

BIWUG



Title Lorem Ipsum

Guest account in Azure Active Directory

Tomislav Lulić
Microsoft MVP, MCT



cd collabdays



Do not forget
sponsors

Platinum



Gold



Silver



Community



SharePoint





Tomislav Lulić

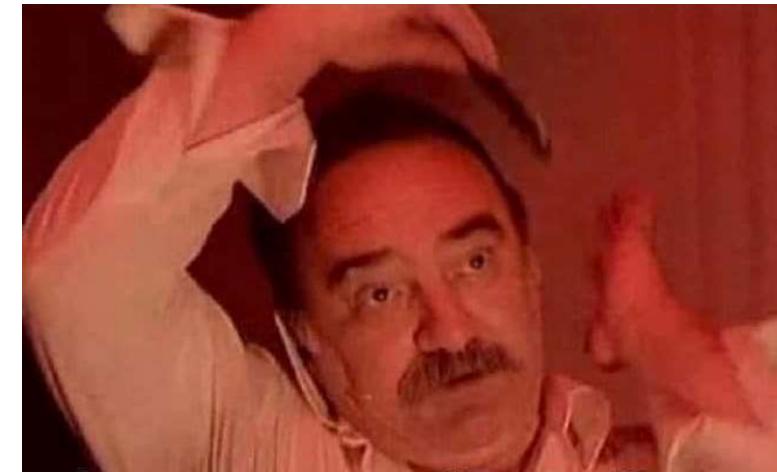
World Bank Office in Croatia
IT analyst
Microsoft MVP, MCT



 @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

- Tenant 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... choose one



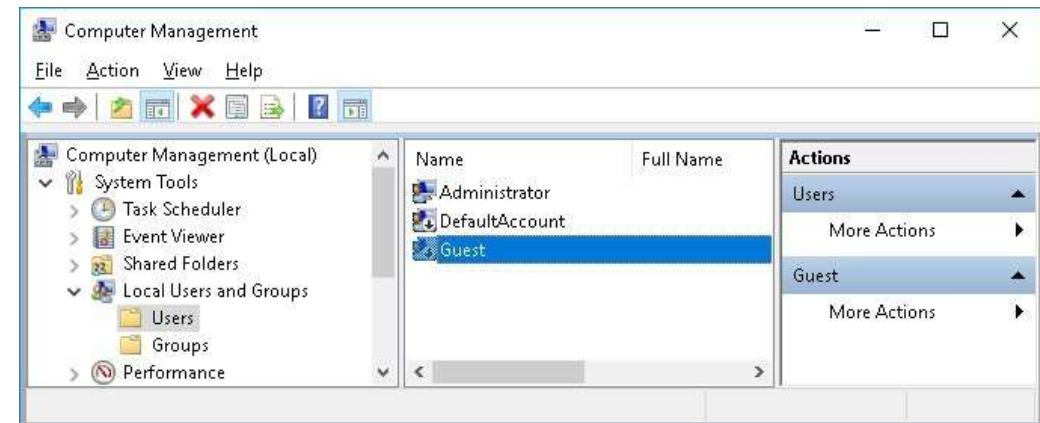
Microsoft news

- **Microsoft Entra**
 - All identity and access capabilities
- **Microsoft Defender**
 - Formerly Office 365 Security p.
- **Microsoft Purview**
 - Formerly Compliance portal
- **Microsoft Priva**
 - Privacy Risk Management
- **Microsoft Endpoint Manager**
 - 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

Sharing

When this setting is selected, all users can add people outside the organization as guests, so they appear on the Guest users page. When this setting isn't selected, only admins can add guests. [Learn more about guests in your organization](#).

You can also [change the external sharing settings for SharePoint](#).

