Making sense of Microsoft 365 Guest & External Access

@thomasvochten

About me

Thomas Vochten

Technology Evangelist ☕ ☁ 💻 🎹 🏃
#Microsoft365 #Azure #CommunityRocks

@thomasvochten
https://thomasvochten.com
mail@thomasvochten.com

Microsoft® Most Valuable Professional

BIWUG

CRONOS GROEP

Agenda

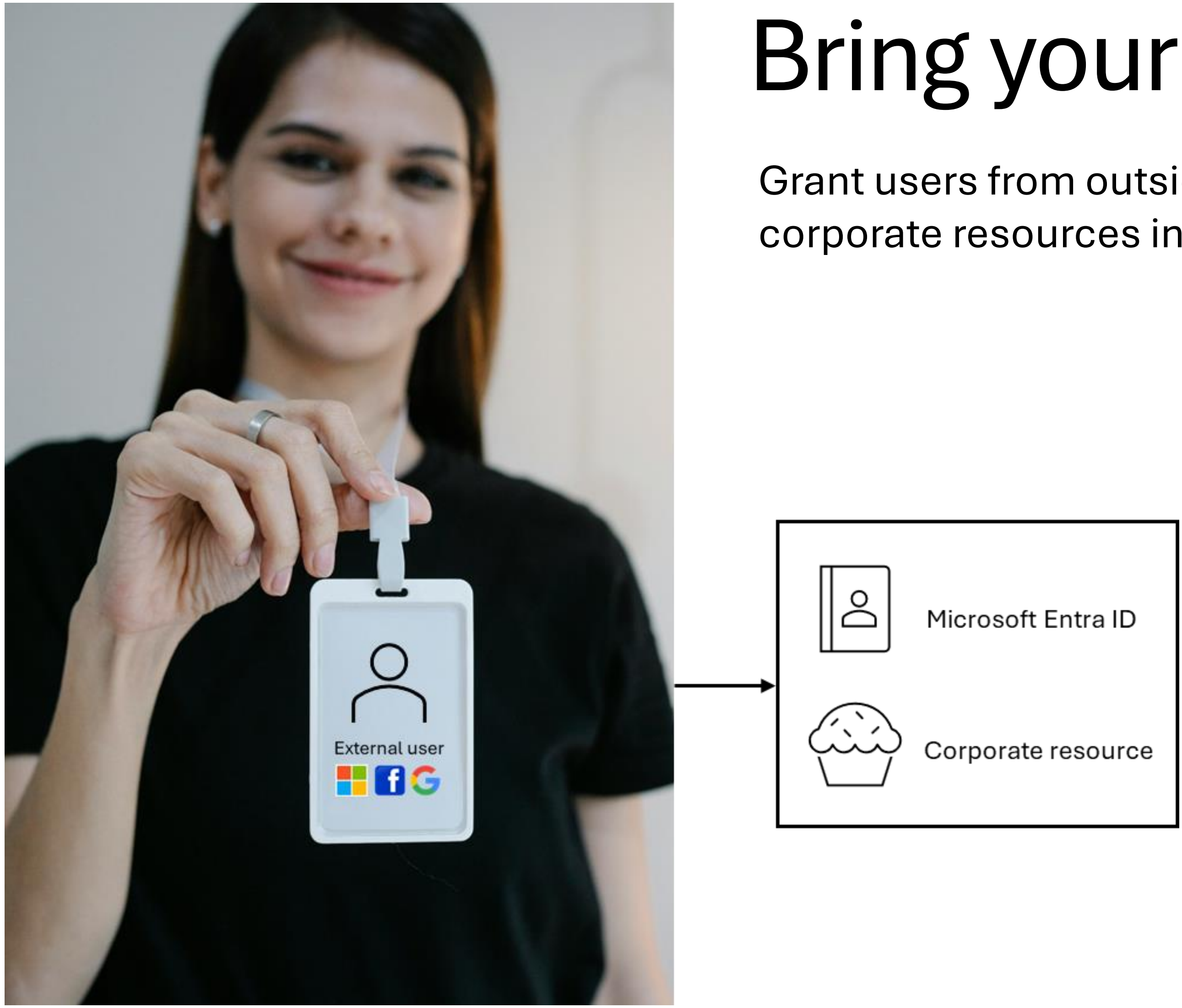
- The what and why of external access
- How to manage guests & external users
- Enforcing security policies on guests
- Microsoft 365 workload specific aspects

External Access in M365: the what and why

@thomasvochten

Bring your own ID

Grant users from outside your organization access to corporate resources in a controlled way.



