
**Note** If you have a lot of users and don’t want to create them one a time, you can create a list of users in a comma-separated values (CSV) file and import them. It takes a little time to make the file, but then you can create all the users in Office 365 at once. For more information, see article [Add several users at the same time to Office 365 - Admin Help](https://support.office.com/en-us/article/Add-several-users-at-the-same-time-to-Office-365-Admin-Help-1f5767ed-e717-4f24-969c-6ea9d412ca88)[[70]](#footnote-71).

To manually create the test user, proceed with the following steps:

1. Open a browsing session and navigate to the Office 365 admin center portal at <https://portal.office.com/adminportal/home>.
2. In the **Users** tile, click **Add a user.** A **New user** pane opens.

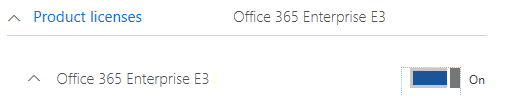


1. Enter a display name and a user name for Phil Berstein:
   1. In **First name**, type “Phil”.
   2. In **Last name**, type “Berstein”. Display name is then automatically completed.
   3. In **User name**, type “PhilBer”.
2. By default, Office 365 auto-generates a new temporary password for the person. However, if you want to create a different initial password for the person, select **Let me create the password** and then type a strong password twice that meets the guidelines, for example for this walkthrough “pass@word1!?”.

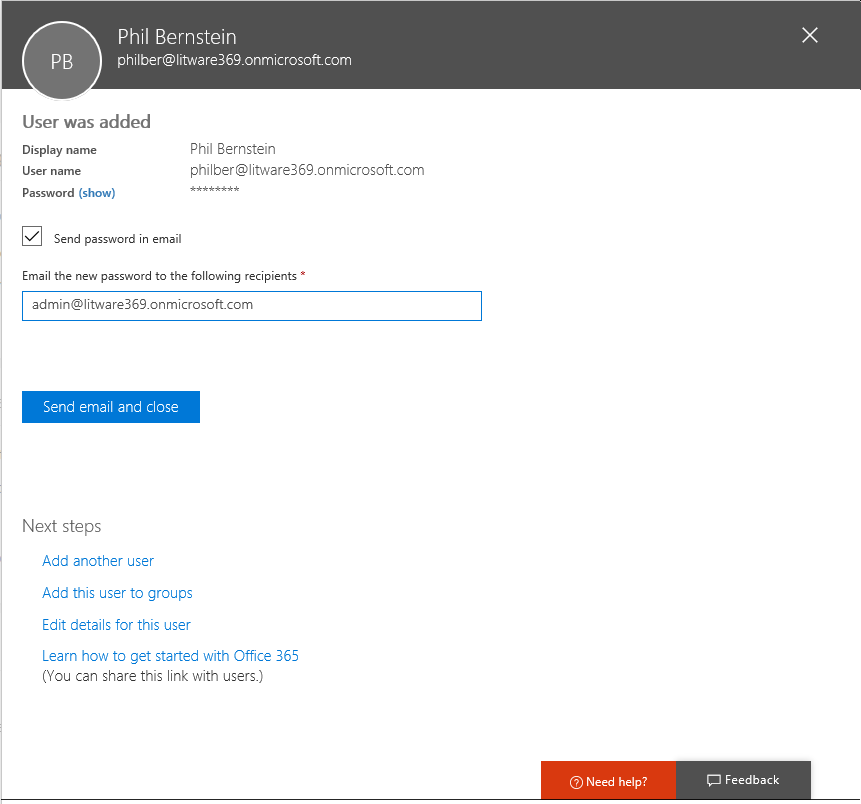


If you want the person to change the password when they first sign on to Office 365, leave **Make this user change their password when they first sign in** checked. When the person signs into <https://portal.office.com> for the first time, they will be prompted to change their password. Conversely, if you uncheck this option, the initial password is always temporary, meaning that the user will need to change it within 90 days.