- Let users add new guests to the organization

Microsoft 365 Groups

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

Microsoft 365 Groups

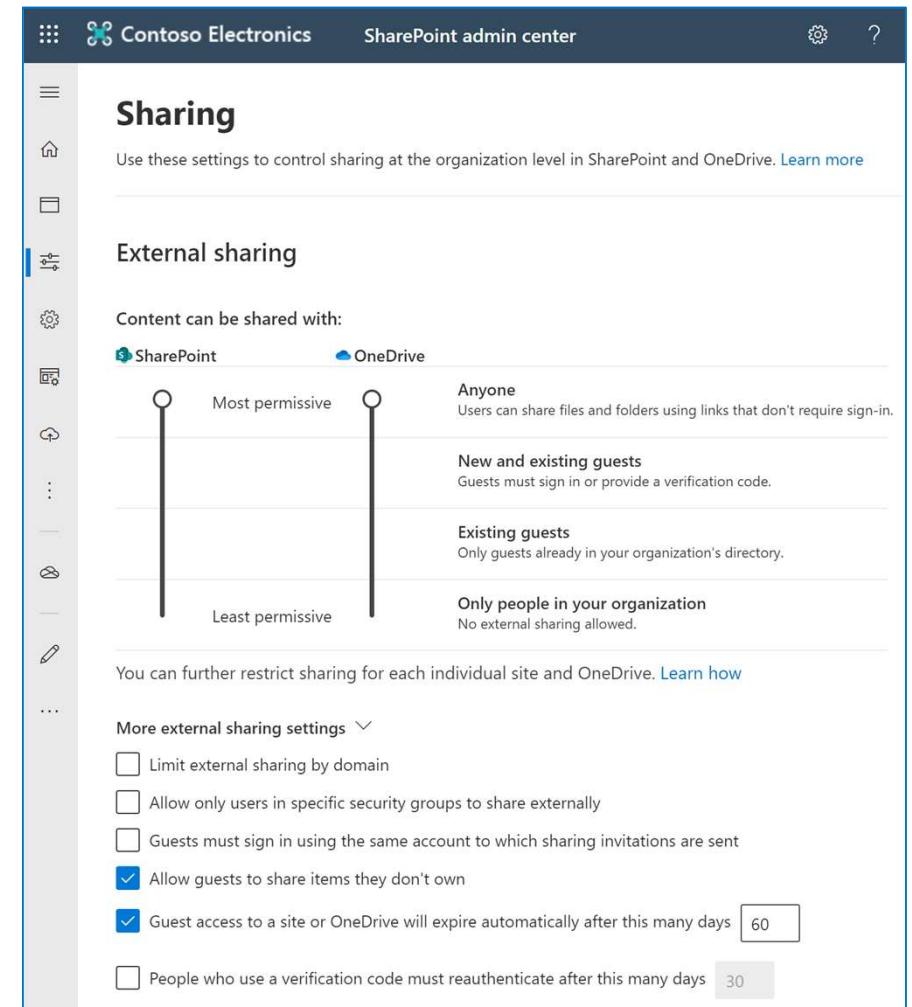
Choose how guests from outside your organization can collaborate with your users in Microsoft 365 Groups. [Learn more about guest access to Microsoft 365 Groups](#)

- Let group owners add people outside your organization to Microsoft 365 Groups as guests
- Let guest group members access group content
If you don't select this, 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 files that were directly shared with them.

Manage file sharing in SharePoint and OneDrive

Use SharePoint admin center

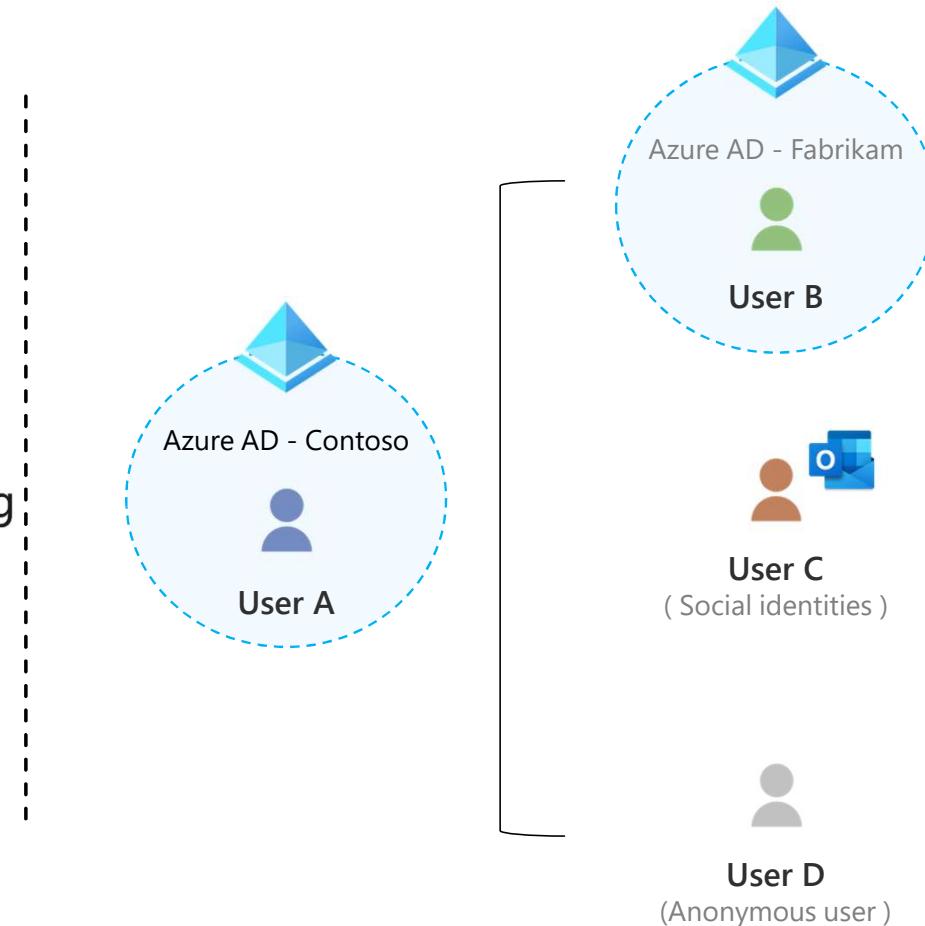
- Policies > Sharing
- OneDrive setting cannot be more permissive than the SharePoint setting
- External sharing and advanced settings
 - Anyone (includes anonymous users)
 - New and existing guests
 - Existing guests
 - Only people in your organization



