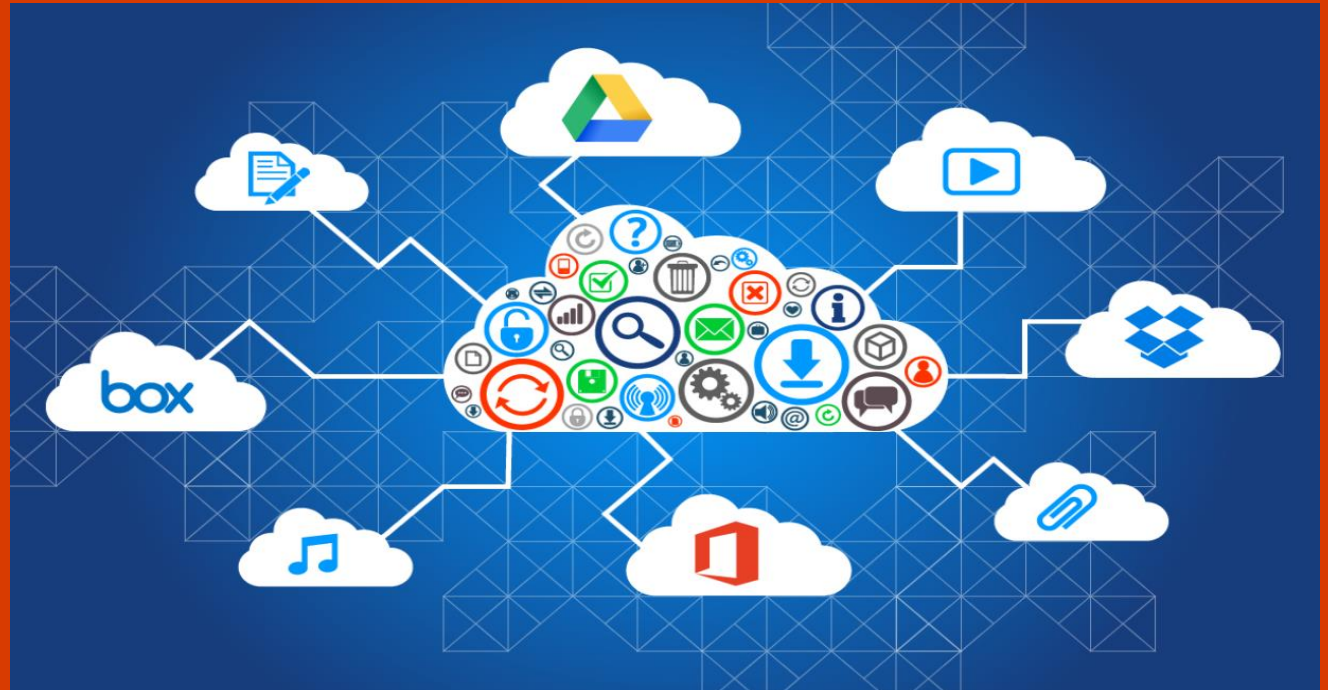


# M365 External Collaboration Scenarios & Controls

Scott McFadden  
MTC Boston  
Infrastructure &  
Security Architect







~~smcfadde@contoso~~@yahoo.com

## Review permissions



The organization NED.mtc-bos.com would like to:

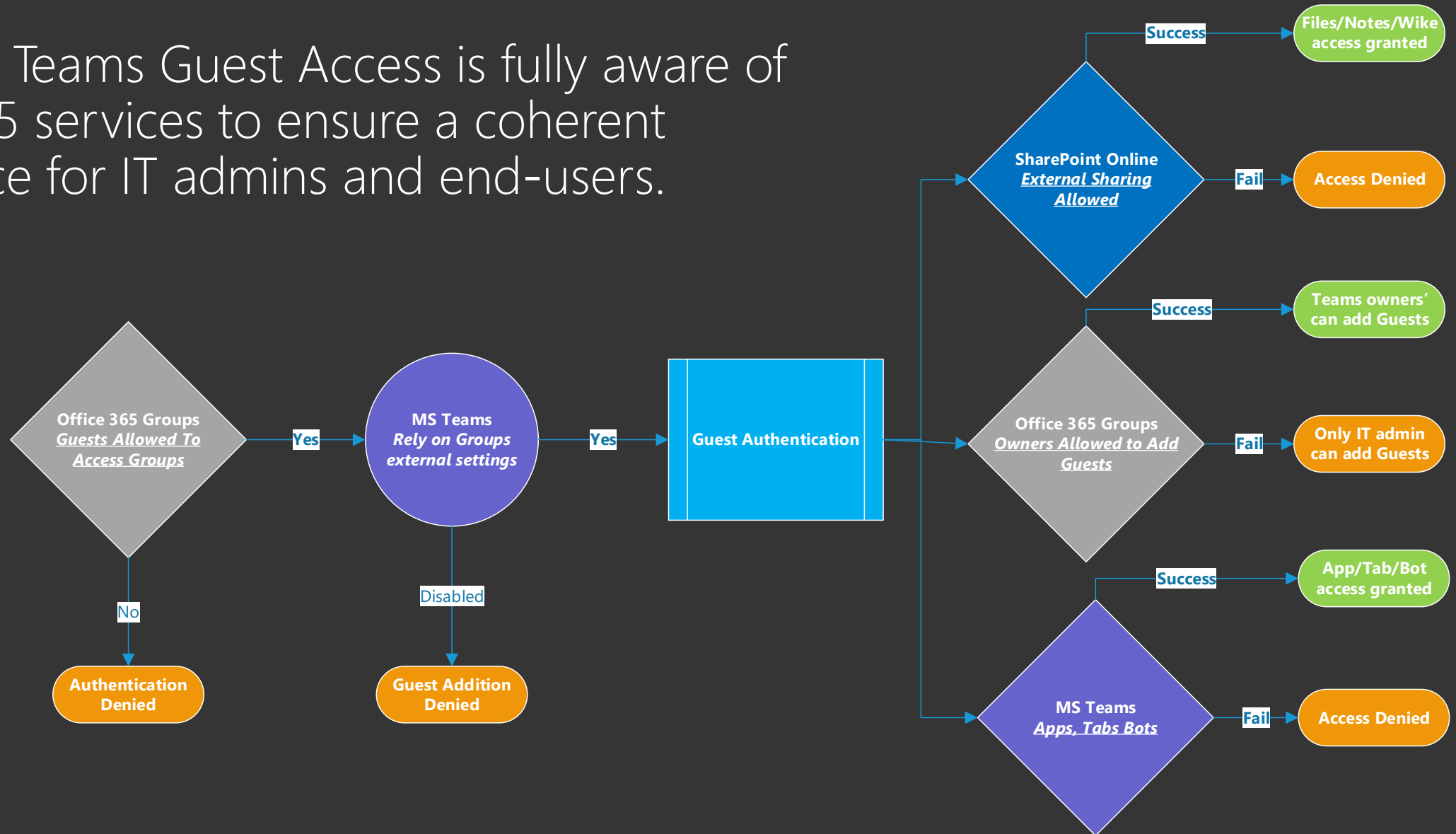
- ✓ Sign you in
- ✓ Read your name, email address, and photo

You should only accept if you trust NED.mtc-bos.com. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. Contact [smcfadde@microsoft.com](mailto:smcfadde@microsoft.com) regarding privacy. NED.mtc-bos.com may log information about your access. You can remove these permissions at <https://myapps.microsoft.com/mtcecbos3.onmicrosoft.com>.

Cancel Accept

# Teams B2B Controls with earlier Controls

Microsoft Teams Guest Access is fully aware of Office 365 services to ensure a coherent experience for IT admins and end-users.

