PPR Documentation

Contents

[What is Azure AD B2B Collaboration? 5](#_Toc473280719)

[How does it work? 5](#_Toc473280720)

[Public Preview Features 9](#_Toc473280721)

[These are the key features in B2B PPR: 9](#_Toc473280722)

[Admins adding B2B users 9](#_Toc473280723)

[Admins adding B2B users to the directory 10](#_Toc473280724)

[Admins adding B2B users to a group 10](#_Toc473280725)

[Admins adding B2B users to an application 10](#_Toc473280726)

[Information Worker adding B2B users 10](#_Toc473280727)

[Information workers adding B2B users to an application 10](#_Toc473280728)

[Information workers adding B2B users to a group 10](#_Toc473280729)

[Add without invitation 10](#_Toc473280730)

[Invitation Email 11](#_Toc473280731)

[Deconstructing the email 12](#_Toc473280732)

[Subject 12](#_Toc473280733)

[From address 13](#_Toc473280734)

[Reply To 13](#_Toc473280735)

[Branding 13](#_Toc473280736)

[Call to action 13](#_Toc473280737)

[Inviter’s information 13](#_Toc473280738)

[Body 13](#_Toc473280739)

[Footer 13](#_Toc473280740)

[Special cases 14](#_Toc473280741)

[Where the inviter doesn’t have an email address in the inviting tenancy 14](#_Toc473280742)

[Where the recipient doesn’t need to redeem the invitation 15](#_Toc473280743)

[Redemption experience 15](#_Toc473280744)

[AAD and MSA users 15](#_Toc473280745)

[Social ID user first time redemption 16](#_Toc473280746)

[B2B user properties 16](#_Toc473280747)

[Defining a “B2B” user 16](#_Toc473280748)

[Before invitation redemption 17](#_Toc473280749)

[After invitation redemption 18](#_Toc473280750)

[UserType 18](#_Toc473280751)

[Member 18](#_Toc473280752)

[Guest 18](#_Toc473280753)

[Source 18](#_Toc473280754)

[Invited User 19](#_Toc473280755)

[External Active Directory 19](#_Toc473280756)

[Microsoft Account 19](#_Toc473280757)

[Windows Server AD 19](#_Toc473280758)

[Azure Active Directory 19](#_Toc473280759)

[Can B2B Users be added as Members instead of Guests? 19](#_Toc473280760)

[Filtering for Guest users in the directory 19](#_Toc473280761)

[Guest user default directory permissions 20](#_Toc473280762)

[Converting UserType 21](#_Toc473280763)

[Removing Guest user limitations 21](#_Toc473280764)

[Adding Guests to a Role 21](#_Toc473280765)

[Default Role: 22](#_Toc473280766)

[Global Administrator Role: 23](#_Toc473280767)

[Limited Administrator Role 24](#_Toc473280768)

[Auditing and reporting 24](#_Toc473280769)

[Resending Invitations 26](#_Toc473280770)

[Customization through APIs 27](#_Toc473280771)

[B2B Invitation API Capabilities The API will offer the following capabilities: 27](#_Toc473280772)

[Authorization Model 28](#_Toc473280773)

[App + User Mode 28](#_Toc473280774)

[App only Mode 28](#_Toc473280775)

[PowerShell 28](#_Toc473280776)

[B2B User management 28](#_Toc473280777)

[Delegating Invitations 29](#_Toc473280778)

[Guest Inviter Role 29](#_Toc473280779)

[Controlling who can Invite 29](#_Toc473280780)

[Dynamic Groups and B2B users 30](#_Toc473280781)

[What are dynamic groups? 30](#_Toc473280782)

[What are the inbuilt dynamic groups? 30](#_Toc473280783)

[Hardening your “All User” dynamic group 30](#_Toc473280784)

[Multi-factor Authentication for B2B users 32](#_Toc473280785)

[Setting up MFA for B2B users 32](#_Toc473280786)

[B2B users MFA experience 33](#_Toc473280787)

[Access Reviews 33](#_Toc473280788)

[Policy & Governance 33](#_Toc473280789)

[B2B User Tokens 34](#_Toc473280790)

[B2B User Claims Mapping 36](#_Toc473280791)

[O365 External Sharing 37](#_Toc473280792)

[B2B and B2C 38](#_Toc473280793)

[Configuring SAS apps for B2B 39](#_Toc473280794)

[DropBox for Business 39](#_Toc473280795)

[Box 47](#_Toc473280796)

[Code & Script Samples 49](#_Toc473280797)

[Code Sample 49](#_Toc473280798)

[PowerShell Example 52](#_Toc473280799)

[Current Limitations 53](#_Toc473280800)

[Licensing guidance 53](#_Toc473280801)

[Troubleshooting B2B issues 54](#_Toc473280802)

[I can’t create an external user due to an existing Contact: 54](#_Toc473280803)

[I’ve added an external user but do not see them in my Global Address book or in the People Picker 54](#_Toc473280804)

[Invitations have been disabled for directory 55](#_Toc473280805)

[The user that I invited is receiving an error during redemption: 55](#_Toc473280806)

[Invitee’s Admin has disallowed EmailVerified Users from being created in their tenant: 55](#_Toc473280807)

[External User does not exist already in Federated Domain 55](#_Toc473280808)

[How does ‘#’ which is normally an invalid character sync with Azure AD? 56](#_Toc473280809)

[I receive an error when adding External users to a Synchronized Group 56](#_Toc473280810)

[My External User did not receive an email to redeem 56](#_Toc473280811)

[My Invitee received multiple emails from me 56](#_Toc473280812)

[Q&A 56](#_Toc473280813)

[Is this functionality available in the classic portal? 56](#_Toc473280814)

[Can B2B users access SharePoint Online and OneDrive? 56](#_Toc473280815)

[Is the CSV upload mechanism still supported? 56](#_Toc473280816)

[How can I customize my invitation emails? 56](#_Toc473280817)

[Can the invited external user leave the organization to which he was invited? 56](#_Toc473280818)

[Can I utilize my Microsoft Account (John@contosomicrosoftacct.com) to log into resources? 56](#_Toc473280819)

[Now that MFA is available for Guest users, can they also reset their MFA method? 56](#_Toc473280820)

[Which org is responsible for MFA licenses? 57](#_Toc473280821)

[What if my partner org already has MFA set up, can we trust their MFA and not use our MFA? 57](#_Toc473280822)

[How can I achieve delayed invitations? 57](#_Toc473280823)

[Can guest users and contacts co-exist? 57](#_Toc473280824)

[Can I make my guest users limited admins? 57](#_Toc473280825)

[Does Azure AD B2B collaboration support permitting B2B users to access the Azure Portal? 57](#_Toc473280826)

[Can I block access to the Azure Portal for guest users? 57](#_Toc473280827)

[What is the timeline by which Azure AD B2B will start support for MFA and consumer email accounts? 59](#_Toc473280828)

[What is the GA timeline for Azure AD B2B? 59](#_Toc473280829)

[Is there a plan to support password reset for Azure AD B2B users? 59](#_Toc473280830)

[Is it also enabled for users in a viral tenant? 59](#_Toc473280831)

[Does CRM provide online support to Azure AD B2B? 60](#_Toc473280832)

[What is the lifetime of an initial password for a newly created B2B user? 60](#_Toc473280833)

[Getting support for AzureAD B2B Collaboration 60](#_Toc473280834)

[More questions or feedback? 61](#_Toc473280835)

# What is Azure AD B2B Collaboration?

Azure AD B2B Collaboration capabilities enables IT Pros and Information Workers to work closely with users in any other organization on the planet. They can provide access to documents, resources and applications, while maintaining complete control over their internal data. Developers can use the Azure AD business-to-business APIs to write applications that bring two organizations together in a secure way that appears seamless to Information Workers and is intuitive for them to navigate.

Through Azure AD B2B collaboration capabilities, our goal is to enable 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.

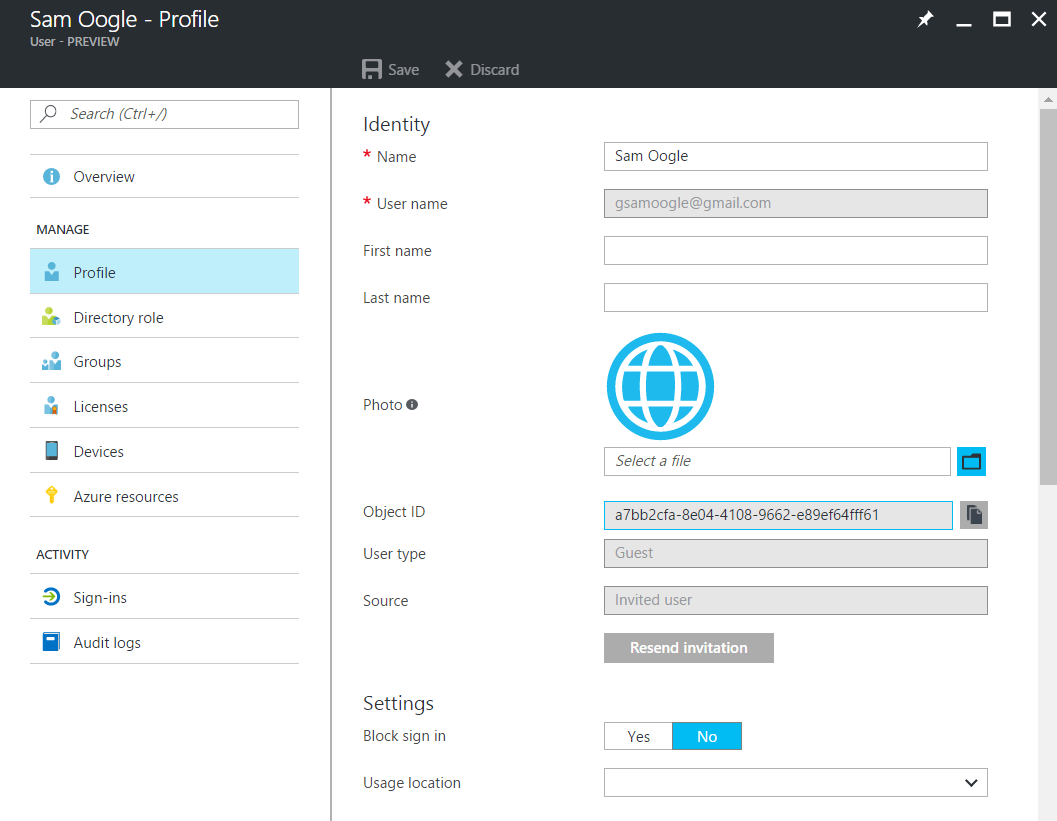
# How does it work?

In the current release, to establish a relationship with an organization, IT Pros and Information Workers can add users from another org one or a few at a time through UX or the Invitation Manager API.

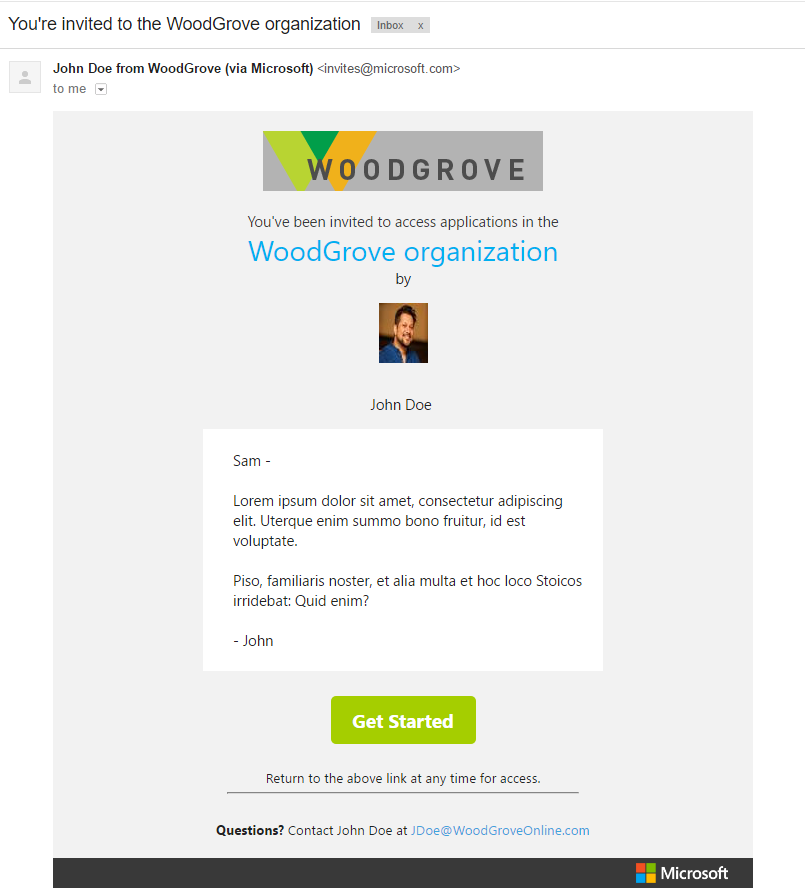
Admins can use the new portal experiences in portal.azure.com and PowerShell for this. And Information workers can use the Access Panel experiences in myapps.microsoft.com. Developers can create applications using the Azure AD B2B invitation manager API to add B2B users and customize the invitation and onboarding workflows.

B2B users are typically onboarded through an invitation + redemption process. Here’s how it works.

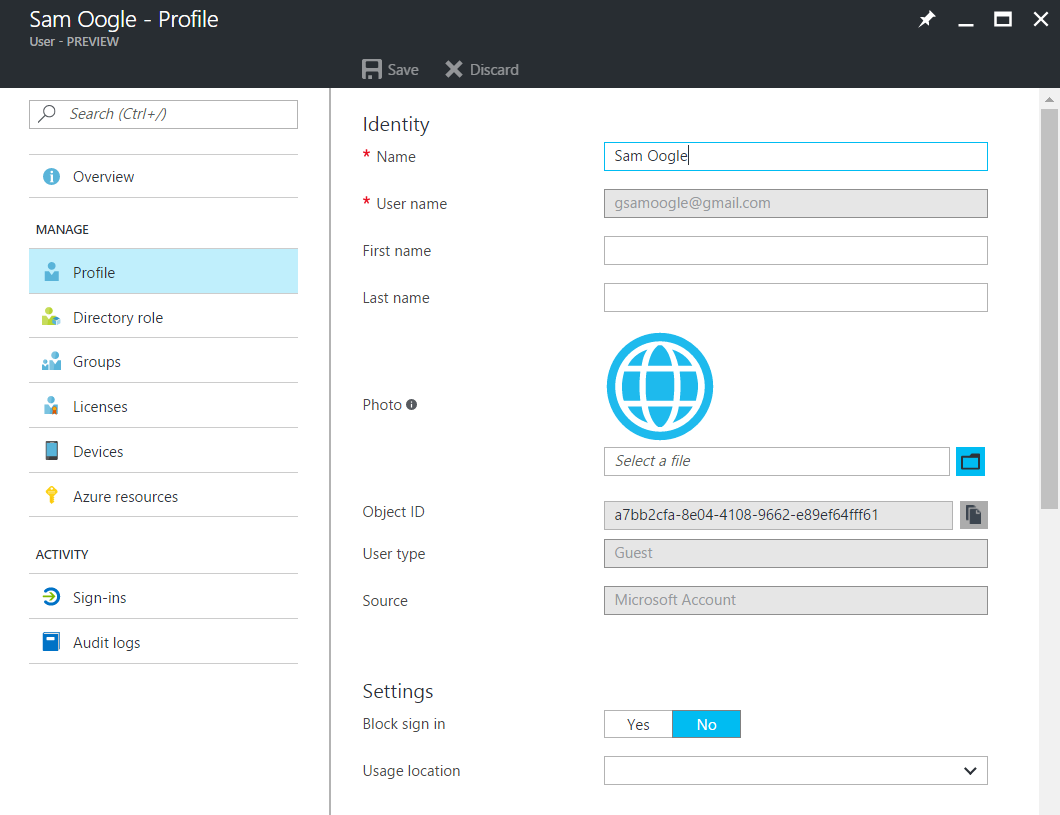
1. John Doe from WoodGrove wants to add Sam Oogle using his gmail address ([gsamoogle@gmail.com](mailto:gsamoogle@gmail.com))
2. John goes to the WoodGrove portal (portal.azure.com) or access panel (myapps.microsoft.com), signs in and adds the user to the WoodGrove directory, or group or application.
3. John specifies a custom message to send to Sam.
4. As soon as he is done, the following user will be created in the WoodGrove AD (screenshot is from the admin UX in portal.azure.com):



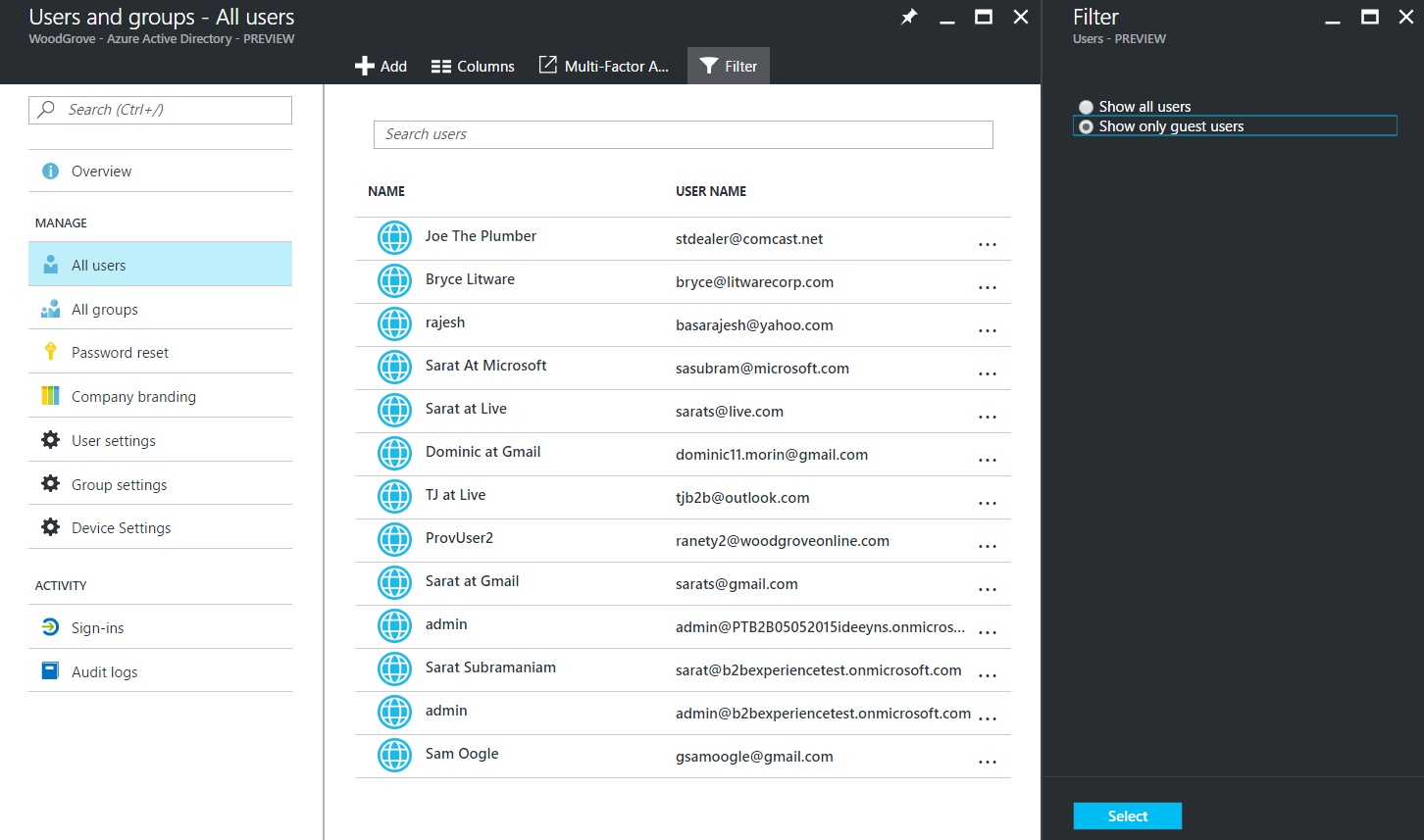
1. As soon as we’re done adding this user, Azure AD will send out an invitation mail to Sam:



1. Now Sam clicks on Get Started and signs in. At this point Azure AD updates his user object in the directory with information from his token (screenshot is from the admin UX in portal.azure.com):



1. Now Sam’s invitation has been redeemed, he can get access to WoodGrove resources and of course can be managed, like any other user in the directory by the administrator (screenshot is from the admin UX in portal.azure.com):



# Public Preview Features

You have been using the B2B capabilities that we had in public preview and have been giving us a ton of excellent feedback. And we’ve been listening! We’re packaging all the improvements we have made in this Public Preview Refresh (PPR).