Work with external users

Define external users

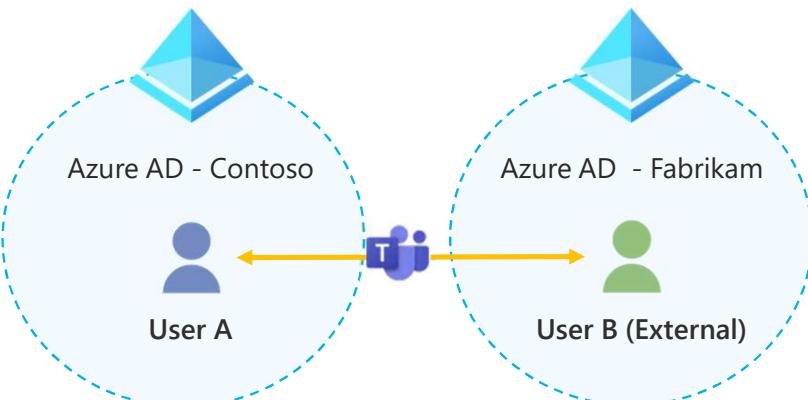
- **User A** : Member user in your organization
- **User B** : Business account (Azure AD account)
- **User C** : Consumer email account (with Outlook.com, Gmail.com, or others).
- **User D** : Anonymous user without authenticating



How it Works in Microsoft Teams

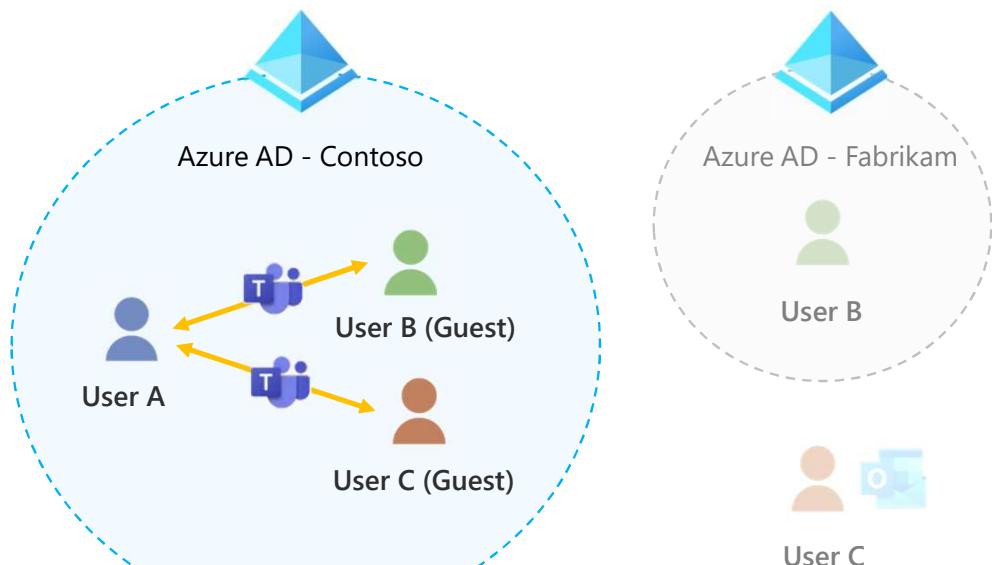
External access (federation)

