

Making sense of Microsoft 365 Guest & External access

@thomasvochten

About me



Thomas Vochten ☕ ☁️ 💻 🎹 🏃

Technology evangelist Microsoft 365 & Security

@thomasvochten

<https://thomasvochten.com>

mail@thomasvochten.com



Microsoft®
Most Valuable
Professional

BIWUG



Agenda

1. The what and why of external access
2. How to manage guests & external users
3. Enforcing security policies on guests
4. Microsoft 365 workload specific aspects



External Access in M365: the what and why

@thomasvochten

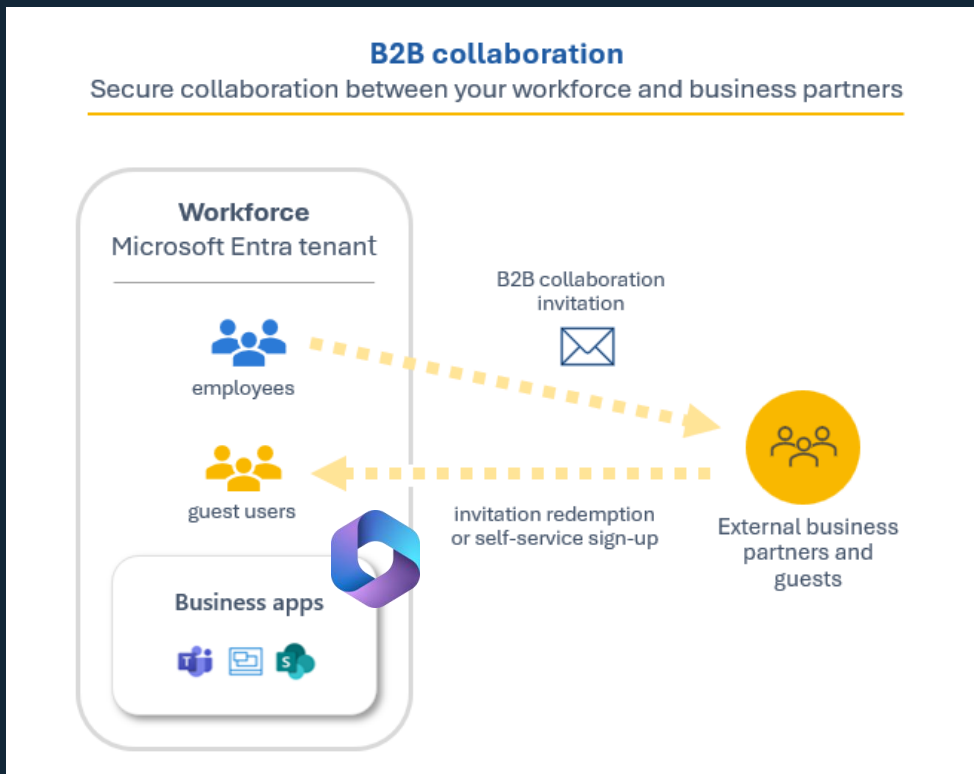


Bring your own ID

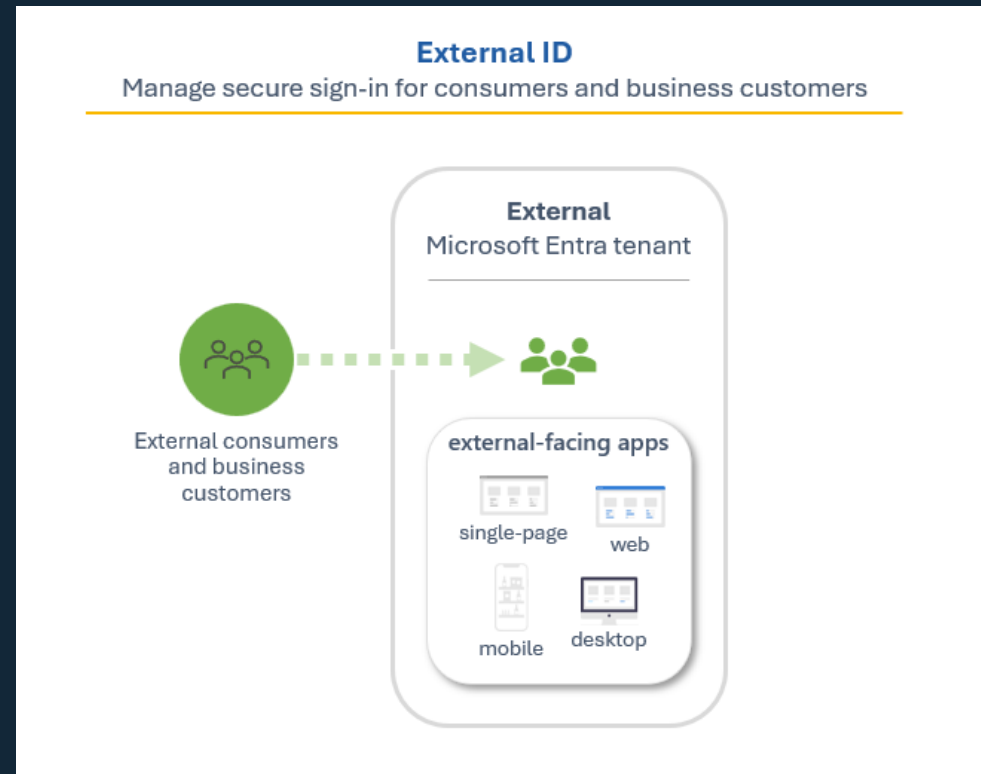
Grant users from outside your organization access to corporate resources in a controlled way.

Meet Entra ID External ID

Workforce tenant configuration

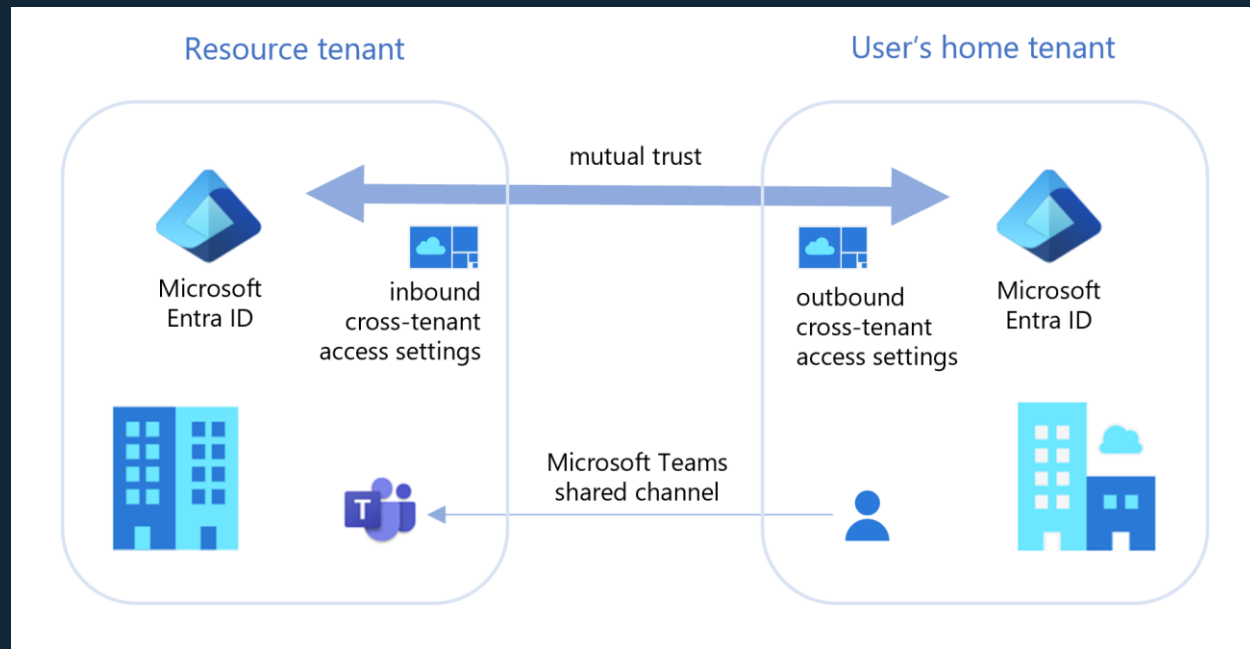
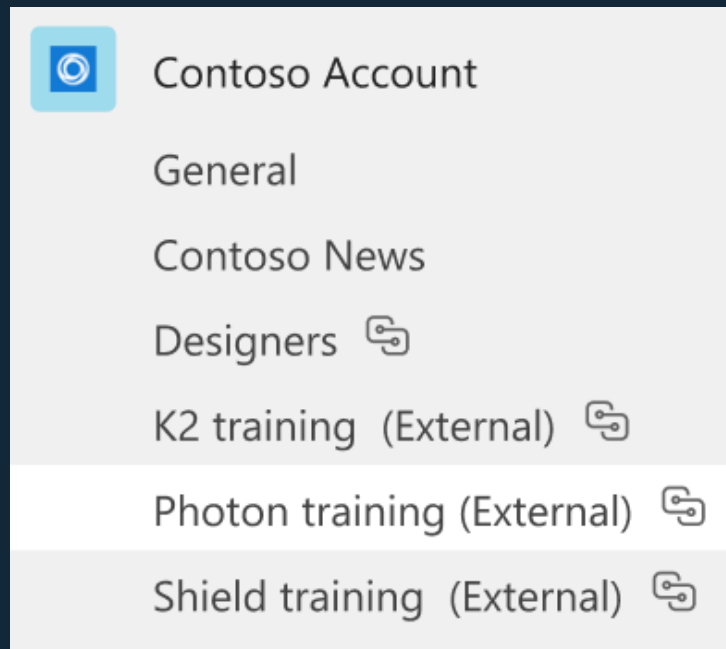