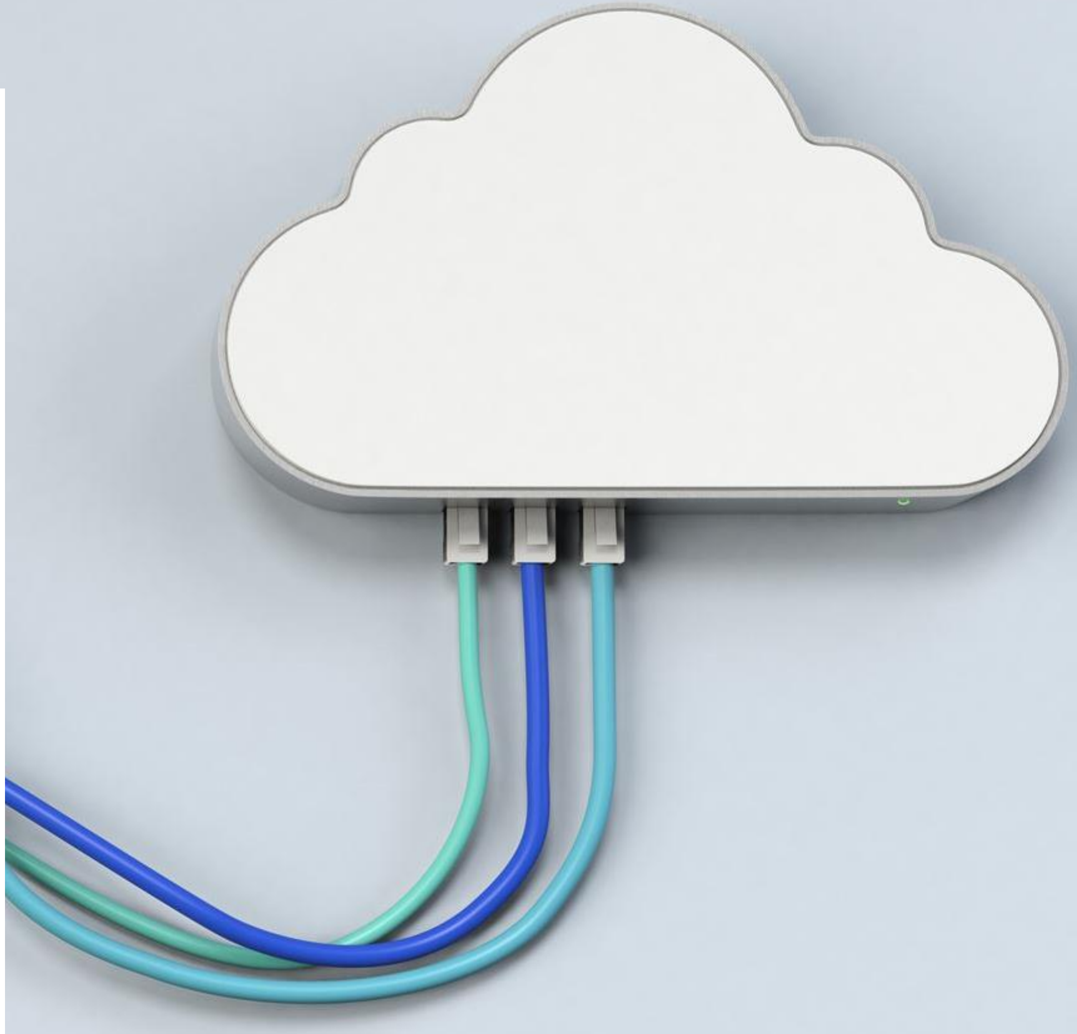
Microsoft Entra ID

Corporate resource

Meet Microsoft Entra External ID

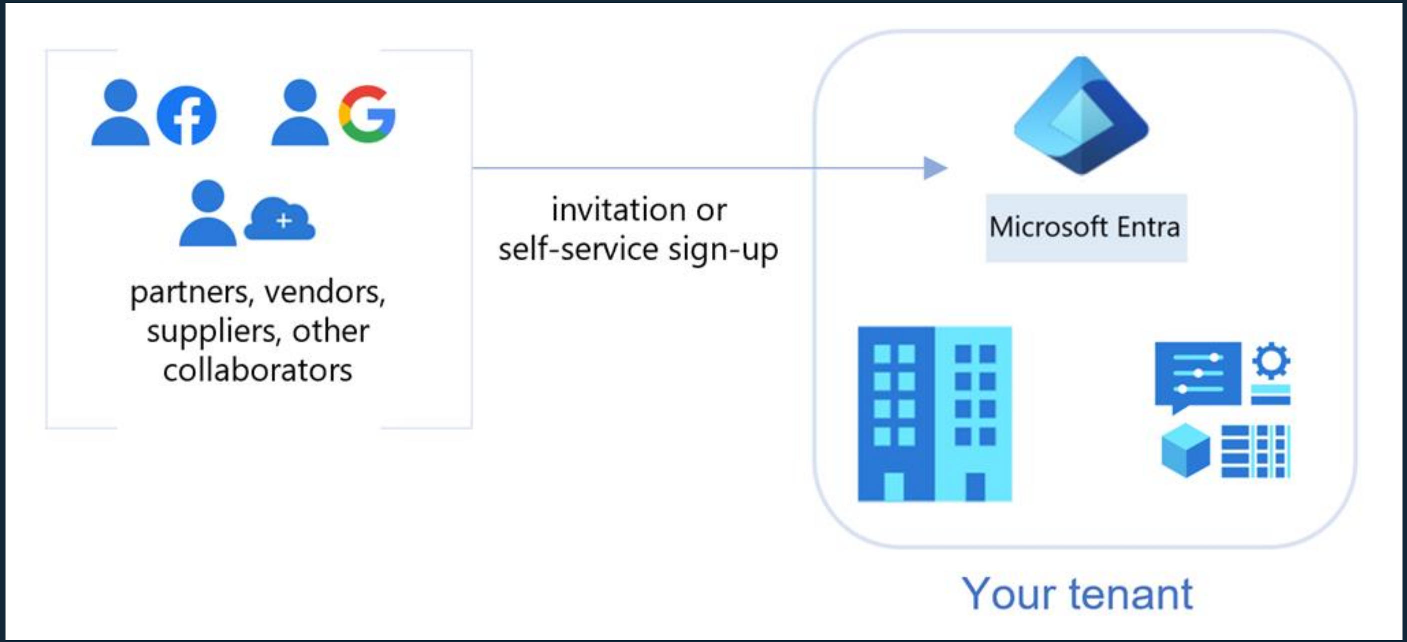
- Foundation for all Microsoft 365 external access scenarios
- Most relevant for us:

B2B Collaboration
B2B Connect



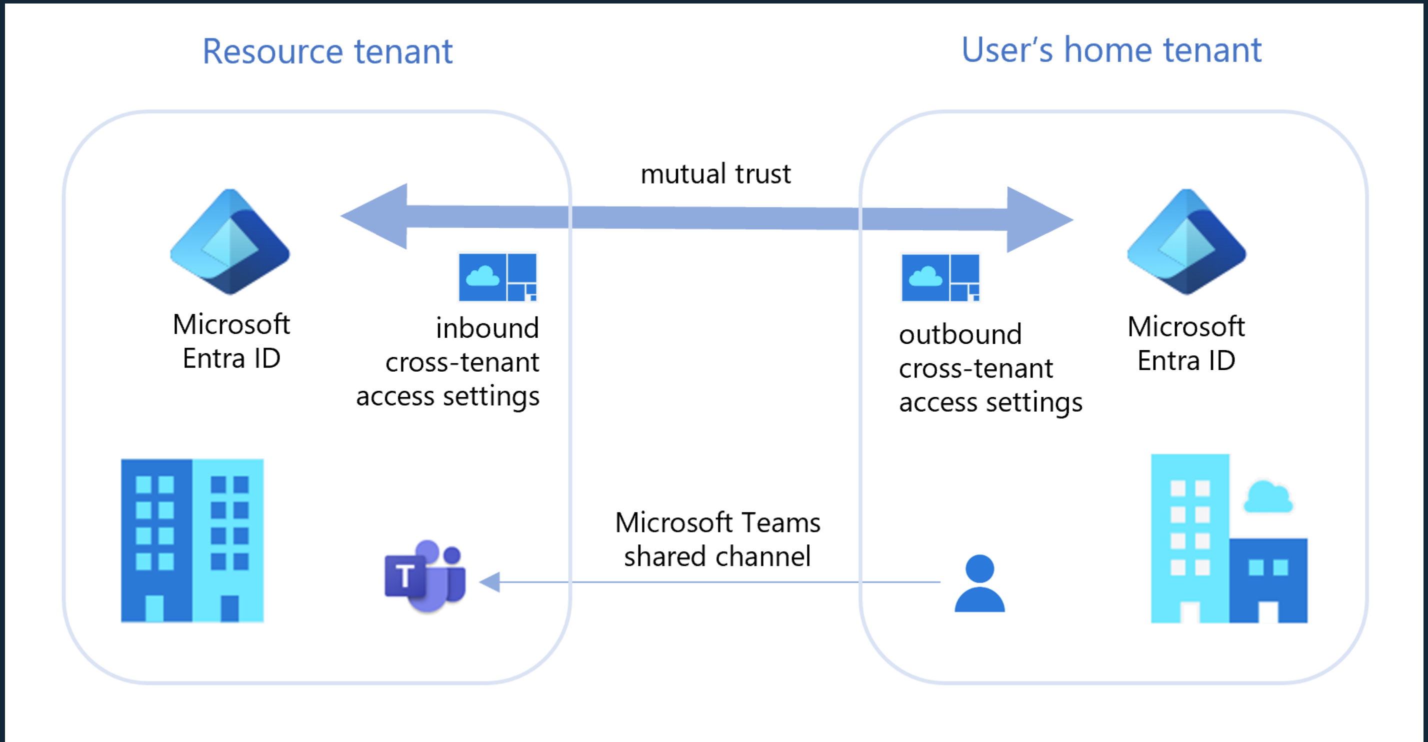
B2B Collaboration

- Resource & user tenants
- Share access to Teams, SharePoint & OneDrive
- One-way trust


partners, vendors, suppliers, other collaborators
invitation or self-service sign-up
Microsoft Entra
Your tenant

B2B Connect

- To support Teams shared channels
- Two-way trust


Resource tenant
User's home tenant
mutual trust
Microsoft Entra ID
inbound cross-tenant access settings
outbound cross-tenant access settings
Microsoft Entra ID
Microsoft Teams shared channel

How to manage guests & external users

Basic operations

- You need at least the Guest Inviter role
- Entra ID portal or PowerShell
- Invitations are sent through e-mail

https://entra.microsoft.com

Demo

Basic guest management

Noteworthy external user properties

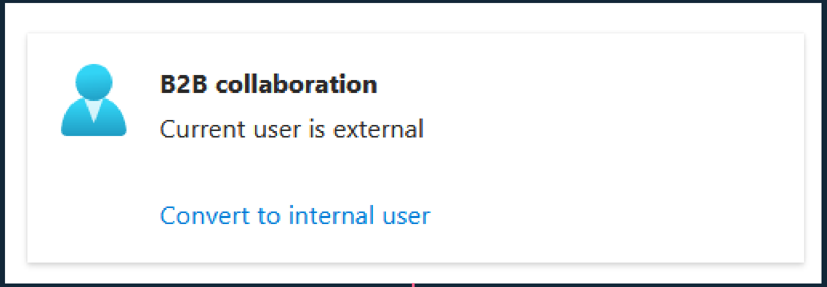
- User Principal Name
- Identities

```
ExternalAzureAD
Microsoft account
google.com
facebook.com
mail
[issuer URI]
```

User Type confusion: guests vs members

- External guest
- External member
- Internal guest
- Internal member

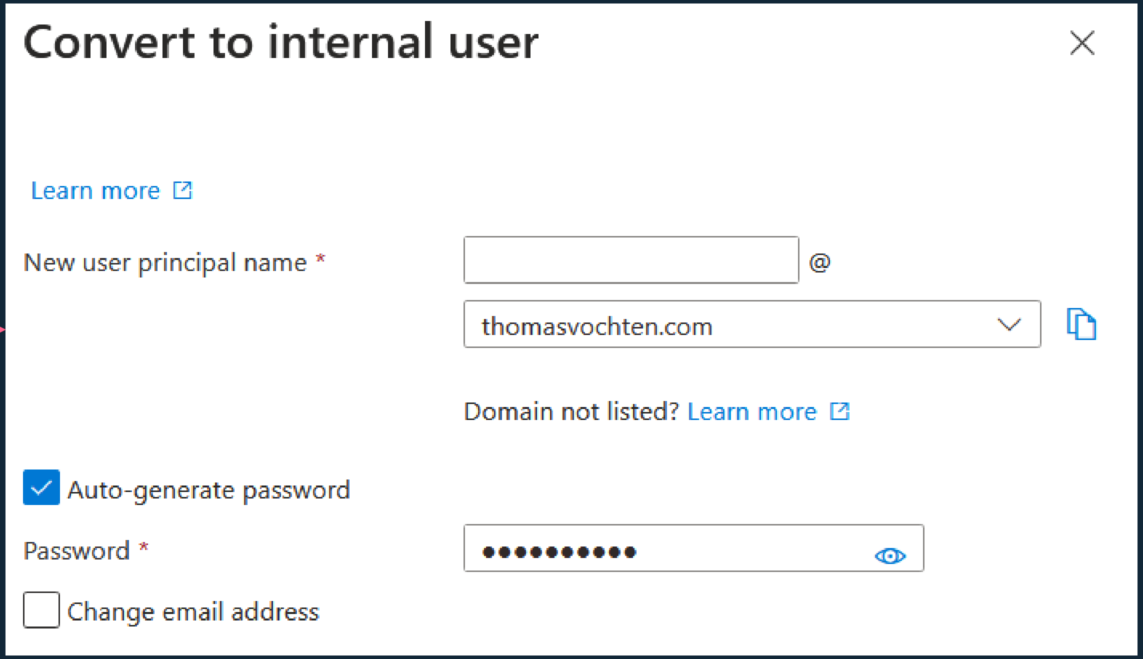
Convert an external user to an internal user