## These are the key features in B2B PPR:

1. Admin UX enhancements to the B2B experience – coming to <https://portal.azure.com>
   * Ability for admins to invite B2B users to the directory, or any group or application
2. B2B self-service invitation capabilities for Information Workers in the Access Panel: <https://myapps.microsoft.com>
   * Ability for Information workers to invite B2B users to any self-service group or application that they manage.
3. You can now 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.), he/she can now seamlessly access the invited organization with inline, lightweight creation of an Azure AD or Microsoft Account.
4. Benefit from a professional, tenant branded invitation email.
5. Extensive ability to customize onboarding using the Invitation APIs.
6. MFA for B2B users in the inviting organization.
7. Ability to delegate invitations to non-administrators.
8. PowerShell support for B2B.
9. Auditing and reporting capabilities.

# Admins adding B2B users

Global Admins and limited admins can use the Azure portal at portal.azure.com to invite B2B users to the directory, any group or application.

## Admins adding B2B users to the directory

**Include animated Gif from here:** <https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F01_Admin_adding_b2b_user_to_directory%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## Admins adding B2B users to a group

**Include animated Gif from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F02_Admin_to_Group%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## Admins adding B2B users to an application

**Include animated Gif from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F03_Admins%20assigning%20guest%20users%20to%20apps%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

# Information Worker adding B2B users

Information workers can use the Application Access Panel at myapps.microsoft.com to add B2B users to Groups and applications that they are administrators of.

## Information workers adding B2B users to an application

**Include animated Gif from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F04_IW%20adds%20guests%20to%20apps%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## Information workers adding B2B users to a group

Information workers can similarly add B2B users to an assigned group, enabled for self-service group management.

Note: You cannot add B2B users to a Group synced from On Premises or into a Dynamic Group.

# Add without invitation

If the inviter belongs to a role that has enumeration privileges in the directory of the partner organization, from which he or she is adding users, the invited users are added into the inviting organization without needing invitations.

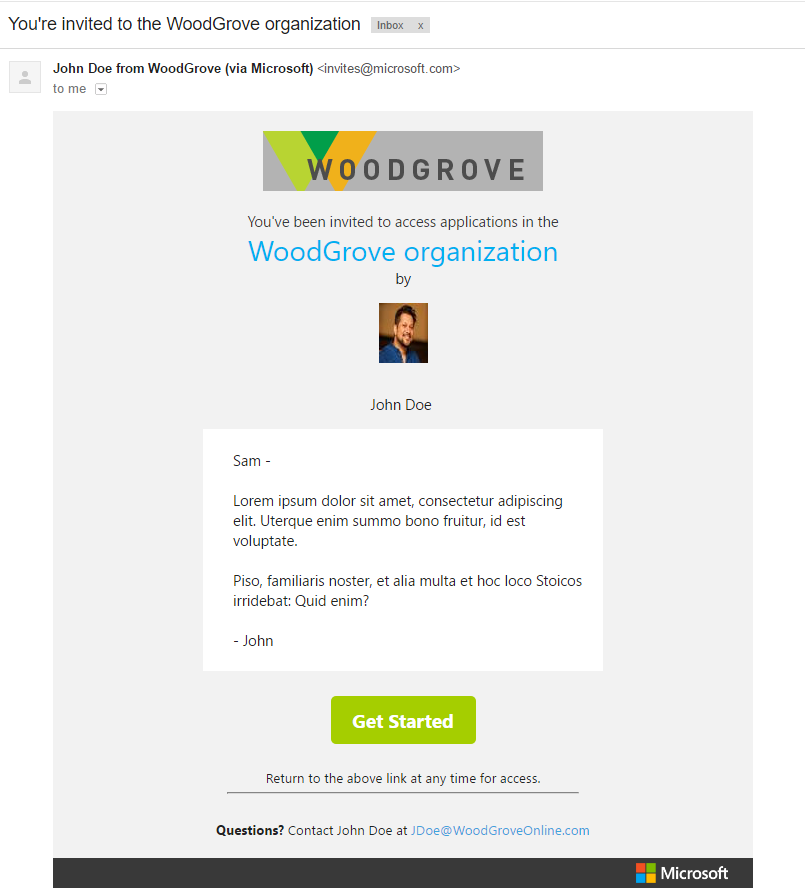
This is the scenario in which this is most useful:

1. User in host organization (say WoodGrove) invites one user from the partner organization (say Sam@litware.com) as Guest.
2. Admin in host organization sets up policies that allow Sam to be able to invite other users.
3. Host organization delegates the responsibility of identifying and adding other users from the partner organization to Sam.
4. Now Sam can add other users from Litware to the WoodGrove directory, groups or applications without needing invitations to be redeemed.

If Sam has the appropriate enumeration privileges in Litware, this happens automatically.

# Invitation Email

Invitation emails are a critical component to onboard collaborators as B2B users in Azure AD. The primary goal for this is to increase trust in the recipient and add legitimacy and social proof to the email to make sure the recipient feels comfortable with clicking on the “Get Started” button and accept the invitation. This is a key component to reducing sharing friction. And of course, we also want the email to look great!



## Deconstructing the email

Let’s look at a few elements of the email so you know how best to make use of these capabilities.

### Subject

The subject of the email follows the following pattern:

You’re invited to the <Tenant Name> organization

### From address

We use a LinkedIn-like pattern for the From address. Our goal here is to be clear who the inviter is and from which company and also clarify that the email is coming from a Microsoft email address.

<Display name of Inviter> from <Tenant Name> (via Microsoft) <invites@microsoft.com>

### Reply To

The reply to email is set to the inviter’s email when available. So replying to the email will send an email back to the inviter.

### Branding

The invitation emails from your tenant use the company branding that you may have set up for your tenant. If you want to take advantage of this, [here](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Factive-directory-add-company-branding&data=02%7C01%7Csasubram%40exchange.microsoft.com%7Cb893952d65d9479252f108d4407af381%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636204344203519772&sdata=gLDq0k46MmB8TPLhgdtjBAhQL6JeD8quqalU9ISwOTE%3D&reserved=0) are the details on how to configure it. The “banner logo” will show up in the email. Follow the image size and quality instructions [here](https://na01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fdocs.microsoft.com%2Fen-us%2Fazure%2Factive-directory%2Factive-directory-add-company-branding&data=02%7C01%7Csasubram%40exchange.microsoft.com%7Cb893952d65d9479252f108d4407af381%7C72f988bf86f141af91ab2d7cd011db47%7C1%7C0%7C636204344203519772&sdata=gLDq0k46MmB8TPLhgdtjBAhQL6JeD8quqalU9ISwOTE%3D&reserved=0) for best results.

In addition, the company name also shows up in the call to action.

### Call to action

The call to action consists of two parts: explaining why the recipient has received the mail and what the recipient is being asked to do about it.

The “Why” is addressed using the following pattern:

You’ve been invited to access applications in the

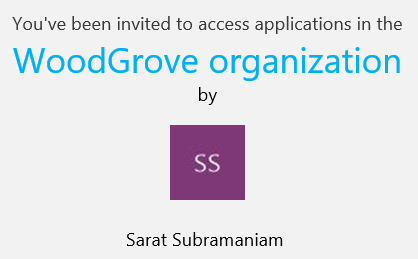
<Tenant Name> organization

And the what you’re being asked to do is indicated by the presence of the “Get Started” button. In the case where the recipient has been added without the need for invitations, this button wouldn’t show up.

### Inviter’s information

The inviter’s display name will be included in the email. And in addition, if you’ve set up a profile picture for your AzureAD account, the inviting email will include that picture as well. Both of these are intended to increase your invitee’s confidence in the email.

If the inviter hasn’t yet set up their profile picture, we just create an icon with the inviter’s initials in place of the picture as shown below:



### Body

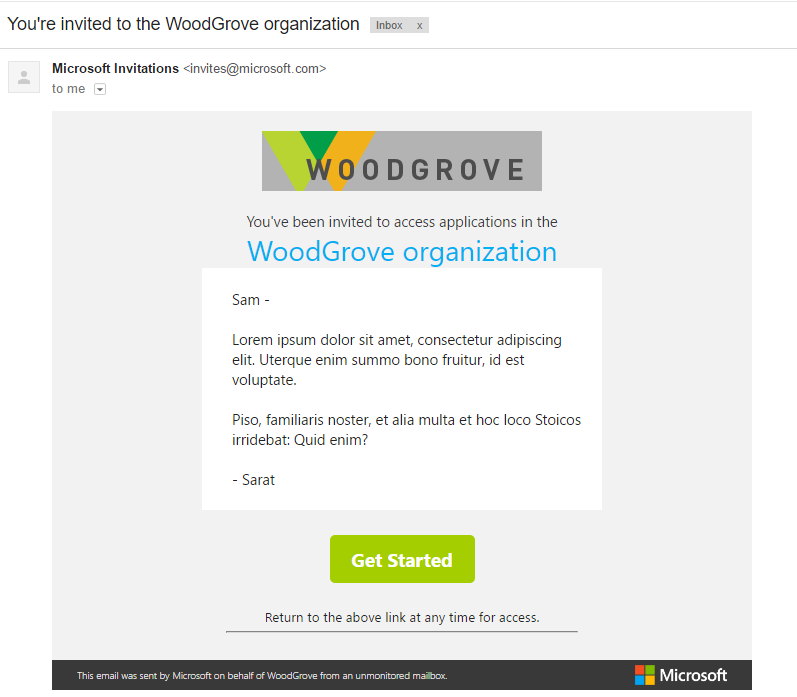
This will contain the message that the inviter typed in the UX or passed through the invitation API. This is just a simple text box, which will not process html tags for security reasons.

### Footer

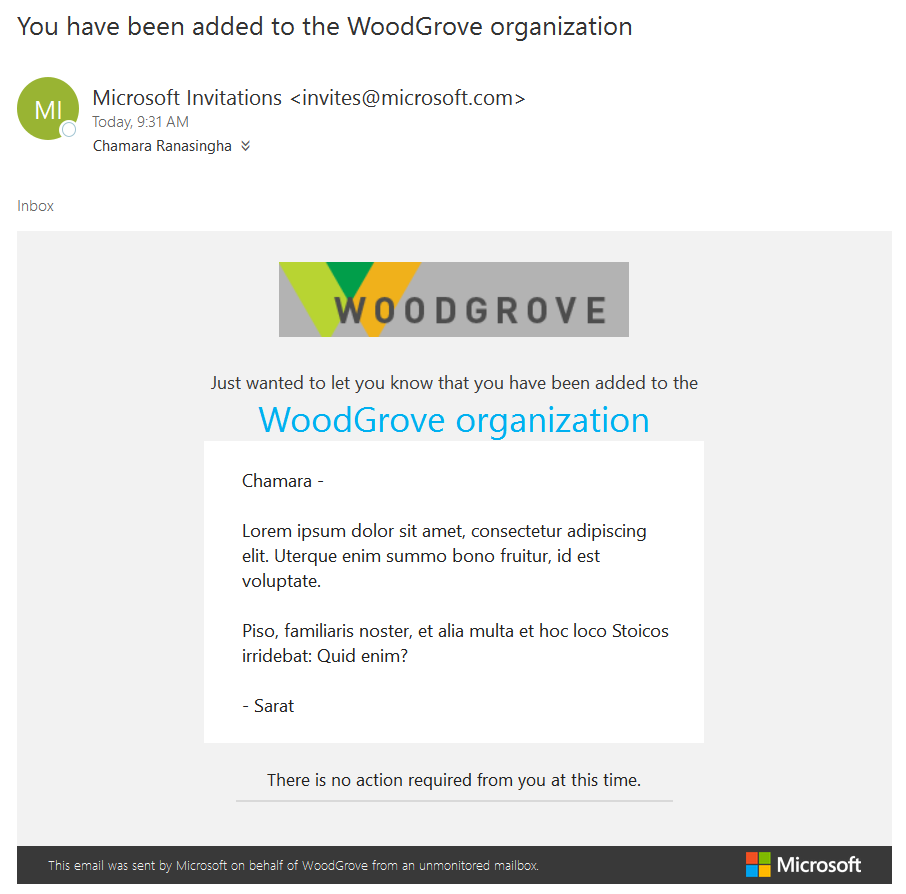
The footer contains the Microsoft company brand and will let the recipient know if the email was sent from an unmonitored alias.

## Special cases

### Where the inviter doesn’t have an email address in the inviting tenancy



### Where the recipient doesn’t need to redeem the invitation



# Redemption experience

## AAD and MSA users

For users with existing AAD and MSA accounts the redemption experience is as easy as signing in. Nothing super fancy here. So let’s take a look at the most interesting/involved case and see how easy the product makes it for any email address to be used for redemption.

## Social ID user first time redemption

Take a look at what the redemption experience looks like when a non-Microsoft email address is used for B2B collaboration. This is the most involved redemption flow, since you may have to create an account at the time of redemption. Check it out in the animated gif below.

**Include the animated Gif from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F05_Redemption_Experience%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

# B2B user properties

## Defining a “B2B” user

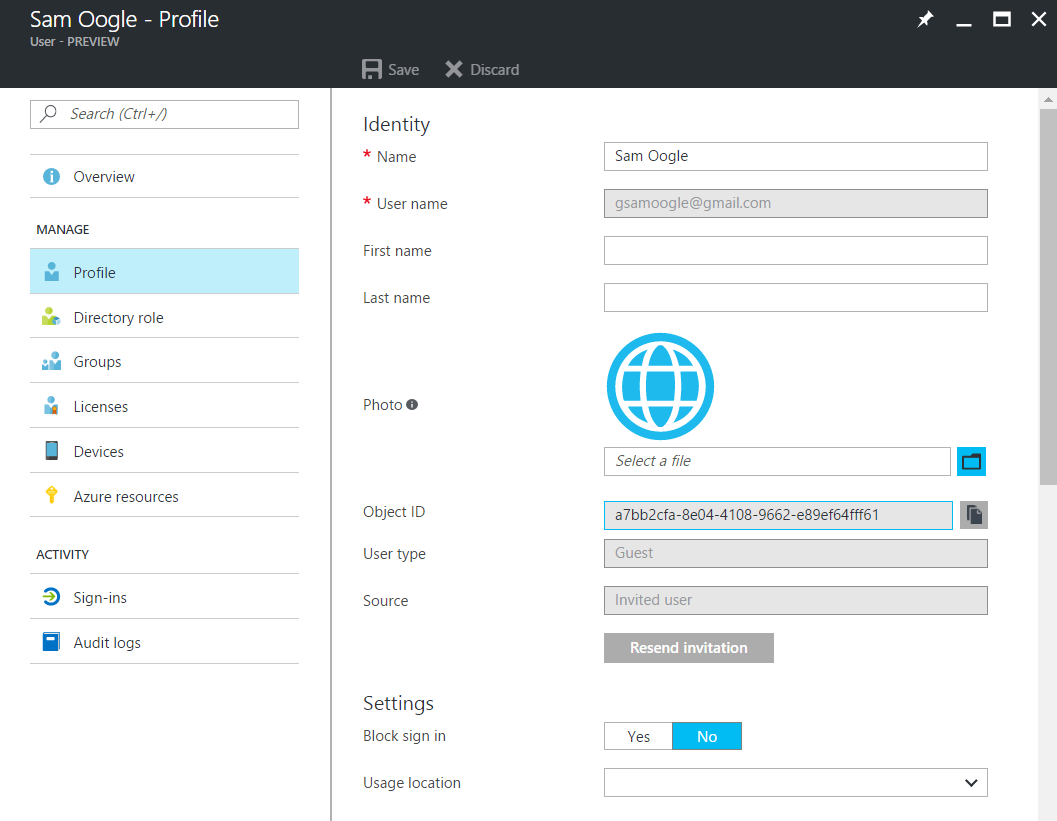
A B2B user is a user with UserType = Guest. We also colloquially refer to a B2B user as a Guest user. This user typically represents a user from a partner organization and has limited privileges in the inviting directory by default.

