Making sense of Microsoft 365 Guest & External access

@thomasvochten

Thomas Vochten ☕ ☁️ 💻 🎹 🏃

Technology evangelist Microsoft 365 & Security

@thomasvochten

https://thomasvochten.com

mail@thomasvochten.com

MVP Microsoft®
Most Valuable
Professional

BIWUG

CRONOS GROEP

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

@thomasvochten

External Access in M365:
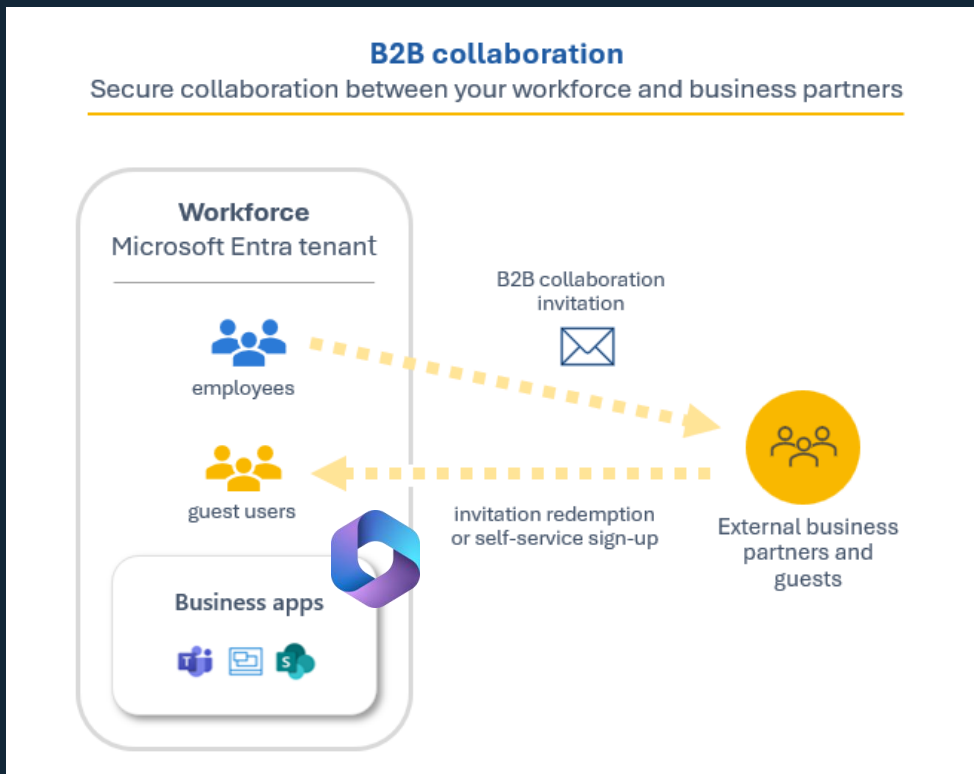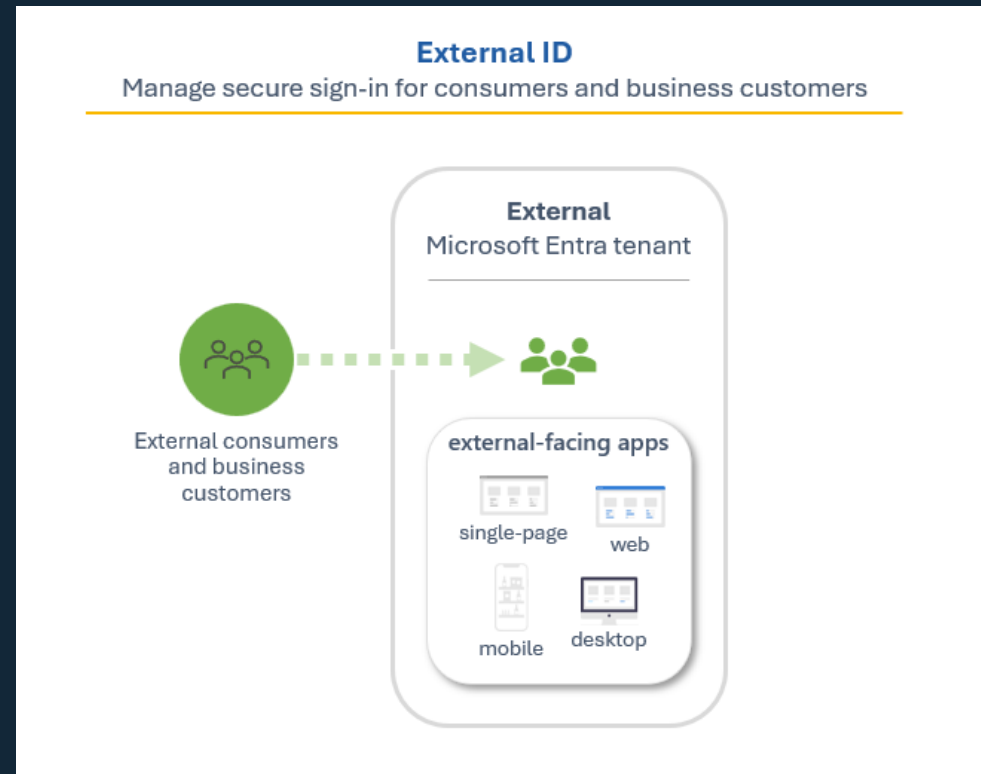# the what and why

