
BIWUG
collabdays
Welcome
All

BIWUG

Guest account in Azure Active Directory

Tomislav Lulić
Microsoft MVP, MCT

collabdays

BIWUG

Do not forget sponsors

Platinum

Kianda

Microsoft

Gold

acolad. DIGITAL

AvePoint

inetum realdolmen Positive digital flow

ORDINA

pointfire Multilingual SharePoint

Quest

spikes

SysKit

The Flow

Xylos

Silver

advantive innovative people valuable solutions

CTG

Docubird™

European SharePoint Office 365 & Azure Conference

Community

EUROPEAN COLLABORATION SUMMIT

SharePint

ShareGate: by GSoft

Tomislav Lulić

World Bank Office in Croatia
IT analyst
Microsoft MVP, MCT

@tlulic
tlulic.wordpress.com
tomislav@tlulic.com
www.linkedin.com/tomislavlulic

Agenda

- Intro...
- Main issue with Guest user
- Mechanism for sharing in M365
- What is about and what we need for B2B - Guest acc
- Securing Guest account
- User concerns
- Procedure for accepting invitation
- Monitoring

About demo

- Tenanat Microsoft 365 E5
- One guest user is on
- Second we will prepare in demo
- MeganB – Global admin
- AdeleV – Guest inviter – add role and create invitation
- Group – Sales and Marketing… choosen one

Microsoft news

- **Microsoft Entra**
- **Microsoft Defender**
- **Microsoft Purview**
- **Microsoft Priva**
- **Microsoft Endpoint Manager**

- All identity and access capabilities
- Formerly Office 365 Security p.
- Formerly Compliance portal
- Privacy Risk Management
- Formely Intune

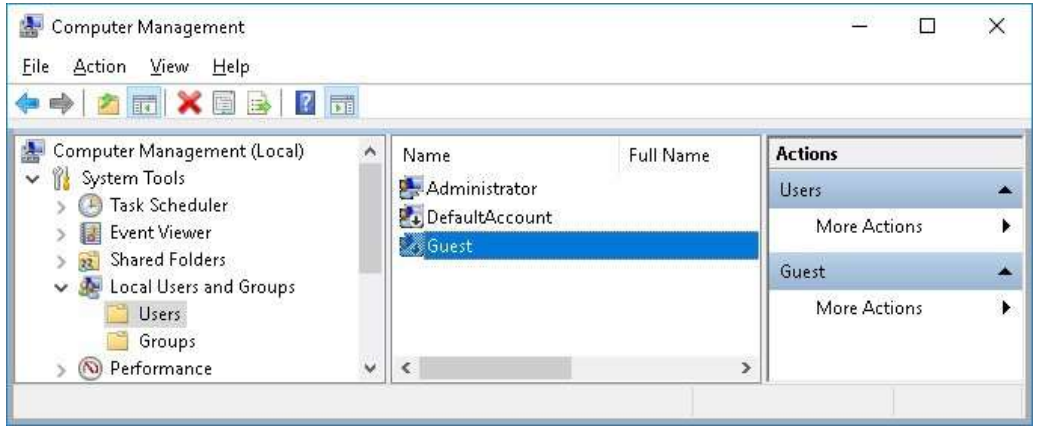
Back to past: on-premise

- Some of you remember guest account.
- One that allow access to shared resources if Everyone group is setup to this resource.

- One that you will see today is

not that kind!

- We are in Cloud ☺



What was main issue with Guest users

to enter your

- Open account inside your organization
- SecurID, Token, RSA token etc
- Access Sensitivity

Two mechanism for sharing in M365

External sharing:

- Sharing links to specific SharePoint and OneDrive assets with external parties

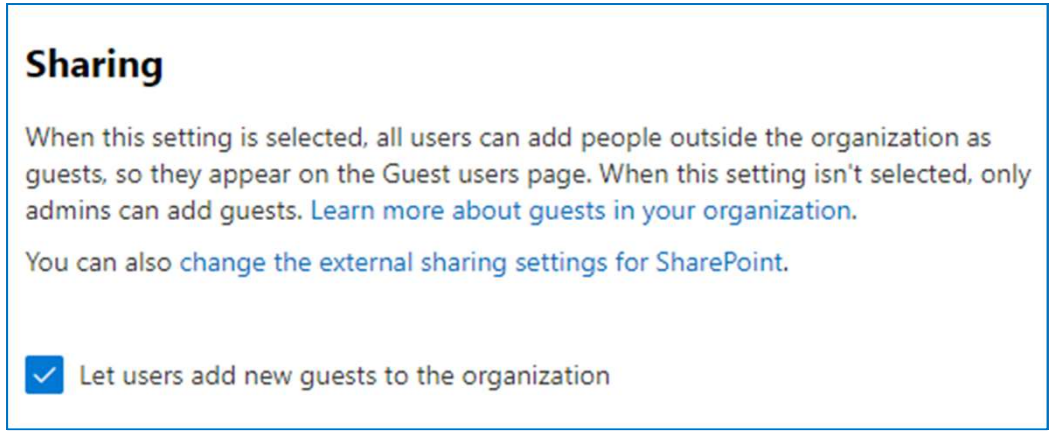
Guest access (B2B):

- Sharing content with guest members in Microsoft 365 groups or Microsoft Teams

Manage external collaboration in Microsoft 365

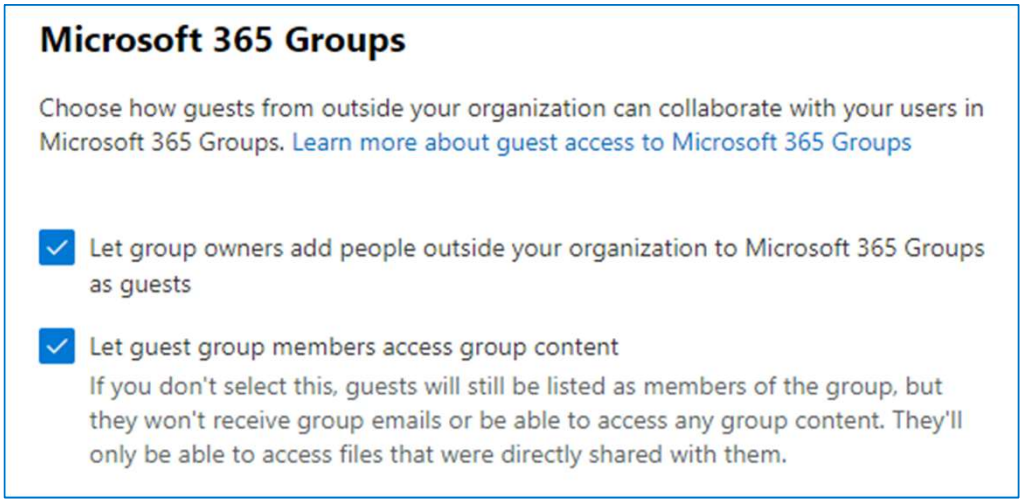
Sharing settings

Microsoft 365 admin center > Settings > Org Settings > Security & privacy tab > Sharing