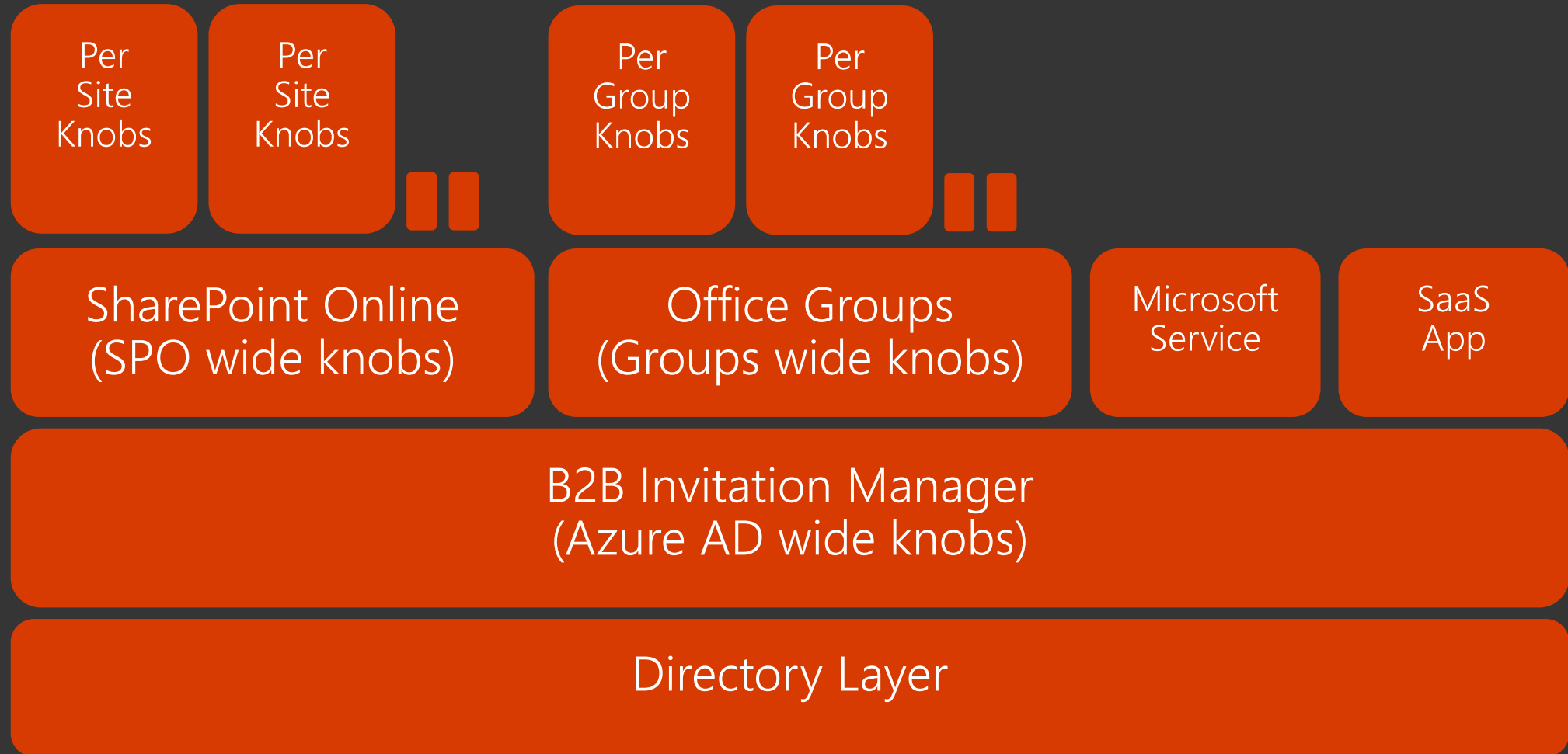




# B2B Basics

- A principal is always created in the inviter directory referring to the principals of the external identities. There are 2 parts to it:
- Invitation
- Redemption
  - For a reminder on how B2B works, check out: <https://aka.ms/b2bmechanics>

# B2B Control Layers



# Azure AD B2B Controls

Dashboard > NED.mtc-bos.com - User settings > External collaboration settings

## External collaboration settings

Save Discard

Guest users permissions are limited ⓘ

Yes  No

Admins and users in the guest inviter role can invite ⓘ

Yes  No

Members can invite ⓘ

Yes  No

Guests can invite ⓘ

Yes  No

Enable Email One-Time Passcode for guests (Preview) ⓘ

[Learn more](#)

Yes  No

### Collaboration restrictions

- Allow invitations to be sent to any domain (most inclusive)
- Deny invitations to the specified domains
- Allow invitations only to the specified domains (most restrictive)

Good. Otherwise Guests have the same directory access as members.