Depending on the inviting organization’s needs, a B2B user can be in one of the following account states:

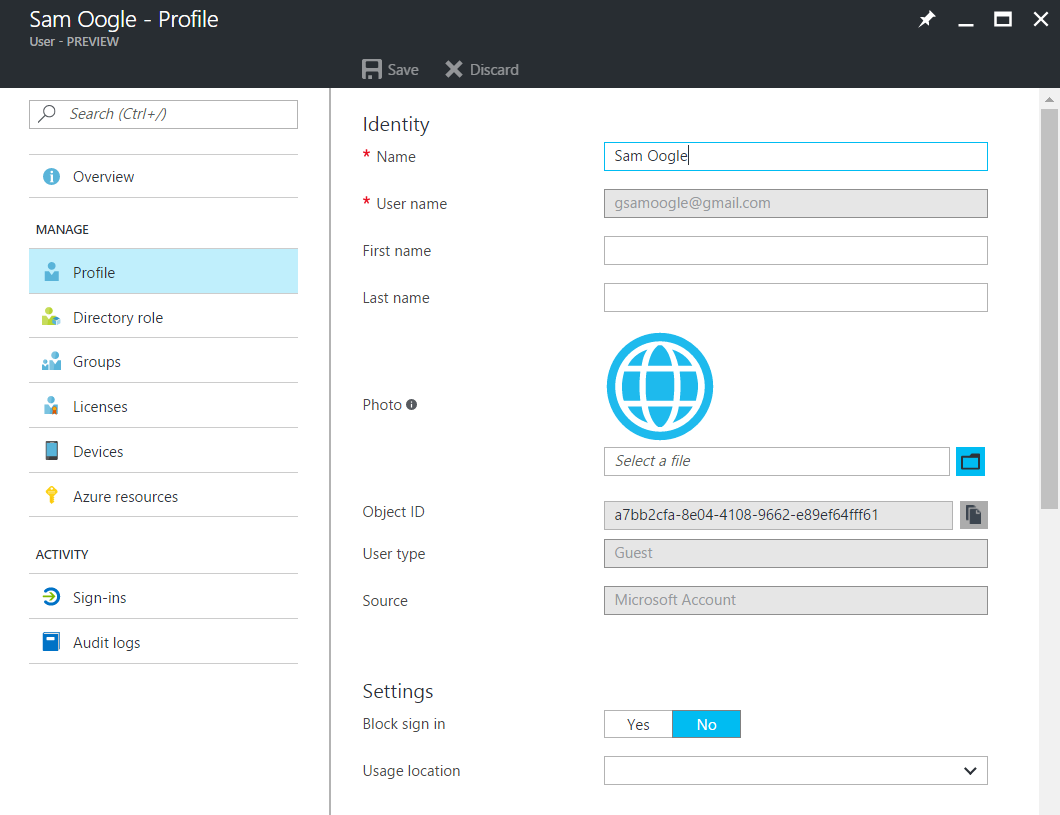
1. **Homed in an external Azure AD, represented as a Guest user in the host organization**
   1. In this case the B2B user signs in with an Azure AD account belonging to his home tenancy
   2. If the external organization that the user belongs to doesn’t have an Azure AD at the time of invitation, it is created just in time when the user redeems his invitation, after verifying his email address. This is also called a JIT tenancy, colloquially referred to as a Viral tenancy.
2. **Homed in Microsoft Account, represented as a Guest user in the host organization**
   1. In this case, the B2B user signs in with a Microsoft account.
   2. In the Azure AD Public Preview Refresh product, the invited user’s non-MSA social identity (google.com, etc.) will be created as a Microsoft account just in time during redemption.
3. **Homed in host organization’s OnPrem AD, synced as to host organizations Azure AD**
   1. During this release, the UserType of such users in the cloud needs to be manually changed to Guest using PowerShell. We will be inherently supporting this as part of Azure AD Connect in future releases.
4. **Homed in host organization’s AzureAD with UserType = Guest, with credentials managed by the org**

Now, let’s see what a B2B user in **State 1** looks like in Azure AD.

## Before invitation redemption



## After invitation redemption



There are some key properties of this user.

## UserType

This attribute indicates the relationship of the user with the host tenancy. This can have two values:

### Member

An employee of the host organization, a user in the organization’s payroll. For example, this is a user who is expected to be able to access “Internal Only” sites. This user would not be considered an external collaborator.

### Guest

This indicates a user that isn’t considered “internal” to the company. An external collaborator, partner, customer, etc. – that isn’t expected to get your CEO’s internal memo for example or get company benefits.

**Note:** the UserType has no relation with how the user signs in, or which directory role the user belongs to, etc. This attribute simply indicates the user’s relationship with the host organization and allows the organization to enforce any policies that depend on this attribute.

## Source

Aka: how the user signs-in.

### Invited User

This user has been invited but has not yet redeemed their invitation.

### External Active Directory

This user is homed in an external organization and authenticates with an Azure AD account belonging to the other organization. This corresponds to State 1 above.

### Microsoft Account

This user is homed in MSA and authenticates with a Microsoft Account. This corresponds to State 2 above.

### Windows Server AD

This user is synced in from On-premises Active Directory belonging to this organization. This corresponds to State 3 above.

### Azure Active Directory

This user authenticates with an Azure AD account belonging to this organization. This corresponds to State 4 above.

**Note:** Source and UserType are independent attributes. A value of source does not imply a particular UserType.

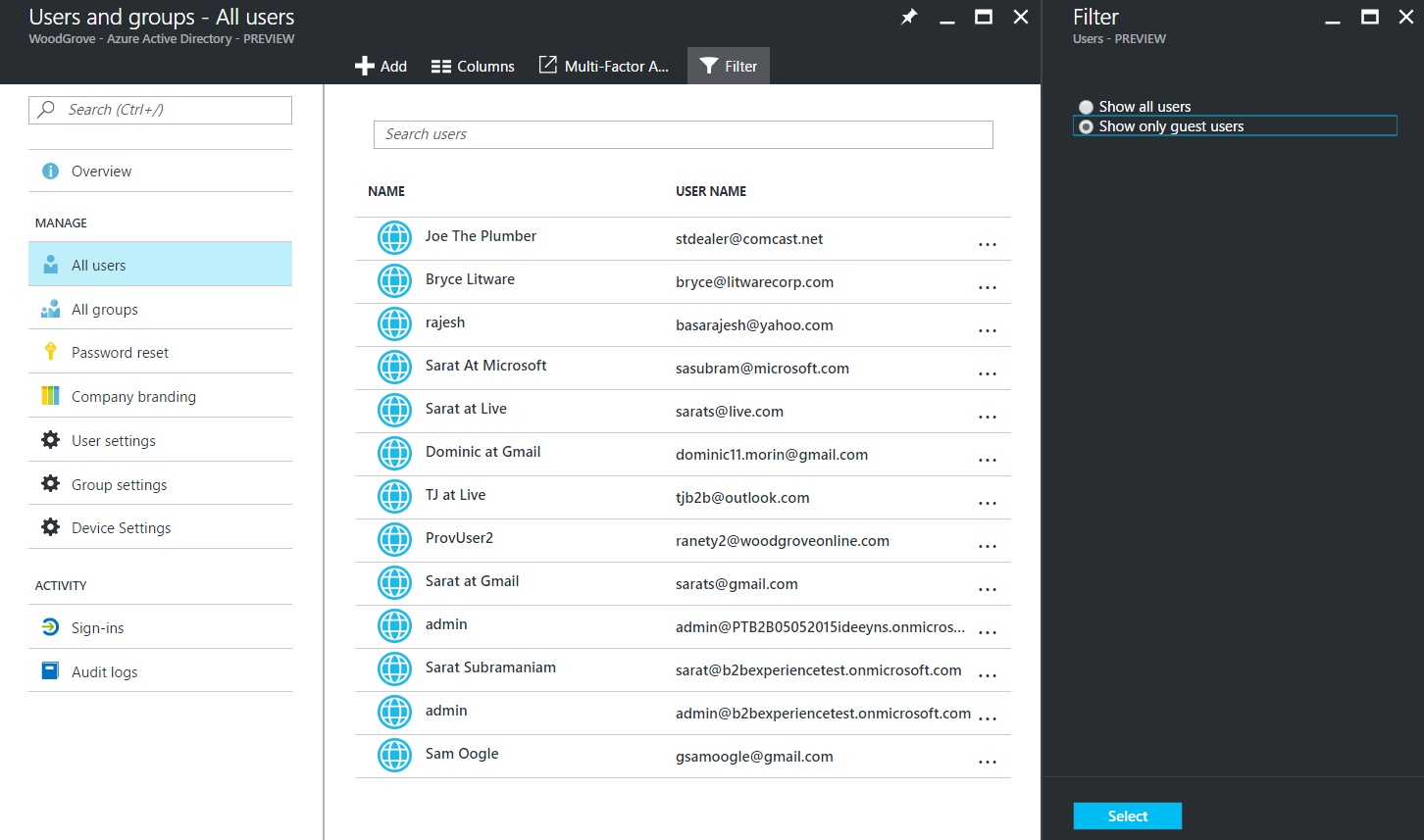
## Can B2B Users be added as Members instead of Guests?

Typically, a B2B user and Guest user are synonymous. Therefore, B2B user is added as a user with “UserType = Guest” by default.

However, in some cases, the partner organization is actually more a member of the larger conglomeration that the host organization belongs to. If this is so, the host organization may want to treat users in the partner organization as Members and not Guests.

In this case, using the B2B Invitation Manager APIs, the admin of the host organization can add or invite a user from the partner organization as a member. More details in the API customization section.

## Filtering for Guest users in the directory



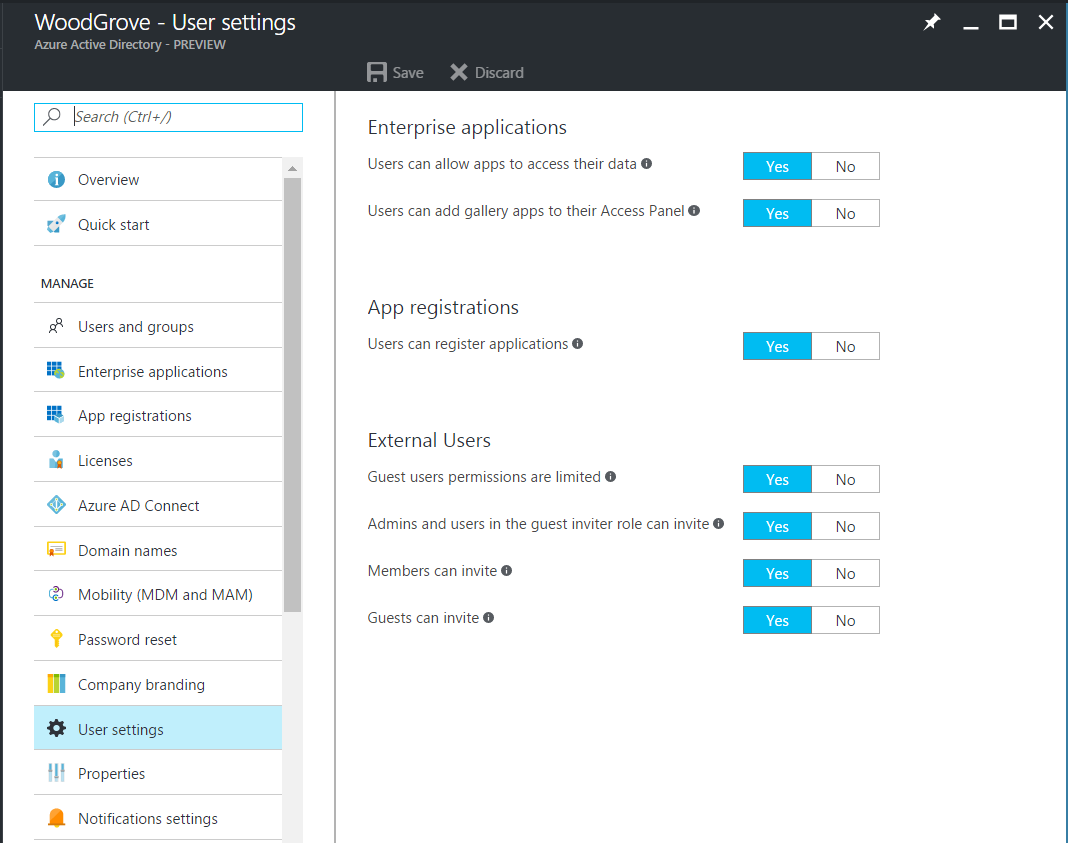
## Converting UserType

Currently, in PowerShell, it is possible for users to convert UserType from Member to Guest and vice-versa. However, the UserType property is supposed to represent the user’s relationship with the organization. Therefore, this property should only change this if the user relationship with the organization has changed. If the user relationship changes, other questions should be answered like, should the UPN change? Should the user continue to have access to the resources they had access to? Should a mailbox be assigned, etc.

Therefore, we do not recommend changing the UserType in PowerShell as an atomic activity. In addition, we will be making this property immutable through PowerShell in future releases, so we do not recommend taking a dependency on this value.

There may, however, be cases where you want to give your guest users higher privileges. For this, you can add a guest user to any role and even remove the default guest user restrictions in the directory to make them behave more like members. Read on to learn more.

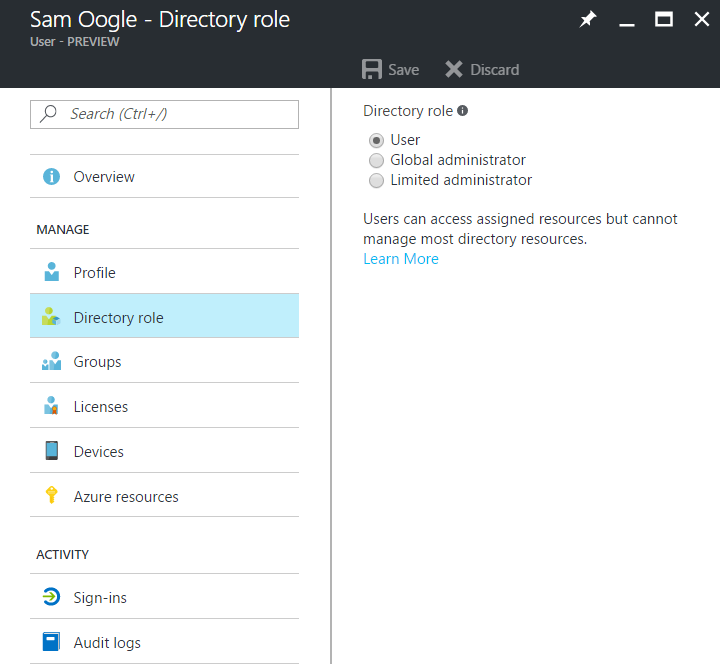
## Removing Guest user limitations

It is possible to turn off the default guest user limitations so that guest users in the company directory are given the same directory permissions that a regular user (member) has. 

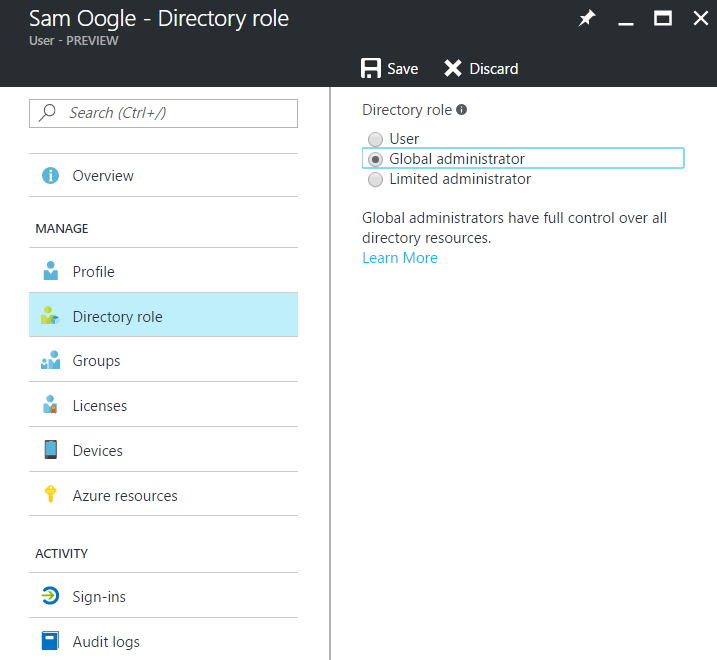
## Adding Guests to a Role

While B2B users are added as “Guest” users in the directory and Guest permissions in the directory are restricted by default, your business may need some Guest users to play higher privilege roles in your organization. To support this, Guest users can be added to any roles you desire, based on your organization’s needs.