1. Under **Product licenses**, assign the user an Office 365 Enterprise E3 license.



1. Click **Add** to create the user account.



1. At this point, an email from the Microsoft Invitations is sent to the email addresses you specified. Click **Close**.

**Note** For more information, see the article [Add users individually to Office 365 - Admin Help](https://support.office.com/en-us/article/Add-users-individually-to-Office-365-Admin-Help-1970f7d6-03b5-442f-b385-5880b9c256ec)[[71]](#footnote-72).

This completes the setup and the configuration of the test lab environment for the business partner organization Litware369.

Let’s now create social identities for some of the invitees to later illustrate the ability to use any email address.

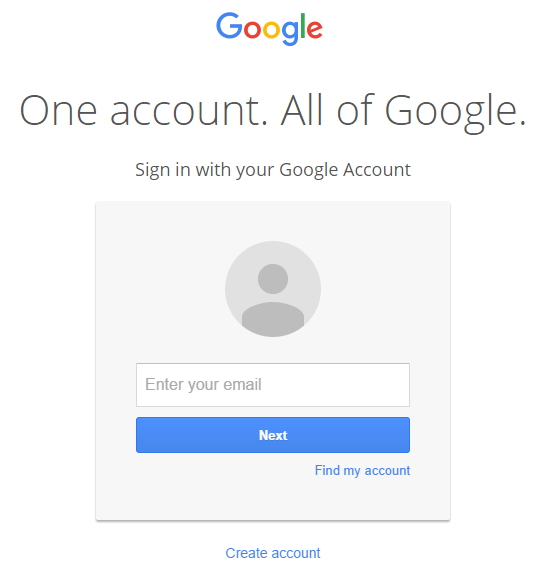
## Setting up the test environment for the social ID invitees

To complete our test lab environment, we will now create two social ID accounts, i.e. a Gmail account, and a Microsoft Account (MSA) one.

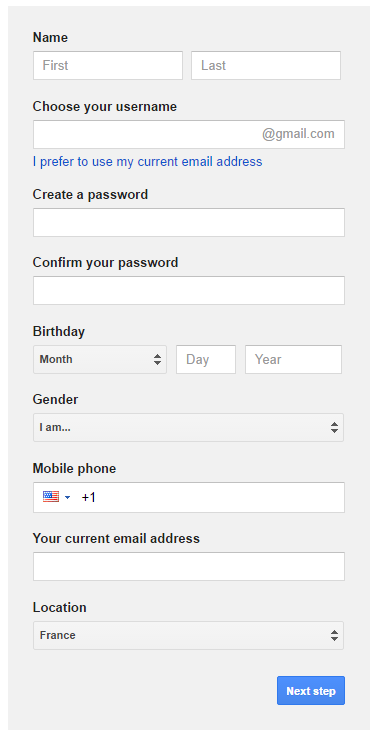
### Creating a Gmail account

To create a Gmail account, proceed with the following steps:

1. Open a browsing session and navigate to <https://accounts.google.com>.



1. Click **Create account**.

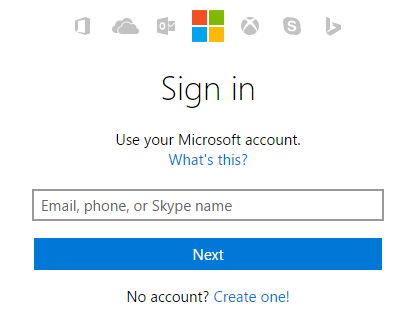


1. Fill in the form for Robert Hatley (contoso369b2binvitee@gmail.com).
2. Click **Next step** and follow the remaining steps of the wizard to complete the creation of the account.