External tenant configuration



What about B2B Direct Connect?

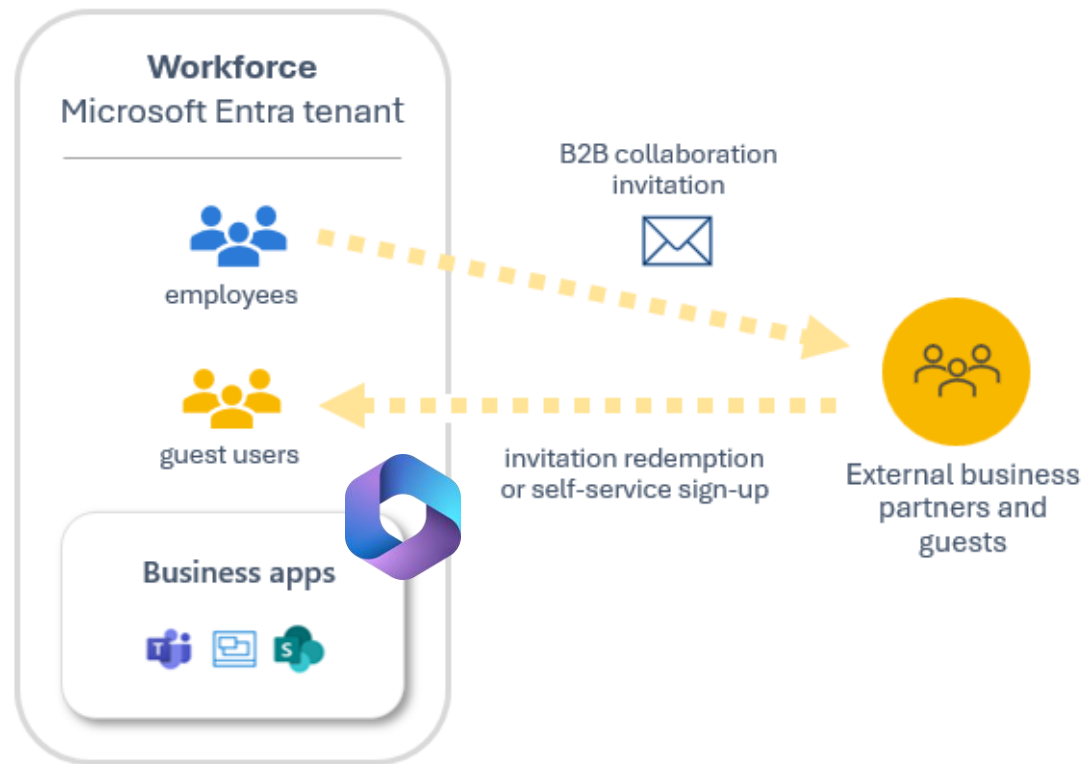
Currently only supports Teams Shared Channels