Microsoft 365 Groups

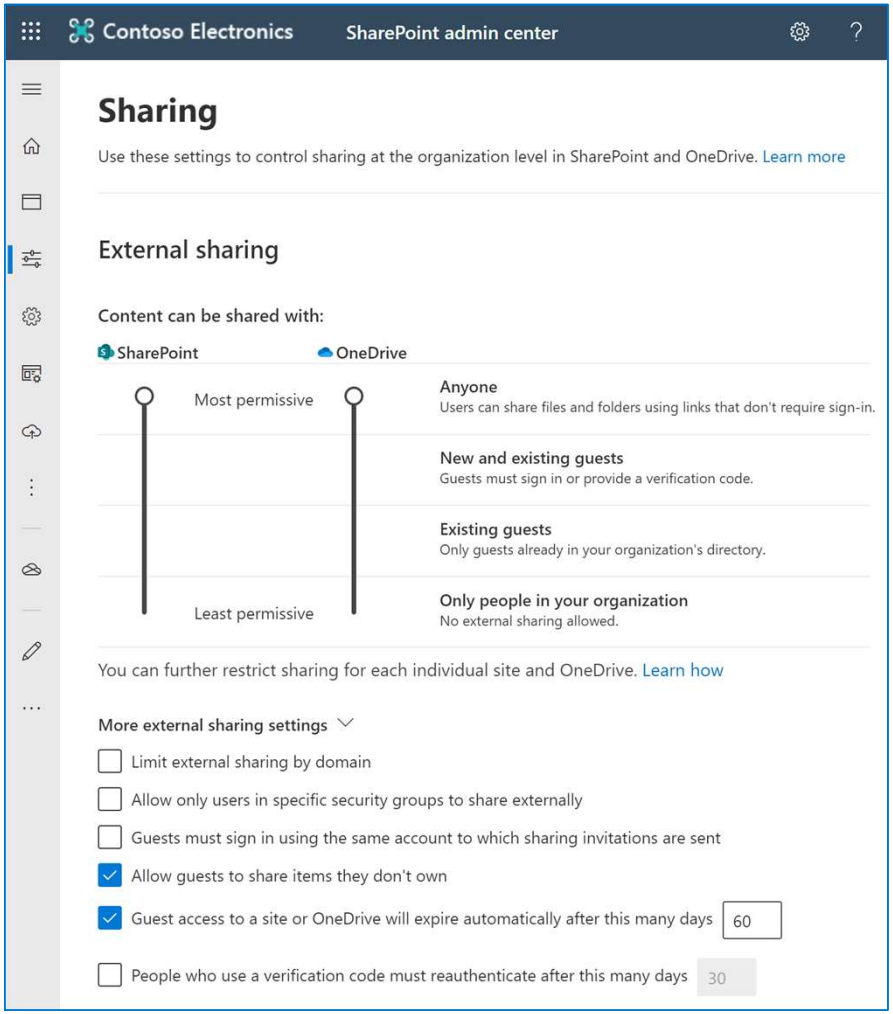
Microsoft 365 admin center > Settings > Org settings > Microsoft 365 Groups



Manage file sharing in SharePoint and OneDrive

Use SharePoint admin center

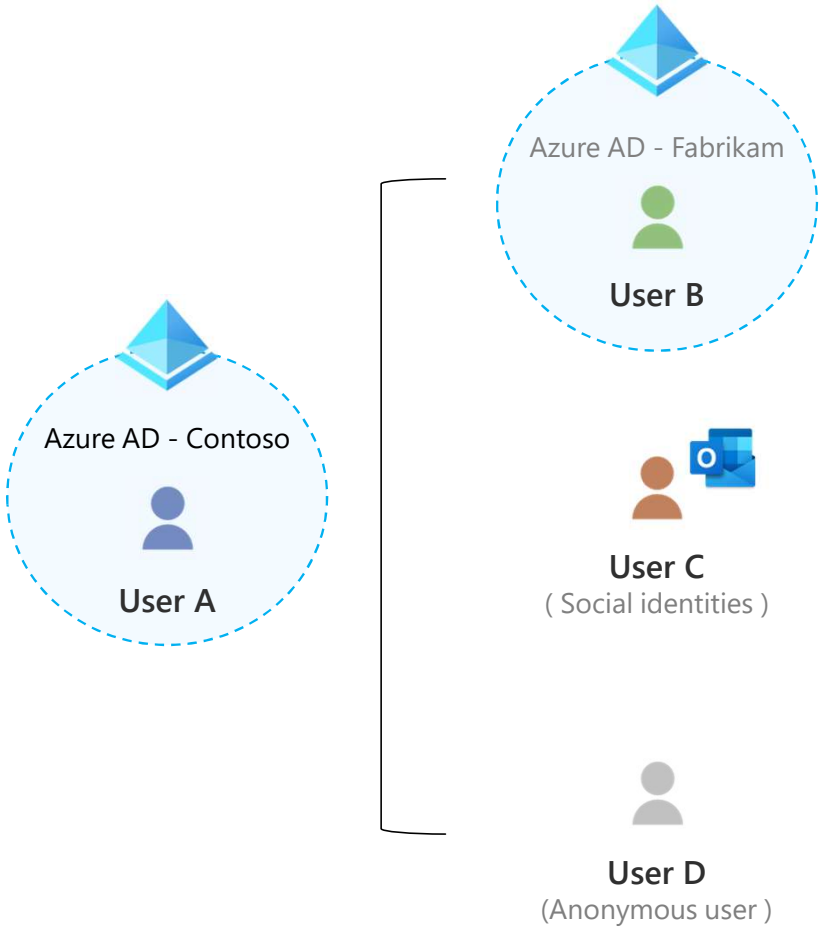
- **Policies > Sharing**
- OneDrive setting cannot be more permissive than the SharePoint setting
- External sharing and advanced settings
  - Anyone (includes anonymous users)
  - New and existing guests
  - Existing guests
  - Only people in your organization



Work with external users

Define external users

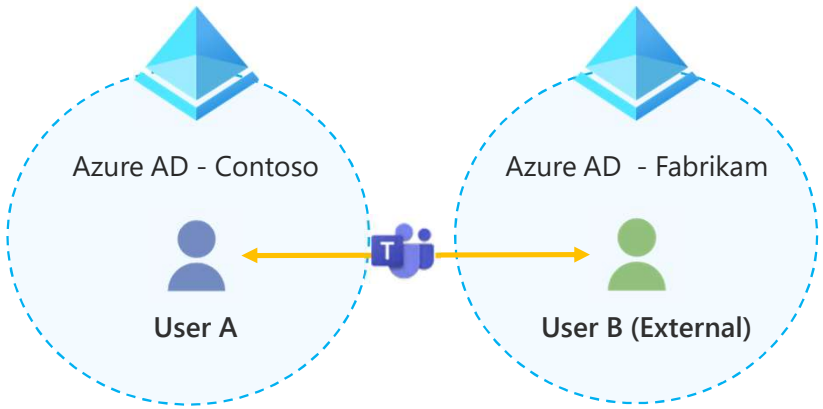
- **User A** : Member user in your organization
- **User B** : Business account (Azure AD account)
- **User C** : Consumer email account (with Outlook.com, Gmail.com, or others).
- **User D** : Anonymous user without authenticating



How it Works in Microsoft Teams

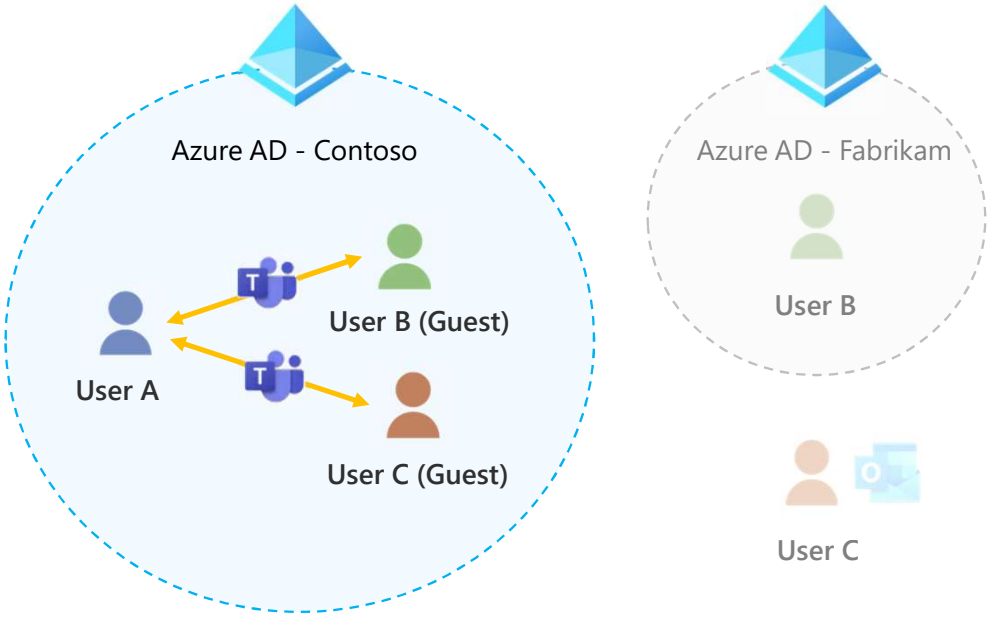
External access (federation)