No means Guest Inviters cannot invite, but Global Admins can always invite.

Good for customers focused on collaboration. Can be secure with Access Reviews and Audit logs

Questionable security wise unless combined with other controls.

Restrict External Sharing to trusted domains

# New - Target Guest Users with Conditional Access

Dashboard > NED.mtc-bos.com > Conditional Access - Policies > CA AWS Example - MFA > Users and groups

## CA AWS Example - MFA

Info Delete

\* Name  
CA AWS Example - MFA

### Assignments

Users and groups  
Specific users included >

Cloud apps  
1 app included >

Conditions  
3 conditions selected >

### Access controls

Grant  
2 controls selected >

Session  
0 controls selected >

### Enable policy

On Off

Save

## Users and groups

Include Exclude

None  
 All users  
 Select users and groups

All guest users (preview) ⓘ  
 Directory roles (preview) ⓘ  
 Users and groups

Select >

AS az stack  
azstack@mtcecbos3.onmi... ⋮

CC Chase Carpenter ⋮

Done



# Office 365 Admin Portal B2B Controls

Office 365 Admin center

Home > Security & privacy

Tarek The Ac

Tarek&#39;s Test Tena

### Password policy

Set the password policy for all users in your organization.

Days before passwords expire	600
Days before a user is notified about expiration	30

### Customer Lockbox

Set requirements for data access

Require approval for all data access requests	Off
---	-----

### Sharing

Control access for people outside your organization.

Let users add new guests to the organization	On
--	----

[Edit](#)

### External users

Guest users permissions are limited ⓘ	Yes	No
Admins and users in the guest inviter role can invite ⓘ	Yes	No
Members can invite ⓘ	Yes	No
Guests can invite ⓘ	Yes	No

# Office 365 Groups Controls

Office 365 | Admin center

Home > **Services & add-ins**

[+ Upload Add-In](#) View: **All**

Name
<b>Mail</b> Set up auditing, track messages, and protect email from
<b>Microsoft Azure Information Protection</b> Update your settings for Microsoft Azure Information
<b>Microsoft Forms</b> Manage and update your Microsoft Forms settings
<b>Microsoft Teams</b> Manage and update your Microsoft Teams settings
<b>Office 365 Groups</b> Control Settings for Office 365 Groups
<b>Office Online</b> Let people use third-party hosted storage services

## Office 365 Groups

Let group members outside the organization access group content  On

If you turn this off, guests will still be listed as members of the group, but they won't receive group emails or be able to access any group content. They'll only be able to access individual group files that were directly shared with them. [Learn more about guest access to Office 365 groups.](#)

Let group owners add people outside the organization to groups  On

Even if you turn this off, guests who are already able to access group content. Guests who are already member of the group can still access group resources.

[Save](#) [Close](#)

If you turn these off for the whole tenant, you can turn them on per group. This article has the powershell cmdlets.

# SharePoint Online B2B Controls

Office 365 Admin Tarek The Admin

SharePoint admin center

- site collections
- infopath
- user profiles
- bcs
- term store
- records management
- search
- secure store
- apps
- sharing**
- settings
- configure hybrid
- device access

### Sharing outside your organization

Control how users share content with people outside your organization.

- Don't allow sharing outside your organization
- Allow sharing only with the external users that already exist in your organization's directory
- Allow users to invite and share with authenticated external users
- Allow sharing to authenticated external users and using anonymous access links
  - Anonymous access links expire in this many days:
  - Anonymous access links allow recipients to:
    - Files:
    - Folders:

### Who can share outside your organization

- Let only users in selected security groups share with authenticated external users and using anonymous links

### Default link type

Choose the type of link that is created by default when users get links. [Learn more.](#)

- Direct - only people who have permission
- Internal - people in the organization only
- Anonymous Access - anyone with the link

### Additional settings

- Limit external sharing using domains (applies to all future sharing invitations). Separate multiple domains with spaces. [Learn more.](#)
- Prevent external users from sharing files, folders, and sites that they don't own
- External users must accept sharing invitations using the same account that the invitations were sent to

When users share via anonymous access links, people who receive the link don't need to sign in to access the shared content. Therefore these additional settings don't apply to anonymous access links.