B2B Collaboration

B2B collaboration

Secure collaboration between your workforce and business partners





How to manage guests & external users

@thomasvochten

Basic operations

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



<https://entra.microsoft.com>

Demo

Basic guest management

@thomasvochten

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  

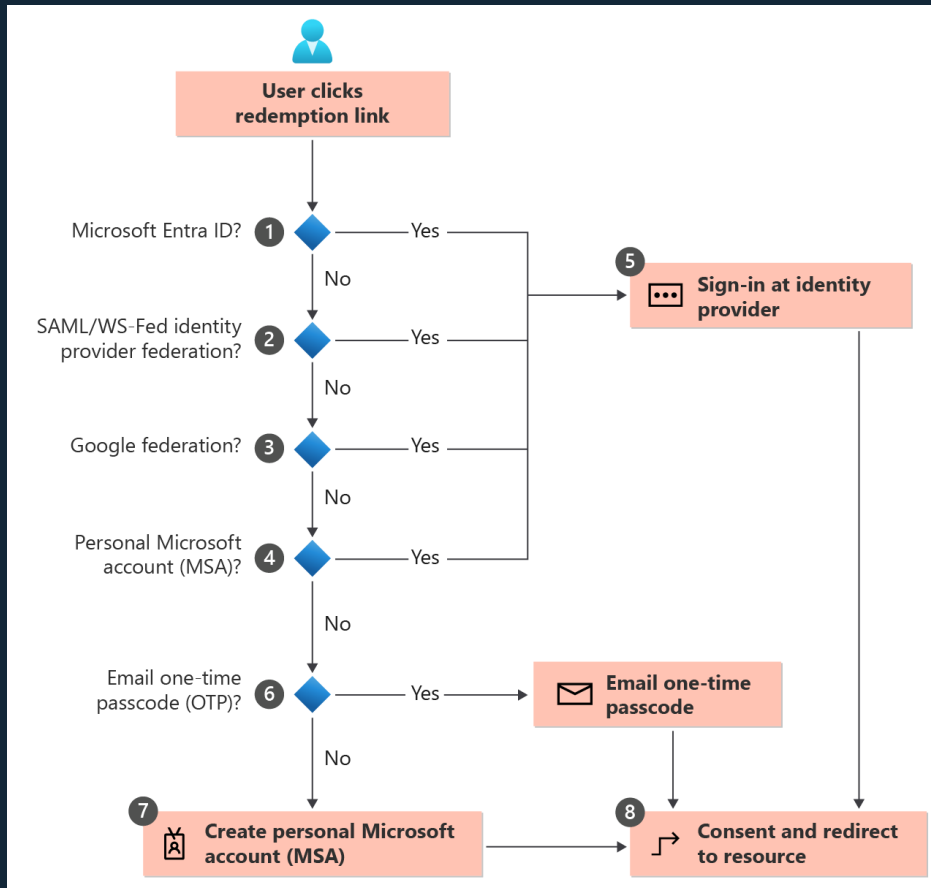
Domain not listed? [Learn more](#) 