@thomasvochten

Bring your own ID

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

Meet Entra ID External ID
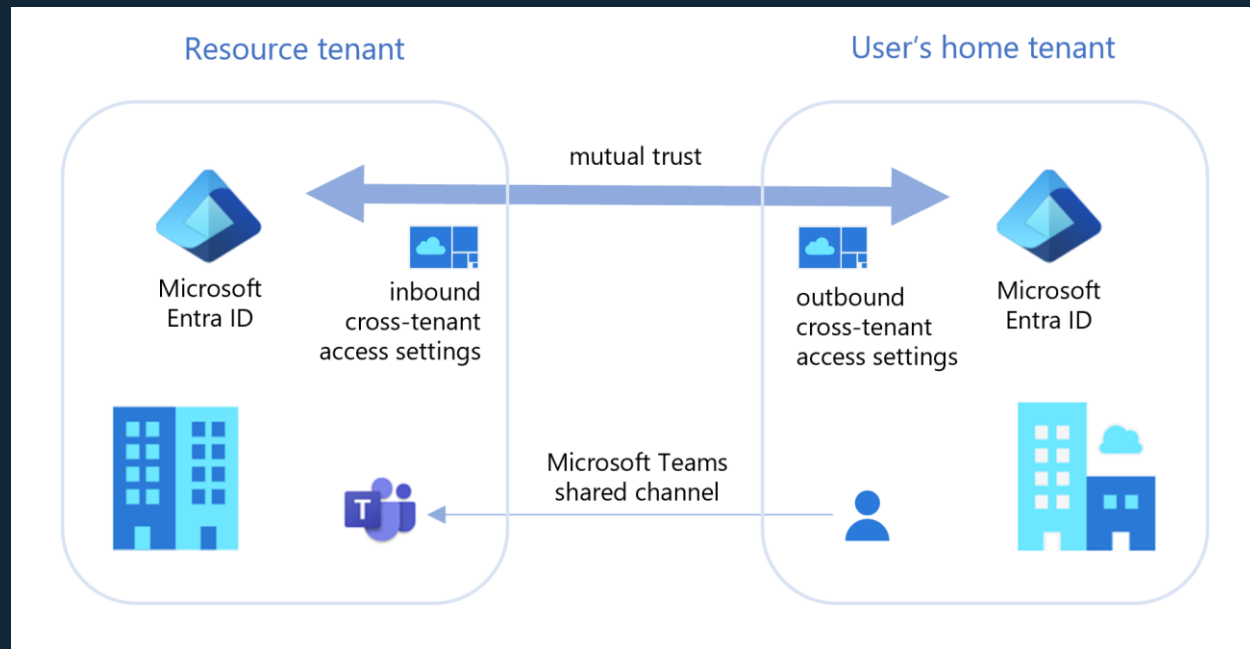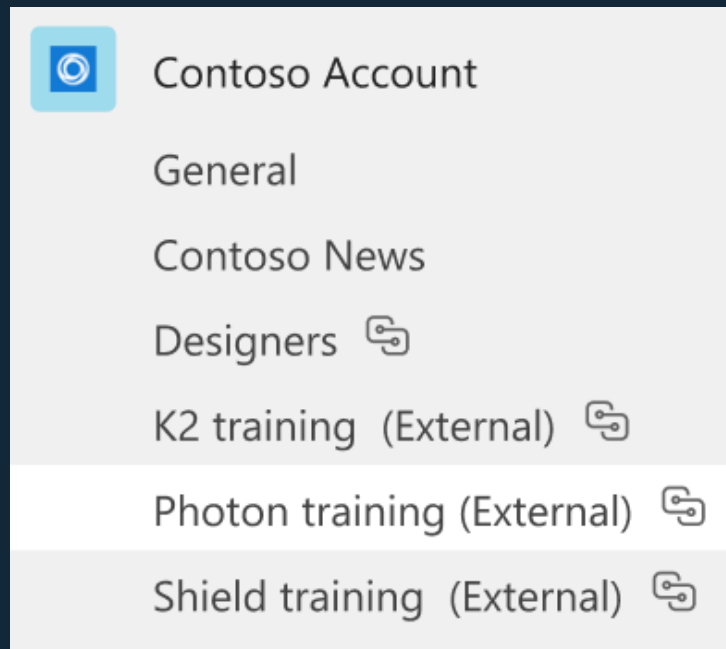
Workforce tenant configuration