### Notifications

E-mail OneDrive for Business owners when

- Other users invite additional external users to shared files
- External users accept invitations to access files
- An anonymous access link is created or changed

Feedback

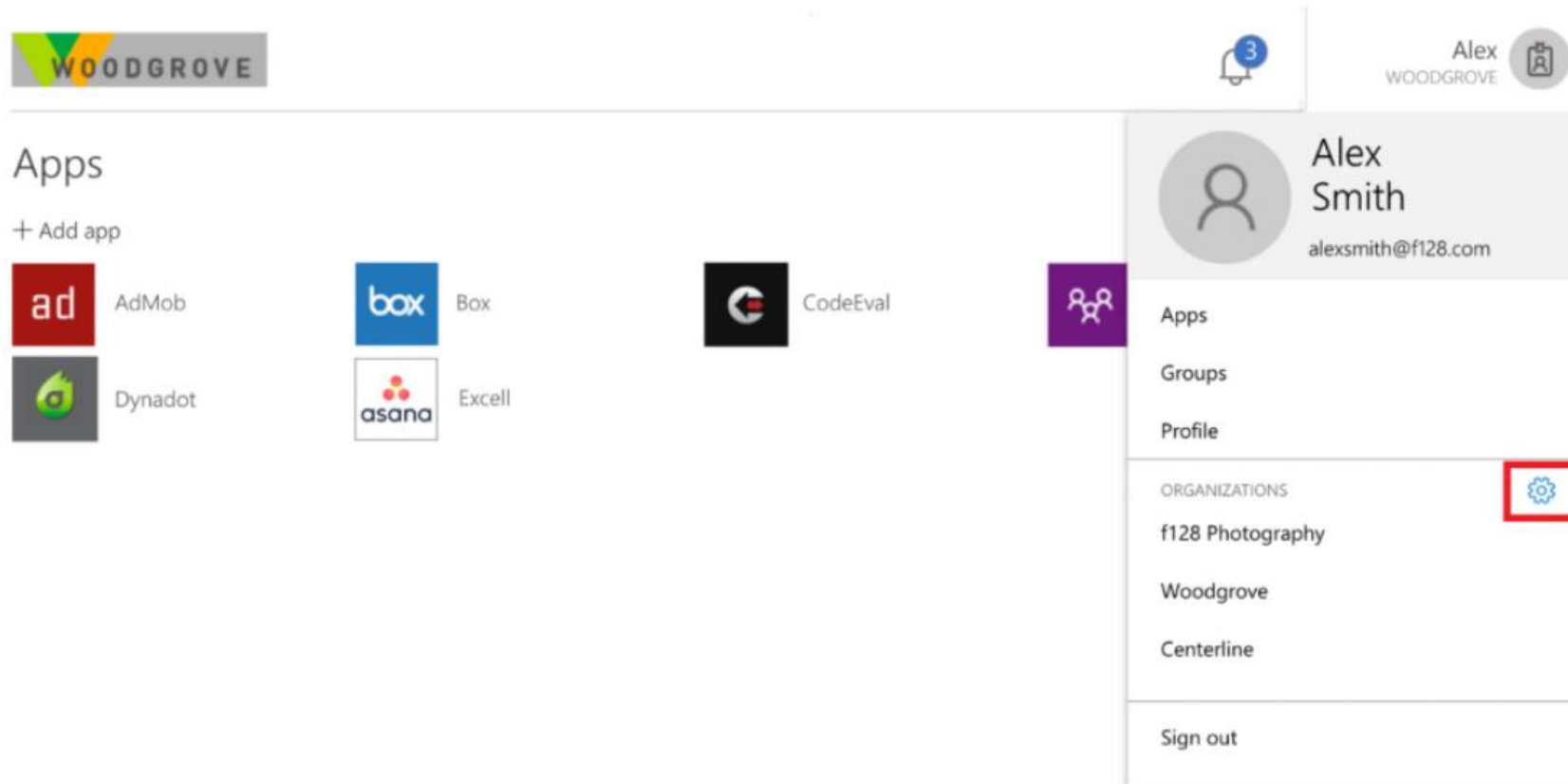
Good synergy with B2B invite solution

Good for highly collaborative customers

Golden Ticket Problem ;(

### 3. B2B users can self-service leaving the inviting organization

Finally, a B2B user can now easily leave an organization to which she has been invited, once her relationship with that organization has come to an end. It's no longer necessary to contact an admin of the inviting organization to have her account removed!



# Access Review for Your Guests

## Access reviews

×

<< **Getting started** [Learn more](#)

Quick start

**Access reviews**

- Overview
- Access reviews
- Programs
- Audit logs

**Terms of Use**

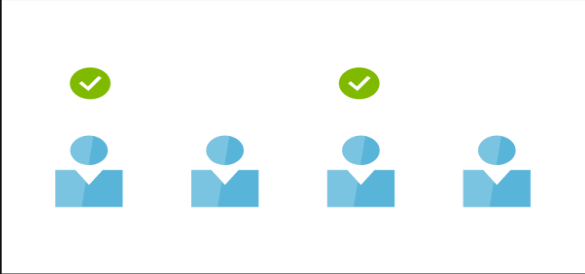
- Terms of use

**Troubleshooting + Support**

- Troubleshoot
- New support request

## Ensure the right people have the right access at the right time

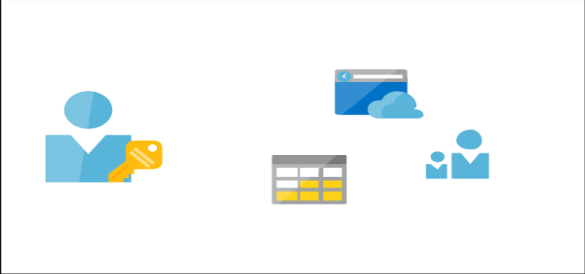
Azure AD Identity Governance allows you to protect, monitor, and audit access to critical assets while ensuring employee productivity