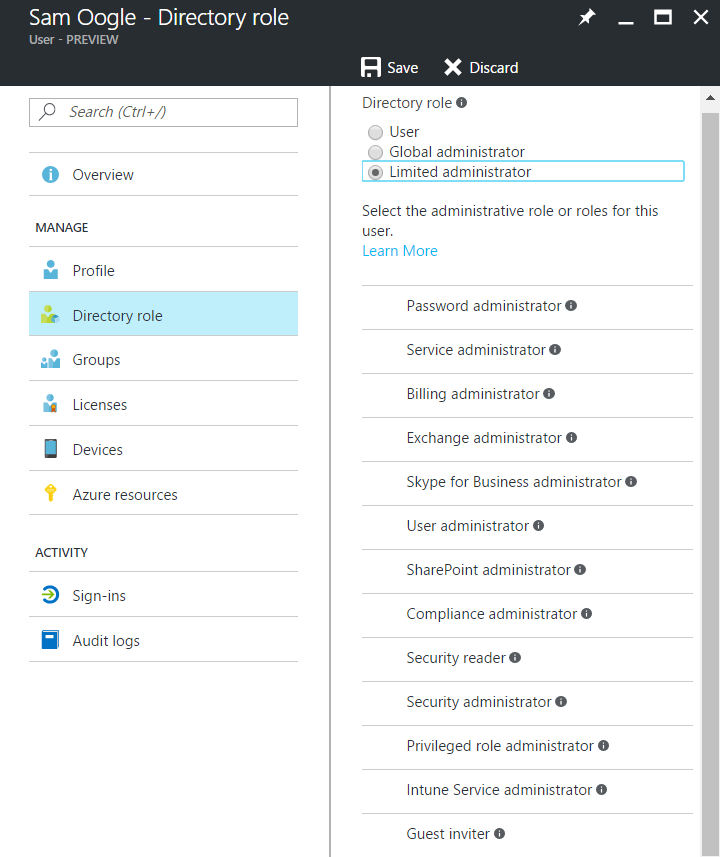
### Default Role:



### Global Administrator Role:

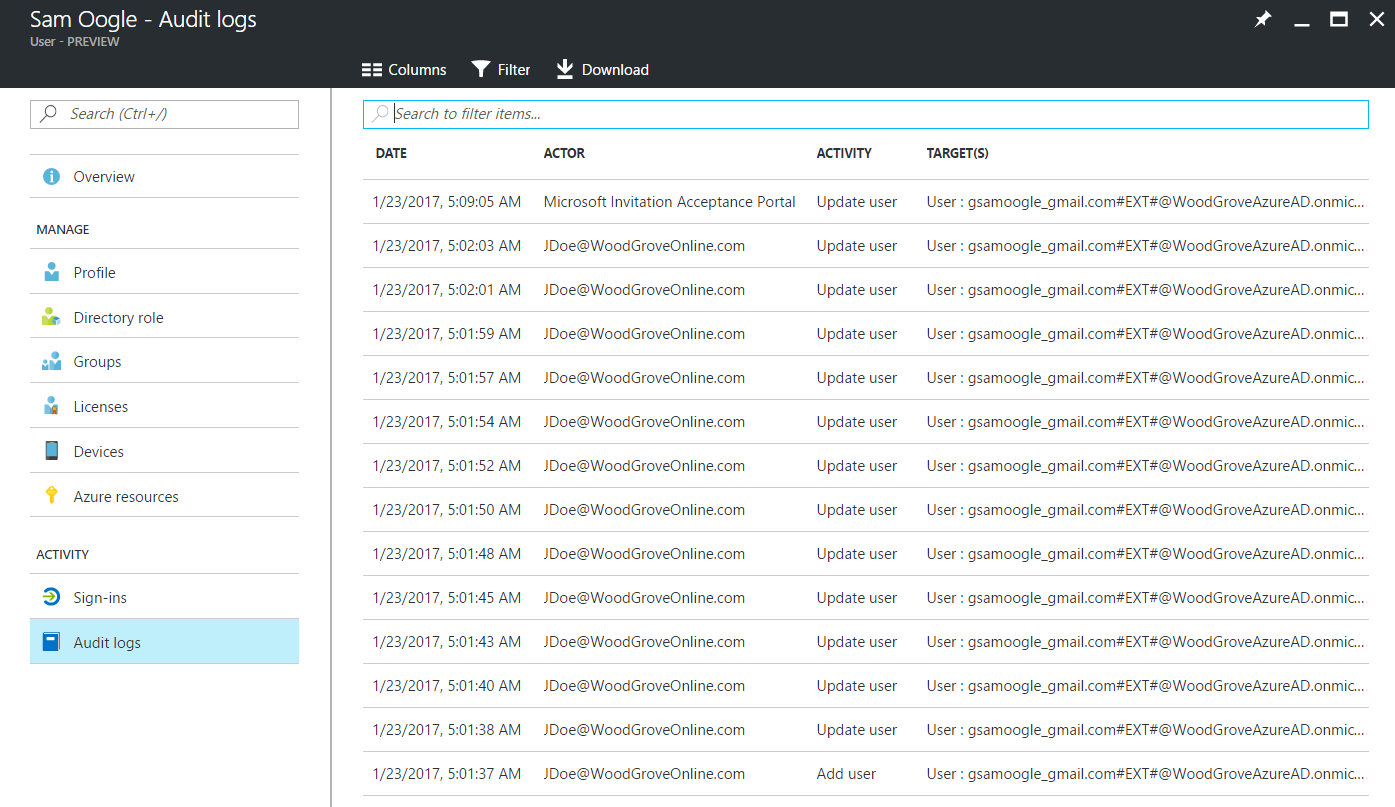


### Limited Administrator Role

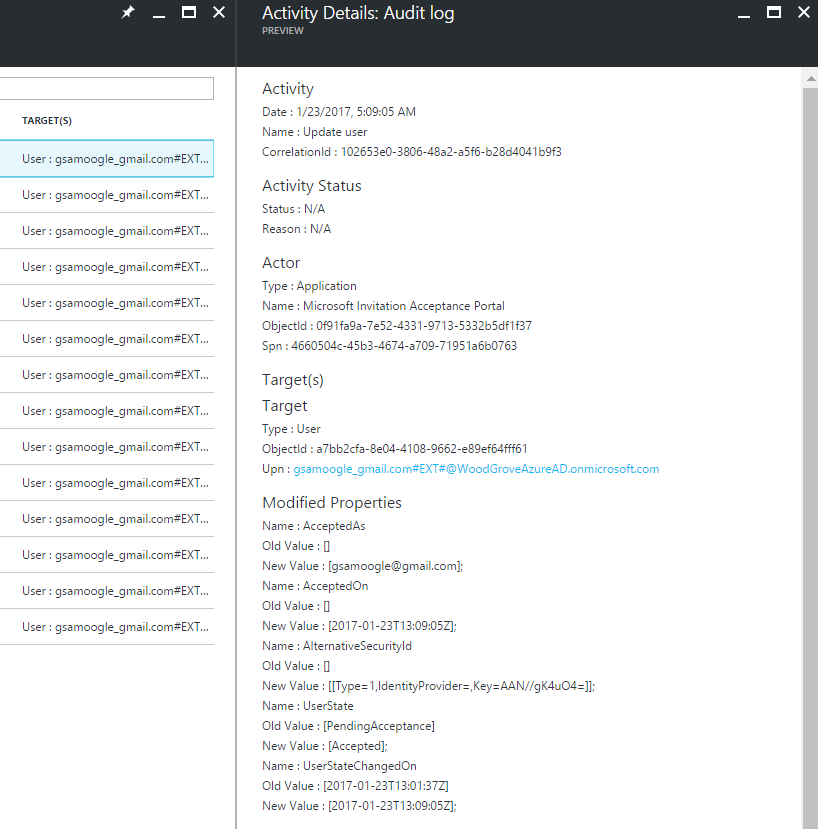


## Auditing and reporting

With Guest users, you now get auditing capabilities on par with member users. Here’s an example below of the invitation and redemption history of the just invited Sam Oogle:



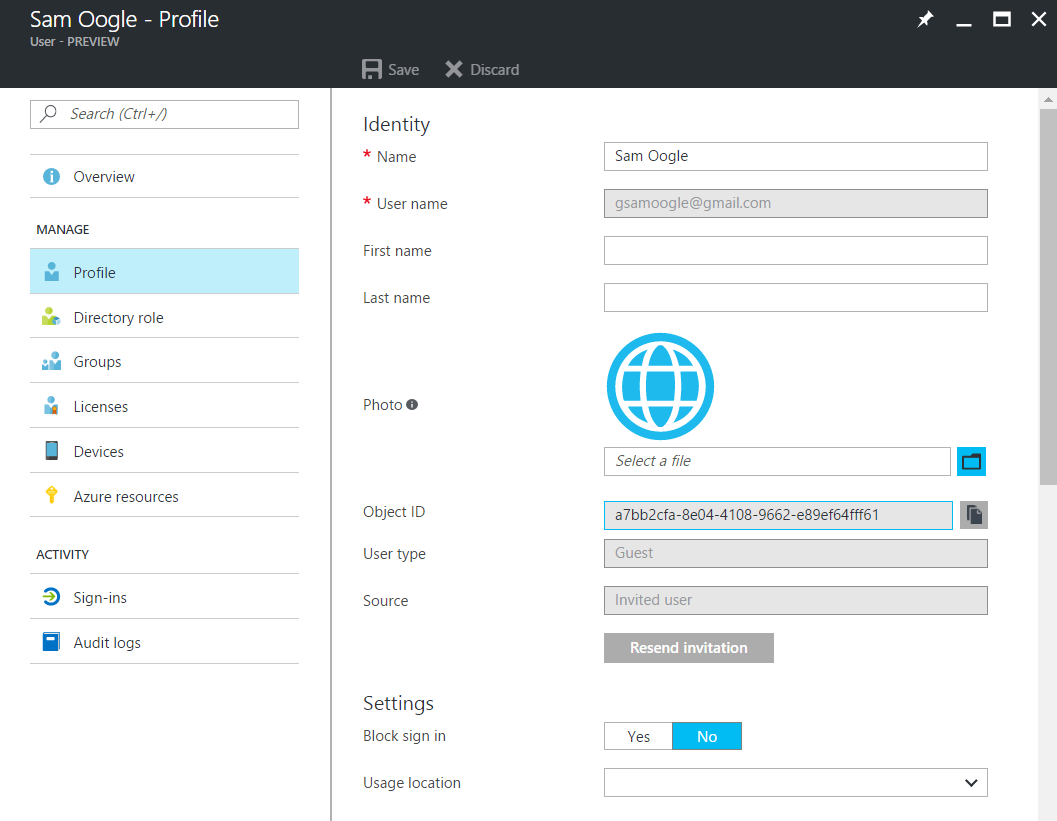
You can dive into each of these events to get the details. For example, let’s look at the acceptance details.



You can also export these logs from Azure AD and use the reporting tool of your choice in order to get customized reports.

# Resending Invitations

It is now possible to go to a B2B user’s profile page and resend invitations to not-yet redeemed guest users for any reason:



**Note**: this will resend an invitation, from the signed-in user – and invite the user to the directory, even if the original invitation was to a specific app or group.

# Customization through APIs

<https://graph.microsoft.io/en-us/docs/api-reference/beta/resources/invitation>

The vast majority of you want customize the invitation process in a way that works best for your organization. We’re really excited to get [this API](http://graph.microsoft.io/en-us/docs/api-reference/beta/resources/invitation) into your hands so you can do just that.

## B2B Invitation API Capabilities The API will offer the following capabilities:

1. Invite an external user with \*any\* email address.

“invitedUserDisplayName”: “Sam”

“invitedUserEmailAddress”: “gsamoogle@gmail.com”

1. Customize where you want your users to land after they accept their invitation.

“inviteRedirectUrl”: “https://myapps.microsoft.com/”

1. Choose to send the standard invitation mail through us

“sendInvitationMessage”: true

with a message to the recipient that you can customize

“customizedMessageBody”: “Hello Sam, let’s collaborate!”

1. and choose to cc: people you want to keep in the loop about your inviting this collaborator.
2. Or completely customize your invitation and onboarding workflow by choosing not to send notifications through Azure AD.

“sendInvitationMessage”: false

In this case, you’ll get back a redemption URL from the API that you can embed in an email template, IM, or other distribution method of your choice.

1. Finally, if you are an admin, you can choose to invite the user as member.

“invitedUserType”: “Member”

## Authorization Model

The API can be run in the following authorization modes:

### App + User Mode

In this mode, the user using the API needs to have the permissions to be create B2B invitations.

### App only Mode

In app only context, the app needs **User.ReadWrite.All** or **Directory.ReadWrite.All** scopes for invitation to succeed.

For more details, refer to: <https://graph.microsoft.io/en-us/docs/authorization/permission_scopes>

# PowerShell

It is now possible to use PowerShell to add and invite external users to an organization easily. Just creat a new invitation using the the cmdlt

New-AzureADMSInvitation

with the following Options:

-InvitedUserDisplayName

-InvitedUserEmailAddress

-SendInvitationMessage

-InvitedUserMessageInfo

whose descriptions follow the invitation API reference here <https://graph.microsoft.io/en-us/docs/api-reference/beta/resources/invitation>

# B2B User management

Management of B2B users both in UX and PowerShell is on par with members.

# Delegating Invitations

With Azure AD B2B Public Preview Refresh, you do not have to be a global admin in order to invite users. You can control who can invite through policies and delegate invitations to users in the allowed roles to invite.

An important new way to delegate Guest user invitations is through the Guest Inviter Role.

## Guest Inviter Role

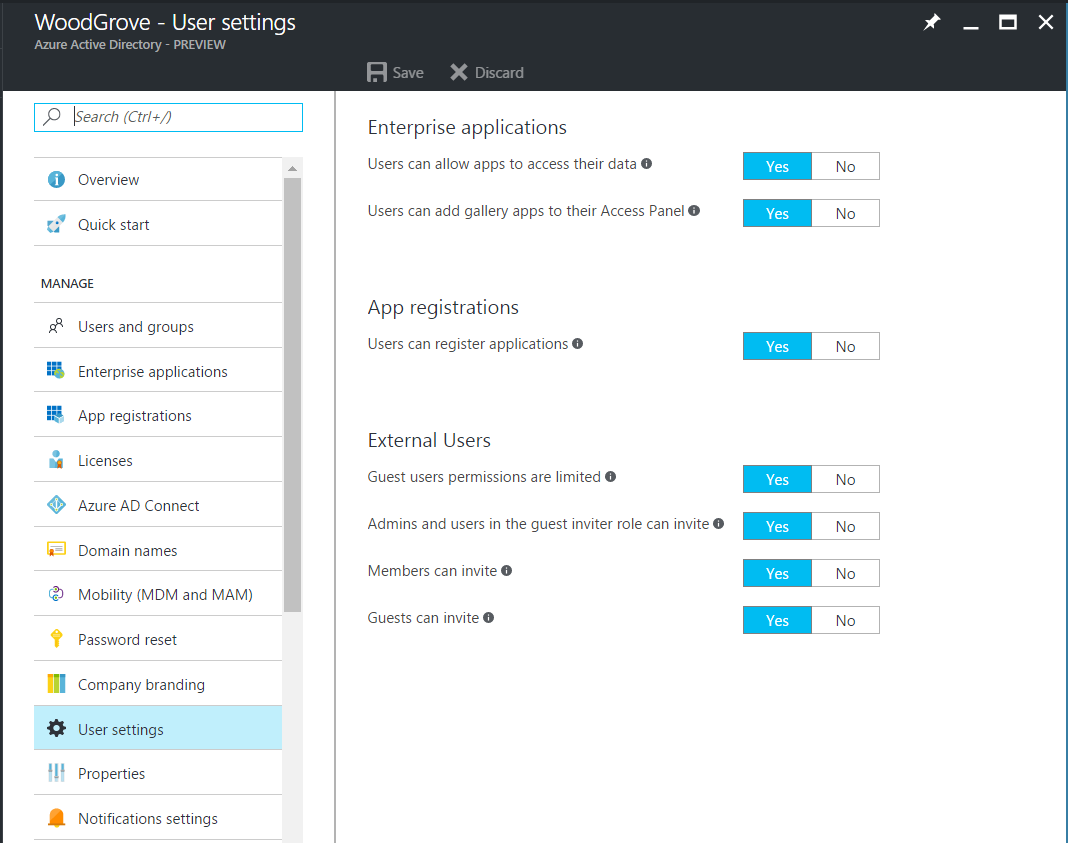
We can assign the user to “Guest Inviter Role” to send invitations. You don’t have to be member of global admin to send invitations. By default, regular users can also invoke invite API unless invitations are disabled for regular users by global admin.

You can do this through the Azure portal UX and also through PowerShell.

Here’s an example showing the addition of a user to the “Guest Inviter Role” through PowerShell:

[Add-MsolRoleMember](https://msdn.microsoft.com/en-us/library/azure/dn194120(v=azure.98).aspx) -RoleObjectId 95e79109-95c0-4d8e-aee3-d01accf2d47b -RoleMemberEmailAddress <RoleMemberEmailAddress >

# Controlling who can Invite



With Azure AD B2B collaboration – we will be allowing the tenant to set the following invitation policies:

1. Turn invitations off
2. Only Admins and users in Guest Inviter Role can invite
3. Admins, Guest Inviter Role and Members can invite
4. All users, including guests can invite

By defaults, tenants are set to #4 (all users, including guests can invite B2B users).

# Dynamic Groups and B2B users

## What are dynamic groups?

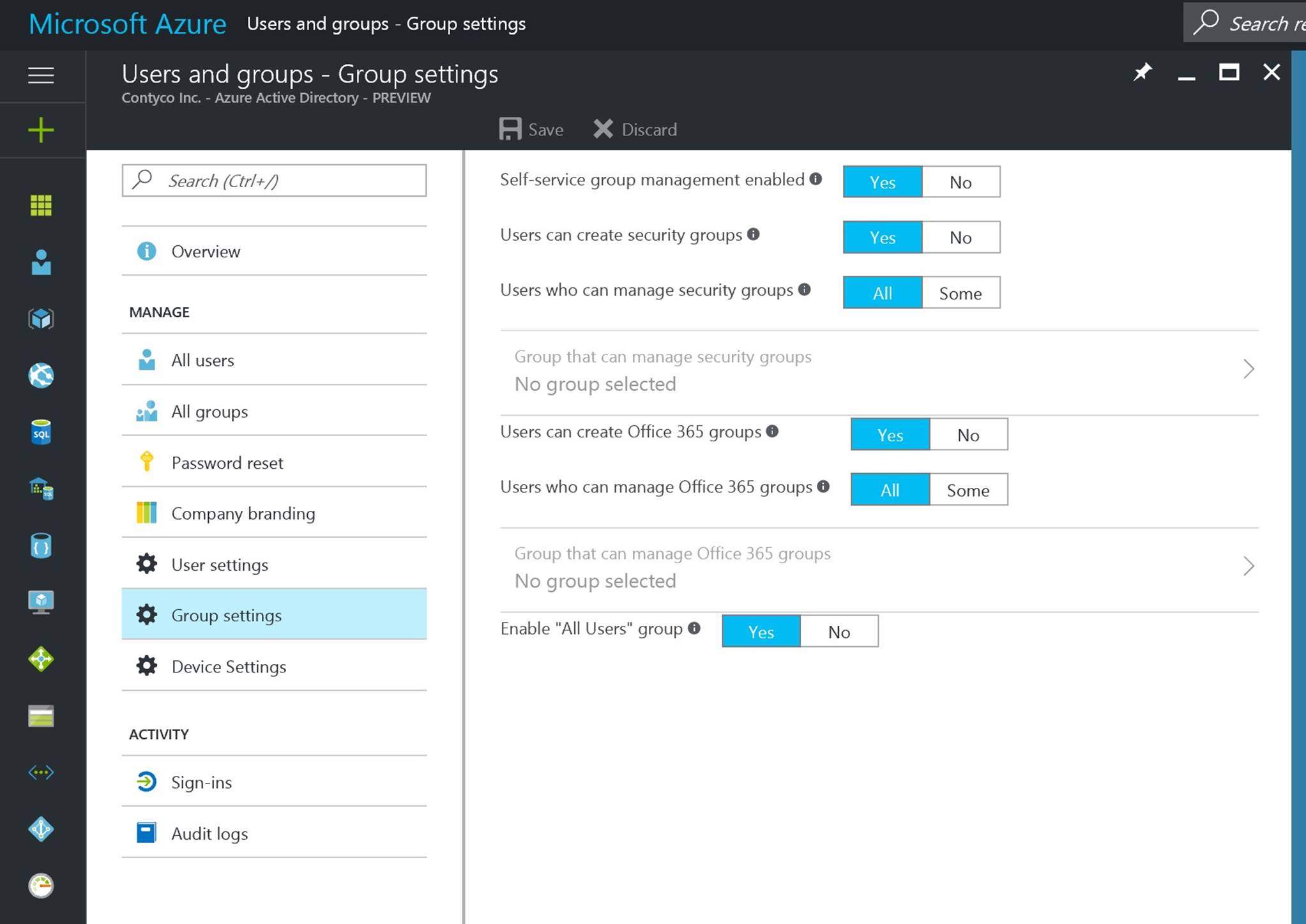
Dynamic configuration of security-group membership for Azure Active Directory is available in public preview. Administrators can set rules for groups that are created in Azure Active Directory based on any user attributes (such as userType, department, country etc.). This allows members to be automatically added to or removed from a security group based on changes to their attributes. These groups can be used to provide access to applications or cloud resources (such as SharePoint sites and documents) and to assign licenses to members. Read more about Dynamic Groups [here](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-dedicated-groups).