B2B collaboration

Current user is external

Convert to internal user



Convert to internal user

Learn more

New user principal name * ______ @

thomasvochten.com

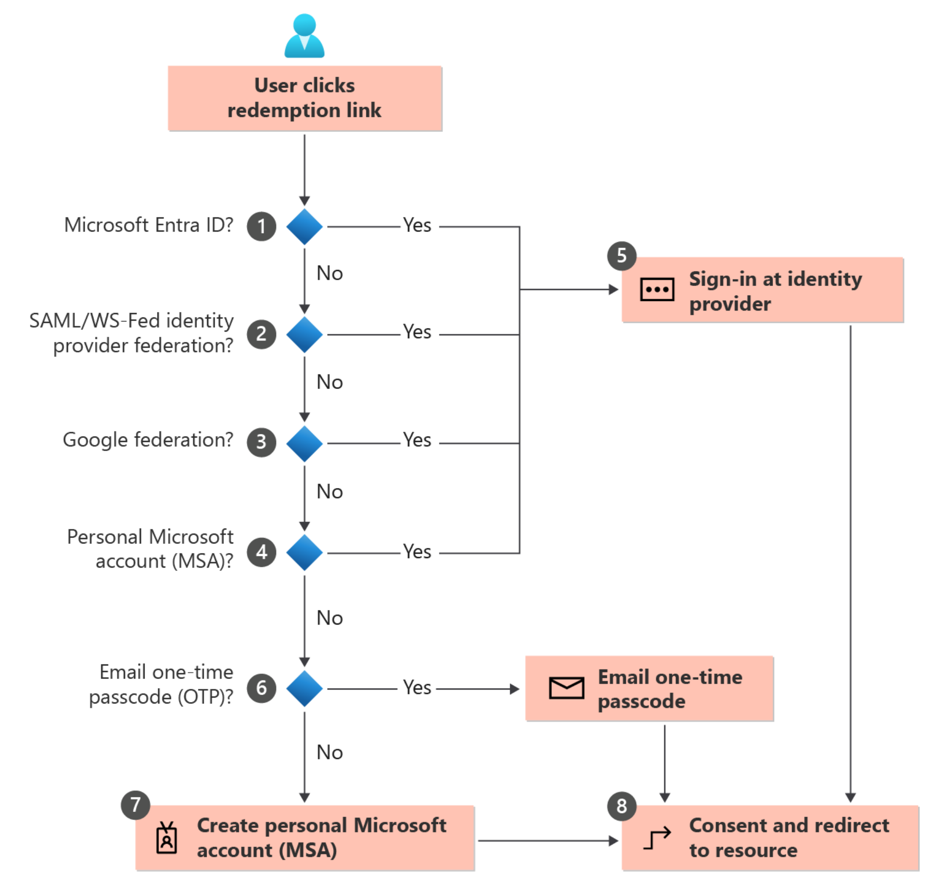
Domain not listed? Learn more

☑ Auto-generate password

Password * ●●●●●●●●●●

□ Change email address

Guest invitation & redemption process



User clicks redemption link

1 Microsoft Entra ID? Yes → 5; No ↓

2 SAML/WS-Fed identity provider federation? Yes → 5; No ↓

3 Google federation? Yes → 5; No ↓

4 Personal Microsoft account (MSA)? Yes → 5; No ↓

5 Sign-in at identity provider → 8

6 Email one-time passcode (OTP)? Yes → Email one-time passcode → 8; No ↓

7 Create personal Microsoft account (MSA) → 8

8 Consent and redirect to resource

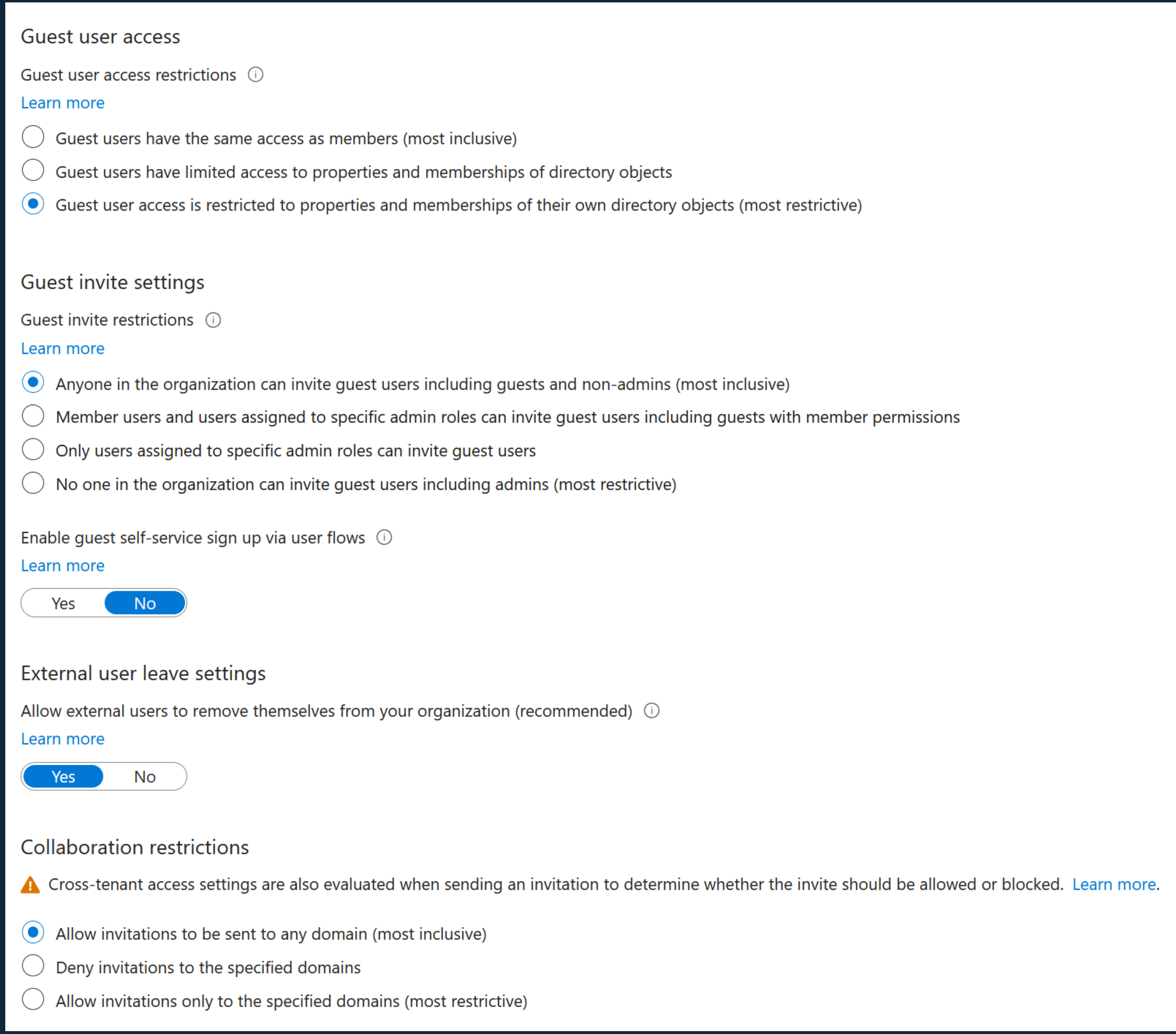
@thomasvochten

Supported Identity Providers

- Microsoft Entra ID
- Microsoft Account
- Email one-time passcode (OTP)
- SAML/WS-Fed
- Google
- Facebook

Collaboration Settings

- Manage invitation settings
- Manage what guests can see
- Manage if guests can remove themselves from your org
- Specific settings for users *not* coming from another Entra ID tenant.