- Enable access permission to an entire external **domain**
- Allow find, call, chat, and set up meetings



Guest access

- Gives access permission to an **individual**
- Allow chat, teams, channels

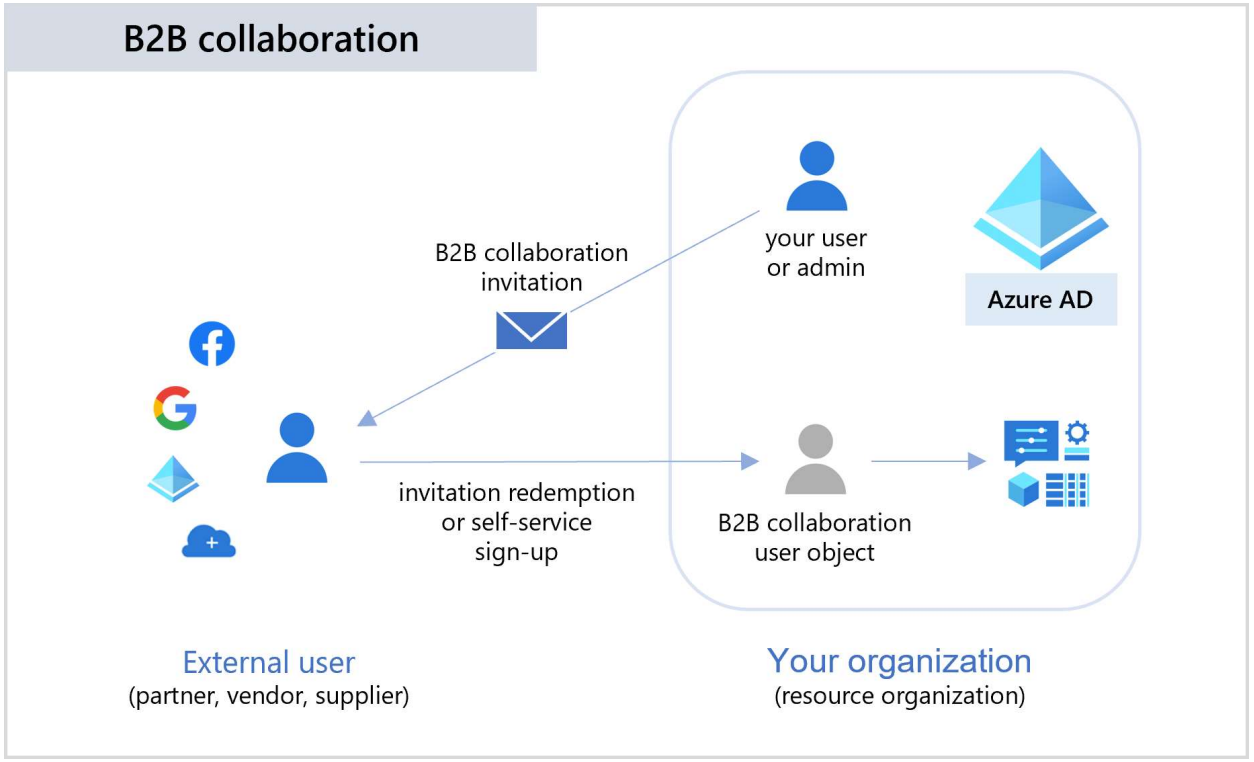


Properties of an Azure Active Directory B2B collaboration user

		UserType property	
		Guest	**Member**
How the user authenticates	**External** 	**External guest** Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	**External member** Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
	Internal 	**Internal guest** Has an account in your Azure AD directory but only guest-level access in your organization. This is often a legacy guest user created before the availability of Azure AD B2B.	**Internal member** Has an account in your Azure AD directory and member-level access in your organization. Generally considered employees of your organization.

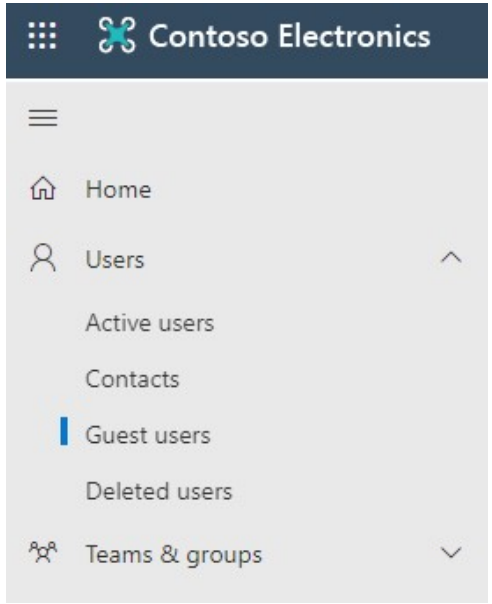
Azure Active Directory (Azure AD) B2B collaboration overview

- Feature within **External Identities** that lets you **invite guest users** to collaborate with your organization
- You can **securely share** your company's applications and services with **external users**, while maintaining control over your own corporate data.
- Work safely and securely with external partners, large or small, even if they don't have Azure AD or an IT department.



And now - …B2B (Guest) users…

- Any Guest you add to Teams, SharePoint, or Azure AD are also added as Guest user
- All Users and Admins can add Guests – it is turned ON!!
- Admins can control whether to allow guest access to groups



- To view guest users, navigate to **Users – Guest users**

Prerequisites to invite…

- A role that allows you to create
  - **Global Administrator**
  - Limited administrator directory role (**Guest inviter** or **User administrator**).

- Access to a **valid email address** outside of your Azure AD tenant,
- Based on this email address you'll create the Guest account in your tenant directory
- User will receive invitation through this email

Add/Invite Guest user…

- Use **Azure Active Directory admin center** – Users - Invite
- **Microsoft 365** – User admin – Guest User (Again back to AAD)
- PowerShell (for bulk users)

```
New-MgInvitation -InvitedUserDisplayName "John Doe" -InvitedUserEmailAddress
John@contoso.com -InviteRedirectUrl "https://myapplications.microsoft.com" -
SendInvitationMessage:$true
```

Licensing ☺

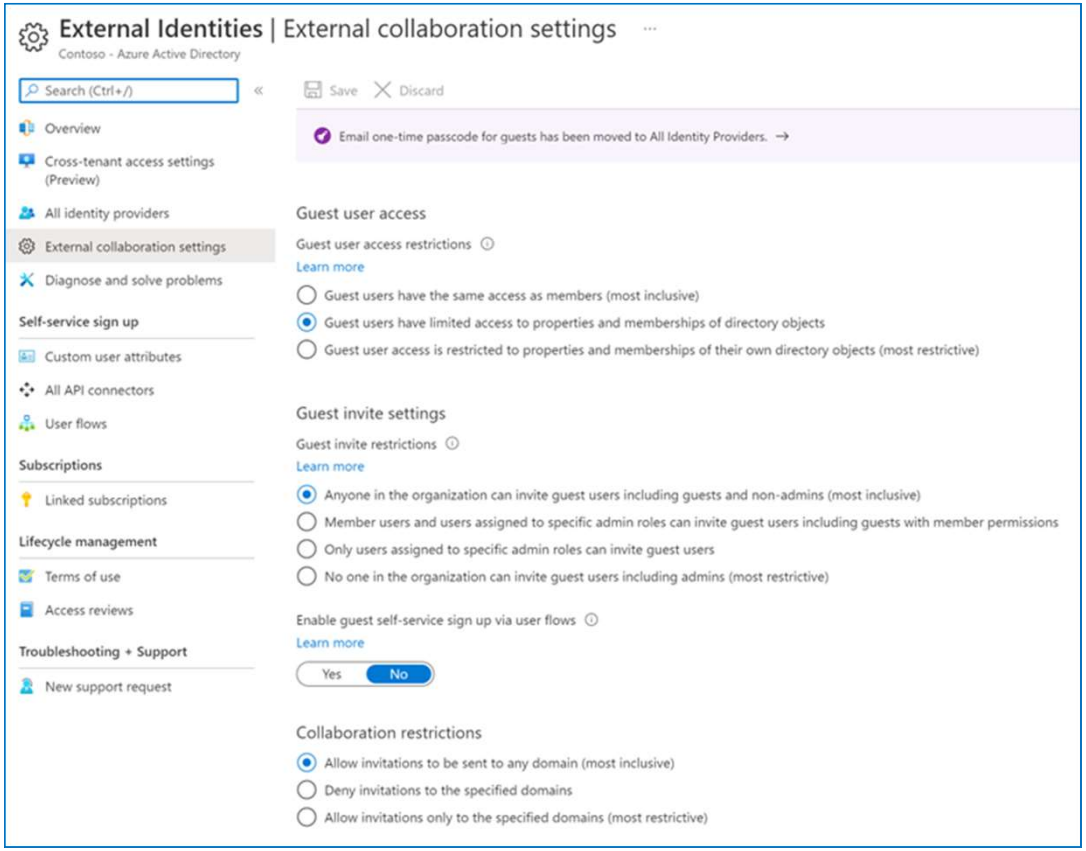
- For each paid license of Azure AD (Basic or Premium) you can add 5 B2B Users