☒ Auto-generate password

Password * 

☐ Change email address

Guest invitation & redemption process



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)

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

 Edit inbound defaults

| 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

 Edit outbound defaults

| 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)

 Edit tenant restrictions defaults

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

Demo

Settings & configuring alternative identity providers

@thomasvochten

Guests lifecycle management

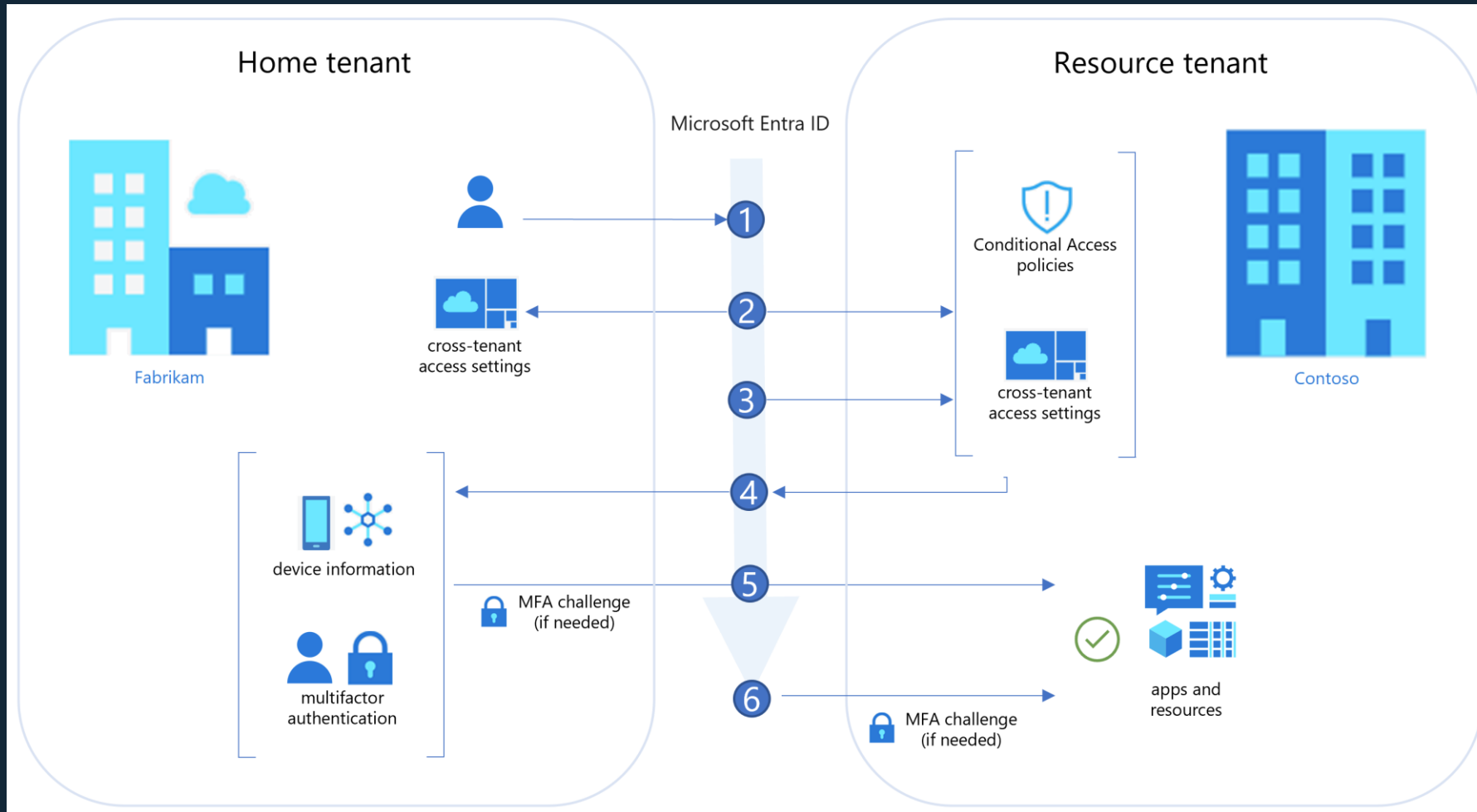
- Allow guests to remove themselves from your organization
- What about self-service capabilities?
- Basic capabilities included for free
- Microsoft Entra ID Governance (add-on 🙄)
 - Access reviews for guests
 - More advanced workflows