- 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

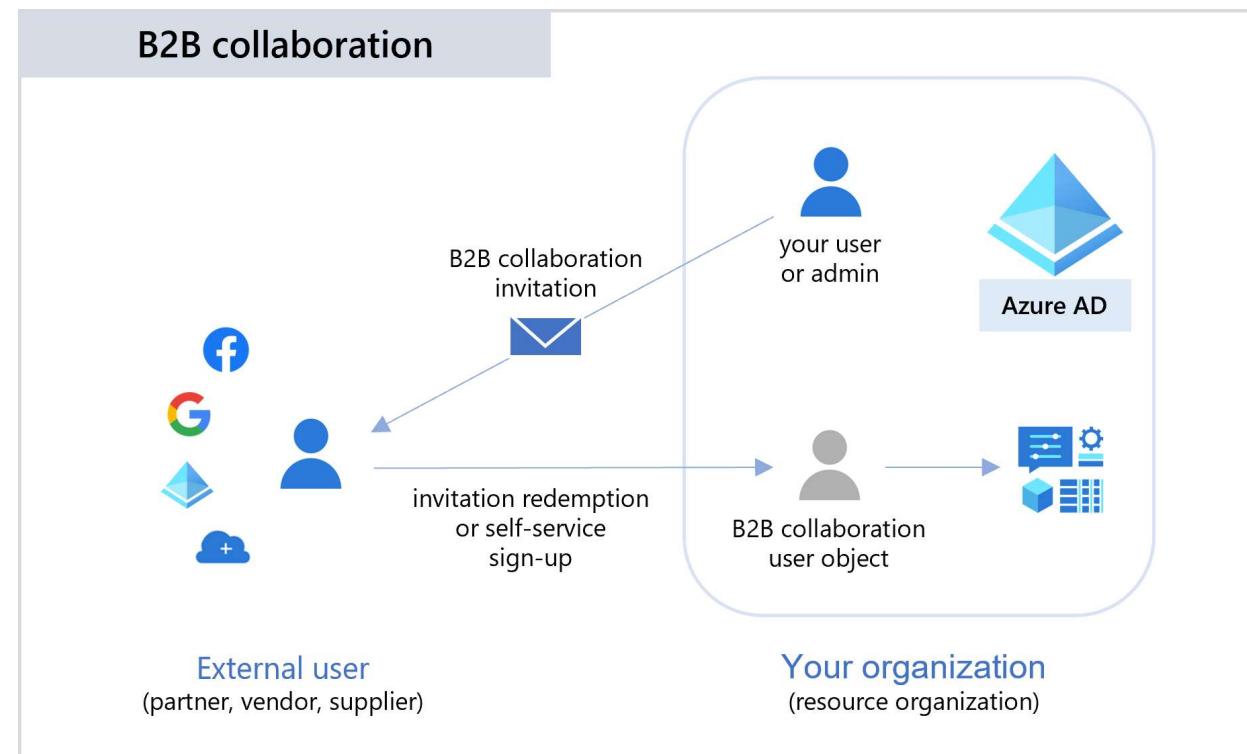


Properties of an Azure Active Directory B2B collaboration user

		UserType property	
		Guest	Member
How the user authenticates	External	External guest	External member
		Uses an external Azure AD account, social identity, or other external identity provider to sign in. Most external users fall into this category.	Uses an external account to authenticate but has member-level access in your organization. Common scenario in multi-tenant organizations.
Internal	External	Internal guest	Internal member
		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.	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

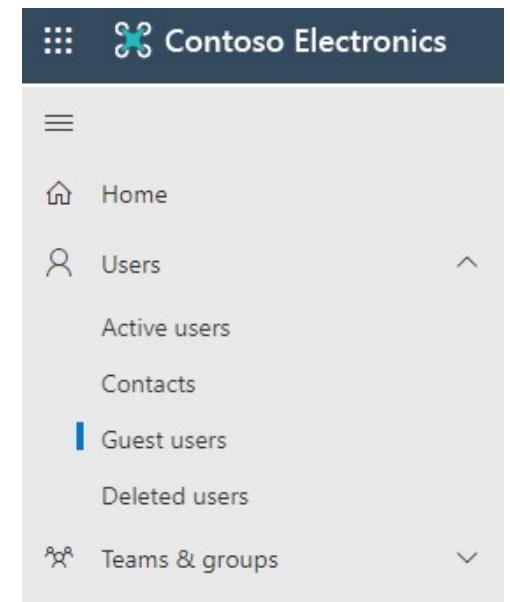
- Feature within **External Identities** that lets you **invite guest users** to collaborate with your organization
- You can **securely share** your company's applications and services with **external users**, while maintaining control over your own corporate data.
- Work safely and securely with external 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**)

 Guest inviterCan invite guest users independent of the 'members can invite guests' setting.
- 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...**