If Users need MFA features & Identity protection

- **MFA** require AAD Premium P1 license (still 1:5)
- **Identity protection** require AAD Premium P2 license (still 1:5) same as **Conditional Access**…

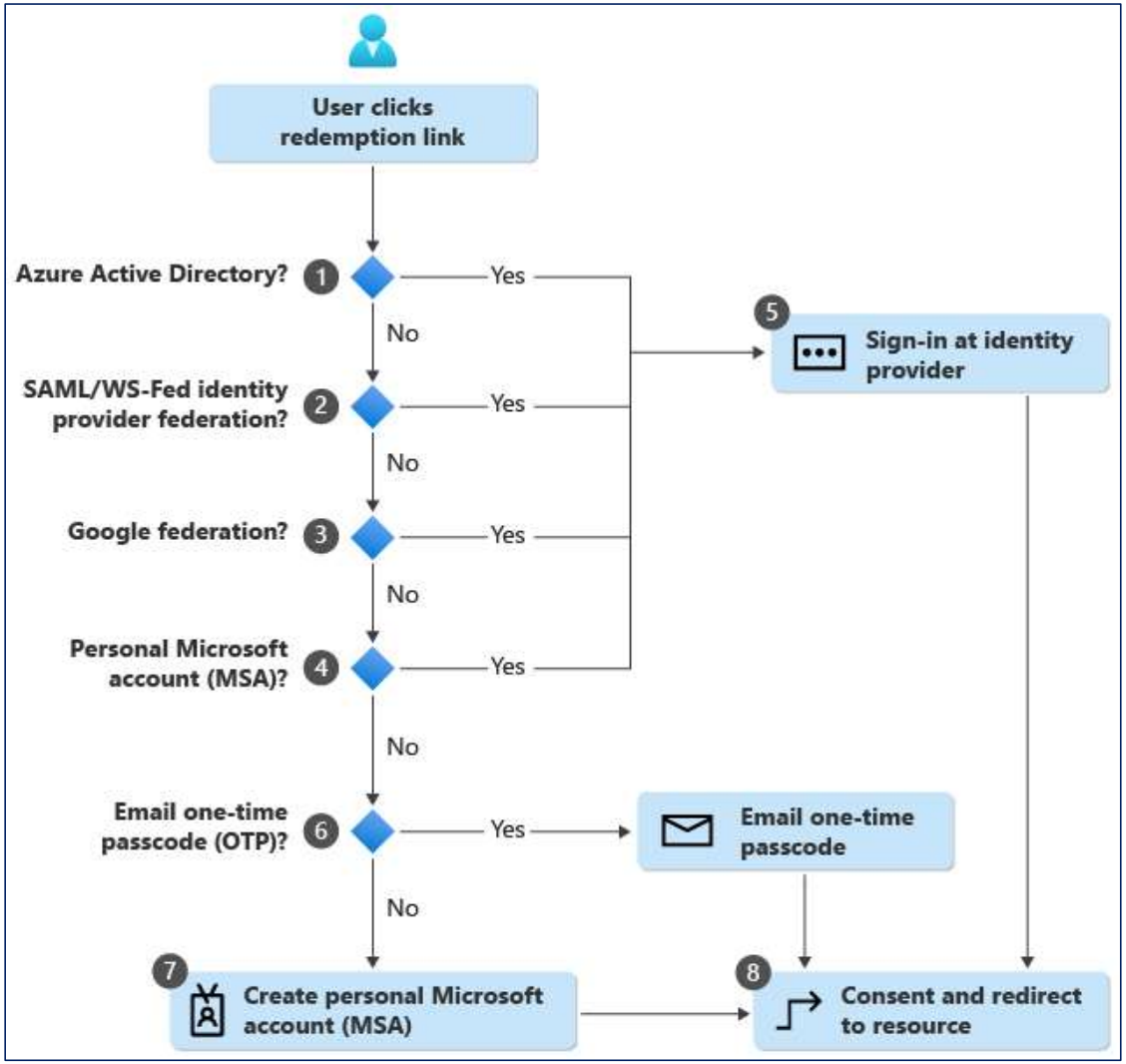
External collaboration settings in Azure AD

- Guest user access
- Guest invite settings
- Enable guest self-service sign up via user flows
- Collaboration restrictions



Invitation flow

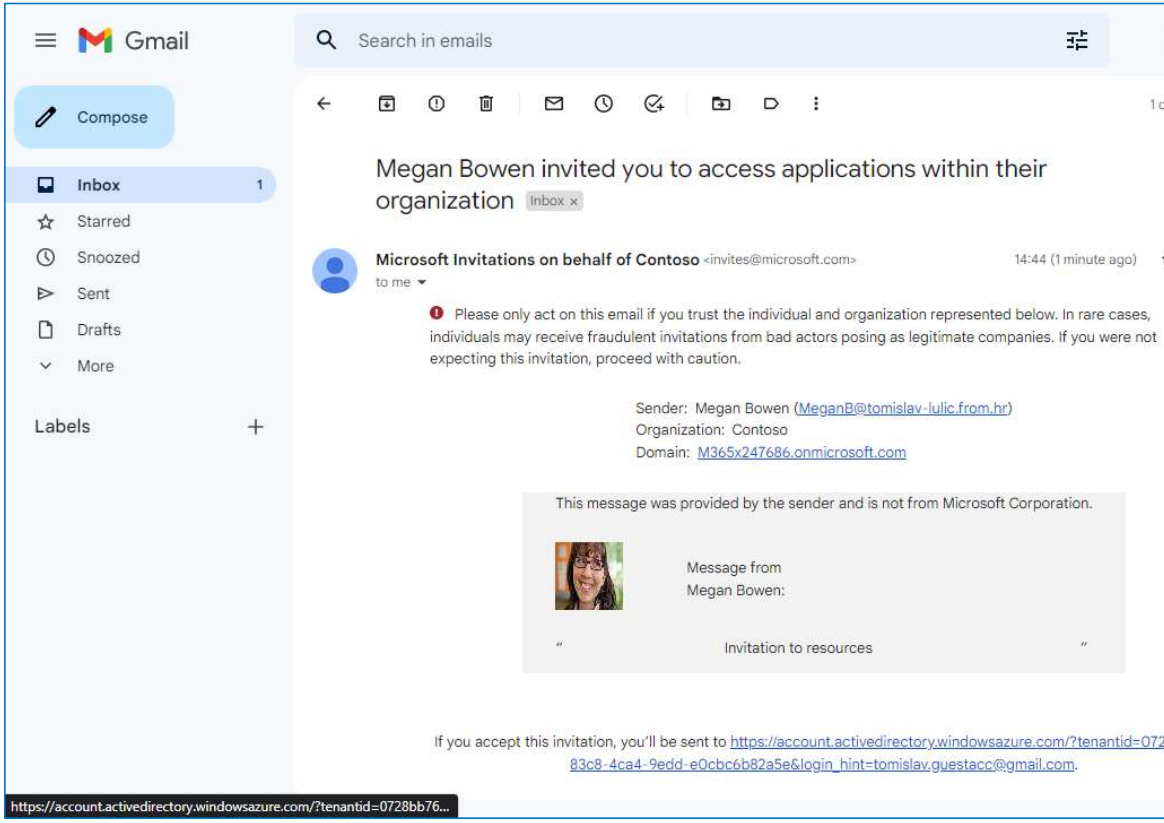
- When a user clicks the Accept invitation link in an invitation email, **Azure AD** automatically redeems the invitation based on the redemption flow as shown below:



Invitation for Guest user

The format is:

- Microsoft Invitations invites@microsoft.com or
- Microsoft invitations on behalf of <tenantname> invites@microsoft.com.