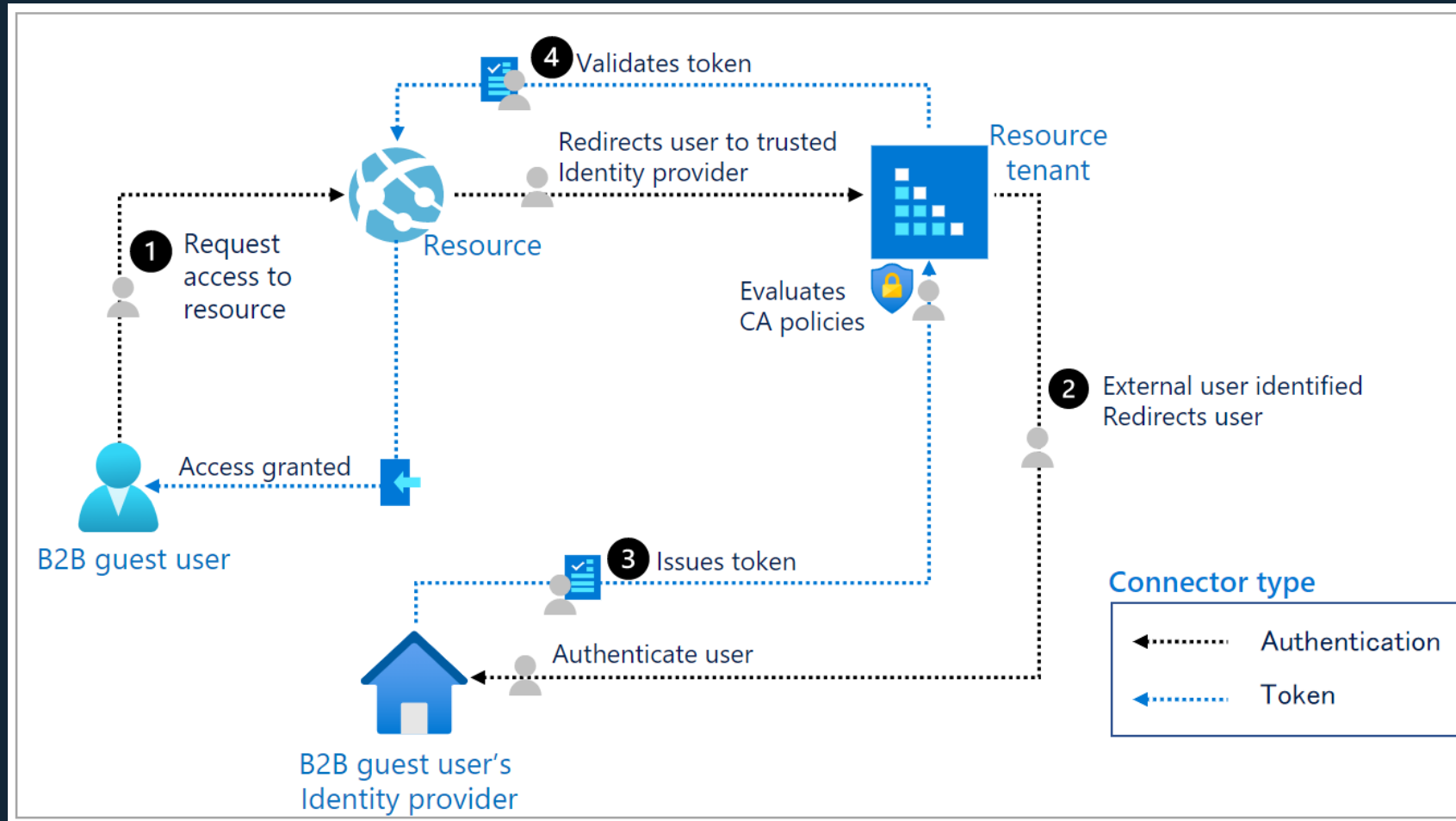
Securing guest access

@thomasvochten

