

Do's and Don'ts with Microsoft Teams Shared Channels

Benno Zelders





<https://www.linkedin.com/in/bzelders/>



Benno Zelders

Throughout my career, I've taken on **various roles**, levels, and contract forms. But for me, it has always been about working with **awesome people** and making **impact**.

Somehow this just never stops :)...

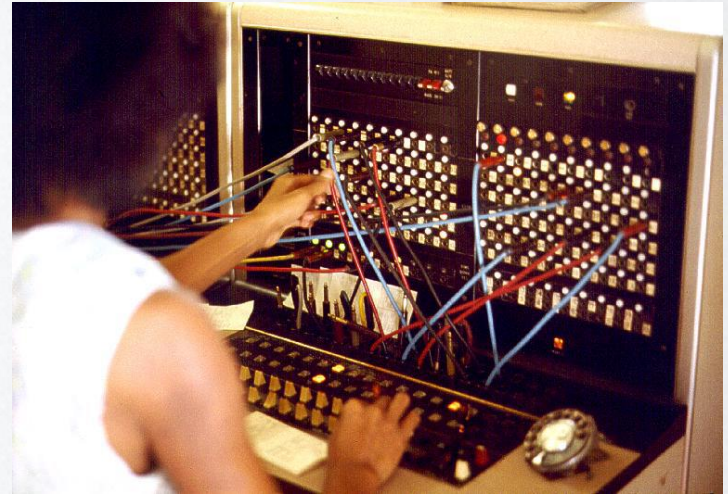




**Thanks for all the sponsors
making this event possible**



Teams = winner (but can be overwhelming)





Imagine this.....

For an M&A organization with 8 different Microsoft Tenants, where collaboration is ramping up on all sides...


(plus customers, partners etc etc etc)



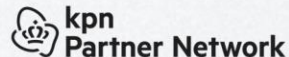


Teams Shared Channels to the Rescue!





Who already uses shared Channels?



Released last year



■ ■ ■ Microsoft Teams: Teams Connect shared channels

Rollout Start: July 2022

Teams Connect shared channels makes collaborating with those inside and outside your organization easier. Multiple organizations can work together in a shared space - have conversations, schedule a meeting, share, and co-author files, and collaborate on apps, without ever switching tenants in a secure, governable and compliant environment.

Feature ID: 94820

Added to roadmap: 5/24/2022

Last modified: 3/27/2023

Product(s): Microsoft Teams

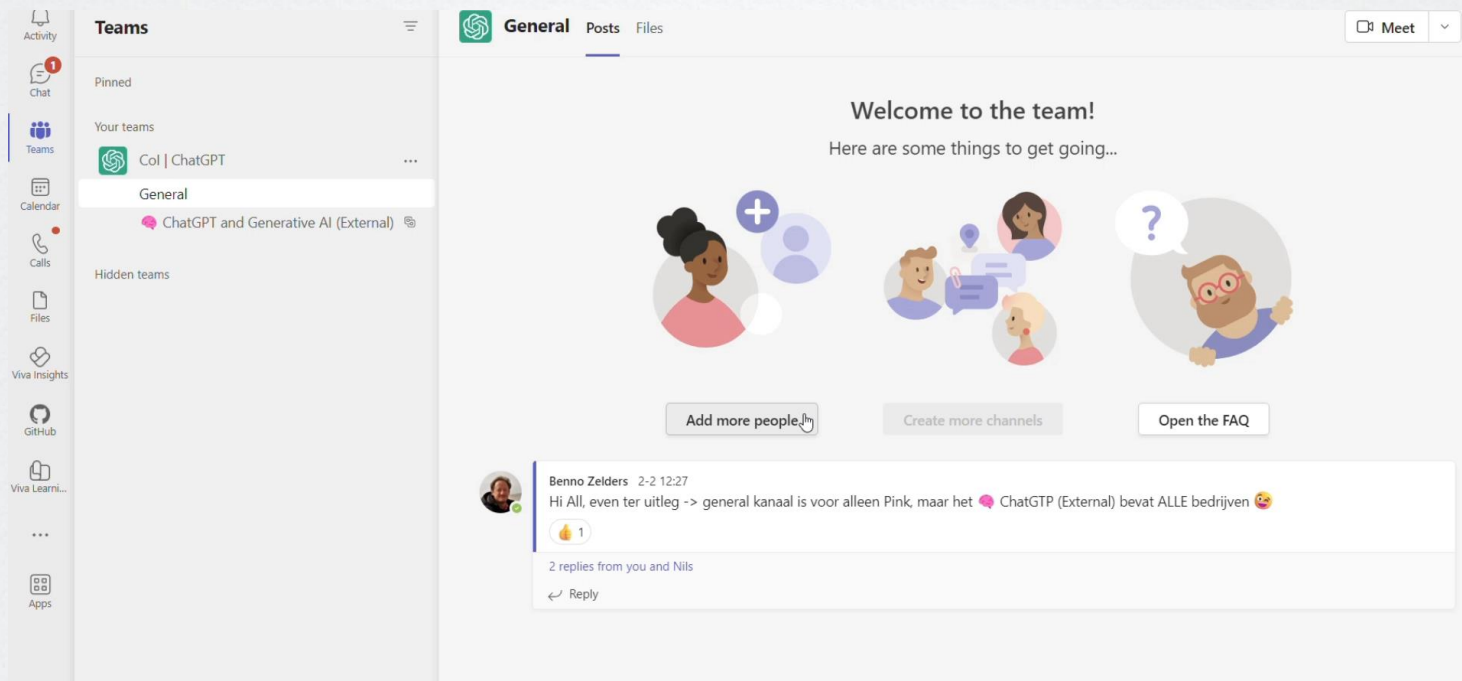
Cloud instance(s): GCC, Worldwide (Standard Multi-Tenant)