### Access Reviews

Azure AD Access Reviews enable organizations to recertify group memberships, application access, and privileged role assignments.

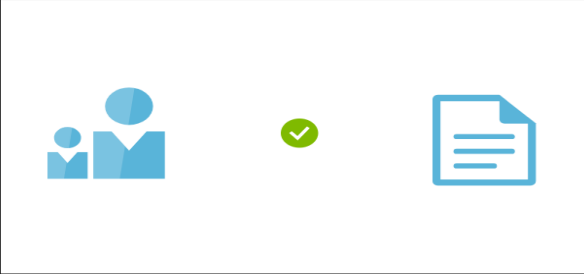
[Create an access review](#)



### Entitlement Management

Share your applications and services with guest users and external partners from any organization while maintaining control over your own corporate data.

[Learn more](#)



### Terms of Use

Azure AD Terms of use ensures users see relevant disclaimers for legal or compliance requirements.

[Publish a Terms of use](#)

# Tenant Trusts

## Admin consent for guest access

- *Private Preview*
- Similar to admin consent for apps
- Useful when there are large numbers of guests from a single partner or when a single organization has multiple directories

Home > WoodGrove > Organizational relationships - Consent options

### Organizational relationships - Consent options

WoodGrove - Azure Active Directory

Search (Ctrl+J)

Save Discard

#### Turn off Azure AD consent

The Azure AD consent screen will not be displayed to users from these specified directory IDs when they use your organization's resources. Admins from these directories will consent on behalf of their users. [Learn more](#)

Delete

NAME OF PARTNER ORGANIZATION	PARTNER'S DIRECTORY ID
Partner ABC	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