Guest user access

Guest user access restrictions ⓘ

Learn more

○ Guest users have the same access as members (most inclusive)
○ Guest users have limited access to properties and memberships of directory objects
● Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Guest invite restrictions ⓘ

Learn more

● Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
○ 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
○ No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows ⓘ

Learn more

Yes [✓ No]

External user leave settings

Allow external users to remove themselves from your organization (recommended) ⓘ

Learn more

[✓ Yes] No

Collaboration restrictions

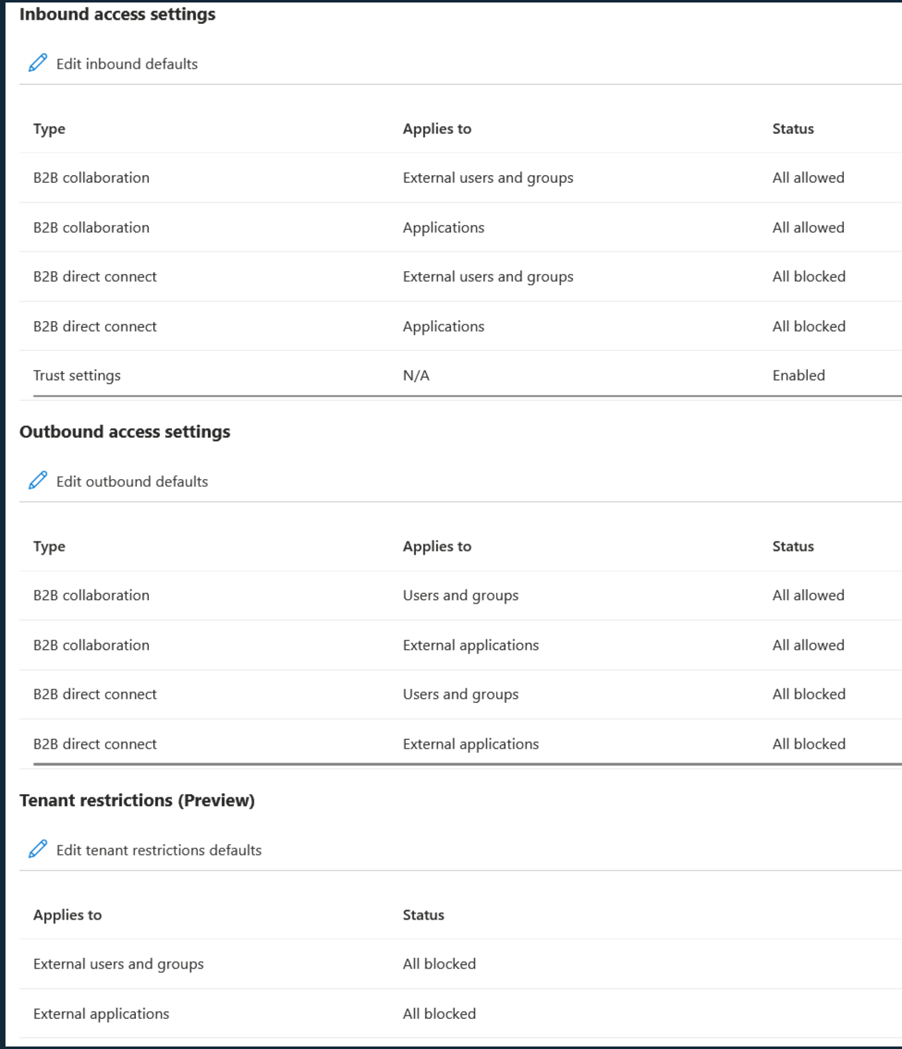
⚠ Cross-tenant access settings are also evaluated when sending an invitation to determine whether the invite should be allowed or blocked. Learn more.

● 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)

@thomasvochten

Cross-tenant access settings

- Valid for guests coming from another Entra ID tenant
- Inbound & Outbound settings
- Organization-specific settings
- Enable or disable collaboration with other Microsoft clouds



Inbound access settings

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Enabled

Outbound access settings

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked

Tenant restrictions (Preview)

Applies to	Status
External users and groups	All blocked
External applications	All blocked

Demo

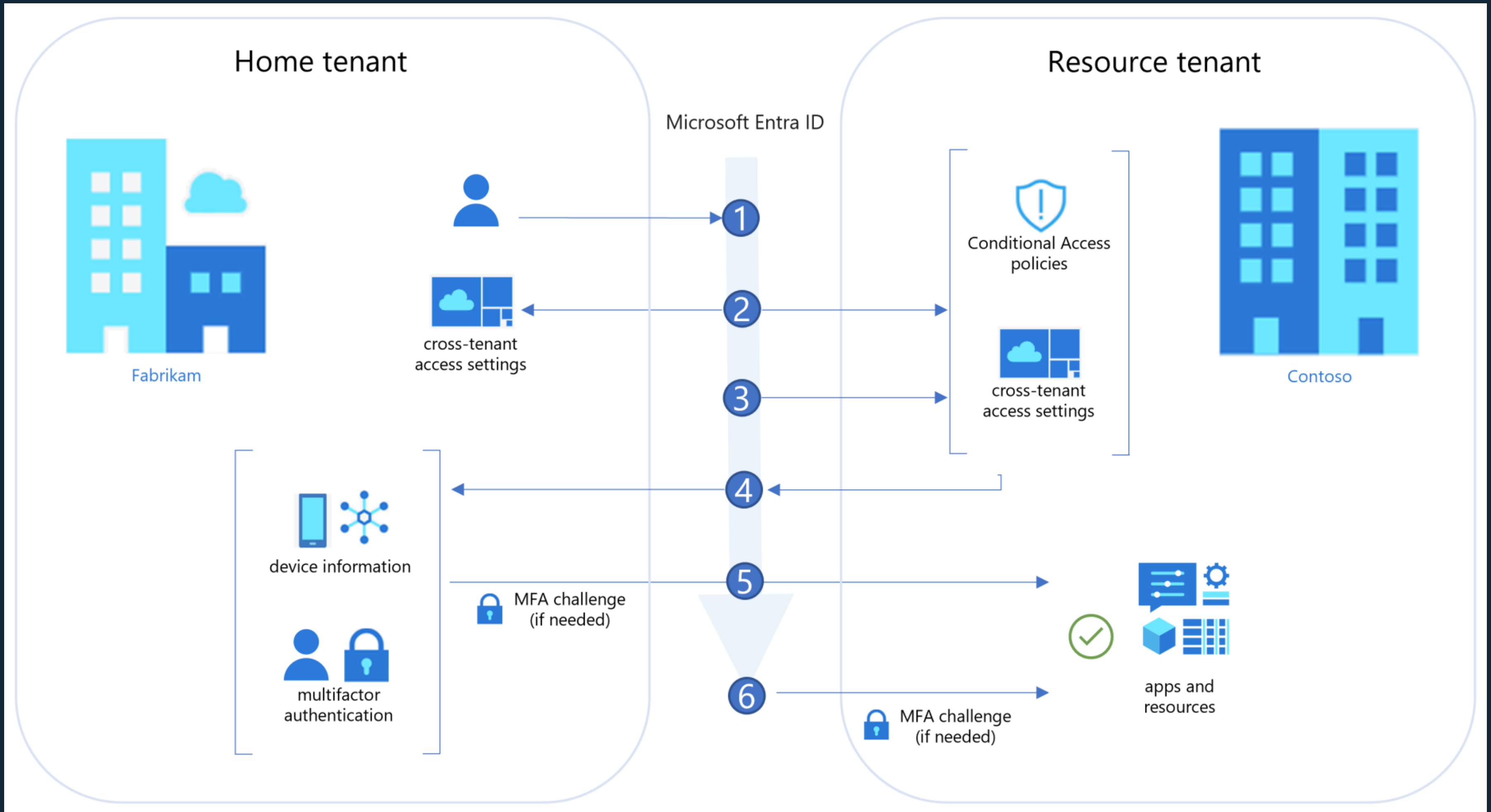
Settings, settings, settings

Guests lifecycle management

- Allow guests to remove themselves from your organization
- What about self-service capabilities?
- Basic capabilities included for free
- Microsoft Entra ID Governance (add-on 😞)
    - Access reviews for guests
    - More advanced workflows