Platform(s): Mobile, Desktop, Web

Release phase(s): General Availability



(really) short demo





It's just a teams channel, but...





It's just a teams channel, but...

- + No switching anymore between orgs. Woohoo!!
- + Use your own MFA registration (no additional needed!)
- + share specific channels instead of the complete team (and private channels). Internally and externally!
- + Most of the functionality is available
- Most of the functionality is available



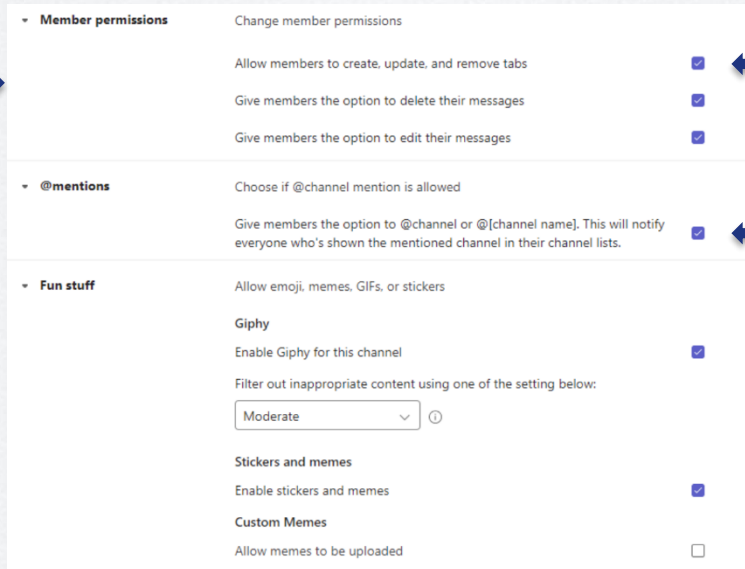
Teams channels compared

To collaborate with:	Shared channel	Standard channel	Private channel
Everyone on your team	x	x	
Specific people on your team	x		x
People outside your team	x		
People outside your org	x	x	x
	(when both orgs use Azure AD B2B direct connect for cross-org access)	(when your org uses Azure AD B2B external collaboration for external guests)	(when your org uses Azure AD B2B external collaboration for external guests)
People outside your org (without them switching orgs)	x		



Shared Channels options

No moderation
(yet)



The image shows a screenshot of the Discord channel settings interface for a shared channel. It is divided into three main sections: Member permissions, @mentions, and Fun stuff. Each section has a list of options with checkboxes to the right. Arrows from the surrounding text boxes point to specific checkboxes: one from 'No moderation (yet)' points to the 'Allow members to create, update, and remove tabs' checkbox, and two from 'Think about these settings with large channels' point to the 'Give members the option to delete their messages' and 'Give members the option to edit their messages' checkboxes.