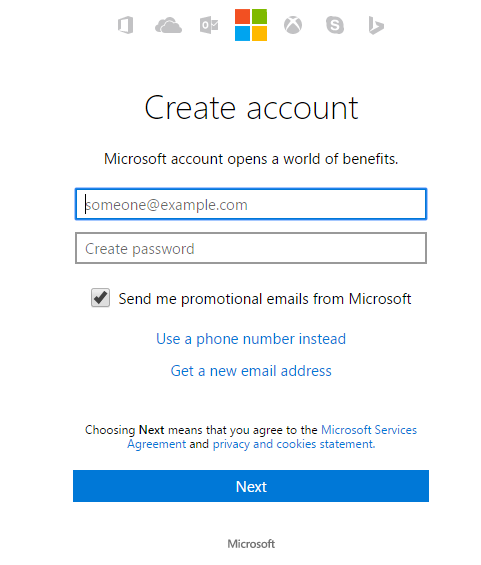
### Creating a Microsoft account

To create a Microsoft account, proceed with the following steps:

1. From the previous session, now navigate to <http://account.microsoft.com>., and then click **Sign in** in the upper right corner.



1. Click **Create one!**.



1. Type “contoso369b2binvitee@outlook.com" for the email address and specify “pass@word1!?” for the password.
2. Click **Next**, and then click **Your info** in the **Account** menu bar.
3. Complete the user’s profile for Alex Schorr.

**This completes the setup and the configuration of the test lab environment illustrate to B2B collaboration features.**

|  |
| --- |
| The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.  This white paper is for informational purposes only. Microsoft makes no warranties, express or implied, in this document.  Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.  Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.  © 2017 Microsoft Corporation. All rights reserved.  The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.  Microsoft, list Microsoft trademarks used in your white paper alphabetically are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.  The names of actual companies and products mentioned herein may be the trademarks of their respective owners. |