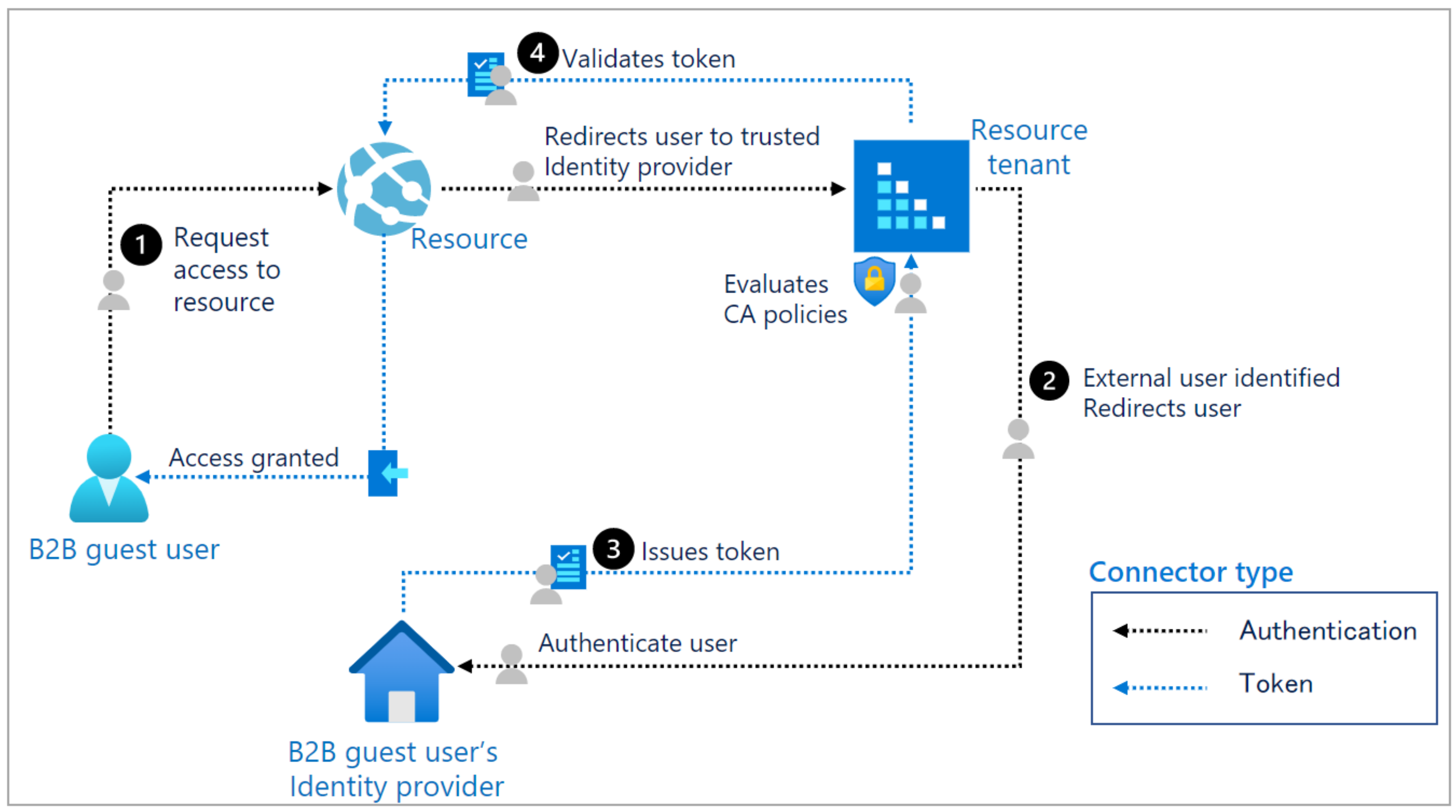
Securing guest access

AuthN for guests coming from another tenant


Home tenant
Resource tenant
Microsoft Entra ID
Fabrikam
1
2
cross-tenant access settings
3
4
5
6
Conditional Access policies
cross-tenant access settings
Contoso
device information
multifactor authentication
MFA challenge (if needed)
MFA challenge (if needed)
apps and resources

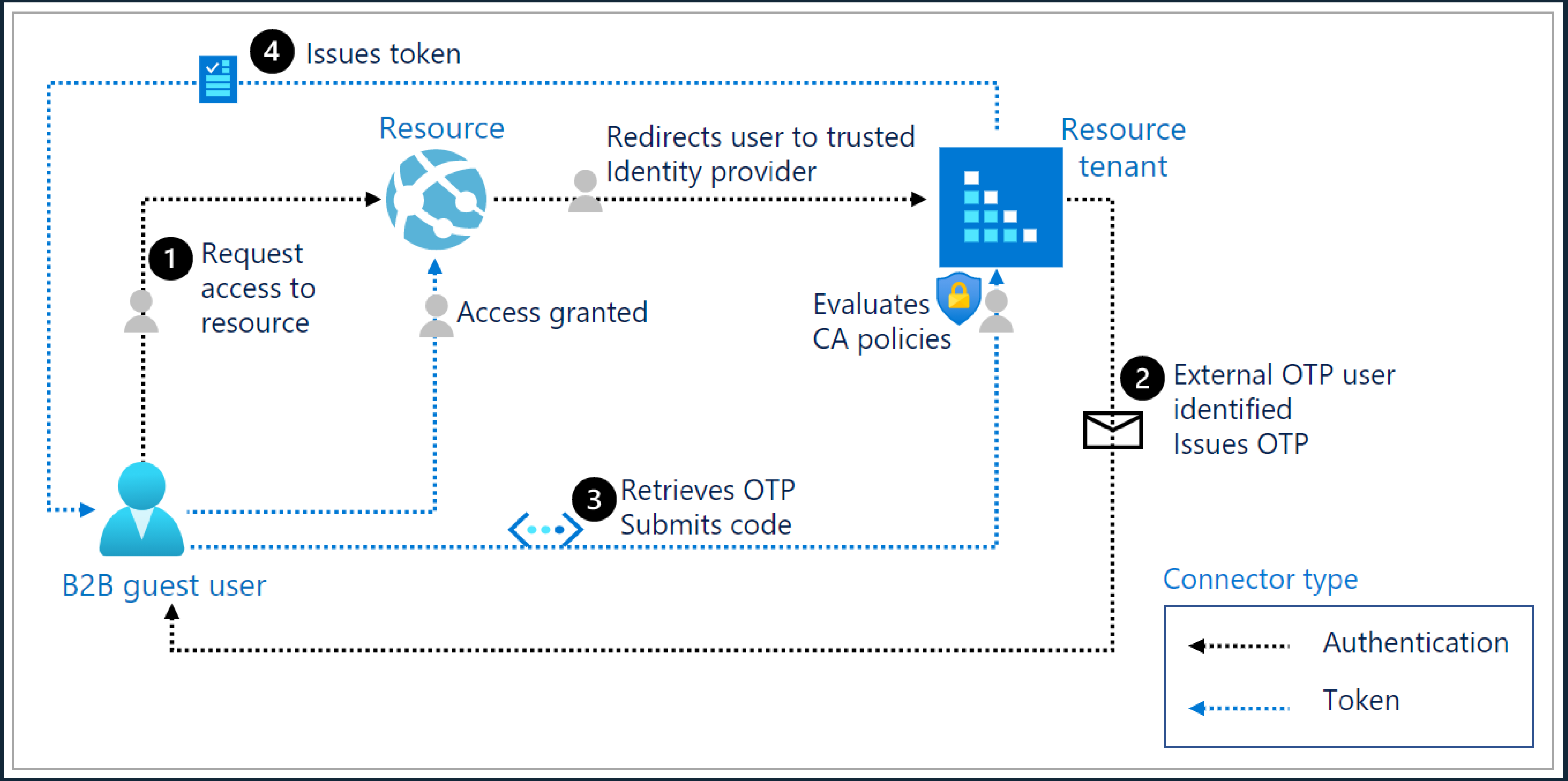
@thomasvochten

AuthN for guests not using another tenant



@thomasvochten

AuthN for guests using OTP


4 Issues token
Resource
Redirects user to trusted Identity provider
Resource tenant
1 Request access to resource
Access granted
Evaluates CA policies
2 External OTP user identified Issues OTP
3 Retrieves OTP Submits code
B2B guest user
Connector type
Authentication
Token

@thomasvochten

Conditional access for guests

Grant controls

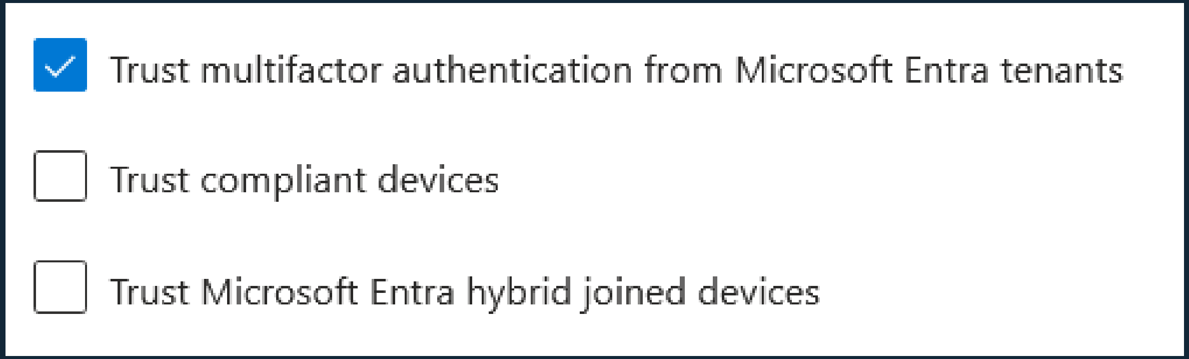
- Block access
- Require MFA
- Require compliant device
- Require hybrid joined device
- Terms of use

Session controls

- Use app enforced restrictions
- Use conditional access app control
- Sign-in frequency
- Persistent browser session

What about MFA?

- Force guest users to register for MFA in **your** tenant or **theirs**
- Entra ID can honor compliancy status from other tenants:

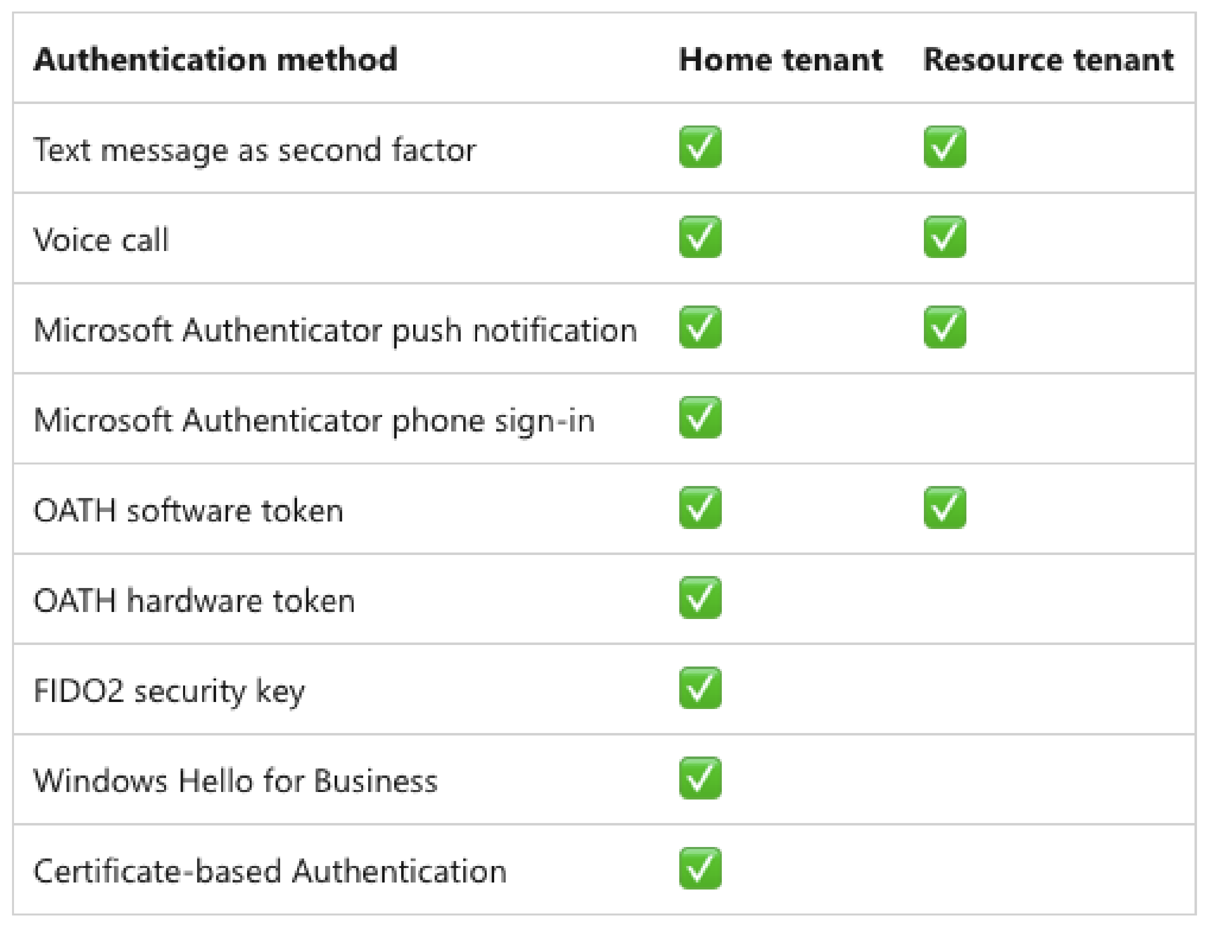


☑ Trust multifactor authentication from Microsoft Entra tenants

□ Trust compliant devices

□ Trust Microsoft Entra hybrid joined devices

MFA Authentication methods for guests

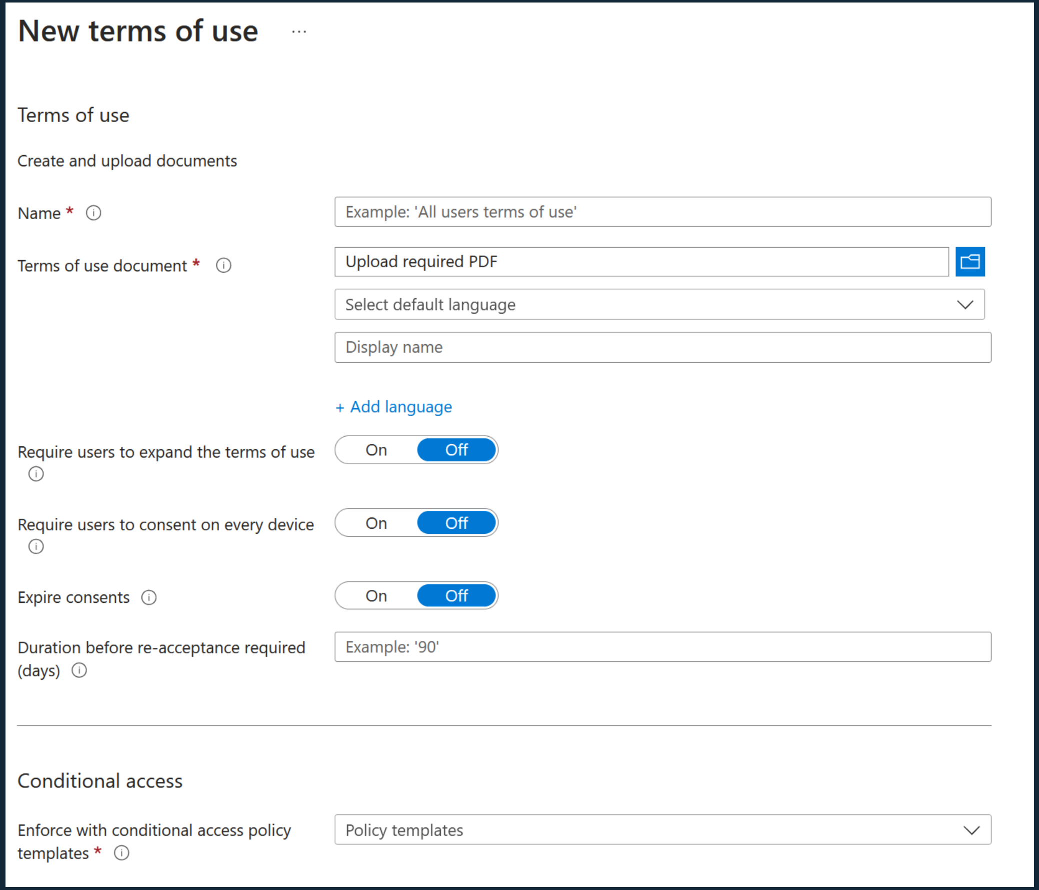


Authentication method	Home tenant	Resource tenant
Text message as second factor	✅	✅
Voice call	✅	✅
Microsoft Authenticator push notification	✅	✅
Microsoft Authenticator phone sign-in	✅	
OATH software token	✅	✅
OATH hardware token	✅	
FIDO2 security key	✅	
Windows Hello for Business	✅	
Certificate-based Authentication	✅	

Demo

Conditional access & MFA

Terms of use for guests



New terms of use

Terms of use

Create and upload documents

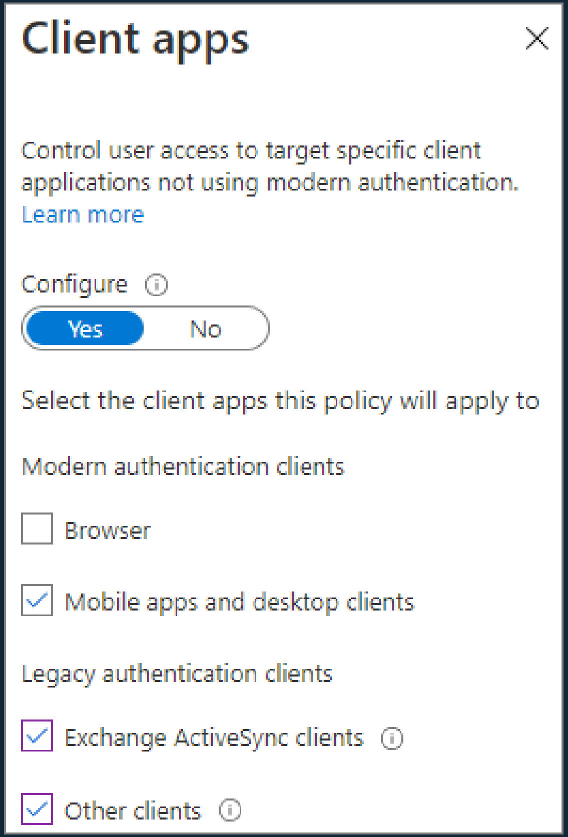
Name *	Example: 'All users terms of use'
Terms of use document *	Upload required PDF Select default language Display name + Add language
Require users to expand the terms of use	On [✓ Off]
Require users to consent on every device	On [✓ Off]
Expire consents	On [✓ Off]
Duration before re-acceptance required (days)	Example: '90'

Conditional access

Enforce with conditional access policy templates *	Policy templates

@thomasvochten

Web-only access for guests



Client apps

Control user access to target specific client applications not using modern authentication.
Learn more

Configure ⓘ

[✓ Yes] No

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☑ Mobile apps and desktop clients