B2B collaboration
Secure collaboration between your workforce and business partners

Workforce
Microsoft Entra tenant

employees

B2B collaboration invitation

guest users

invitation redemption
or self-service sign-up

External business
partners and
guests

Business apps

External tenant configuration

External ID
Manage secure sign-in for consumers and business customers

External
Microsoft Entra tenant

External consumers
and business
customers

external-facing apps

single-page   web

mobile   desktop

@thomasvochten

What about B2B Direct Connect?

Currently only supports Teams Shared Channels

@thomasvochten

B2B Collaboration

@thomasvochten

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

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

Guest invitation & redemption process
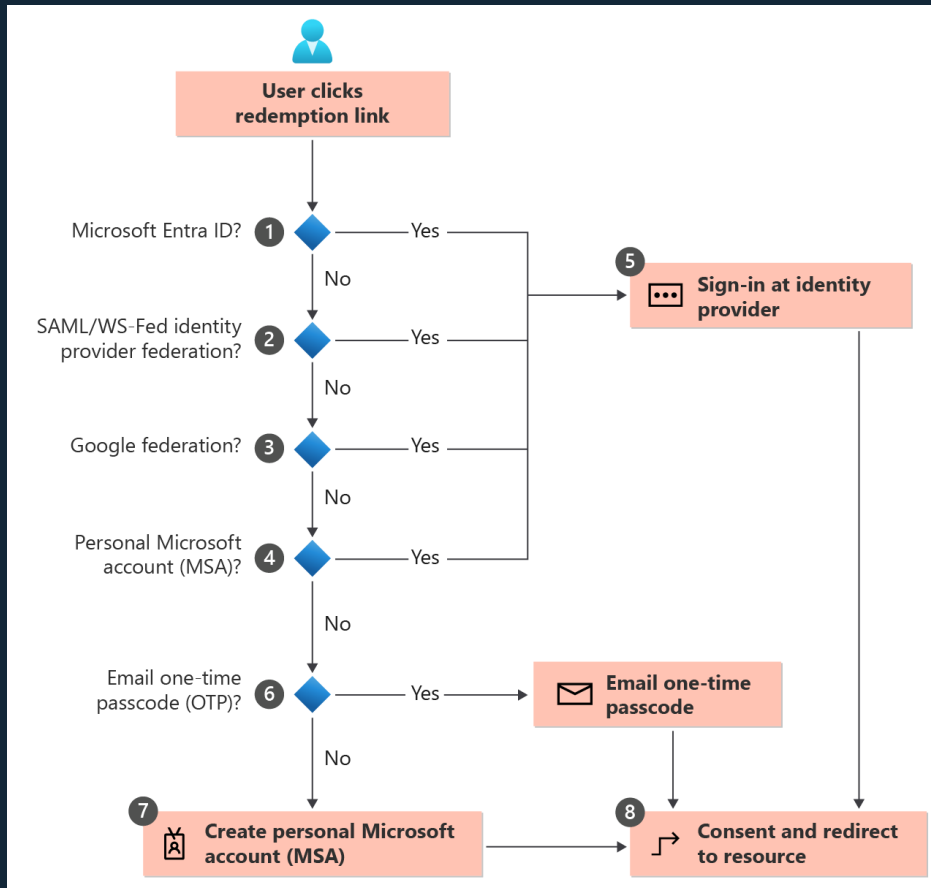
Supported Identity Providers

- 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.