1. Microsoft Azure is a flexible and open cloud computing platform hosted in Microsoft datacenters delivering scalable and reliable Internet-scale services. As an Infrastructure as-a-Service (IaaS) platform, Microsoft Azure Infrastructure Services enables to deploy (complex) workloads (servers, networking and storage infrastructure) in the cloud that you can control and manage on your terms. Also, as a Platform as-a-Service (PaaS) platform, it includes a number of features, which can be used individually or composed together in a public or hybrid cloud fashion. [↑](#footnote-ref-2)
2. A “tenant” is directory operated by an organization [↑](#footnote-ref-3)
3. Modern business applications: https://www.microsoft.com/en-us/cloud-platform/mobile-application-development [↑](#footnote-ref-4)
4. Microsoft recognized in Leader Quadrant of Gartner’s Magic Quadrant for Identity and Access Management as a Service, Worldwide: https://info.microsoft.com/EMS-IDaaS-MQ-2016.html [↑](#footnote-ref-5)
5. #AzureAD a leader in the 2016 Gartner IDaaS MQ!: https://blogs.technet.microsoft.com/enterprisemobility/2016/06/07/azuread-a-leader-in-the-2016-gartner-idaas-mq/ [↑](#footnote-ref-6)
6. Ibid [↑](#footnote-ref-7)
7. Azure AD B2B Collaboration is Generally Available!: https://blogs.technet.microsoft.com/enterprisemobility/2017/04/12/azure-ad-b2b-collaboration-is-generally-available/ [↑](#footnote-ref-8)
8. Extend cloud identity and access management to your customer and partner relationships: https://blogs.technet.microsoft.com/enterprisemobility/2017/04/12/extend-cloud-identity-and-access-management-to-your-customer-and-partner-relationships-2/ [↑](#footnote-ref-9)
9. Microsoft Enterprise Mobility + Security: https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security [↑](#footnote-ref-10)
10. Azure Active Directory editions: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-editions [↑](#footnote-ref-11)
11. Azure Active Directory Pricing: http://azure.microsoft.com/en-us/pricing/details/active-directory/ [↑](#footnote-ref-12)
12. Azure subscription and service limits, quotas, and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#active-directory-limits [↑](#footnote-ref-13)
13. Introducing Enterprise Mobility + Security: https://blogs.technet.microsoft.com/enterprisemobility/2016/07/07/introducing-enterprise-mobility-security/ [↑](#footnote-ref-14)
14. Microsoft Enterprise Agreement: http://www.microsoft.com/en-us/Licensing/licensing-programs/enterprise.aspx [↑](#footnote-ref-15)
15. Microsoft Cloud Solution Provider program: https://partner.microsoft.com/en-us/cloud-solution-provider [↑](#footnote-ref-16)
16. Microsoft Open Programs: https://www.microsoft.com/en-us/licensing/licensing-programs/open-license.aspx [↑](#footnote-ref-17)
17. Azure AD and Enterprise Mobility Suite now available without an Enterprise Agreement: http://blogs.technet.com/b/ad/archive/2015/03/12/azure-ad-and-enterprise-mobility-suite-now-broadly-available-outside-of-an-enterprise-agreement.aspx [↑](#footnote-ref-18)
18. Azure Active Directory B2B collaboration frequently-asked questions (FAQ): https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-faq [↑](#footnote-ref-19)
19. Azure Active Directory B2B collaboration current limitations: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-current-limitations [↑](#footnote-ref-20)
20. Getting started with Azure AD: http://msdn.microsoft.com/en-us/library/dn655157.aspx [↑](#footnote-ref-21)
21. Active Directory from the on-premises to the cloud: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-22)
22. An overview of Azure AD: http://www.microsoft.com/en-us/download/details.aspx?id=36391 [↑](#footnote-ref-23)
23. Azure Active Directory community forum: http://social.msdn.microsoft.com/Forums/en-US/WindowsAzureAD/ [↑](#footnote-ref-24)
24. Enterprise Mobility + Security Team blog: https://blogs.technet.microsoft.com/enterprisemobility/?product=azure-active-directory [↑](#footnote-ref-25)
25. What is Self-Service Signup for Azure?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-self-service-signup [↑](#footnote-ref-26)
26. Azure AD Connect: https://www.microsoft.com/en-us/download/details.aspx?id=47594 [↑](#footnote-ref-27)
27. An overview of Azure AD B2C: https://aka.ms/aadpapers [↑](#footnote-ref-28)
28. Compare B2B collaboration and B2C in Azure Active Directory: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-compare-b2c [↑](#footnote-ref-29)
29. Azure Active Directory B2B collaboration licensing guidance: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-licensing [↑](#footnote-ref-30)
30. Azure Active Directory Premium free for one month: https://azure.microsoft.com/en-us/trial/get-started-active-directory/ [↑](#footnote-ref-31)
31. Getting started with Azure Active Directory Premium: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-get-started-premium [↑](#footnote-ref-32)
32. How do Azure Active Directory admins add B2B collaboration users?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-admin-add-users [↑](#footnote-ref-33)
33. Managing access to resources with Azure Active Directory groups: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups [↑](#footnote-ref-34)
34. Azure Active Directory B2B collaboration code and PowerShell samples: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-code-samples [↑](#footnote-ref-35)