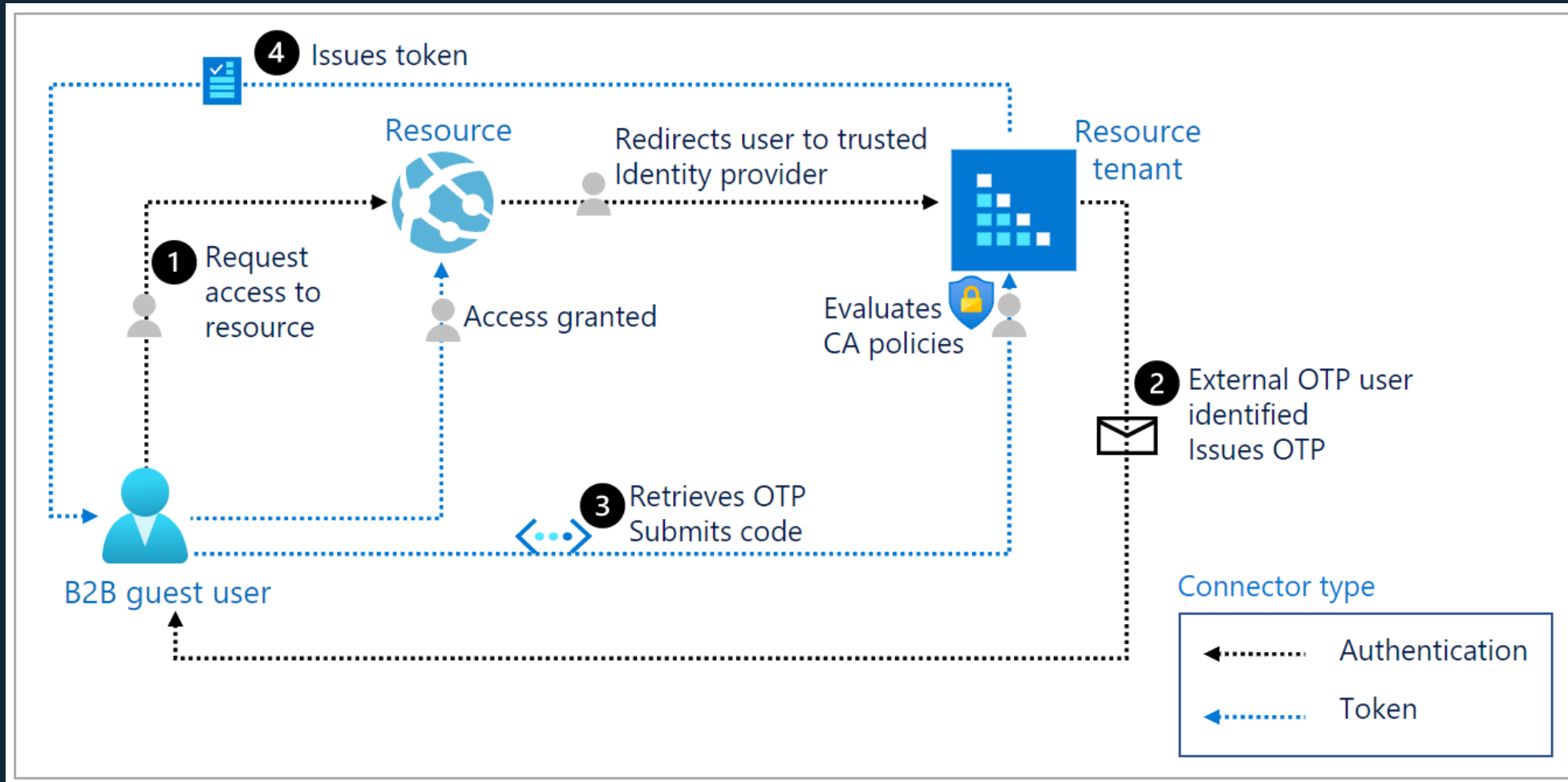
AuthN for guests coming from another tenant