@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

🖊 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

@thomasvochten

Demo

Settings & configuring alternative identity providers
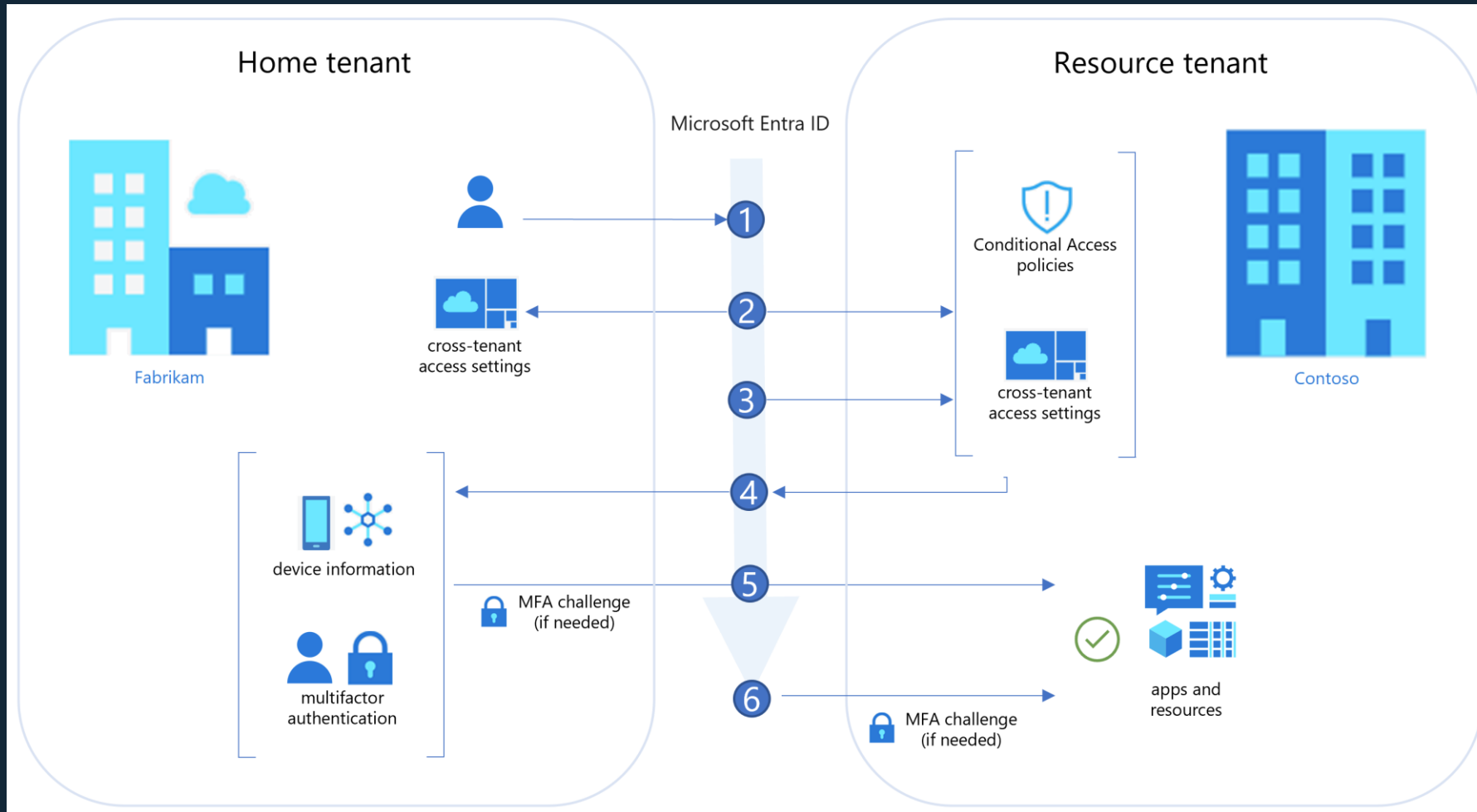
Guests lifecycle management