With an AAD Premium Subscription, the Azure portal now provides you with the ability to create advanced rules to enable more complex attribute-based dynamic memberships for Azure Active Directory (Azure AD) preview groups. Learn more about creating advanced rules [here](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-groups-dynamic-membership-azure-portal).

## What are the inbuilt dynamic groups?

The “All Users” Dynamic Group enables tenant admins to create a group containing all users in the tenant with a single click. By default, the All Users group includes all users in the directory, including Members and Guests.

Within the new [Azure Active Directory admin portal](https://portal.azure.com/), you can choose to enable the “All Users” group in the Group Settings view.

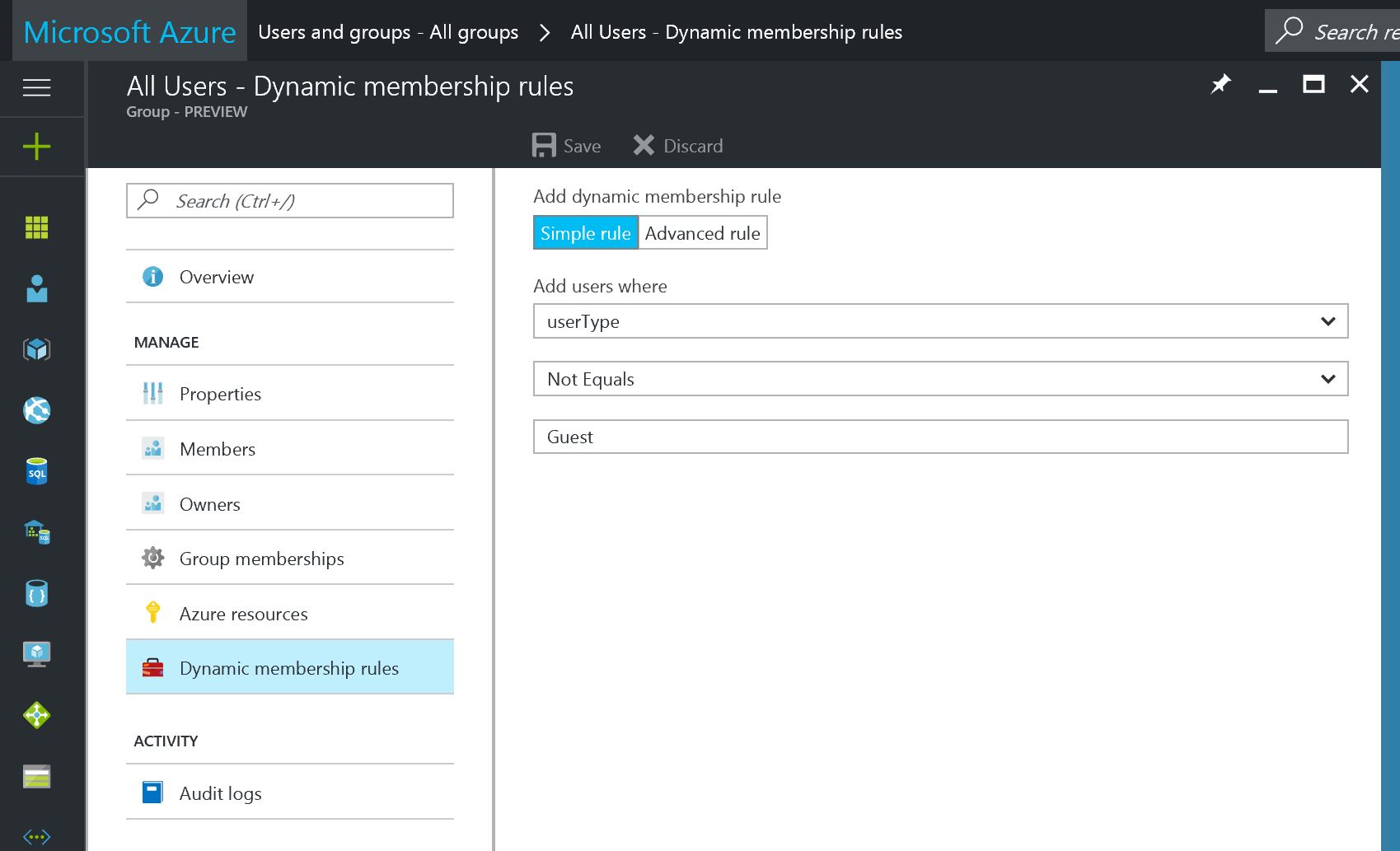


## Hardening your “All User” dynamic group

Note that by default, the “All User” group contains your B2B (aka Guest) users as well.

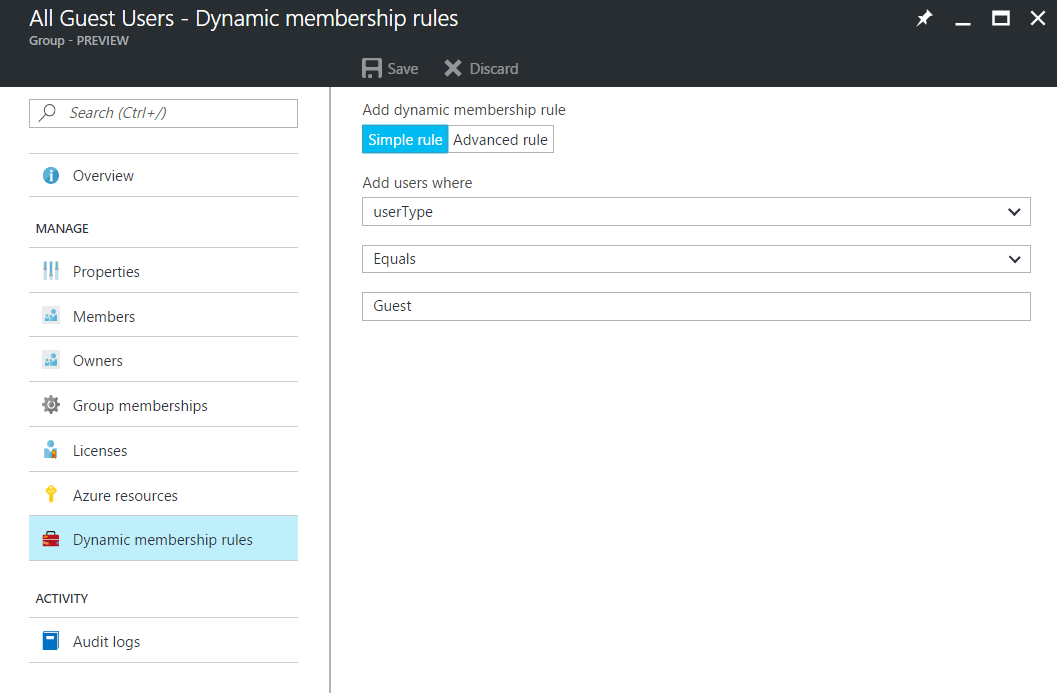
If you wish to further secure your “All Users” group by removing Guest users from the “All Users” group, you can accomplish this easily by modifying the “All Users” group’s attribute-based Simple Rule.

The illustration below shows the All Users group modified to exclude “Guests”.



You might also find it useful to create a new dynamic group that only contains Guest users. This can be quite handy in targeting policies (such as Conditional Access policies) to Guest users.

Here’s an illustration of what such a group might look like:



# Multi-factor Authentication for B2B users

With Azure AD B2B Public Preview Refresh, we are introducing the capability for organizations to enforce Multifactor Authentication (MFA) policies for B2B users also. In the Public Preview refresh, MFA is always enforced at the resource tenancy.

This means:

1. Admin or Information worker in Company A invites user from company B to an application “Foo” in Company A.
2. Application “Foo” in Company A is configured to require MFA on access.
3. When user from company B attempts to access app Foo from company A tenant, they will be asked to complete an MFA challenge as required by company A’s MFA policy.
4. User can set up their MFA with Company A, choose their MFA option
5. This will work for any identity (Azure AD or MSA – for example if users in Company B authenticate using social ID)
6. Company A will need to have adequate premium Azure AD SKUs which support MFA. The user from Company B will consume this license from Company A.
7. In summary, the inviting tenancy is \*always\* responsible for MFA of B2B users from the partner organization, not the partner organization (even if it has MFA capabilities). In future releases, we will be enabling the inviting organization to trust specific partner organizations’ MFA instead of using the inviting organization’s MFA.

## Setting up MFA for B2B users

It’s super easy! Check out the animation below.

**Include animated gif inline from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F06_CA%20setup%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## B2B users MFA experience

Check out the animation below to see the redemption experience.

**Include animated gif inline from here:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F07_MFA%20redemption%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## MFA Reset for B2B users

Currently, the admin cannot require B2B users to proof up again in the UX. Therefore, the following PowerShell cmdlts should be used if you want to reset a B2B users’s proof up method.

Note: To use the new cmdlet, you need to install the Azure AD PowerShell V2 module, which you can get from here: <https://www.powershellgallery.com/packages/AzureADPreview>

1. **Connect to Azure AD**

Connect-AzureAd and login

1. **Get all users with proof up methods**

Get-MsolUser | where { $\_.StrongAuthenticationMethods} | select UserPrincipalName, @{n="Methods";e={($\_.StrongAuthenticationMethods).MethodType}}

**Here is an example:**

PS C:\Users\tjwasser> Get-MsolUser | where { $\_.StrongAuthenticationMethods} | select UserPrincipalName, @{n="Methods";e

={($\_.StrongAuthenticationMethods).MethodType}}

UserPrincipalName                                               Methods

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

[tjb2b\_outlook.com#EXT#@WoodGroveAzureAD.onmicrosoft.com](mailto:tjb2b_outlook.com#EXT#@WoodGroveAzureAD.onmicrosoft.com)         {OneWaySMS, TwoWayVoiceMobile}

[gsamoogle\_gmail.com#EXT#@ WoodGroveAzureAD.onmicrosoft.com](mailto:gsamoogle_gmail.com#@WoodGroveOnline.com)                   {OneWaySMS, TwoWayVoiceMobile}

[AbbieS@WoodGroveOnline.com](mailto:AbbieS@WoodGroveOnline.com)                                      {OneWaySMS, TwoWayVoiceMobile}

[KeithB@WoodGroveOnline.com](mailto:KeithB@WoodGroveOnline.com)                                      {OneWaySMS, TwoWayVoiceMobile}

[NitikaG@WoodGroveOnline.com](mailto:NitikaG@WoodGroveOnline.com)                                     {OneWaySMS, TwoWayVoiceMobile}

[RobD@WoodGroveOnline.com](mailto:RobD@WoodGroveOnline.com)                                        {OneWaySMS, TwoWayVoiceMobile, PhoneAppOTP, PhoneApp...

[mwahl@woodgroveonline.com](mailto:mwahl@woodgroveonline.com)                                       {OneWaySMS, TwoWayVoiceMobile}

[AudreyO@WoodGroveOnline.com](mailto:AudreyO@WoodGroveOnline.com)                                     {OneWaySMS, TwoWayVoiceMobile, PhoneAppOTP, PhoneApp...

[SaratS@WoodGroveOnline.com](mailto:SaratS@WoodGroveOnline.com)                                      {OneWaySMS, TwoWayVoiceMobile}

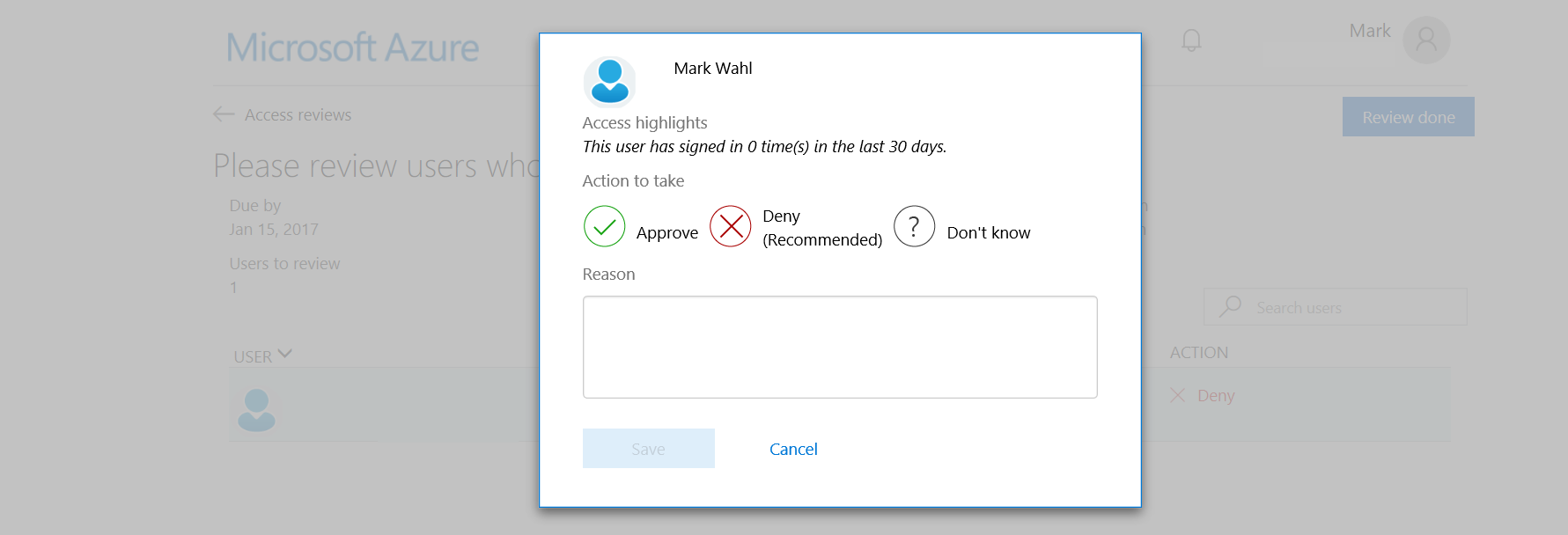
1. **Reset the MFA method for a specific user**

You can then use that UserPrincipalName to run the reset command to require the B2B user to set proof-up methods again. **Example:**

Reset-MsolStrongAuthenticationMethodByUpn -UserPrincipalName   
gsamoogle\_gmail.com#EXT#@ WoodGroveAzureAD.onmicrosoft.com

# Access Reviews

Our future updates to Azure AD, currently in private preview, expand the controls available for managing the lifecycle of guest user access, with additional access reviews features.   Access review enable an organization to ensure that there is regular oversight and sign off o access rights in Azure AD.  Today, Azure AD PIM leverages access reviews for oversight into users who are assigned access to Azure AD roles.  In the future, an organization leveraging B2B will be able to also create access reviews of guests who are members of a group, and access reviews of guests who are assigned access to an application.  In these planned access review scenarios, the organization’s administrators will be able to select a designated set of reviewers, who will be notified to review and confirm that the users who currently have access to a resource should continue to do so.  Additionally, the administrators will also be able to ask the members of the group, or users who are assigned access to an app, to self-review to their own access rights.   The denied members can be removed from the groups or application access, and the results of these reviews can then be archived for subsequent audit investigations.



# Policy & Governance

There are three key features for Policy and Governance:

1. MFA: Link to MFA section
2. Who can invite B2B users? Link to section
3. Access Reviews: Link to Access Reviews

# B2B User Tokens

If you’re interested in knowing what the token looks like for a B2B user, here are the bearer token details and token content for AAD Guest and MSA Guest in the resource tenant (tenantid:04dcc6ab-388a-4559-b527-fbec656300ea).

You can use <https://jwt.io/> or <http://calebb.net/> to see the JWT token contents.

**AAD Guest**

|  |
| --- |
| **Authorization: Bearer** eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ilk0dWVLMm9hSU5RaVFiNVlFQlNZVnlEY3BBVSIsImtpZCI6Ilk0dWVLMm9hSU5RaVFiNVlFQlNZVnlEY3BBVSJ9..Vllr1hGXpBlpXDBKRHHYbMr\_1\_DwKNY3eCObBOfEaxJirwqujqCZodPrAkIOJlFYyhkILyHZQUi\_D1w7XoPsd6U4GQlgOoFfzbye-P\_NdRFabHMlv32gCgHz1xo11aPP453EiwwG5OHnWaHYLBpuqi3sNeKx06xbTFj07HmADDaR4aM0jwy031d6GkD0LdU-Xkazi5-h8parVRLOkkLZA0oxMFoxl\_-VHr1hOzxCkbWgRoug4t97161i5tGil99CcpJ6NK8uQld7TveC40sjJ735Sksn-Uq\_NZcJuXCEVsH0xK5evaeFBFSEqACXjKTvYkJWtAx8Kr8yWZAcEg0YMQ |

|  |
| --- |
| **cid:image001.png@01D271D3.9B9ECF00** |

**MSA Guest**

|  |
| --- |
| **Authorization: Bearer** eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Ilk0dWVLMm9hSU5RaVFiNVlFQlNZVnlEY3BBVSIsImtpZCI6Ilk0dWVLMm9hSU5RaVFiNVlFQlNZVnlEY3BBVSJ9..LSIBlJpElXpsGXOGaFINW-jOBHsI0Dxe3oX-YIEsccegDCspl6UnRjpwzs0nBL09B4N0oqLd7ZwXZAQURpgaAFnWvROxkIGpNTE\_ppSKU1suud8keG5VnTEu82em95G1\_c\_eW1nOemPvbADCC8h08p2wxNm8QyEhmYqauN6qYbeqOnioRERXO3zOPg8nSXFcGPhvumJ\_BW8XKnW4zLdhK78c3PgynPnwtIm08SksMRDzGMgUc9RK1bpPQtgX8iFQByEljf5cuE\_h\_e1Nr5Y4StrhS3JCiQLTYZ727YY-lSm5DERiQrt7MkP5BHprEmSByofSvACj5TmVdqBFUjobuA |

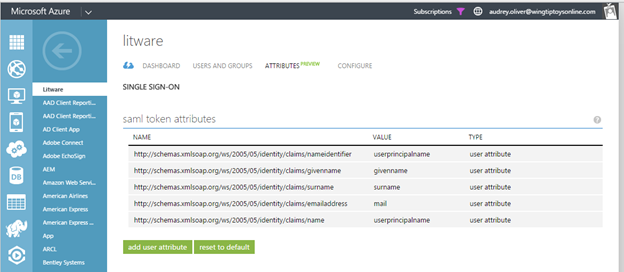
|  |
| --- |
| **cid:image003.png@01D271D3.9B9ECF00** |

# B2B User Claims Mapping

Azure AD supports customizing the claims issued in the SAML token for B2B users.