Azure Active
Directory



Azure AD Identity
Protection



Azure AD 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

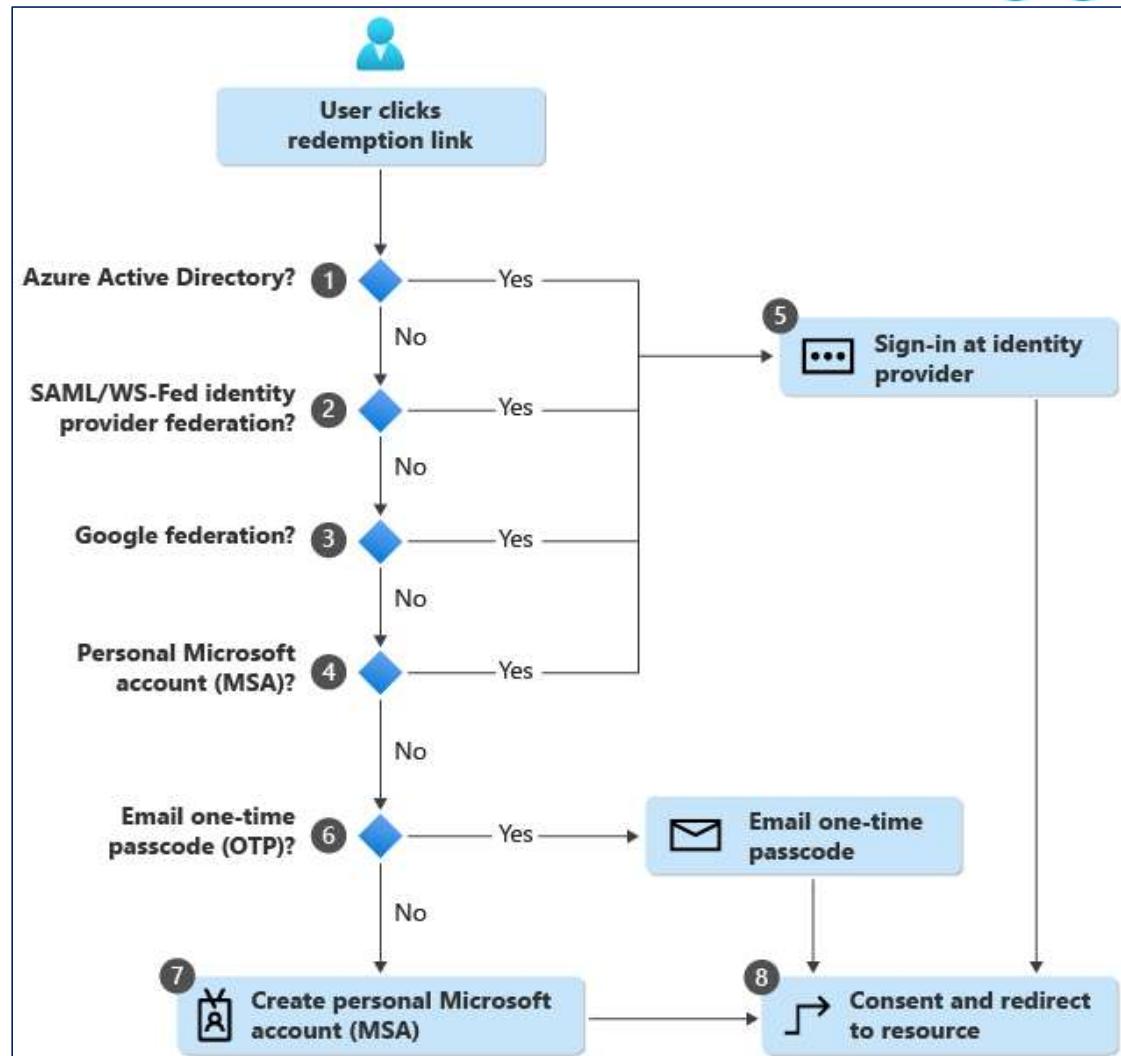
The screenshot shows the 'External Identities' blade in the Azure portal, specifically the 'External collaboration settings' section for the Contoso tenant. The left sidebar lists various management options like Overview, Cross-tenant access settings, All identity providers, External collaboration settings (which is selected and highlighted in grey), Diagnose and solve problems, Self-service sign up, Custom user attributes, All API connectors, User flows, Subscriptions, Lifecycle management, Terms of use, Access reviews, Troubleshooting + Support, and New support request. The main content area is titled 'External Identities | External collaboration settings'. It contains several configuration sections:

- Guest user access:** A note says 'Email one-time passcode for guests has been moved to All Identity Providers.' Below are three radio button options: 'Guest users have the same access as members (most inclusive)' (unselected), 'Guest users have limited access to properties and memberships of directory objects' (selected), and 'Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)' (unselected).
- Guest invite settings:** A note says 'Learn more' about invite restrictions. Below are four radio button options: 'Anyone in the organization can invite guest users including guests and non-admins (most inclusive)' (selected), 'Member users and users assigned to specific admin roles can invite guest users including guests with member permissions', 'Only users assigned to specific admin roles can invite guest users', and 'No one in the organization can invite guest users including admins (most restrictive)'.
- Enable guest self-service sign up via user flows:** A note says 'Learn more'. Below are two buttons: 'Yes' (selected) and 'No'.
- Collaboration restrictions:** A note says 'Learn more'. Below are three radio button options: 'Allow invitations to be sent to any domain (most inclusive)' (selected), 'Deny invitations to the specified domains', and 'Allow invitations only to the specified domains (most restrictive)'.



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:

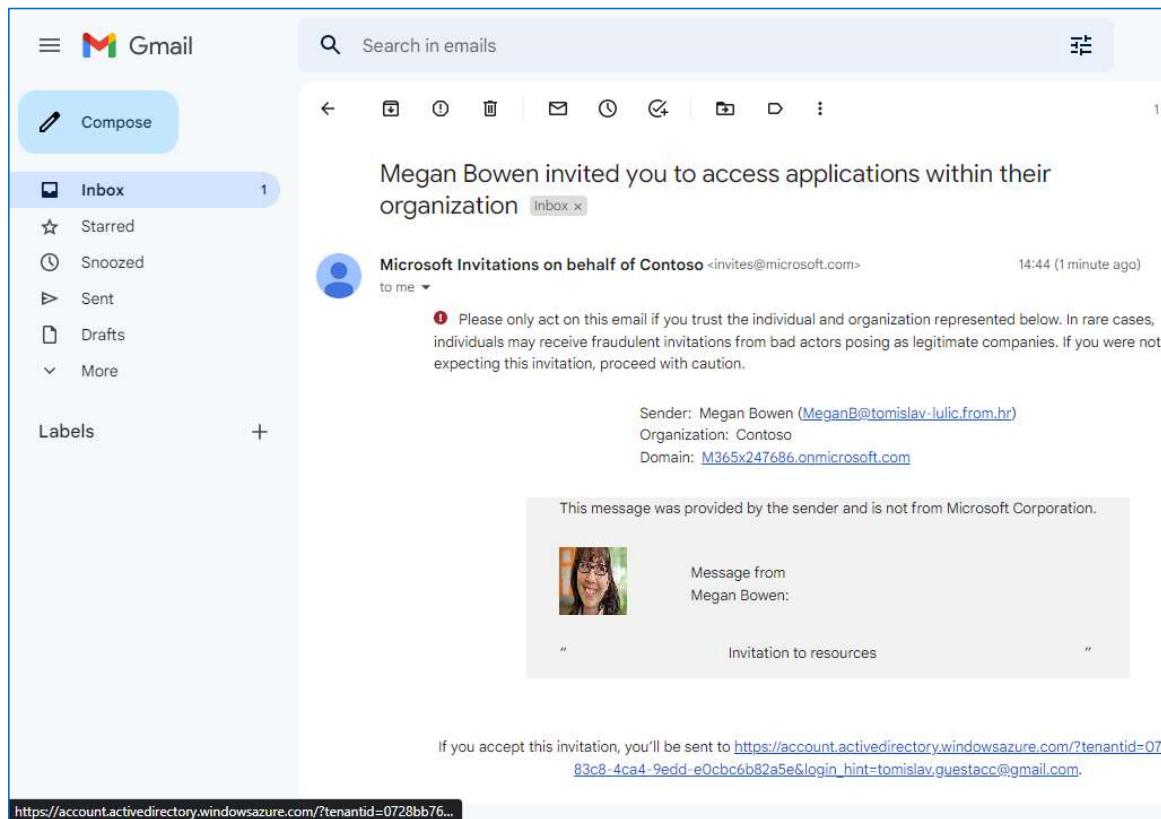




Invitation for Guest user

The format is:

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



The screenshot shows a Gmail inbox with one unread email. The email is from "Microsoft Invitations on behalf of Contoso <invites@microsoft.com>" to the recipient. The subject line is "Megan Bowen invited you to access applications within their organization". The email body contains a warning message: "Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution." Below the message, it shows the sender's information: "Sender: Megan Bowen (MeganB@tomislav-lulic.from.hr)", "Organization: Contoso", and "Domain: M365x247686.onmicrosoft.com". At the bottom of the email, there is a note: "This message was provided by the sender and is not from Microsoft Corporation." It also includes a small profile picture of Megan Bowen and the text "Message from Megan Bowen:". At the very bottom of the email, there is a link: "https://account.activedirectory.windowsazure.com/?tenantid=0728bb76...".



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.

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.

Microsoft Invitations on behalf of Contoso <invites@microsoft.com>
To: tomislavlulic@yahoo.com

External images are now more secure, and shown by default. [Change in Settings](#)

Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Sender: Megan Bowen (MeganB@tomislav-lulic.from.hr)
Organization: Contoso
Domain: tomislav-lulic.from.hr



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.

If you accept this invitation, you'll be sent to https://account.activedirectory.windowsazure.com/?tenantid=0728bb76-83c8-4ca4-9edd-e0cbc6b82a5e&login_hint=tomislavlulic@yahoo.com.

[Accept invitation](#)

[Block future invitations](#) from this organization.

This invitation email is from Contoso (tomislav-lulic@from.hr) and may include advertising content. Contoso has not provided a link to their privacy statement for you to review. Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the [Microsoft Privacy Statement](#).
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052



If you accept this invitation, you'll be sent to https://account.activedirectory.windowsazure.com/?tenantid=0728bb76-83c8-4ca4-9edd-e0cbc6b82a5e&login_hint=tomislav.guestacc@gmail.com.

[Accept invitation](#)



Procedure

for accepting invitation



First screen after click on invitation

- Confirming your identity
- Verification Code

The screenshot shows a Gmail inbox with several Microsoft invitation emails and one Google Community email. A specific email from Contoso (via Microsoft) is selected, displaying its contents. The subject line is "Your Contoso account verification code". The email body contains instructions: "To access Contoso's apps and resources, please use the code below for account verification. The code will only work for 30 minutes." Below this, the account verification code is prominently displayed in a blue box: **17782629**. At the bottom of the email, it says, "If you didn't request a code, you can ignore this email."

CONTOSO demo
tomislav.guestacc@gmail.com
Sign in
We'll send a code to tomislav.guestacc@gmail.com

CONTOSO demo
← tomislav.guestacc@gmail.com
Enter code

Gmail

Compose

Inbox 1

Starred

Snoozed

Sent

Drafts

More

Labels +

Search in emails

Your Contoso account verification code

Contoso (via Microsoft) <account-security-noreply@accountprotection.microsoft.com> to me 14:50 (1 minute ago)

Contoso

Account verification code

To access Contoso's apps and resources, please use the code below for account verification. The code will only work for 30 minutes.