- 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
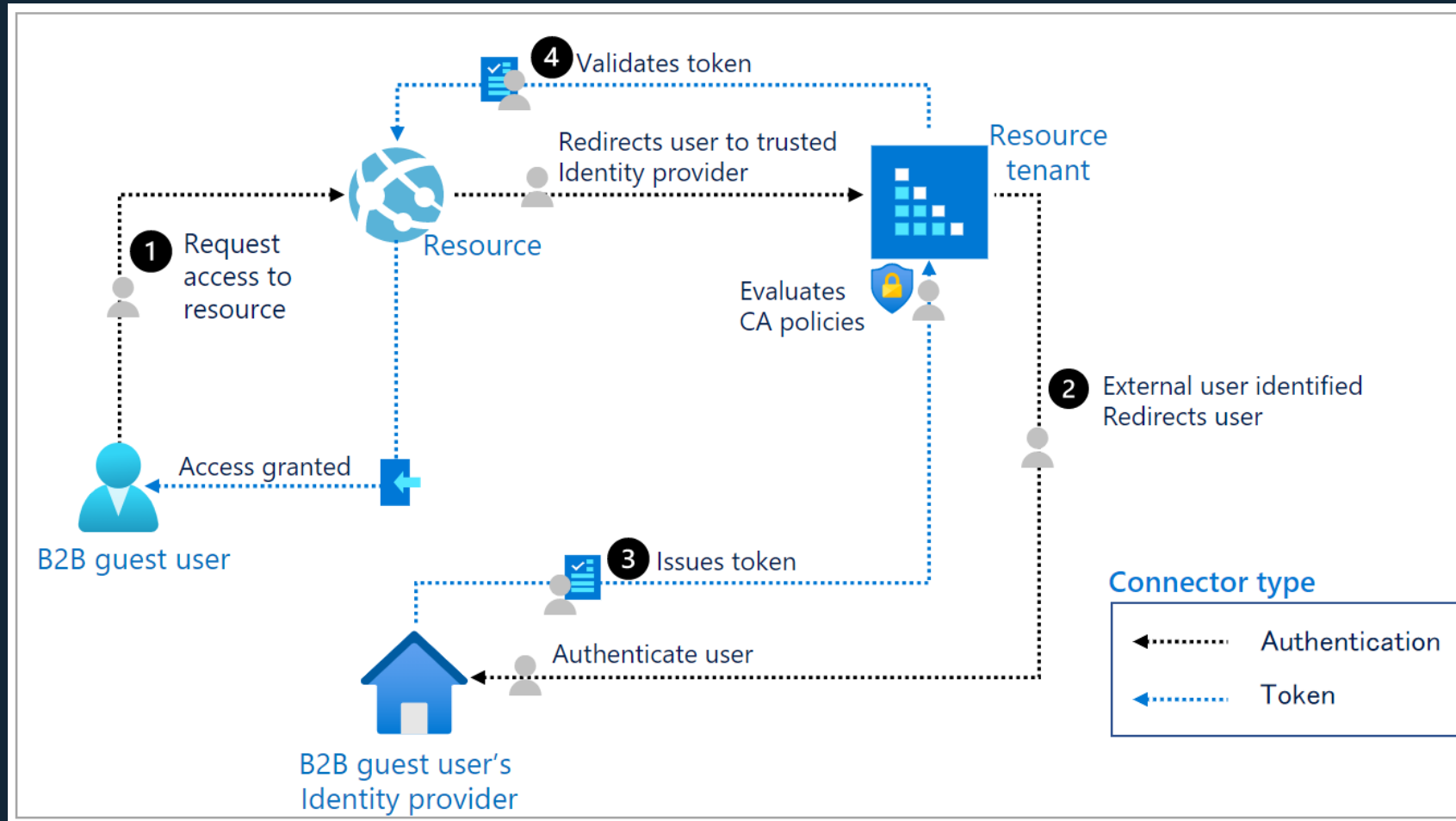 - More advanced workflows