When a user authenticates to the application, Azure AD will issue a SAML token to the app that contains information (or claims) about the user that uniquely identifies them. By default, this includes the user's username, email address, first name, and last name.

You can view or edit the claims sent in the SAML token to the application under the **Attributes** tab.



There are two possible reasons why you might need to edit the claims issued in the SAML token:

1. The application has been written to require a different set of claim URIs or claim values
2. Your application has been deployed in a way that requires the NameIdentifier claim to be something other than the username (AKA user principal name) stored in Azure Active Directory.

For information on how to add and edit claims for these scenarios, check out this [article on claims customization](http://go.microsoft.com/fwlink/?LinkId=615928&clcid=0x409).

Note that for B2B users, for security reasons, mapping of NameID and UPN cross-tenant are prevented.

# O365 External Sharing

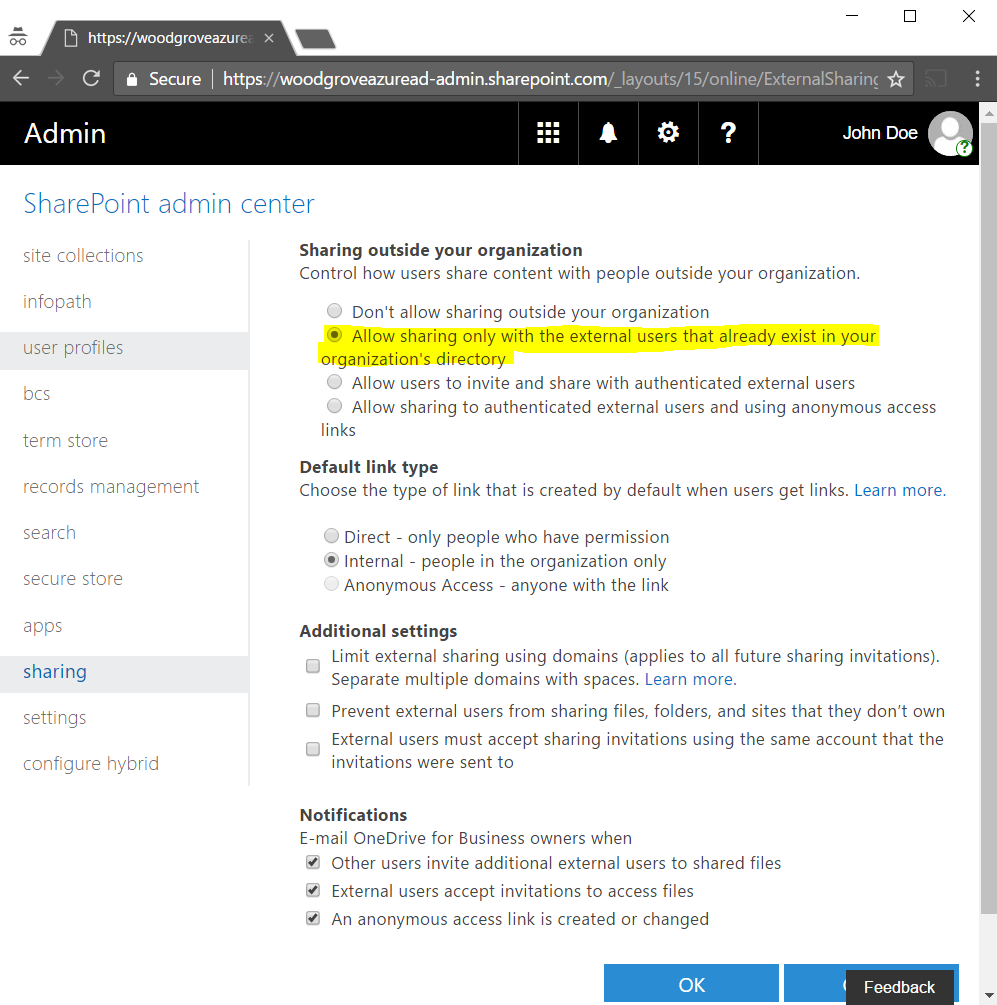
External sharing in Office365 (OneDrive, SharePoint Online, Unified Groups, etc.) and using Azure AD B2B are technically the same thing.

All of external sharing, (except OneDrive/ SharePoint Online), including Guests in Unified Groups is already using the Azure AD B2B Invitation Manager APIs for sharing.

OneDrive/ SharePoint Online (ODSP) has a separate invitation manager – because the ODSP support for external sharing started before it was inherently supported as part of the Azure AD fabric. Over time ODSP external sharing has accrued several features and many million users that use the product’s in-built sharing pattern. We are working with ODSP to onboard to the Azure AD B2B Invitation Manager APIs (referred to in this documentation), to unify all end to end benefits and accrue to them all the innovations in experiences that Azure AD is making.

In the meantime, there are some subtle differences between how ODSP external sharing works and how Azure AD B2B works:

1. ODSP adds the user to the directory after the user has redeemed their invitation. So, till such time that the user has not redeemed, you won’t actually see the user in Azure AD portal. When a user is invited from another site in the meantime, a new invitation is generated. However, with Azure AD B2B, we add the user immediately on invitation so he shows up everywhere.
2. The redemption experience in ODSP looks different from that of Azure AD B2B.
3. However, when the user has redeemed the invitation they look alike.
4. Azure AD B2B invited users can be picked from ODSP sharing dialogs. ODSP invited users also show up in Azure AD after they have redeemed their invitation.
5. An excellent, seamless way to use external sharing in ODSP together with Azure AD B2B in a managed, admin controlled way would be to set the ODSP external sharing setting to “Only allow sharing with external users already in the directory” (the setting below) – so that users can go to “Externally shared” sites and pick from external collaborators the admin has added. The admin can add the external collaborators through the Azure AD B2B Invitation Manager APIs.



# B2B and B2C

|  |  |
| --- | --- |
| **Azure AD B2B Collaboration**  **(Partnerships and relationships with any organization on the planet with any identity)** | **Azure AD B2C**  **(Organizational and individual customer facing applications with any customer on the planet with any identity)** |
| **What is it for?** | |
| Providing access to organizational data, resources and applications to **partner organizations and collaborators.** | **Consumer facing** mobile & web apps that reach out to the customers and citizens. |
| **Security, Policy and Compliance** | |
| Offer the same level of **enterprise grade security** to partners and collaborators as you would to your employees. Conditional Access, Identity protection, etc. | Depends on the application, but usually **lighter weight security**, focused on increasing consumer confidence in the application. |
| **Relationship** **Lifecycle** | |
| Owned by your **organization’s IT** | **Self-Serve** or managed by the application. |
| **Branding** | |
| **Organizational branding** – host organization’s brand for resources, home organization’s brand for identity. | **Product branded**, organization fades into the background. |
| **Which directory are the external users in?** | |
| **Organizational** directory | **Application** directory |
| **Marketing, Business Development, Behavior analysis, retention** | |
| Not intended for partnerships. Usage reporting is interesting for B2B. | Marketing to customers, retaining them etc. are key here. |

# Configuring SAS apps for B2B

Azure AD B2B works with most applications that integrate with Azure AD. In this section, we’ll walk through instructions on how to configure some popular SAS apps for use with Azure AD B2B.

Before we look at application specific instructions, here are some rules of thumb to remember:

1. Remember that for most of the applications, user provision needs to happen manually ( i.e. users have to be created manually in application as well)
2. For apps that support automatic provisioning (like Dropbox), there will be separate invitations created from applications. User need to make sure to accept them
3. In User Attributes: always set User Identifier to user.mail ( to mitigate issues with mangled upn in guest users)

## DropBox for Business

For users to be able to sign in using their organization account, Dropbox for Business must be manually configured to use your Azure Active Directory as a SAML identity provider. Dropbox for Business cannot prompt or otherwise allow users to sign in using Azure Active Directory if it has not been configured to do so.

1. Add DropBox for Business application in in the AAD as shown in the screenshot:

Machine generated alternative text:
Microsoft Azure 
ravikirannetylive (Default Directory) > Enterprise applications > Categories > Add an application 
ravikirannetyli... 
Active 
Search (Ctrl+/) 
O Overview 
Quick start 
MANAGE 
Users and groups 
Enterprise applications 
App registrations 
Azure AD Connect 
Domain names 
Mobility (MOM and MAM) 
Password reset 
Company branding 
Enterprise applications 
- Actiw - PREVIEW 
Search (Ctrl+/) 
O Overview 
MANAGE 
All applications 
Application proxy 
onditional access 
Sign-ins 
Audit logs 
+ Add 
Total Apps 
Top 3 Applications 
App usage between 12/24" 
25 
AZURE a_ASSK PORTAL 
SIGN-INS 

Machine generated alternative text:
Add an application 
PREVIEW 
Search thousands of pre-configured applications, or add your own. 
dropboxl 
I applications matched "dropbox•. Choose one below or add your own application. 
Dropbox for Business 
Collaboration 

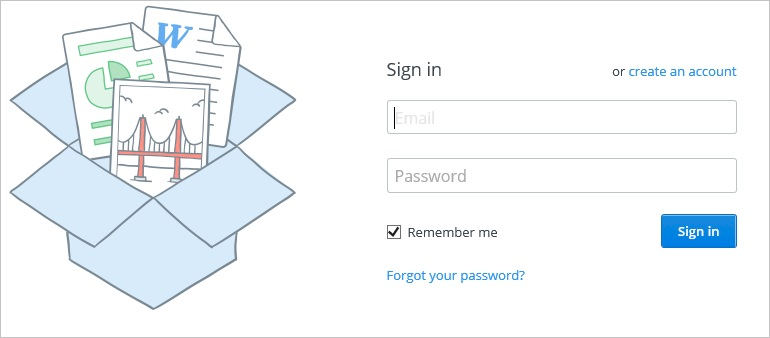
1. Configure the application:

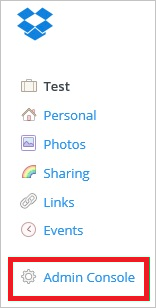
Machine generated alternative text:
DropBox1 - Single sign-on 
Applicaton - PREVIEW 
Search (Ctrl+/) 
O Overview 
Quick start 
MANAGE 
Properti es 
RR Users and græps 
Single sign-on 
Provisioning 
C' Self-service 
O Conditional access 
Permissions 
Sign-ins 
Audit logs 
Save X Discard 
Mode SAM L-based Sign-on 
Federated single sign-on enables rich and secure authentication to applications using the SAML 
protocol. Follow the steps below to connect Salesforce to Azure AD using SAML 
DropBox1 Domain and URLs 
Input the URLs and other details about your Drop80xI tenant into Azure AD. 
* Sign on URL O https://mvw.dropbox.com/sso/3438145437 
Identifier O 
Show advanced URL settings 
user Attributes 
Edit the user information sent in the SAML token when user sign in to DropBoxI 
user Identifier O user.mail 
and edit all other user attributes 
SAML Signing Certificate 
Manage the certificate used by Azure AD to sign SAML tokens issued to Dropaoxl. 
STATUS 
Active 
EXPIRATION 
1/19/2019 
THUMBPRINT 
D714B3DCC4CF64A86E68705C41EICEA1813FE... 
DOWNLOAD 
Certificate (8ase64) 
Create new certificate 

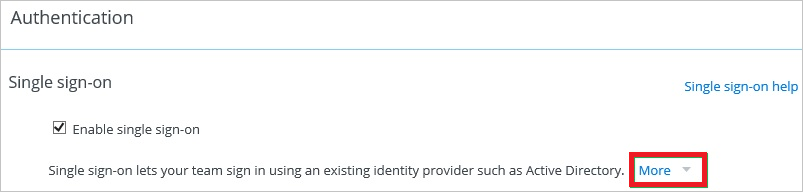
1. Select single sign-on configuration and change user identifier to user.mail (it’s UPN by default)
2. Download the certificate to use in DropBox configuration

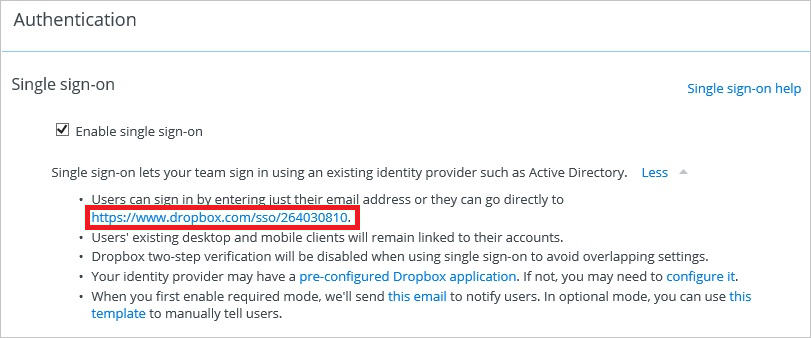
Machine generated alternative text:
user Attributes 
Edit the user information sent in the SAML token when user sign in to DropBoxI 
User Identifier O 
user.mail 
and edit all other user attributes 
SAML Signing Certificate 
Manage the certificate used by Azure AD to sign SAML tokens issued to Dropaoxl. 
STATUS 
Active 
EXPIRATION 
1/19/2019 
THUMBPRINT 
D714B3DCC4CF64A86E68705C41EICEA1813FE... 
ravikiran.nety@live.com 
DOWNLOAD 
Certificate (8ase64) 
Create new certificate 
* Notification Email O 
DropBox1 Configuration 
Drop80xI must be configured to use Azure AD as a SAML identity provider. Click below to view 
instructions on how to do this. 
Configure Drop80x1 
Review the process for configuring SAML identity providers in Dropbox for Business. To 
determine the correct process, View the documentation for Dropbox for Business or contact 
your Dropbox for Business representative for more information. 
2. Note: Some guidance on how to configure Dropbox for Business can be found on 
Azure.com, and we are in the process of migrating the application-specific steps to this guide. 
The older article on how to configure Dropbox for Business can be found here, where only 
the steps related to uploading the Azure AD files and URLs to Dropbox for Business need to 
be followed. 
3 During this process, you will be pmmpted to provide files and URLs that correspond to Azure 
Active Directory. When prompted, use the files and URLs shown below. 
o SAML Single Sign-On Service URL: https://login.microsoftonline.com 
/e64ac786-965b-4ebf-8e75-1addbf9543e7/sam12 
o SAML Entity ID: https://sts.windows.net/e64ac786-965b-4ebf-8e75-Iaddbf9543e7/ 
o Sign-Out URL: https://login.microsoftonline.com/common 
o SAML Signing Certificate 
- 8ase64 encoded 
o SAML Signing Certificate - 
Raw 
o SAML XML Metadata 
4. Once this information has been provided and configured in Dropbox for Business, Dropbox 
for Business will begin to require or otherwise allow users to sign in using your instance of 
Azure Active Directory. 
Next steps 
To ensure users can sign-in to Dropbox for Business after it has been configured to use Azure Active 
Directory, review the following tasks and topics: 

1. Use configure DropBox option ( the process described is explained in detail with screenshots below)
2. Get the SAML single sign on URL to be used in config
3. Get the sign-on URL from the DropBox config page:

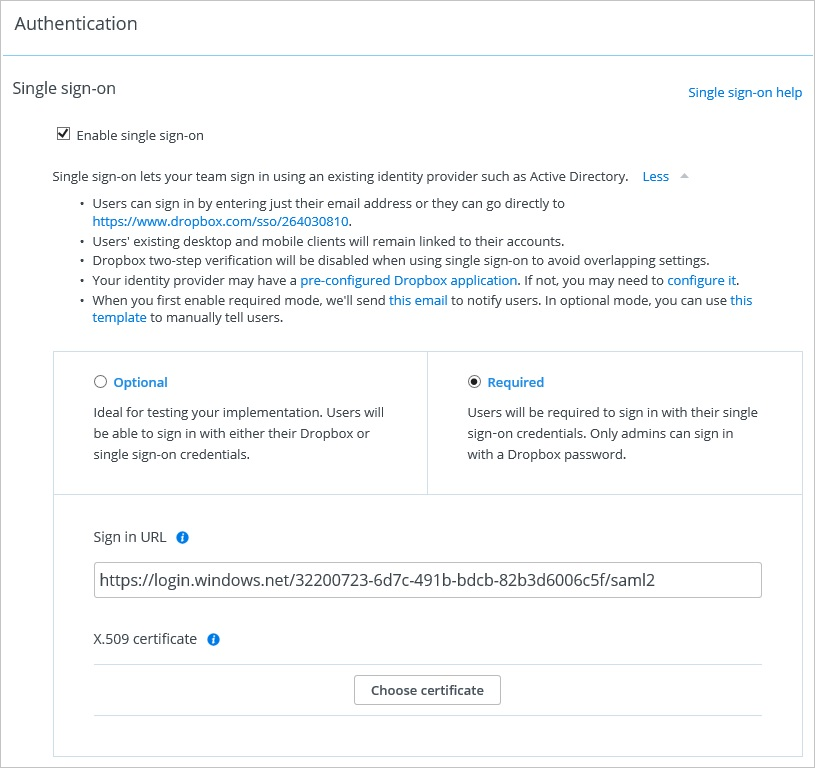








1. Upload certificate & paste SAML single sign on URL here



1. Configure automatic user-provision in portal:

Machine generated alternative text:
DropBox1 - Provisioning 
Applicaton - PREVIEW 
Search (Ctrl+/) 
O Overview 
Quick start 
MANAGE 
Properti es 
RR Users and græps 
Single sign-on 
Provisioning 
C' Self-service 
O Conditional access 
Permissions 
Sign-ins 
Audit logs 
Save X Discard 
Provisioning Mode Automatic 
use Azure AD to manage the creation and synchronization of user accounts in DropBoxI based on 
user and group assignment. 
Admin Credentials 
Azure AD needs authorization to connect to Drop80xI 's API and synchronize user data. 
Test Connection 
Notification Email O ravikiran.nety@live.com 
Send an email notification when a failure occurs 
Mappings 
Mappings allow you to define how data should flow between Azure Active Directory and Dropbox. 
Synchronize Azure Active Directory Users to Dropbox 
Restore default mappings 
Settings 
Start and stop provisioning to Drop80xI, and view provisioning status. 
Provisioning Status O 
Clear current state and restart synchronization 
Synchronization Details 
Summary 
We have synchronized 7 object(s) of type User to user. 
Synchronization was last run on Mon Jan 23 2017 09:23:37 GMT-0800 (Pacific Standard Time) 
Most recent full synchronization was completed Mon Jan 23 2017 09:23:37 GMT-0800 (Pacific 
Standard Time) 
We completed the first full synchronization on Tue Jan 17 2017 20:00:05 GMT-0800 (Pacific Standard 

1. Once provisioned in the DropBox application, the guest/member user will get a separate invite from DropBox. The invitees must accept it by clicking the link, to SSO into DropBox.