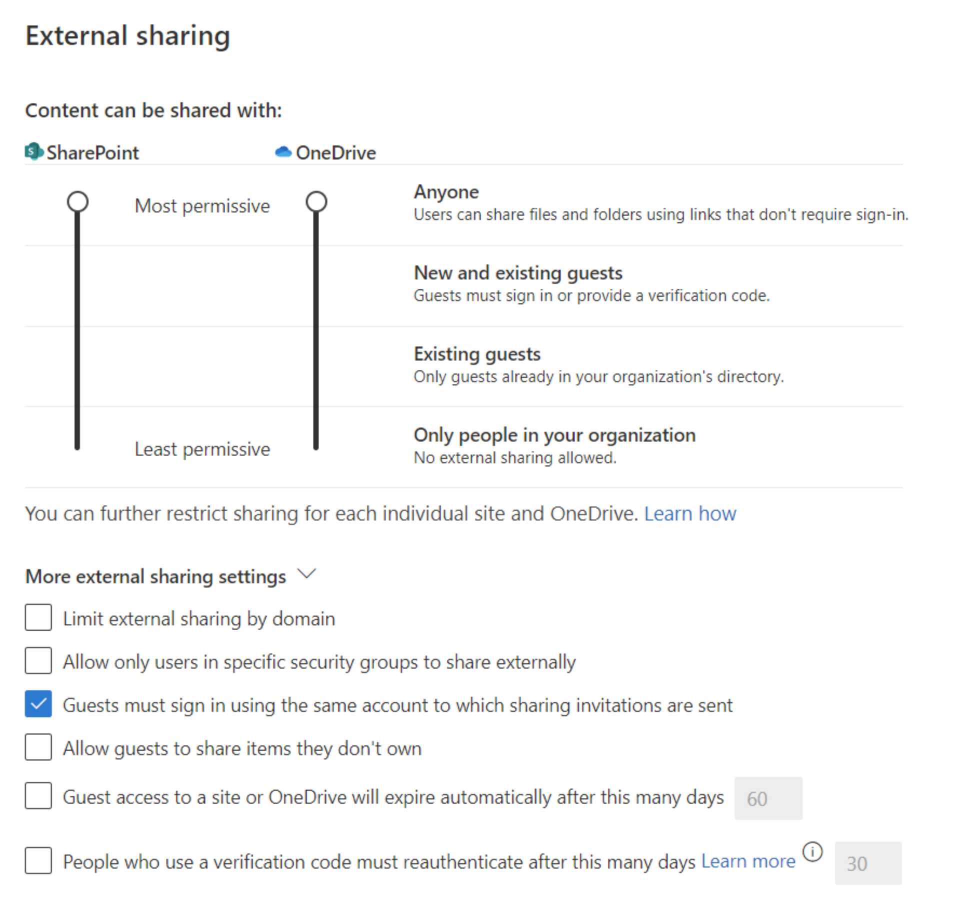
Legacy authentication clients

☑ Exchange ActiveSync clients ⓘ

☑ Other clients ⓘ

M365 Workloads

Sharing in SharePoint & OneDrive



External sharing

Content can be shared with:

Anyone
Users can share files and folders using links that don't require sign-in.

New and existing guests
Guests must sign in or provide a verification code.

Existing guests
Only guests already in your organization's directory.

Only people in your organization
No external sharing allowed.

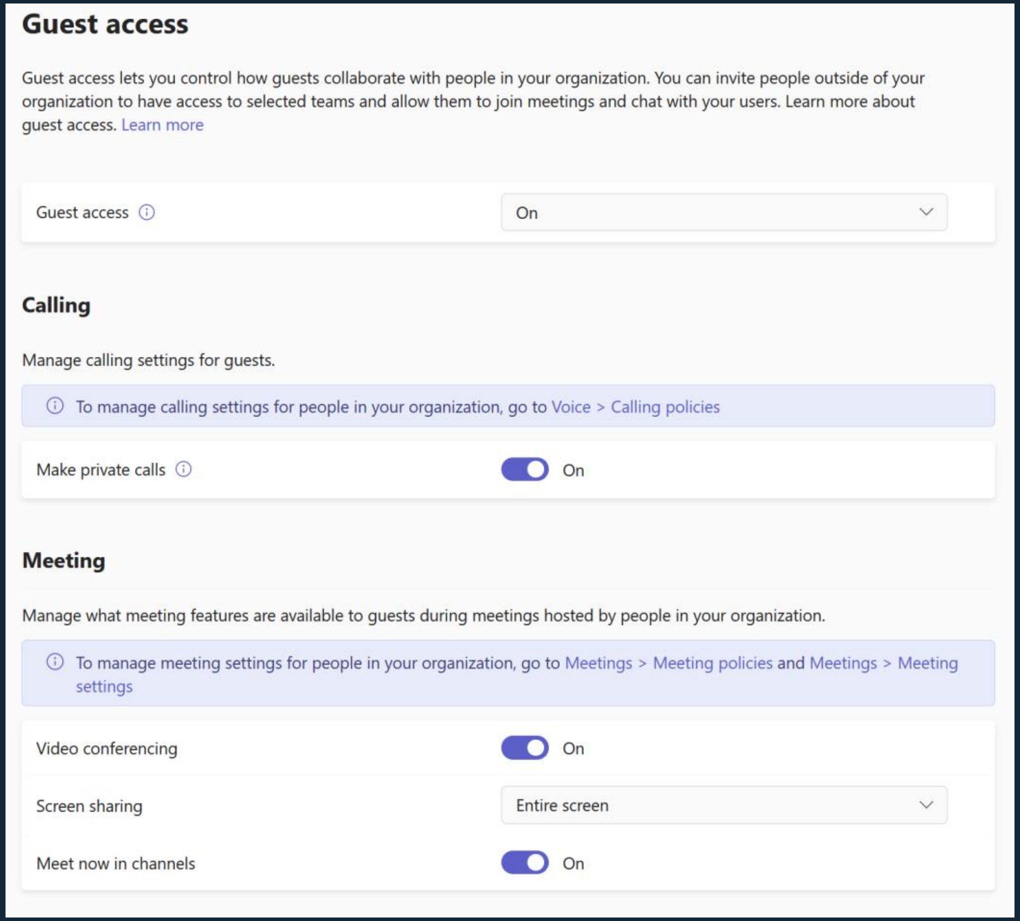
You can further restrict sharing for each individual site and OneDrive. Learn how

More external sharing settings

- □ Limit external sharing by domain
- □ Allow only users in specific security groups to share externally
- ☑ Guests must sign in using the same account to which sharing invitations are sent
- □ Allow guests to share items they don't own
- □ Guest access to a site or OneDrive will expire automatically after this many days 60
- □ People who use a verification code must reauthenticate after this many days Learn more ⓘ 30

@thomasvochten

Microsoft Teams – Guest Access



Guest access

Guest access lets you control how guests collaborate with people in your organization. You can invite people outside of your organization to have access to selected teams and allow them to join meetings and chat with your users. Learn more about guest access. Learn more

Guest access ⓘ	On

Calling

Manage calling settings for guests.

ⓘ To manage calling settings for people in your organization, go to Voice > Calling policies

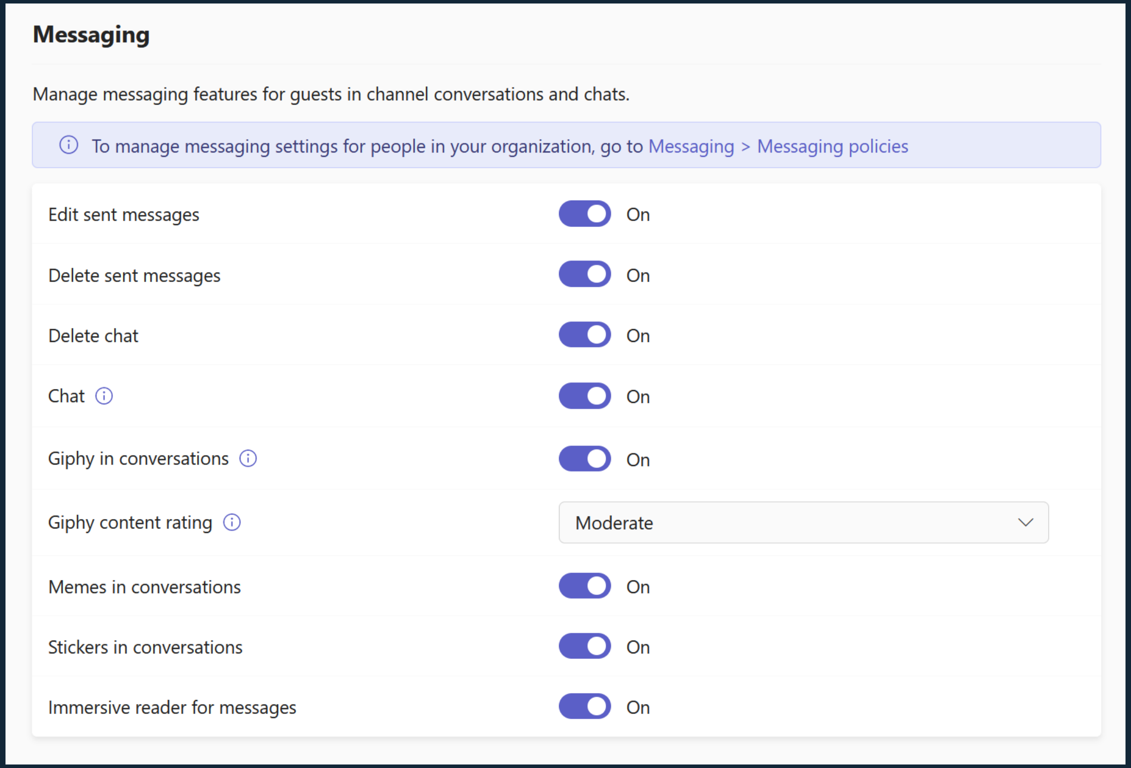
Make private calls ⓘ	On

Meeting

Manage what meeting features are available to guests during meetings hosted by people in your organization.