#### I consent on behalf of my users

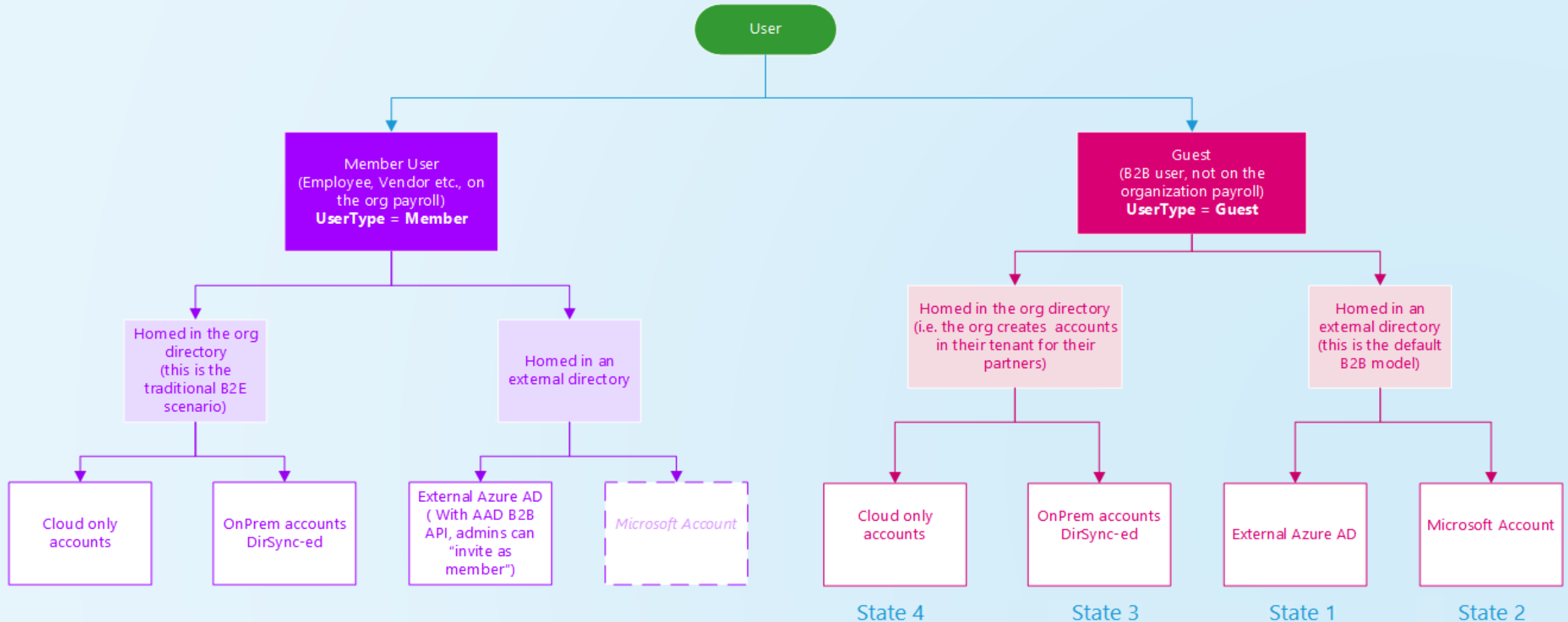
My users will not have to consent individually when using these organizations' resources. The admins from these organizations will turn off Azure AD Consent for my users. [Learn more](#)

Delete

NAME OF PARTNER ORGANIZATION	PARTNER'S DIRECTORY ID
Partner ABC	XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX



# AAD B2B Guest User Properties



# Audit B2B

This is now available in both PowerShell (<https://docs.microsoft.com/en-us/azure/active-directory/b2b/customize-invitation-api#invitation-status>) and Microsoft Graph (query for unredeemed users is <https://graph.microsoft.com/beta/users?filter=externalUserState eq 'PendingAcceptance'>). Try it out and let us know what you think!

# Resources

[Manage guest access in Office 365 Groups](#)

[Guest access in Office 365 groups](#)

[Guest access in Office 365 groups – Admin Help](#)

[Azure AD access reviews](#)

[Azure Active Directory Terms of Use feature](#)

[Google Federation](#)

[Authorize guest access in Microsoft Teams](#)

[Azure B2B – UserVoice Feedback](#)