## Box

The objective of this section is to outline how to enable users to authenticate Guest user to Box with their account in Azure AD using federation based on the SAML protocol. As part of this procedure, you are required to upload metadata to Box.com.

1. Add Box from the enterprise applications
2. Configure single sign-on

Machine generated alternative text:
box256 - Single sign-on 
Applicaton - PREVIEW 
Search (Ctrl+/) 
O Overview 
Quick start 
MANAGE 
Properti es 
RR Users and græps 
Single sign-on 
Provisioning 
C' Self-service 
O Conditional access 
Permissions 
Sign-ins 
Audit logs 
R save X 
Discard 
Mode SAM L-based Sign-on 
Federated single sign-on enables rich and secure authentication to applications using the SAML 
protocol. Follow the steps below to connect Salesforce to Azure AD using SAML 
box256 Domain and URLs 
Input the URLs and other details about your box256 tenant into Azure AD. 
* Sign on U RL O https://B28demo.box.com 
* Identifier O 
https://828demo.box.com 
Show advanced URL settings 
user Attributes 
Edit the user information sent in the SAML token when user sign in to box256. 
user Identifier user. mail 
and edit all other user attributes 
SAML Signing Certificate 
No certificates have been configured yet. 
Create new certificate 
* Notification Email O 
ravikiran.nety@live.com 
box256 Configuration 
box256 must be configured to use Azure AD as a SAML identity provider. Click below to view 
instructions on how to do this. 
Configure box256 

1. First, ensure that the Sign-on URL is set appropriately for Box in the Azure management portal. This is the URL of your Box.com tenant and should follow the format: https://.box.com.
2. The Identifier is not applicable for this application but still shows as mandatory field, just be aware of that fact.
3. User identifier to user.mail ( to make sure SSO for guest accounts)
4. Create new SAML certificate
5. To begin configuring your Box.com tenant to use Azure Active Directory as an identity provider, start by downloading the following metadata file, and saving it locally on your computer: Download metadata file ( make sure to make it active)
6. Forward that metadata file to Box support team. The support team configures single sign-on for you.
7. Set-up for automatic user provisioning

box256 - Provisioning 
Applicaton - PREVIEW 
Search (Ctrl+/) 
O Overview 
Quick start 
MANAGE 
Properti es 
RR Users and græps 
Single sign-on 
Provisioning 
C' Self-service 
O Conditional access 
Permissions 
- Mozilla Firefox 
R save 
Discard 
Provisioning Mode Automatic 
use Azure AD to manage the creation and synchronization of user accounts in box256 based on user 
and group assignment. 
Admin Credentials 
Azure AD needs authonzation to connect to box256•s API and synchronize user data. 
Aut horize 
Admin Username O 
* Admin Password 
* appkey 
Test Connection 
Notification Email O 
Send an email notification when a failure occurs 
co https%3a%2f%2fportal.azurE 
box 
Log in to grant access to Box 
ravikiran_nety@gmail.com 
Authorize 

1. Invitees must redeem invitation from the Box application.

# Code & Script Samples

## Code Sample

In this sample, you’ll see how to call the invitation API, in App only mode, to get the redemption URL for the resource to which you are inviting the B2B user and not send the generic B2B invitation email. Then you’ll see how the email can be composed with an http client, so you can completely customize how it looks and sent through Graph API.

namespace SampleInviteApp

{

    using System.Globalization;

    using System;

    using System.Net;

    using System.Collections.Generic;

    using System.Linq;

    using System.Net.Http;

    using System.Net.Http.Headers;

    using System.Text;

    using System.Threading.Tasks;

    using Microsoft.Graph;

    using Microsoft.IdentityModel.Clients.ActiveDirectory;

    using Newtonsoft.Json;

    class Program

    {

        /// <summary>

        ///  Authentication endpoint to get token.

        /// </summary>

        static readonly string EstsLoginEndpoint = "<https://login.microsoftonline.com>";

        /// <summary>

        /// Initialize this to Tenant you want to invite users to.

        /// </summary>

        private static readonly string TenantID = "";

        /// <summary>

        /// Client id of the app.

        /// </summary>

        private static readonly string TestAppClientId = "";

        /// <summary>

        /// Client secret of the app.

        /// </summary>

        private static readonly string TestAppClientSecret = @"";

        /// <summary>

        /// Admin user principal name

        /// </summary>

        private static readonly string InviterUserPrincipalName = "";

        static void Main(string[] args)

        {

            CreateInvitation();

        }

        private static void CreateInvitation()

        {

            string accessToken = null;

            string GraphResource = string.Format("https://{0}", "graph.microsoft.com");

            // Get the token for our app to talk to graph.

            try

            {

                AuthenticationContext testAuthContext = new AuthenticationContext(string.Format("{0}/{1}", EstsLoginEndpoint, TenantID));

                AuthenticationResult testAuthResult = testAuthContext.AcquireToken(

                    GraphResource,

                    new ClientCredential(TestAppClientId, TestAppClientSecret));;

                accessToken = testAuthResult.AccessToken;

            }

            catch (AdalException ex)

            {

                Console.WriteLine("An exception was thrown: {0}.", ex);

                throw;

            }

            // setup http client.

            HttpClient httpClient = new HttpClient();

            httpClient.Timeout = TimeSpan.FromSeconds(300);

            httpClient.DefaultRequestHeaders.Authorization = new AuthenticationHeaderValue("Bearer", accessToken);

            httpClient.DefaultRequestHeaders.Add("client-request-id", Guid.NewGuid().ToString());

            Console.WriteLine("CorrelationID for the request: {0}", httpClient.DefaultRequestHeaders.GetValues("client-request-id").Single());

            var inviteEndPoint = string.Format("<https://graph.microsoft.com/beta/invitations>");

            // Set the invitation object.

            Invitation invitation = new Invitation();

            invitation.InvitedUserDisplayName = "displayName";

            invitation.InvitedUserEmailAddress = "Give the invitee email";

            invitation.InviteRedirectUrl = "<https://www.microsoft.com>";

            invitation.SendInvitationMessage = false;

            // Make the invite call. Your app needs to have User.ReadWrite.All or Directory.ReadWrite.All scope to invite

            HttpContent content = new StringContent(JsonConvert.SerializeObject(invitation));

            content.Headers.Add("ContentType", "application/json");

            var postResponse = httpClient.PostAsync(inviteEndPoint, content).Result;

            string serverResponse = postResponse.Content.ReadAsStringAsync().Result;

            Console.WriteLine(serverResponse);

            // Build the mail message. Here we are including the server response from inviation request, but you can customize it.

            // To send the email you need Mail.Send scope.

            var emailEndPoint = string.Format("[https://graph.microsoft.com/beta/users/{0}/sendMail](https://graph.microsoft.com/beta/users/%7b0%7d/sendMail)", InviterUserPrincipalName);

            Email mail = new Email();

            mail.message = new Message();

            mail.message.Subject = "Inviation Email";

            mail.message.Body = new ItemBody();

            mail.message.Body.Content = serverResponse;

            Recipient recipient = new Recipient();

            recipient.EmailAddress = new EmailAddress();

            recipient.EmailAddress.Address = invitation.InvitedUserEmailAddress;

            mail.recipients = new List<Recipient>();

            mail.recipients.Add(recipient);

           // Make the call to send email.

            content = new StringContent(JsonConvert.SerializeObject(mail));

            Console.WriteLine(content);

            content.Headers.Add("ContentType", "application/json");

            postResponse = httpClient.PostAsync(emailEndPoint, content).Result;

            serverResponse = postResponse.Content.ReadAsStringAsync().Result;

            Console.WriteLine(serverResponse);

        }

        /// <summary>

        /// Invitation class.

        /// </summary>

        public class Invitation

        {

            /// <summary>

            /// Gets or sets display name.

            /// </summary>

            public string InvitedUserDisplayName { get; set; }

            /// <summary>

            /// Gets or sets display name.

            /// </summary>

            public string InvitedUserEmailAddress { get; set; }

            /// <summary>

            /// Gets or sets a value indicating whether Invitation Manager should send the email to InvitedUser.

            /// </summary>

            public bool SendInvitationMessage { get; set; }

            /// <summary>

            /// Gets or sets invitation redirect URL

            /// </summary>

            public string InviteRedirectUrl { get; set; }

        }

        /// <summary>

        /// The email message.

        /// </summary>

        public class Email

        {

            public Message message;

            public List<Recipient> recipients;

        }

    }

}

## PowerShell Example

The following example will walk you through how you can bulk invite external users to an organization from email addresses that you may have stored in a CSV file.

1. **Prepare your CSV file**

Create a new CSV file and name it “invitations.csv”. In this example, the file is saved in C:\data.

Your CSV file could look like the following:

|  |
| --- |
| InvitedUserEmailAddress |
| [user1@contoso.com](mailto:user1@contoso.com) |
| [user2@outlook.com](mailto:user2@outlook.com) |
| [user3@gmail.com](mailto:user3@gmail.com) |
| [user4@yahoo.com](mailto:user4@yahoo.com) |

1. **Get Azure AD PowerShell V2**

To use the new cmdlet, you need to install the Azure AD PowerShell V2 module, which you can get from here: <https://www.powershellgallery.com/packages/AzureADPreview>

1. **Login to your tenancy**

Connect-AzureAd and login

1. **Run the PowerShell cmdlt**

$Invitations = import-csv C:\data\invitations.csv

foreach ($email in $invitations) {New-AzureADMSInvitation -InvitedUserEmailAddress $email.InvitedUserEmailAddress -InviteRedirectUrl <http://google.com> -SendInvitationMessage $true}

This will send an invitation to the email address in invitations.csv.

Additional features of the cmdlet include customized text in the email message, include a display name for the invited user, sending messages to CCs or suppressing email messages altogether.

# Current Limitations

1. **Azure AD Invitaion APIs are in Beta**

That API surface is the direction forward however like all beta, it’s subject to the [beta namespace contract](https://blogs.msdn.microsoft.com/aadgraphteam/2015/04/09/graph-api-versioning-and-the-new-beta-version/).  We will move the API to a numbered version with our GA release.

1. **Possibility of double MFA if your partner already has an MFA policy in place**

Azure AD B2B MFA will be performed and managed at the inviting organization. This is a desirable pattern since it covers all identities and allows you to have control over the authentication strength of your B2B invitees. However, if you have a partner who already has MFA set up and enforces it, their users may have to perform MFA once in their home organization and then again in your organization. In future releases, we will be introducing a policy where you can choose to trust certain partners’ MFA to avoid the double MFA issue.

1. **Instant ON**

In the Azure AD B2B flows, we add users to the directory and dynamically update them during invitation redemption, app assignment etc. The updates and writes generally happen in one directory instance and has to be replicated across all the instances – we have observed that in some cases, the finite amount of time it can take to complete replication can result in issues that manifest as authorization issues. We are working hard to minimize/eliminate this set of issues before General Availability. In the meantime, this shouldn’t be an issue you hit, but if you do, refreshing or retrying will generally help.

# Licensing guidance

Azure Active Directory (AD) B2B collaboration extends a select set of existing Azure AD features to guest users invited into the Azure AD tenant. Hence, Azure AD B2B collaboration guest users will be licensed through Azure AD licenses, and align with the existing Free, Basic, and Premium P1/P2 license tiers as seen here: <https://azure.microsoft.com/en-us/pricing/details/active-directory/>.

There is no charge for inviting B2B users and assigning them to an application in Azure AD. Also, up to 10 apps per guest user and 3 basic reports are also free for B2B users, since they are part of Azure AD 'Free' tier.

Any paid Azure AD features, extended to B2B users via B2B collaboration functionality, 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 B2B 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 B2B users invited to the tenant.

Licensing examples:

* + A customer wants to invite 100 B2B users to its Azure AD tenant, and will use Group based access management and provisioning for all users, but 50 of those users will also be requiring MFA and conditional access. The customer here must purchase 10 Azure AD Basic licenses, and 10 Azure AD Premium P1 licenses to cover all their B2B users correctly. Similarly, if an inviting tenant plans to use Identity Protection features with B2B users, then it must have enough Azure AD Premium P2 licenses to cover all these B2B users in the 5:1 ratio.
  + A customer has 10 employees who are all currently licensed with Azure AD Premium P1. They now want to invite 60 B2B users, who will all require MFA. Per the 5:1 licensing rule, the customer must have at least 12 Azure AD Premium P1 licenses to cover all 60 B2B users. Since they already have 10 Premium P1 licenses for their 10 employees, they already have rights to invite 50 B2B users with Premium P1 features like MFA. So in this example, they need to purchase 2 additional Premium P1 licenses to cover the remaining 10 B2B users.

Note that there is no facility or need to assign licenses to the B2B users to enable these B2B collaboration user rights. Customer that owns the inviting tenant, will need to determine how many B2B users need paid Azure AD capabilities and depending on whether they are Basic, Premium P1, or Premium P2 level features, customers must have the sufficient number of the appropriate Azure AD paid licenses to cover their B2B users in the 5:1 ratio. If a company needs additional B2B user rights, they need to buy the necessary Azure AD paid licenses.

**Salient points:**

1. B2B collaboration can provide different capabilities to B2B users based on the existing model of Azure AD editions
2. Every Azure AD paid license will include rights to 5 “B2B users” (5:1 model)
3. There is no need to, actually, assign licenses to B2B user accounts, there will be automatic calculation and reporting.
4. Every invited user gets the rights that the Azure AD Free edition offers if no paid Azure AD license exists in the tenant
5. If a B2B user has a paid Azure AD license as an employee from his organization, he will not consume one of the B2B licenses of the inviting tenant.

# Troubleshooting B2B issues

## I can’t create an external user due to an existing Contact:

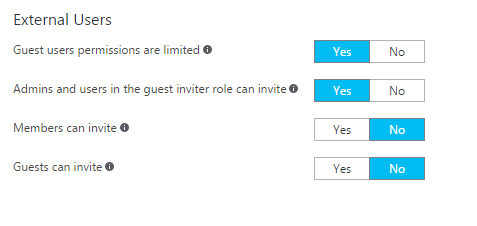
If the external user you are inviting already has a pre-existing contact object, you will be unable to invite that user until you resolve the conflict, usually by removing the Contact object.

Until General Availability, the conflict must be resolved manually.

## I’ve added an external user but do not see them in my Global Address book or in the People Picker

In cases where external users are not populated in the list, the object may take a few minutes to replicate.

## Invitations have been disabled for directory

If you receive an error message indicating that you do not have permissions to invite users, verify that your user account is authorized to invite external users. This can be done under User Settings: 

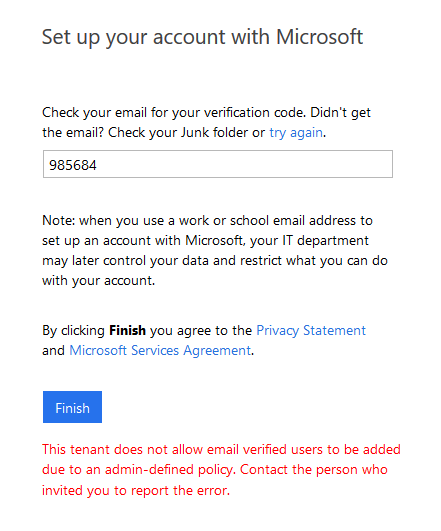
If you have recently modified these settings or assigned the Guest Inviter role to a user, there may be a 15-60 minute delay before the changes take effect.

## The user that I invited is receiving an error during redemption:

Common errors include:

### Invitee’s Admin has disallowed EmailVerified Users from being created in their tenant:

When inviting users whose organization is utilizing Azure Active Directory where the specific user’s account does not exist (User does not exist in AAD contoso.com). The administrator of contoso.com may have a policy in place preventing users from being created. The External User must check with their admin to determine if external users are allowed, the external user’s admin may need to allow Email Verified users in their domain (see this [article](https://docs.microsoft.com/en-us/powershell/msonline/v1/set-msolcompanysettings#parameters) on allowing EmailVerified Users)



### External User does not exist already in Federated Domain

In cases where the external user is using a Federation solution where authentication is being performed on-premises and does not already exist in Azure Active Directory, the user cannot be invited.

To resolve this issue, the external user’s admin must synchronize the user’s account to their Azure Active Directory.

## How does ‘#’ which is normally an invalid character sync with Azure AD?

“#” is a reserved character in UPNs for Azure AD B2B or external users (i.e. [user@contoso.com](mailto:user@contoso.com) invited, becomes [user\_contoso.com#EXT@fabrikam.onmicrosoft.com](mailto:user_contoso.com#EXT@fabrikam.onmicrosoft.com)) so # in UPNs coming from on-premises are not allowed to login to the Azure portal.

## I receive an error when adding External users to a Synchronized Group

External Users can only be added to “assigned” or “Security” groups and not groups that are mastered on-premises.