Securing Guest account (Conditional Access)

- Setting up multi-factor authentication (MFA) for guests.
- Setting up a terms of use for guests.
- Setting up quarterly guest access reviews to periodically validate whether guests continue to need permissions to teams and sites.
- Restricting guests to web-only access for unmanaged devices.

Securing Guest account (Conditional Access)

- Configuring a session timeout policy to ensure guests authenticate daily.
- Creating a sensitive information type for a highly sensitive project.
- Automatically assigning a sensitivity label to documents that contain a sensitive information type.
- Automatically removing guest access from files with a sensitivity label.

BIWWUG

collabdays

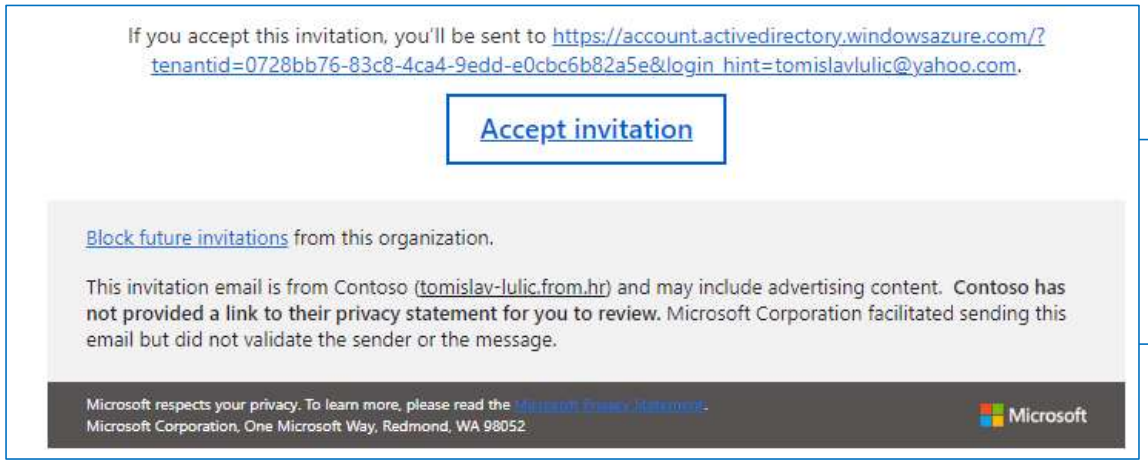
User concerns

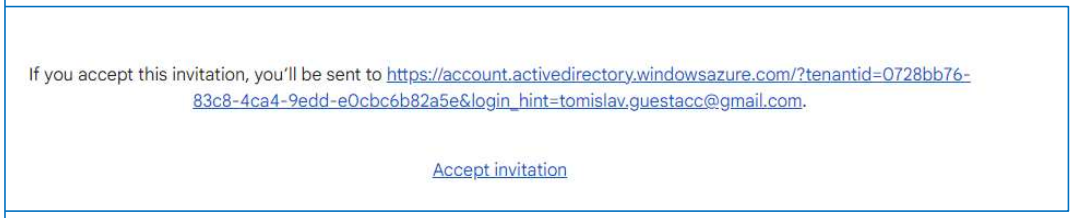
Phishing warning

- The email starts with a brief warning to the user about phishing
- It is alerting them that they should only accept invitations they're expecting.
- It’s good practice to make sure the partners you’re **inviting** will not be **surprised** by your invitation by mentioning it to them ahead of time.

Accept button and redirect URL

- The next section of the email contains information about where the invitee will be taken after they accept the invitation, as well as a button to do so. In the future, the invitee can always use this link to return to your resources directly.