AuthN for guests not using another tenant



AuthN for guests using OTP



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

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

Web-only access for guests

Client apps

×

Control user access to target specific client applications not using modern authentication.
[Learn more](#)

Configure ⓘ

YesNo

Select the client apps this policy will apply to

Modern authentication clients

☐ Browser

☒ Mobile apps and desktop clients

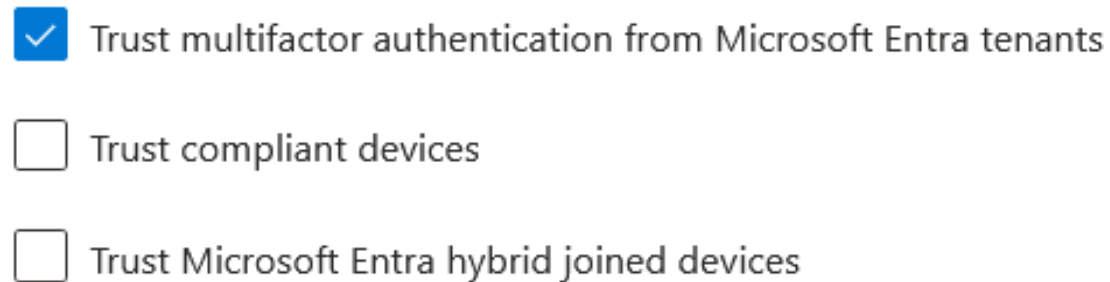
Legacy authentication clients

☒ Exchange ActiveSync clients ⓘ

☒ Other clients ⓘ

What about MFA?

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

- 
- A screenshot of a settings panel with a white background. It contains three items, each with a checkbox on the left and text on the right. The first item has a blue checkbox with a white checkmark and the text 'Trust multifactor authentication from Microsoft Entra tenants'. The second item has an empty white checkbox and the text 'Trust compliant devices'. The third item has an empty white checkbox and the text 'Trust Microsoft Entra hybrid joined devices'.
- ☒ 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

@thomasvochten




M365 Workloads


@thomasvochten

Sharing (links) in SharePoint & OneDrive

External sharing

Content can be shared with:

 SharePoint

 OneDrive

Most permissive

Least permissive

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
- ☐ People who use a verification code must reauthenticate after this many days [Learn more](#) ⓘ

Integrating with B2B Collaboration

Set-SPOTenant -EnableAzureADB2BIntegration \$true

| Sharing method | Files and folders | Sites |
|---|---|--|
| SharePoint external authentication (Microsoft Entra B2B integration not enabled) | No guest account created* Microsoft Entra settings don't apply | N/A (Microsoft Entra B2B always used) |
| Microsoft Entra B2B integration enabled | Guest account always created Microsoft Entra settings apply | Guest account always created Microsoft Entra settings apply |

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.

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

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. [i](#)



Manage external user profiles

What about monitoring?

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

@thomasvochten

Activity Details: Sign-ins

| Basic info | Location | Device info | Authentication Details | Conditional Access | Report-only |
|------------------------------|----------|---|------------------------|--------------------|-------------|
| 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 | | | |
| | | Follow these steps: | | | |
| Troubleshoot Event | | 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 | | | |

Licensing & costs

- Legacy: 1:5 Microsoft Entra ID to guest license ratio
- 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
- Sharing links don't use Entra External ID

Thank you

@thomasvochten

<https://thomasvochten.com>

mail@thomasvochten.com

Get the slides