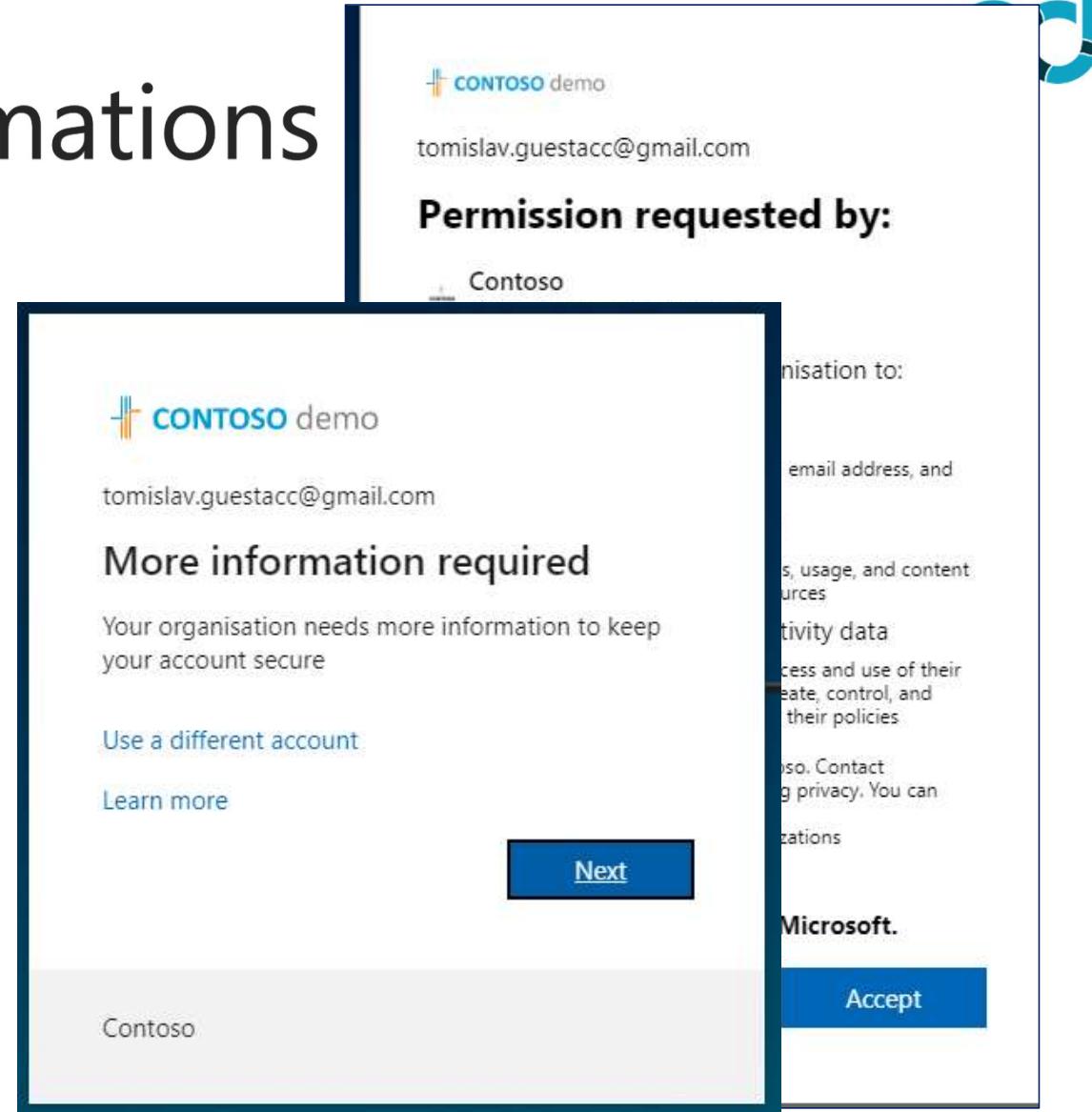
Account verification code:

17782629

If you didn't request a code, you can ignore this email.

Provide more informations

- Permission...
- Setup more information





Verification methods

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how.

Step 1: How should we contact you?

Authentication phone

Select your country or region

Method Send me a code by text message

Your phone numbers will only be used for account security. Standard telephone and S

©2022 Microsoft Legal | Privacy

Microsoft

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account.

Step 1: How should we contact you?

Mobile app

How do you want to use the mobile app?
 Receive notifications for verification
 Use verification code

To use these verification methods, you must set up the Microsoft Authenticator app.

Set up Please configure the mobile app.