Section	Option	Checked
Member permissions	Allow members to create, update, and remove tabs	<input checked="" type="checkbox"/>
	Give members the option to delete their messages	<input checked="" type="checkbox"/>
	Give members the option to edit their messages	<input checked="" type="checkbox"/>
@mentions	Choose if @channel mention is allowed	<input type="checkbox"/>
	Give members the option to @channel or @[channel name]. This will notify everyone who's shown the mentioned channel in their channel lists.	<input checked="" type="checkbox"/>
Fun stuff	Allow emoji, memes, GIFs, or stickers	<input type="checkbox"/>
	Giphy	<input type="checkbox"/>
	Enable Giphy for this channel	<input checked="" type="checkbox"/>
	Filter out inappropriate content using one of the setting below:	
	Moderate	<input type="checkbox"/>
	Stickers and memes	<input type="checkbox"/>
Enable stickers and memes	<input checked="" type="checkbox"/>	
Custom Memes	<input type="checkbox"/>	
Allow memes to be uploaded	<input type="checkbox"/>	

Think about these
settings with large
channels 😊



Not (yet) available / limitations

- **Moderation** functionality not available
- Only **Azure AD work** or **school accounts** are supported for external participants.
- Shared channels support tabs except for **Stream, Planner, and Forms**.
- **Bots, connectors, and message extensions** are not supported.
- **Org-wide** teams are not supported to be added as members of a shared channel
- When you create a team from an existing team, any shared channels in the existing team won't be copied over.
- **Notifications** from shared channels are not included in missed **activity emails**.
- Shared channels are not supported in **class teams**.



Some more limitations



Only users from "home" tenant can
schedule or **start meetings** in the
Shared Channel and **add** or **remove**
members

Sharing the Shared Channel

1



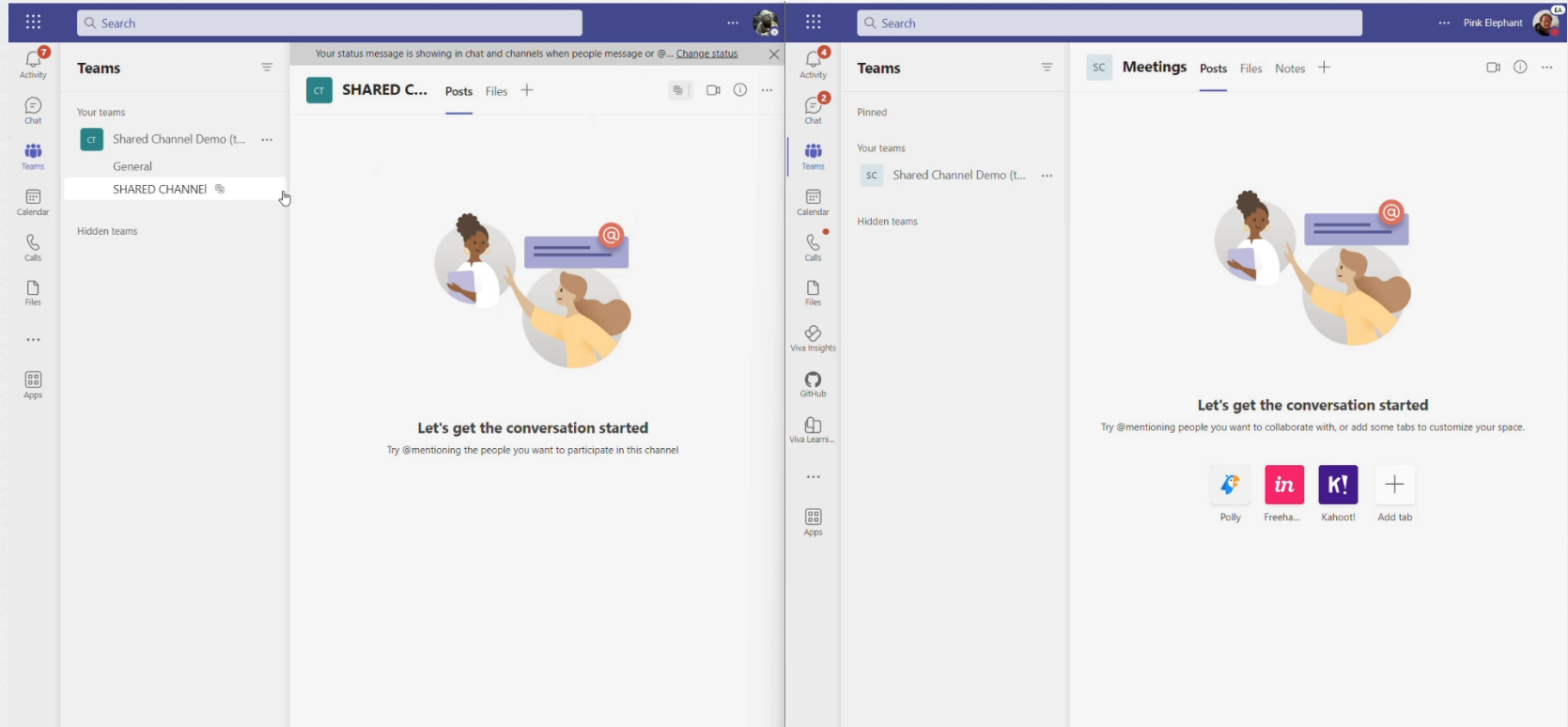
With a **Microsoft Teams** user
from a connected Azure tenant