## My External User did not receive an email to redeem

The invitee should check with their ISP or spam filter to ensure that the following address is allowed: [Invites@microsoft.com](mailto:Invites@microsoft.com)

## My Invitee received multiple emails from me

In some cases, where the Invited user has multiple aliases for their account, they may receive 2 invitations. In these cases, the first link redeemed would be the account that gets created, the 2nd redemption link would be invalid.

# Q&A

## Is this functionality available in the classic portal?

All of the new exciting capabilities in the Azure AD B2B Public Preview Refresh are available through the [new Azure portal](https://blogs.technet.microsoft.com/enterprisemobility/2016/09/12/the-azuread-admin-experience-in-the-new-azure-portal-is-now-in-public-preview/) – <https://portal.azure.com> and the [new Access Panel](https://blogs.technet.microsoft.com/enterprisemobility/2016/11/28/new-azuread-access-panel-is-now-generally-available/). We couldn’t be more excited to have you try these new experiences. We know you’ll like it!

## Can B2B users access SharePoint Online and OneDrive?

Absolutely! These Guest users are in the directory. You can add them to Groups that you can permission OD or SPO sites to, or even directly pick them from the SPO people picker. Since these are Guest users, the SPO sites need to have external sharing enabled.

## Is the CSV upload mechanism still supported?

Yes! Refer to the PowerShell sample we have included.

## How can I customize my invitation emails?

You can customize almost anything about the inviter process using the B2B invitation APIs.

## Can the invited external user leave the organization to which he was invited?

This is currently not available in the Public Preview.

## Can I utilize my Microsoft Account (John@contosomicrosoftacct.com) to log into resources?

In the event, you have a non-standard Microsoft account suffix (@contoso.com) an Azure Active Directory will be created for your use. It is not possible during Public Preview to utilize your Microsoft Account.

## Now that MFA is available for Guest users, can they also reset their MFA method?

Yes, absolutely! Just the same way as regular users can.

## Which org is responsible for MFA licenses?

The inviting organization always steps in and performs MFA. Hence the inviting organization is responsible to make sure they have enough licenses for their B2B users who are performing MFA.

## What if my partner org already has MFA set up, can we trust their MFA and not use our MFA?

We will be supporting this in future releases, where you can select specific partners to exclude from the your (inviting org’s) MFA.

## How can I achieve delayed invitations?

We understand sometimes organizations want to be able to add B2B users, provision them to applications that require provisioning and then send the invitations out. If that is you, you can use the B2B Invitation API to customize the onboarding workflow in many powerful ways.

## Can guest users and contacts co-exist?

So, your organization has traditionally added contacts representing external collaborators so that they show up in the GAL and email address suggestions during email composition. And you’re wondering what happens when you now add these same collaborators as B2B users in the directory, right? We hear you, by the end of Q1 of 2017, B2B users and your contact objects will be able to co-exist in your company directory. Stay tuned for our announcements!

## Can I make my guest users limited admins?

Absolutely. If this is what your organization needs, refer to the “Adding Guest users to a Role” section.

## Does Azure AD B2B collaboration support permitting B2B users to access [**the Azure Portal**](https://portal.azure.com/)?

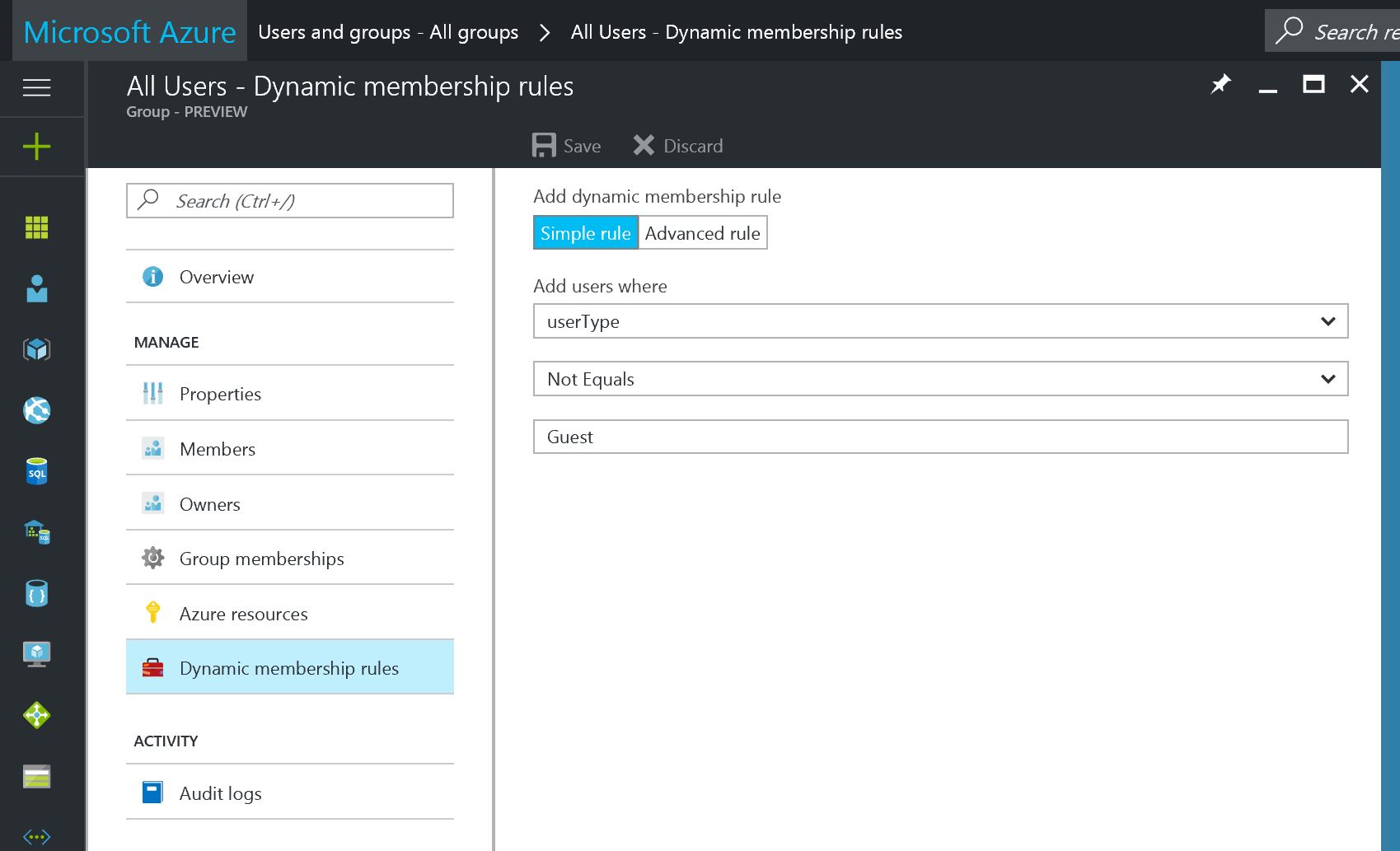
B2B users should not need to access the Azure Portal unless they are assigned a limited administrator or global administrator role. In this case, they can access the portal. If a guest user who is not in these roles accesses the portal, then he/she may be able to access certain parts of the experience because the Guest user role has certain permissions in the directory as described in previous sections.

## Can I block access to the Azure Portal for guest users?

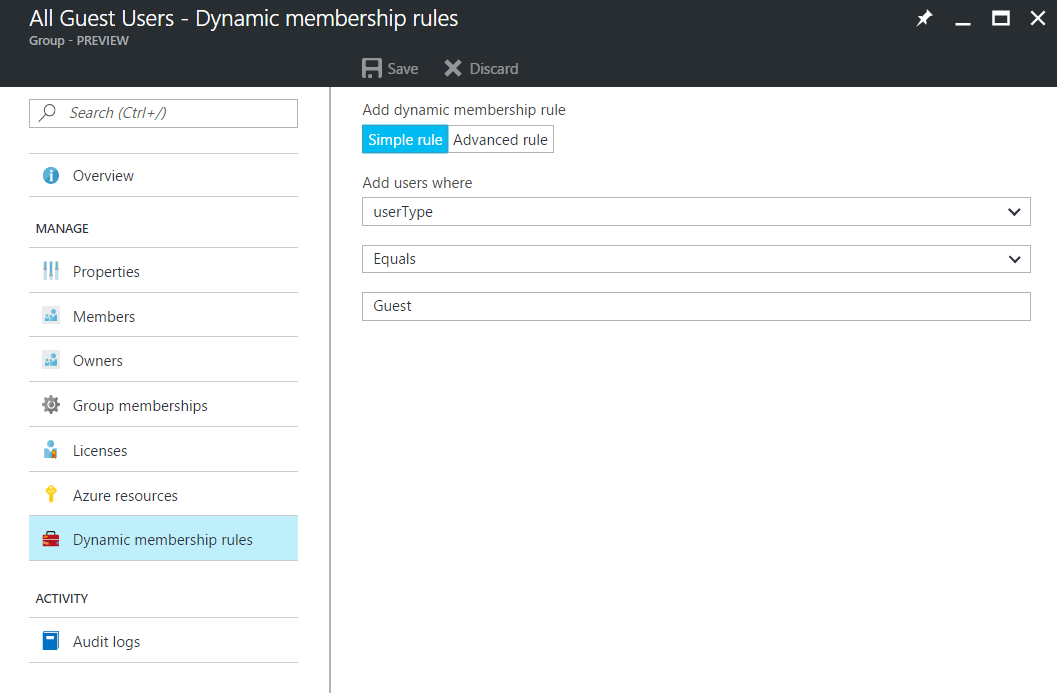
Yes! But be careful while configure this policy to avoid accidentally blocking access to members and admins.

You can block access to Azure Portal by guest users through conditional access policy on Windows Azure Service Management API through the following three steps.

1. Modify the “All Users” dynamic group to only contain Members



1. Create a dynamic group that contains Guest users



1. Set up a conditional Access Policy to block Guest users from accessing the portal

The animation below walks you through the stages.

**Include the animated gif from here inline:**

<https://microsoft.sharepoint.com/teams/activedirectory/Active%20Directory%20Doc%20Library/Forms/AllItems.aspx?id=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs%2F08_Block_Guests_from_Portal_Access%2Egif&parent=%2Fteams%2Factivedirectory%2FActive%20Directory%20Doc%20Library%2FScenario%20Tracking%2FB2B%2FAnnouncements%2C%20Blogs%20%26%20Documentation%2FDocumentation%2FPublic%20Preview%20Refresh%20Documentation%2FAnimated%20Gifs>

## What is the timeline by which Azure AD B2B will start support for MFA and consumer email accounts?

Both MFA and consumer email accounts are supported now.

## What is the GA timeline for Azure AD B2B?

This is the next stop in our journey. When we do this depends on the feedback that the current feature set receives from customers.

## Is there a plan to support password reset for Azure AD B2B users?

Yes, both of these are supported for B2B (guest) users.

## Is it also enabled for users in a viral tenant?

Not currently.

## Does CRM provide online support to Azure AD B2B?

CRM will provide support to Azure AD B2B after it is Generally Available.

## What is the lifetime of an initial password for a newly created B2B user?

Azure AD has a fixed set of character, password strength, and account lockout requirements that apply equally to all Azure AD cloud user accounts. Cloud user accounts are the accounts that are not federated with another IDP such as Microsoft Account, Facebook, ADFS, or even another cloud tenant (in the case of B2B). For federated account the password policy depends on the policy in the identity tenancy and the user’s Microsoft account settings.

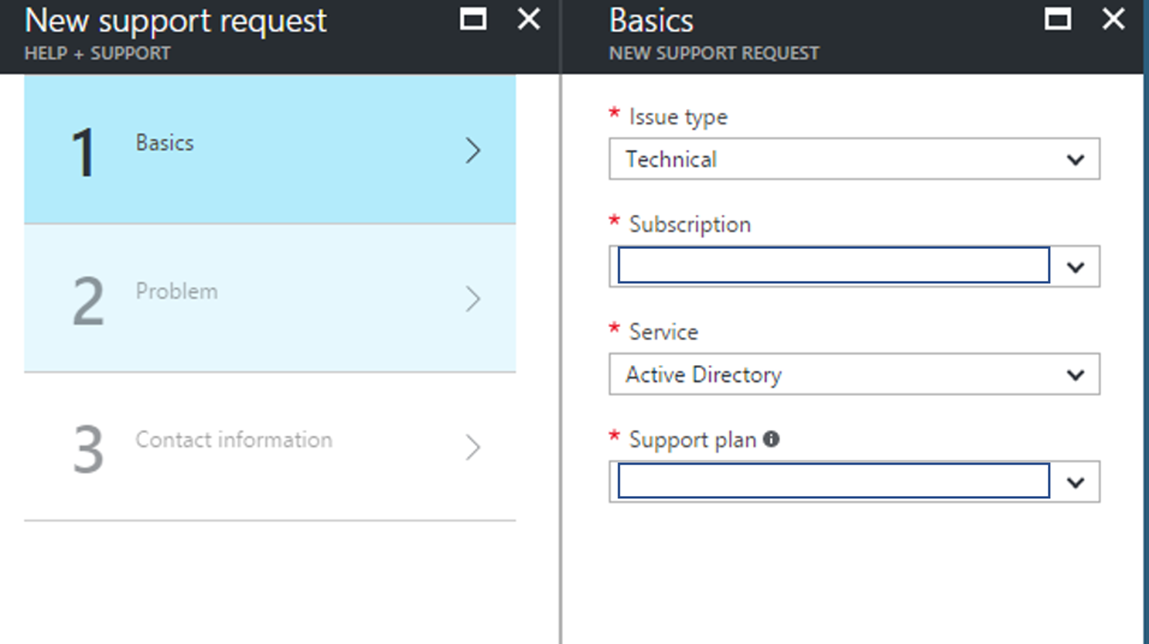
# Getting support for AzureAD B2B Collaboration

You’ve read through the documentation, you’ve done the right things, but still can’t get something to work?

**Open a Support Ticket (Requires Support plan):**

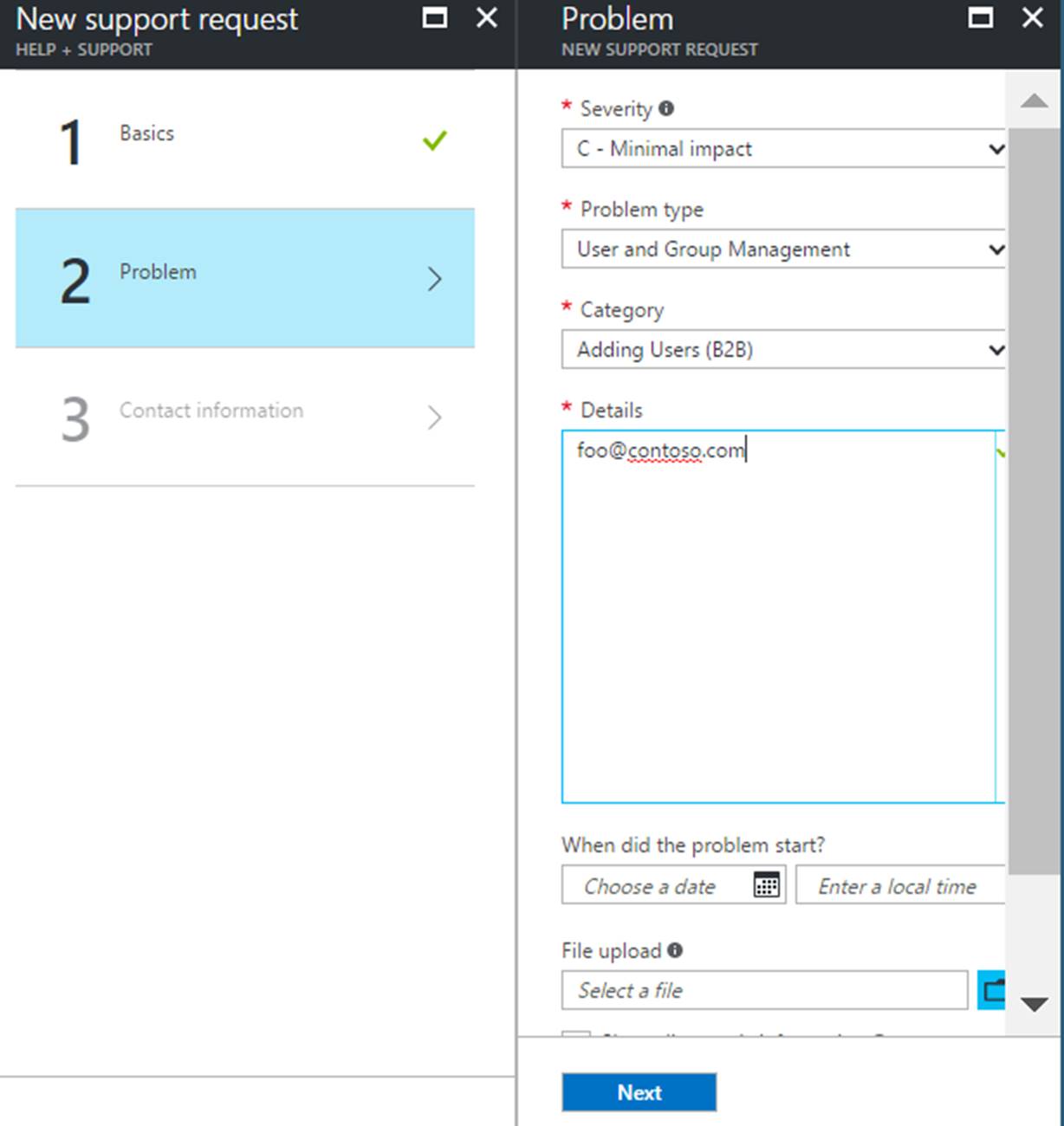
1. In the Azure Portal, navigate to the Help blade and select New Support Request:

* Issue type: Technical
* Subscription: Choose affected subscription
  + Service: Active Directory
  + Support Plan: Choose relevant Support plan



1. Describe your problem:

* **Choose the appropriate severity that reflects.**
* Choose Problem Type as **User and Group Management**
* Choose Category as **Adding Users ( B2B )**
* Include any error messages such as CorrelationID, affected users, etc.



Input your Contact Information and a support representative will contact you for further troubleshooting.

# More questions or feedback?

We love to hear from you!

If you have suggestions for future capabilities or suggestions for changes, [let us know on this forum](https://feedback.azure.com/forums/169401-azure-active-directory/category/165471-b2b)!

If you have questions that are not support related, let us know on the MSDN forum.

To get support, follow these instructions <link to the support section>.