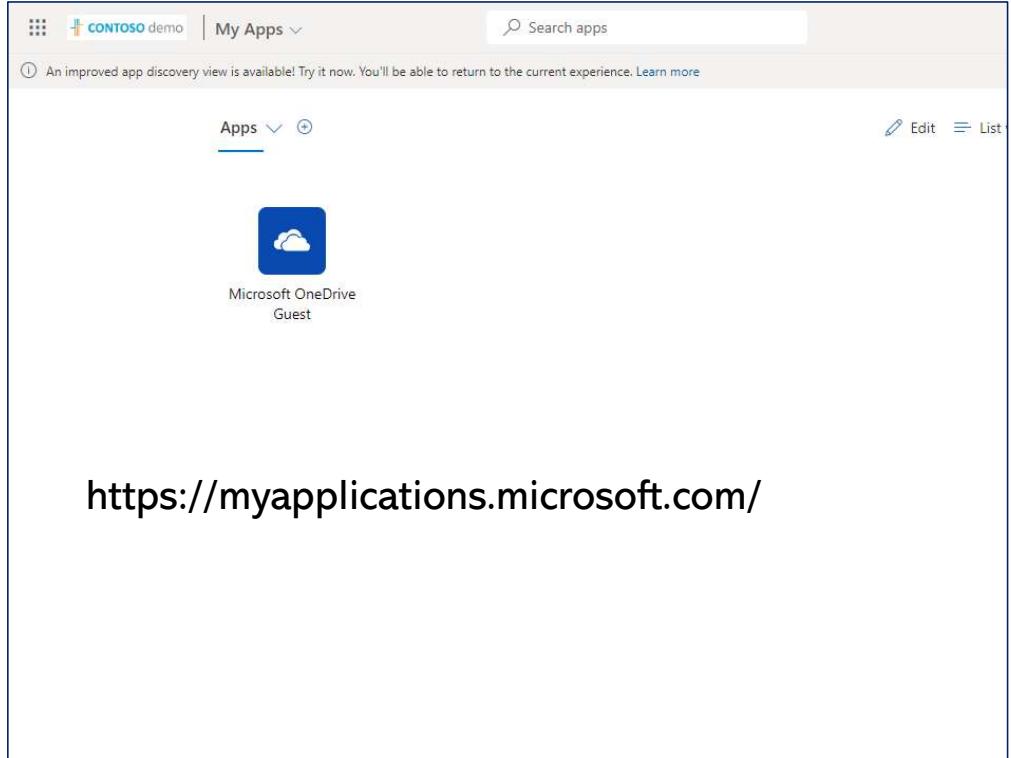
Next

©2022 Microsoft Legal | Privacy



Access to resources

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



The screenshot shows the Microsoft My Apps portal. At the top, there's a header with a grid icon, the text 'CONTOSO demo | My Apps', a search bar labeled 'Search apps', and a message about an improved app discovery view. Below the header, there are three tabs: 'Apps' (which is selected), 'Grid', and 'List'. Under the 'Apps' tab, there is one item listed: 'Microsoft OneDrive Guest', represented by a blue square icon with a white cloud and a person icon.

<https://myapplications.microsoft.com/>



Addin/extension for Chrome

Microsoft OneDrive Guest

Before you can access this application, you
an extension.

Install Now

Tip: After installing, please refresh your browser. Mo
Report a problem.

The screenshot shows a Microsoft OneDrive Guest interface. A yellow banner at the top states: "You cannot add extensions in incognito or guest windows". Below it, a message says: "Before you can access this application, you an extension." A large green button labeled "Install Now" is present. A tip at the bottom reads: "Tip: After installing, please refresh your browser. Mo Report a problem."

The right side of the image shows the Chrome Web Store. It displays the "My Apps Secure Sign-in Extension" page. The extension has a 4.5-star rating, 62 reviews, and 1,000+ installs. It is categorized under Productivity. A modal window is open, asking if the user wants to add the extension. The modal includes a "Cancel" button and a "Checking..." button. Another screenshot of the extension's interface is shown, titled "Sign into your apps faster", displaying various app icons like Microsoft 365, OneDrive, and SharePoint.

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+)

Home > Contoso

Contoso | Audit logs

Azure Active Directory

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@contoso
12/2/2020, 11:28:53 ...	Core Directory	UserManagement	Add app role assign...	Success		Salesforce, PattiF_M...	admin@contoso
12/2/2020, 11:28:24 ...	Core Directory	UserManagement	Add app role assign...	Success		LinkedIn, PattiF_M36...	admin@contoso
12/2/2020, 11:27:27 ...	MyApps	ApplicationManage...	Delete application c...	Success		Sales and Marketing ...	admin@contoso
12/2/2020, 11:18:50 ...	Core Directory	UserManagement	Add app role assign...	Success		Box, PattiF_M365x82...	admin@contoso
12/2/2020, 9:13:04 AM	Self-service Passwor...	UserManagement	Change password (s...	Success	None	AlexW@contoso.com	AlexW@contoso
12/2/2020, 9:13:04 AM	Core Directory	UserManagement	Update StsRefreshTo...	Success		AlexW@contoso.com	AlexW@contoso
12/2/2020, 9:13:04 AM	Core Directory	UserManagement	Change user password	Success		AlexW@contoso.com	AlexW@contoso
12/2/2020, 9:10:37 AM	Self-service Passwor...	UserManagement	Reset password (by a...	Success	None	AlexW@contoso.com	admin@contoso
12/2/2020, 9:10:37 AM	Core Directory	UserManagement	Update StsRefreshTo...	Success		AlexW@contoso.com	fin_password_...
12/2/2020, 9:10:37 AM	Core Directory	UserManagement	Reset user password	Success		AlexW@contoso.com	fin_password_...
12/1/2020, 7:03:37 PM	Core Directory	UserManagement	Add a deletion-mark...	Success		Office 365 SharePoin...	admin@contoso
12/1/2020, 7:03:37 PM	Core Directory	UserManagement	Remove app role ass...	Success		Office 365 SharePoin...	admin@contoso
12/1/2020, 7:02:25 PM	Core Directory	ApplicationManage...	Add service principal	Success		Microsoft_Azure_Su...	Windows Azur...

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 Classification on your data



Thank you

Questions?