BIWWUG

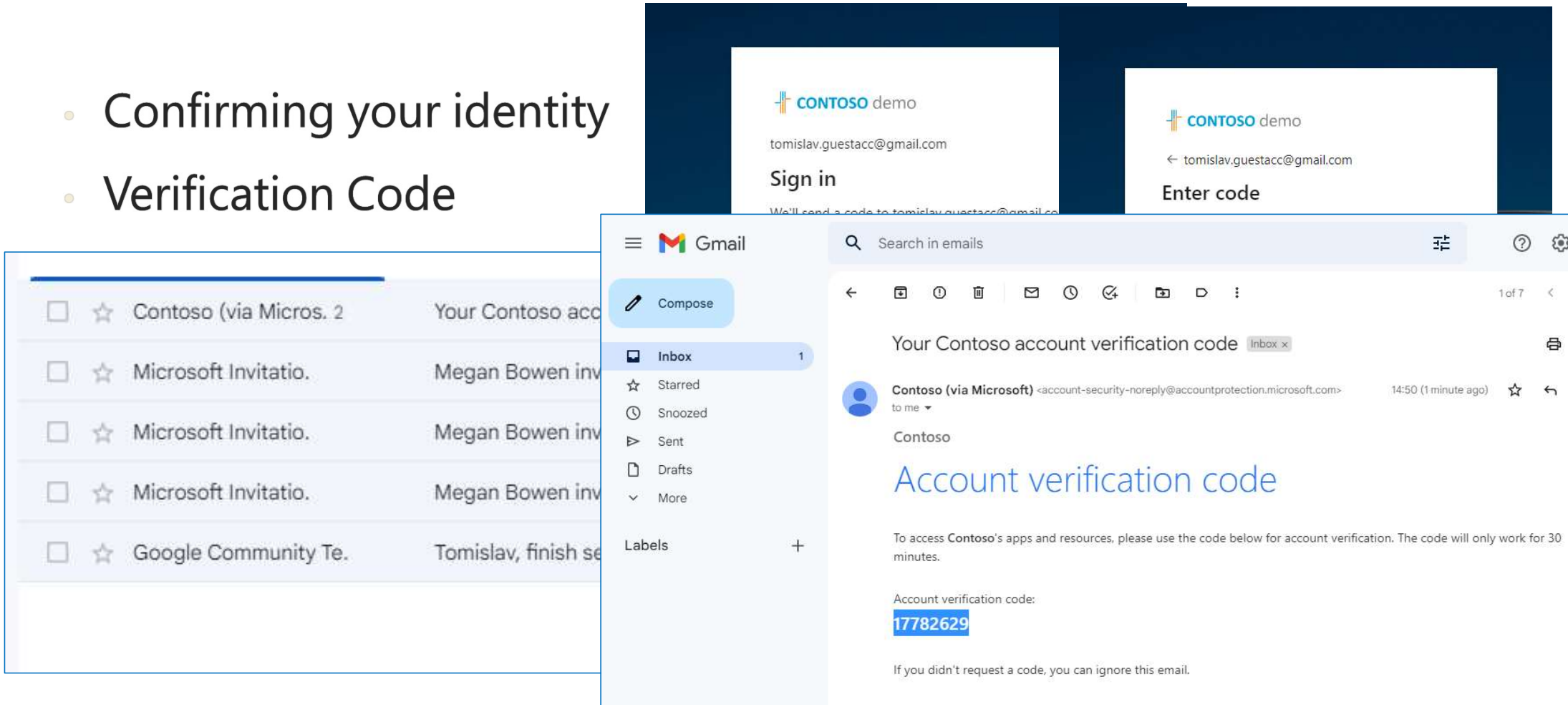
collabdays

Procedure

for accepting invitation

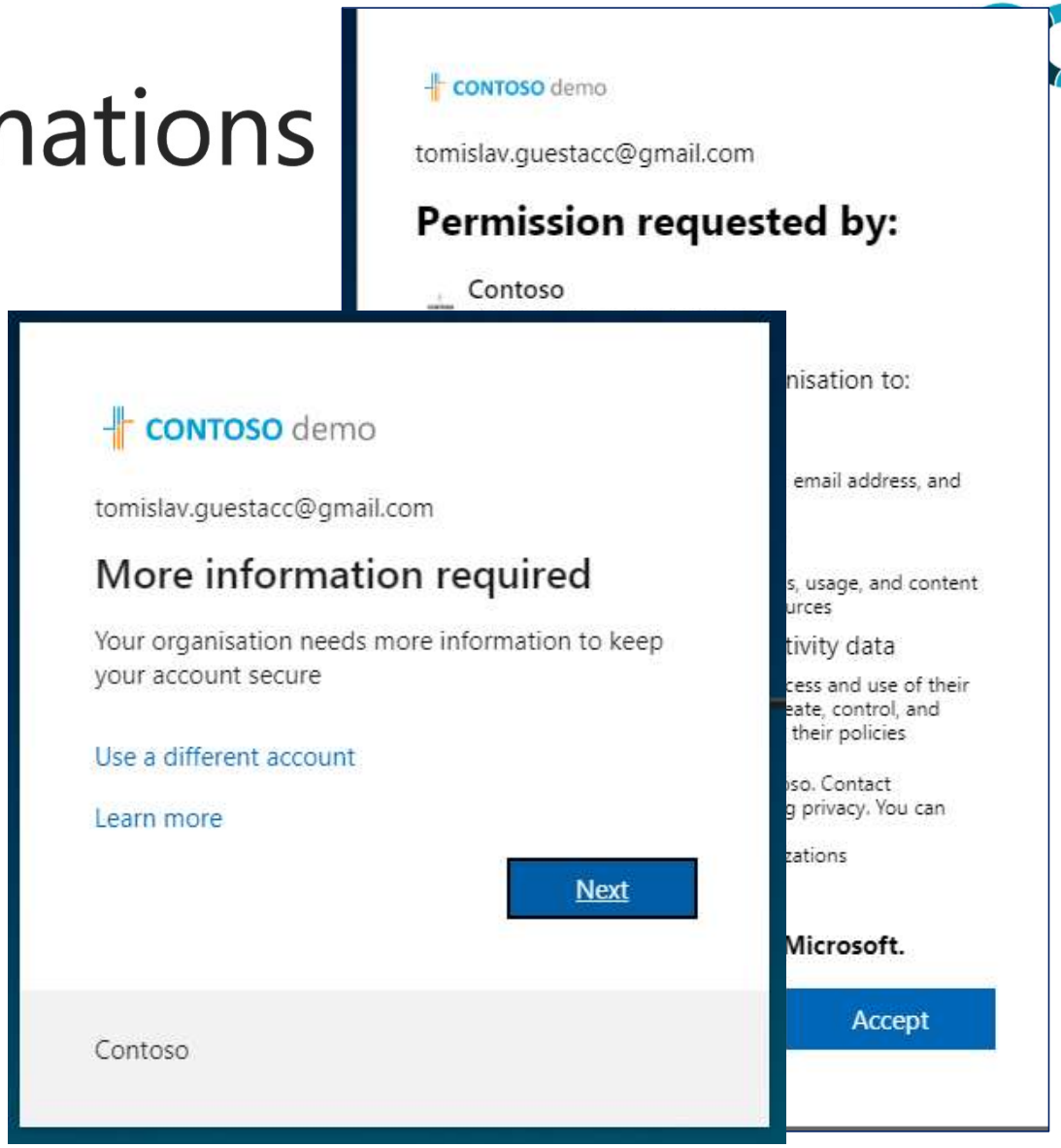
First screen after click on invitation

- Confirming your identity
- Verification Code

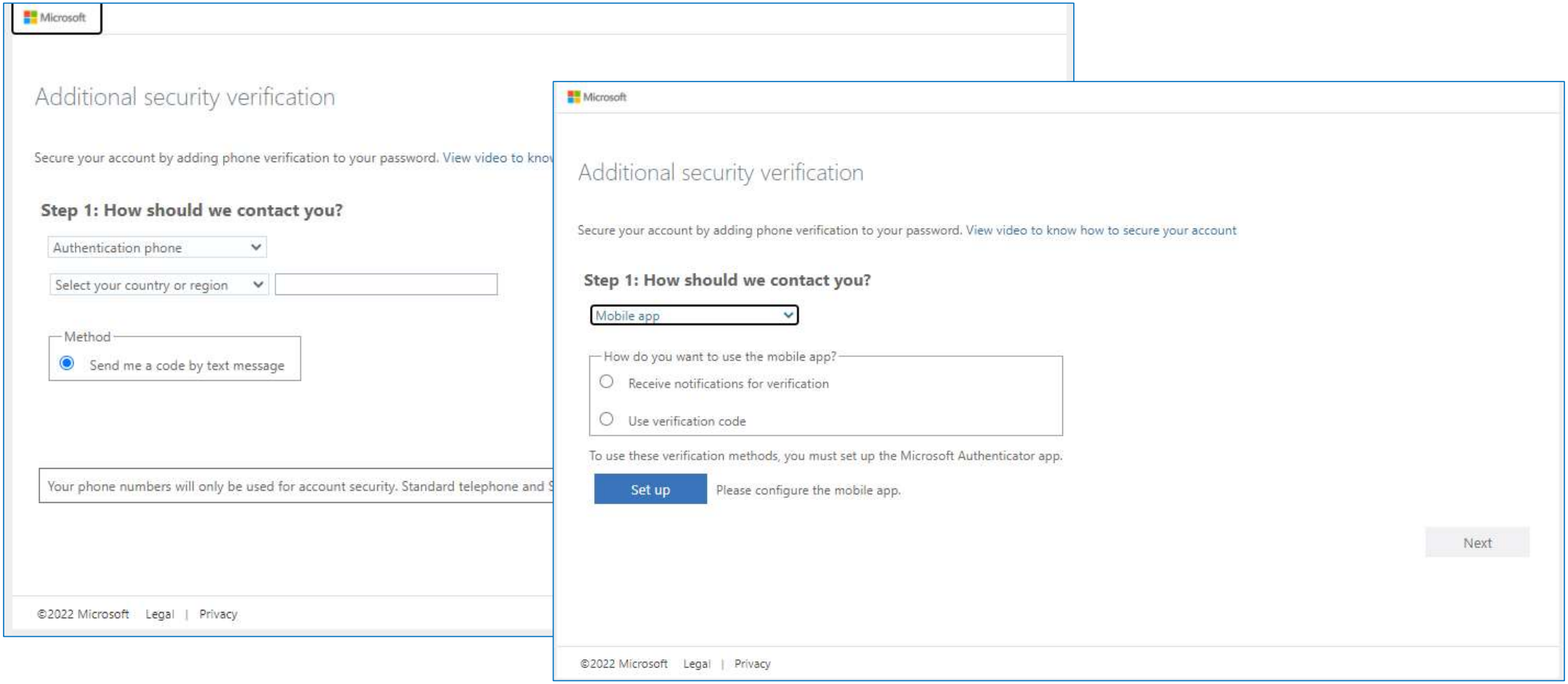


Provide more informations

- Permission…
- Setup more information

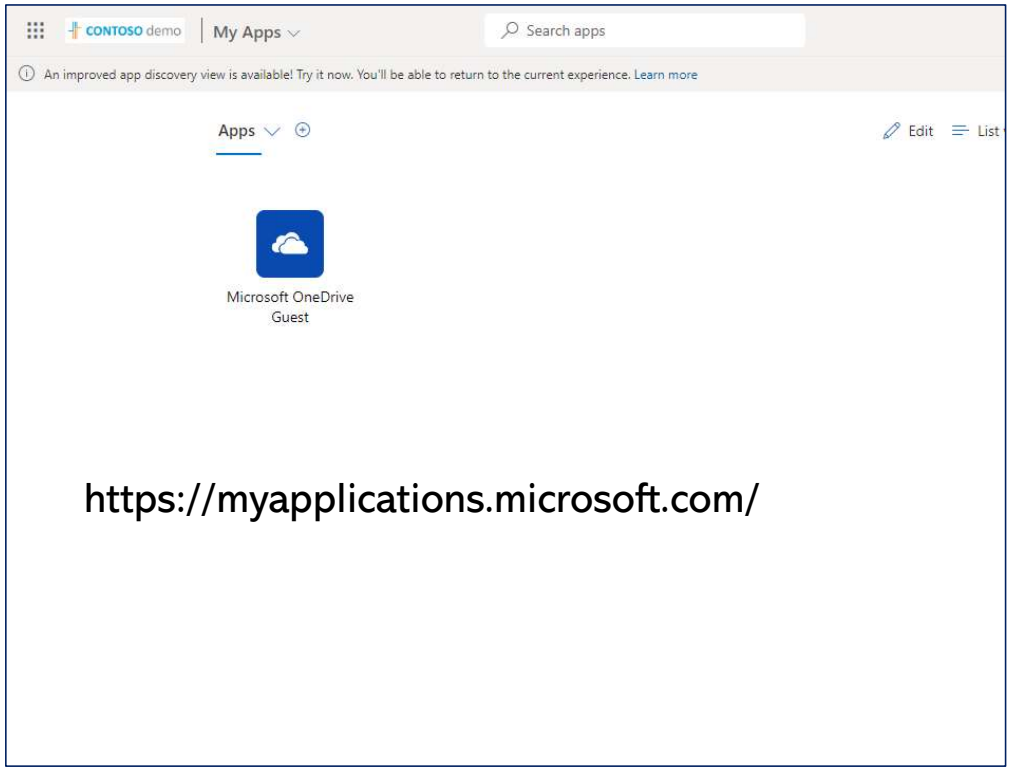


Verification methods

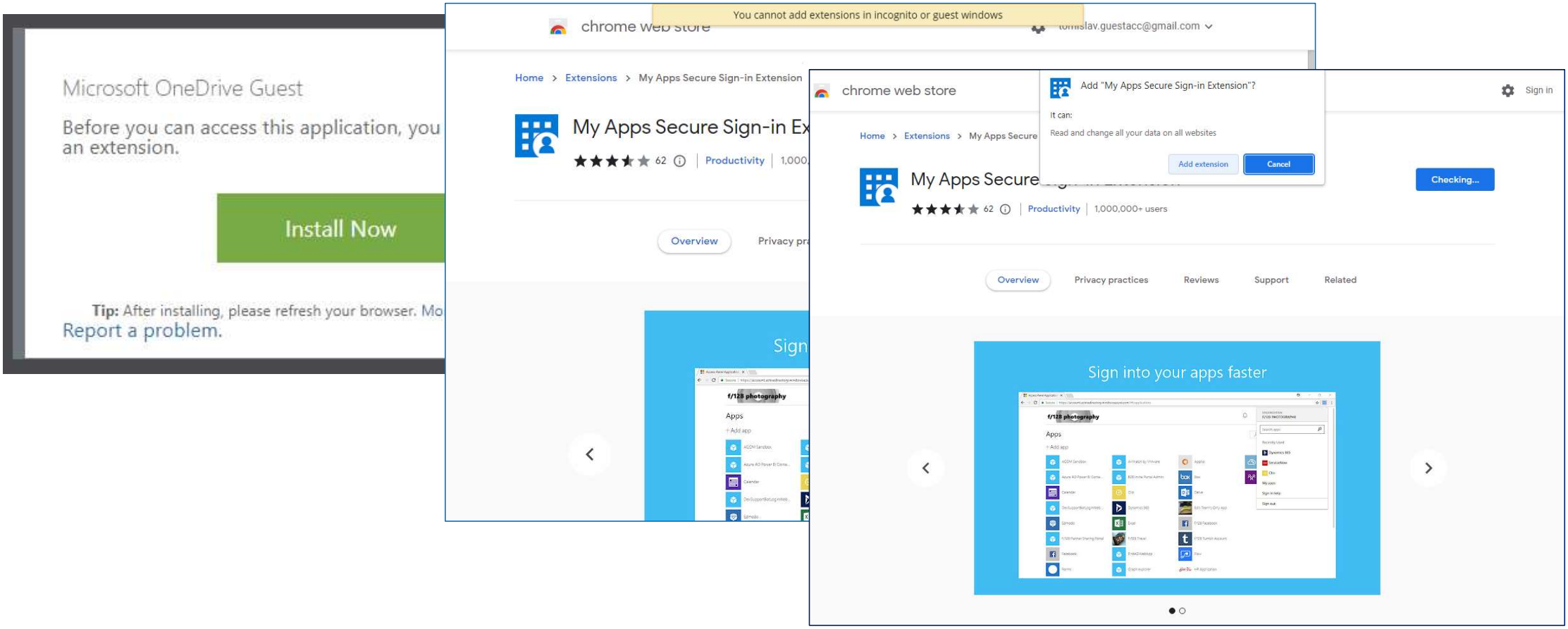


Access to resources

- Access to build-in My apps
- Redirect to other web/app place



Addin/extension for Chrome

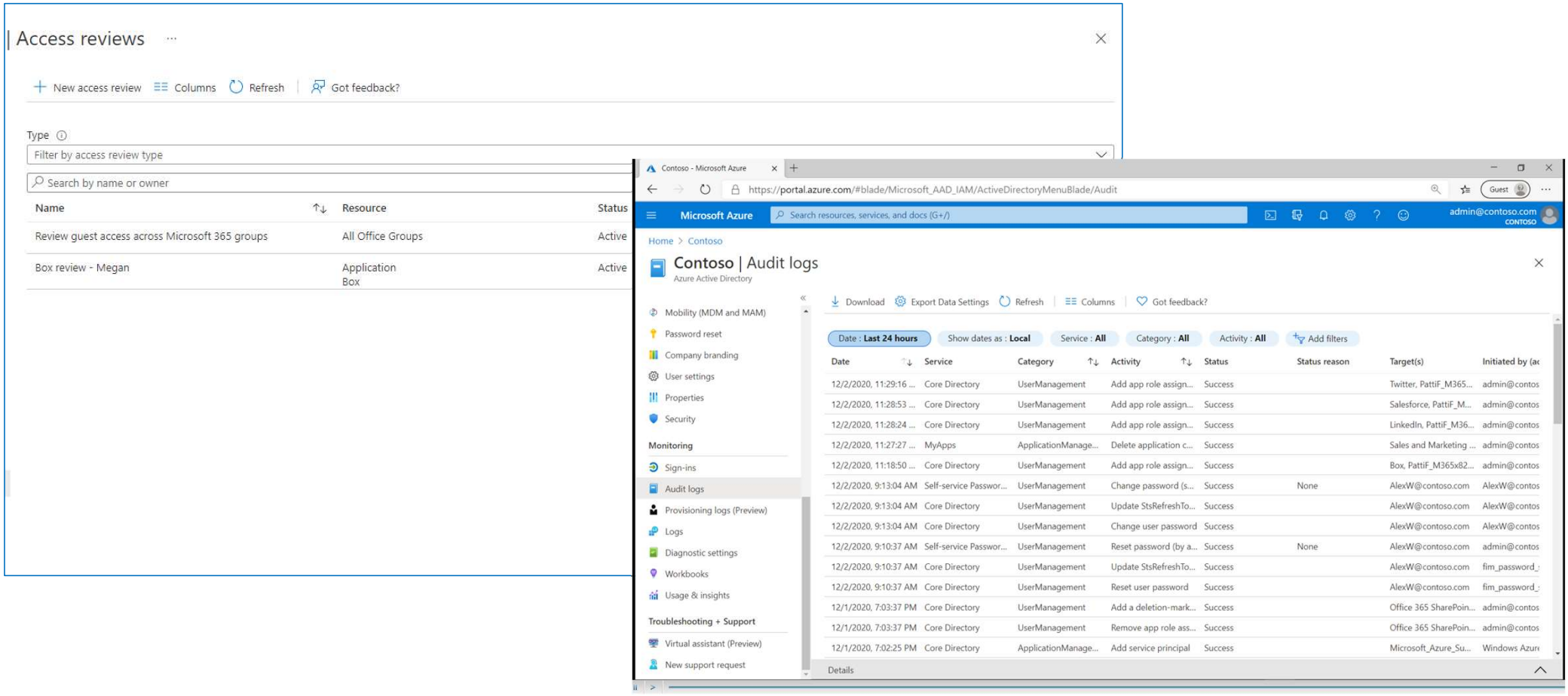


BIWUG

collabdays

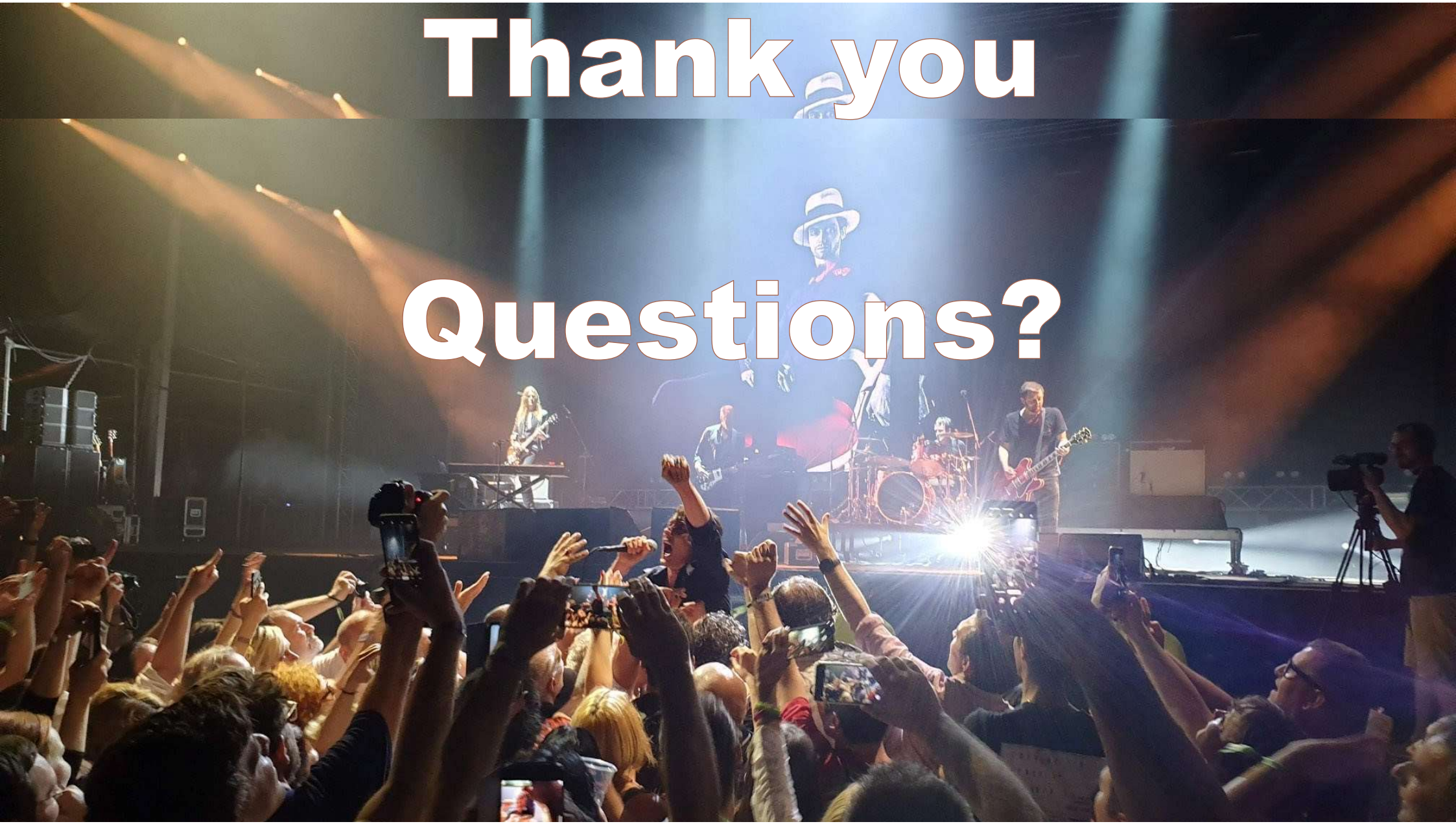
Monitoring

Audit log, Access review


Access reviews
New access review
Columns
Refresh
Got feedback?
Type
Filter by access review type
Search by name or owner
Name
Resource
Status
Review guest access across Microsoft 365 groups
All Office Groups
Active
Box review - Megan
Application
Box
Active
Contoso - Microsoft Azure
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Audit
Microsoft Azure
Search resources, services, and docs (G+/)
admin@contoso.com
CONTOSO
Home > Contoso
Contoso | Audit logs
Azure Active Directory
Download
Export Data Settings
Refresh