2

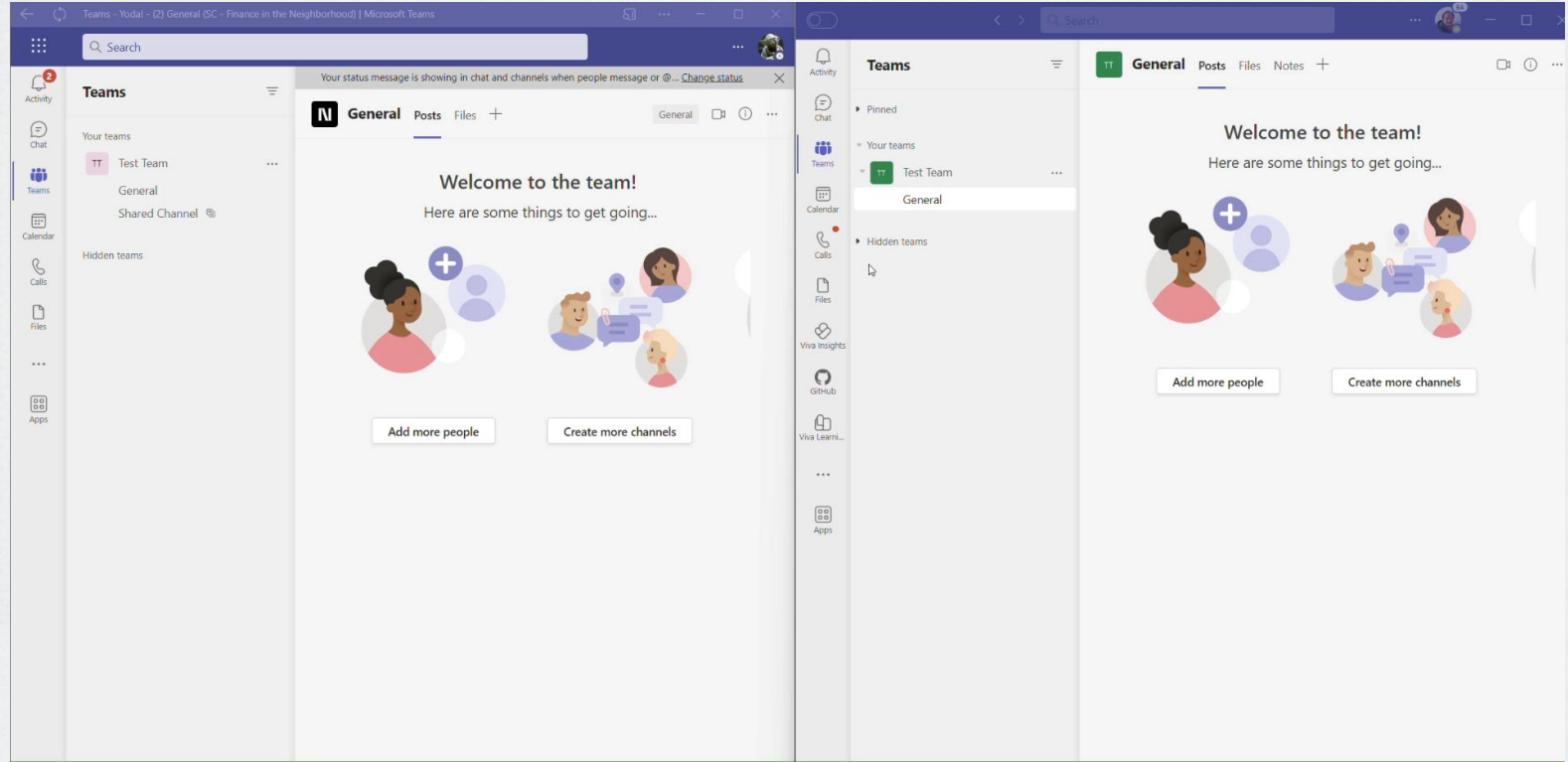


With an **existing Microsoft Team** from a
connected Azure tenant