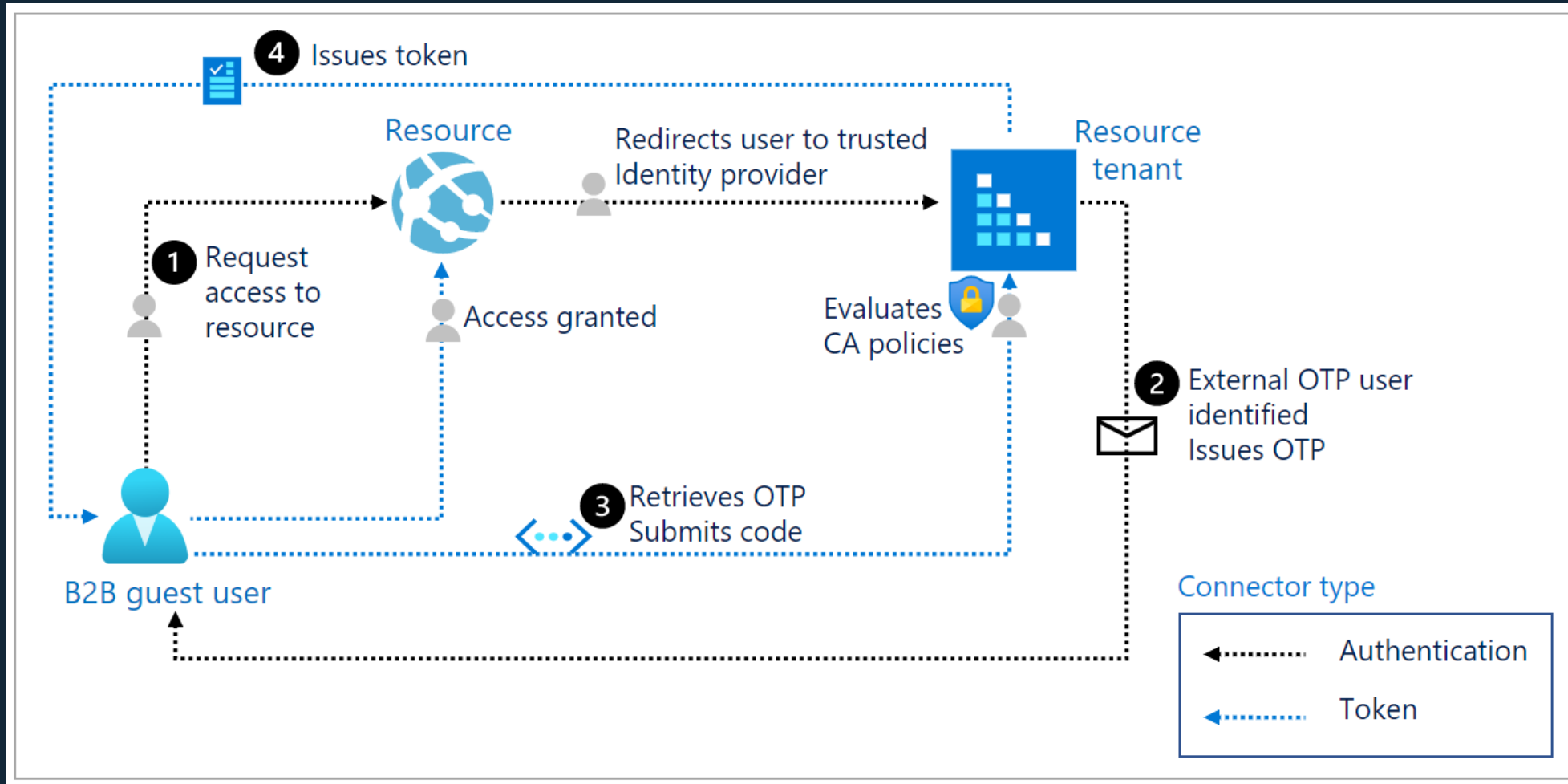# Securing guest access

@thomasvochten

AuthN for guests coming from another tenant

@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

Terms of use for guests

@thomasvochten

Web-only access for guests
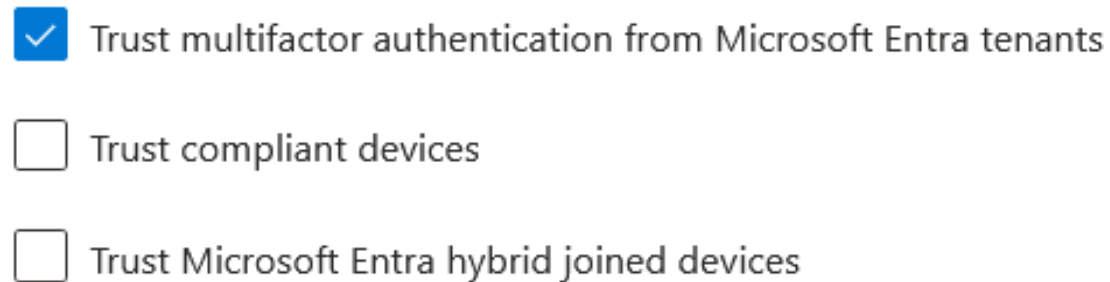
What about MFA?

- Force guest users to register for MFA
  in **your** tenant or **theirs**

- Entra ID can honor compliancy status from other tenants:

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	✅	

@thomasvochten

Demo

Conditional access & MFA

M365 Workloads

Sharing (links) in SharePoint & OneDrive

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

@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

@thomasvochten

What about monitoring?

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

@thomasvochten

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

@thomasvochten

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 *by default*

Thank you

@thomasvochten

https://thomasvochten.com

mail@thomasvochten.com

Get the slides