Columns
Got feedback?
Mobility (MDM and MAM)
Password reset
Company branding
User settings
Properties
Security
Monitoring
Sign-ins
Audit logs
Provisioning logs (Preview)
Logs
Diagnostic settings
Workbooks
Usage & insights
Troubleshooting + Support
Virtual assistant (Preview)
New support request
Date : Last 24 hours
Show dates as : Local
Service : All
Category : All
Activity : All
Add filters
Date
Service
Category
Activity
Status
Status reason
Target(s)
Initiated by (ac
12/2/2020, 11:29:16 ... Core Directory UserManagement Add app role assign... Success Twitter, PattiF_M365... admin@contos
12/2/2020, 11:28:53 ... Core Directory UserManagement Add app role assign... Success Salesforce, PattiF_M... admin@contos
12/2/2020, 11:28:24 ... Core Directory UserManagement Add app role assign... Success LinkedIn, PattiF_M36... admin@contos
12/2/2020, 11:27:27 ... MyApps ApplicationManage... Delete application c... Success Sales and Marketing ... admin@contos
12/2/2020, 11:18:50 ... Core Directory UserManagement Add app role assign... Success Box, PattiF_M365x82... admin@contos
12/2/2020, 9:13:04 AM Self-service Passwor... UserManagement Change password (s... Success None AlexW@contoso.com AlexW@contos