ⓘ To manage meeting settings for people in your organization, go to Meetings > Meeting policies and Meetings > Meeting settings

Video conferencing	On
Screen sharing	Entire screen
Meet now in channels	On



Messaging

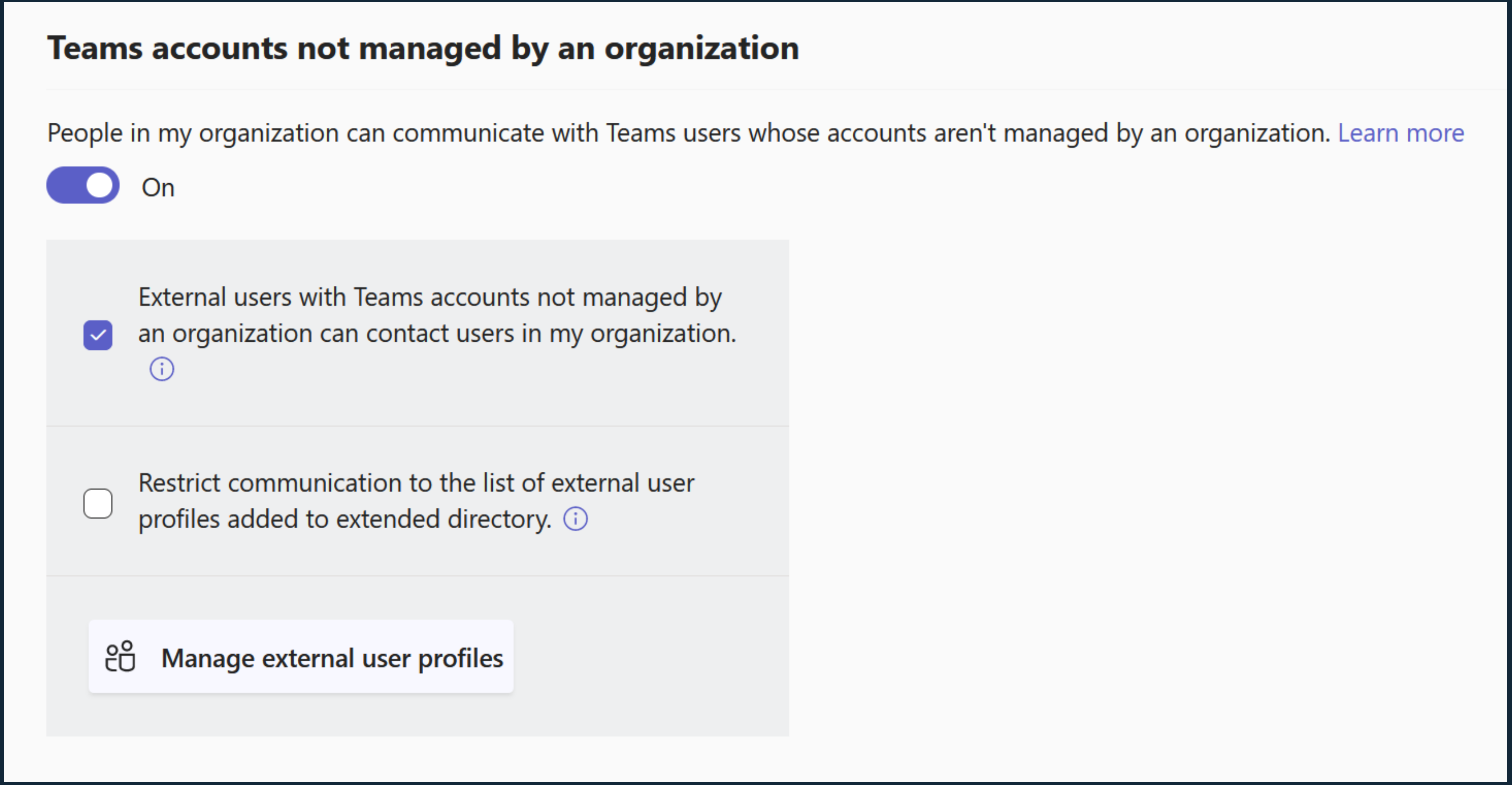
Manage messaging features for guests in channel conversations and chats.

ⓘ To manage messaging settings for people in your organization, go to Messaging > Messaging policies

Edit sent messages	On
Delete sent messages	On
Delete chat	On
Chat ⓘ	On
Giphy in conversations ⓘ	On
Giphy content rating ⓘ	Moderate
Memes in conversations	On
Stickers in conversations	On
Immersive reader for messages	On

@thomasvochten

Microsoft Teams - External Access



Teams accounts not managed by an organization

People in my organization can communicate with Teams users whose accounts aren't managed by an organization. Learn more

● On

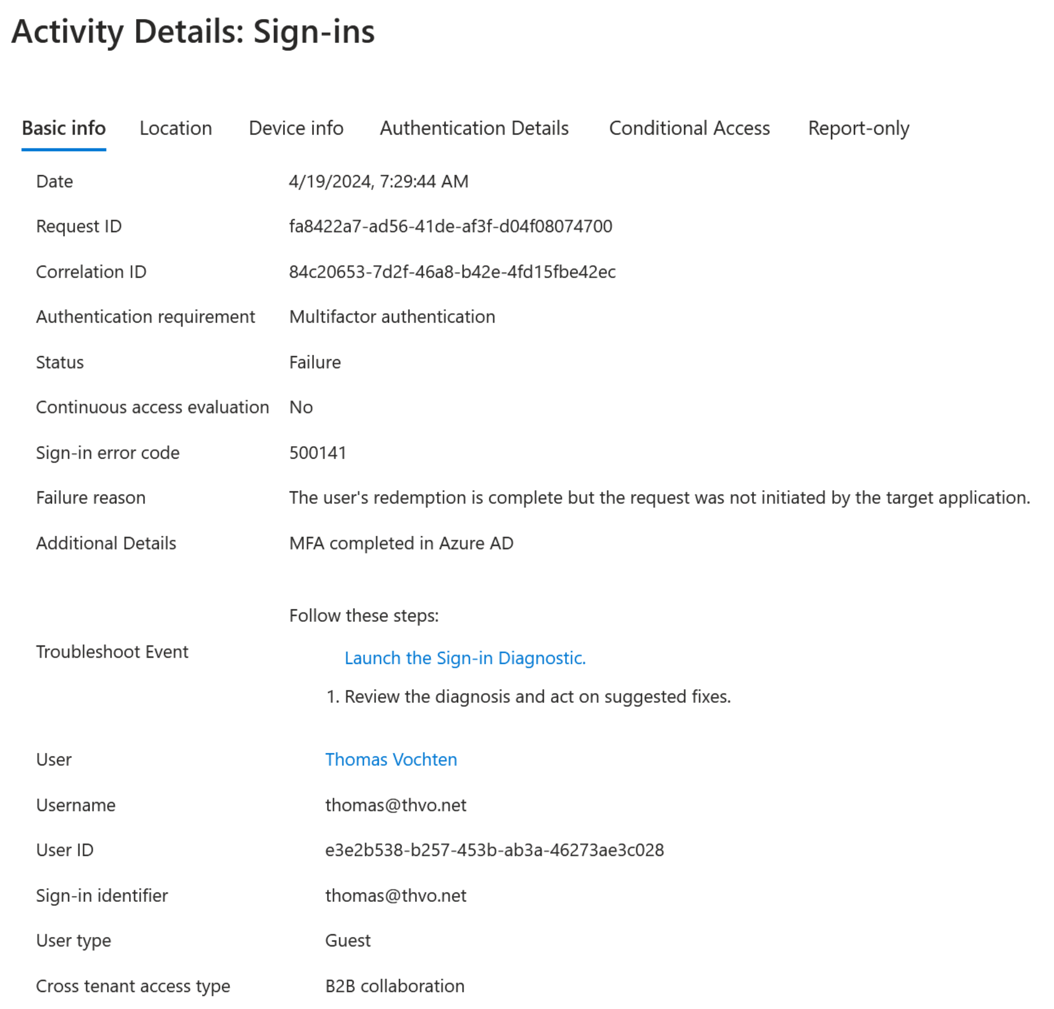
☑ External users with Teams accounts not managed by an organization can contact users in my organization. ⓘ

□ Restrict communication to the list of external user profiles added to extended directory. ⓘ

@thomasvochten

What about monitoring?

- Audit guests as you would with normal users (sign-in or audit logs, Sentinel,…)
- Try the “Cross-tenant activity workbook”



Activity Details: Sign-ins

Date	4/19/2024, 7:29:44 AM
Request ID	fa8422a7-ad56-41de-af3f-d04f08074700
Correlation ID	84c20653-7d2f-46a8-b42e-4fd15fbe42ec
Authentication requirement	Multifactor authentication
Status	Failure
Continuous access evaluation	No
Sign-in error code	500141
Failure reason	The user's redemption is complete but the request was not initiated by the target application.
Additional Details	MFA completed in Azure AD
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	Thomas Vochten
Username	thomas@thvo.net
User ID	e3e2b538-b257-453b-ab3a-46273ae3c028
Sign-in identifier	thomas@thvo.net
User type	Guest
Cross tenant access type	B2B collaboration

@thomasvochten

Licensing & costs

- 1:5 Microsoft Entra ID to guest license ratio
- Or switch to the “Monthly Active Users” settings
  first 50k guest users are free
- Tip: you can have one Entra ID P2 license to unlock P2 functionalities for all your guest users

Takeaways

- Get familiar with “B2B Collaboration” options
- Evaluate authentication options such as login providers
- Learn about the cross-tenant access settings
- Force Multi Factor Authentication for guests too
- Apply additional conditional access settings

Thank you

@thomasvochten

https://thomasvochten.com

mail@thomasvochten.com

Get the slides