35. Adding an Azure Active Directory B2B collaboration user to a role: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-add-guest-to-role [↑](#footnote-ref-36)
36. Add B2B collaboration users without an invitation: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-add-user-without-invite [↑](#footnote-ref-37)
37. Add company branding to your Sign In and Access Panel pages: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-add-company-branding [↑](#footnote-ref-38)
38. Improving the branding logic of Azure AD login pages: https://blogs.technet.microsoft.com/enterprisemobility/2017/04/07/improving-the-branding-logic-of-azure-ad-login-pages/ [↑](#footnote-ref-39)
39. Ibid [↑](#footnote-ref-40)
40. Azure Active Directory B2B collaboration invitation redemption: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-redemption-experience [↑](#footnote-ref-41)
41. The elements of the B2B collaboration invitation email: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email [↑](#footnote-ref-42)
42. Fiddler: http://www.telerik.com/fiddler [↑](#footnote-ref-43)
43. JWT Decoder: http://calebb.net/ [↑](#footnote-ref-44)
44. JWT.io: https://jwt.io/ [↑](#footnote-ref-45)
45. My Apps for Android: https://play.google.com/store/apps/details?id=com.microsoft.myapps [↑](#footnote-ref-46)
46. Apple App Store: https://itunes.apple.com/us/app/my-apps-windows-azure-active/id824048653?mt=8 [↑](#footnote-ref-47)
47. Azure Active Directory B2B collaboration invitation redemption: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-redemption-experience [↑](#footnote-ref-48)
48. The elements of the B2B collaboration invitation email: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email [↑](#footnote-ref-49)
49. The elements of the B2B collaboration invitation email: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-invitation-email [↑](#footnote-ref-50)
50. How do information workers add B2B collaboration users to Azure Active Directory?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-iw-add-users [↑](#footnote-ref-51)
51. Delegate invitations for Azure Active Directory B2B collaboration: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations [↑](#footnote-ref-52)
52. Multi-factor authentication for Azure Active Directory B2B collaboration users: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-mfa-instructions [↑](#footnote-ref-53)
53. Azure Active Directory B2B collaboration code and PowerShell samples: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-code-samples [↑](#footnote-ref-54)
54. Azure Active Directory B2B collaboration API and customization: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-api [↑](#footnote-ref-55)
55. Properties of an Azure Active Directory B2B collaboration user: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-user-properties [↑](#footnote-ref-56)
56. Dynamic groups and Azure Active Directory B2B collaboration: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-dynamic-groups [↑](#footnote-ref-57)
57. Create your free Azure account today: https://azure.microsoft.com/en-us/free/ [↑](#footnote-ref-58)
58. Monthly Azure credit for Visual Studio subscribers: https://azure.microsoft.com/en-us/pricing/member-offers/msdn-benefits-details/ [↑](#footnote-ref-59)
59. Managing access to resources with Azure Active Directory groups: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-manage-groups [↑](#footnote-ref-60)
60. Azure Active Directory V2 PowerShell module: https://docs.microsoft.com/en-us/powershell/azuread/v2/azureactivedirectory [↑](#footnote-ref-61)
61. Azure AD PowerShell V1: http://connect.microsoft.com/site1164/Downloads/DownloadDetails.aspx?DownloadID=59185 [↑](#footnote-ref-62)
62. In case you missed it: #AzureAD PowerShell v2.0 is now in public preview!: https://blogs.technet.microsoft.com/enterprisemobility/2016/10/13/in-case-you-missed-it-azuread-powershell-v2-0-is-now-in-public-preview/ [↑](#footnote-ref-63)
63. Azure Active Directory V2 PowerShell module: https://docs.microsoft.com/en-us/powershell/azuread/v2/azureactivedirectory [↑](#footnote-ref-64)
64. Configure SaaS apps for B2B collaboration: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-configure-saas-apps [↑](#footnote-ref-65)
65. Authentication Scenarios for Azure AD: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-authentication-scenarios [↑](#footnote-ref-66)
66. active-directory-dotnet-webapp-openidconnect project: https://github.com/Azure-Samples/active-directory-dotnet-webapp-openidconnect [↑](#footnote-ref-67)
67. WebApp-OpenIdConnect-DotNet-completed.zip file: https://github.com/AzureADQuickStarts/WebApp-OpenIdConnect-DotNet/archive/complete.zip [↑](#footnote-ref-68)
68. Microsoft.Owin.Security.OpenIdConnect 3.0.1 NuGet package: h http://www.nuget.org/packages/Microsoft.Owin.Security.OpenIDConnect/ [↑](#footnote-ref-69)
69. What is Self-Service Signup for Azure?: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-self-service-signup [↑](#footnote-ref-70)
70. Add several users at the same time to Office 365 - Admin Help: https://support.office.com/en-us/article/Add-several-users-at-the-same-time-to-Office-365-Admin-Help-1f5767ed-e717-4f24-969c-6ea9d412ca88 [↑](#footnote-ref-71)
71. Add users individually to Office 365 - Admin Help: https://support.office.com/en-us/article/Add-users-individually-to-Office-365-Admin-Help-1970f7d6-03b5-442f-b385-5880b9c256ec [↑](#footnote-ref-72)