12/2/2020, 9:13:04 AM Core Directory UserManagement Update StsRefreshTo... Success AlexW@contoso.com AlexW@contos
12/2/2020, 9:13:04 AM Core Directory UserManagement Change user password Success AlexW@contoso.com AlexW@contos
12/2/2020, 9:10:37 AM Self-service Passwor... UserManagement Reset password (by a... Success None AlexW@contoso.com admin@contos
12/2/2020, 9:10:37 AM Core Directory UserManagement Update StsRefreshTo... Success AlexW@contoso.com fim_password_
12/2/2020, 9:10:37 AM Core Directory UserManagement Reset user password Success AlexW@contoso.com fim_password_
12/1/2020, 7:03:37 PM Core Directory UserManagement Add a deletion-mark... Success Office 365 SharePoin... admin@contos
12/1/2020, 7:03:37 PM Core Directory UserManagement Remove app role ass... Success Office 365 SharePoin... admin@contos
12/1/2020, 7:02:25 PM Core Directory ApplicationManage... Add service principal Success Microsoft_Azure_Su... Windows Azure
Details

Remember from today's lecture...

- Check what you need from B2B feature
- Check licenses on your Tenant (Basic, Business, P1, P2)
- When you send invitation, inform/train your B2B – Guest users
- Prepare your informations workflow
- Build Clasification on your data


Thank you
Questions?