(share with owner of team who selects the correct team)

Invite a User



Invite a Team

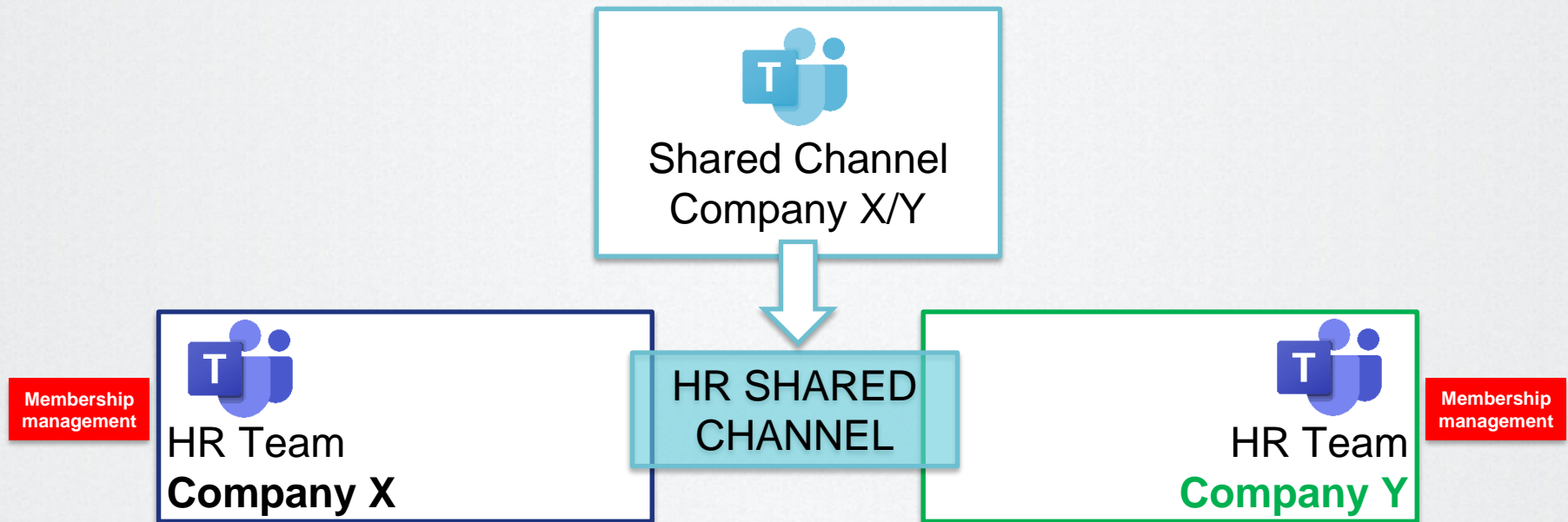




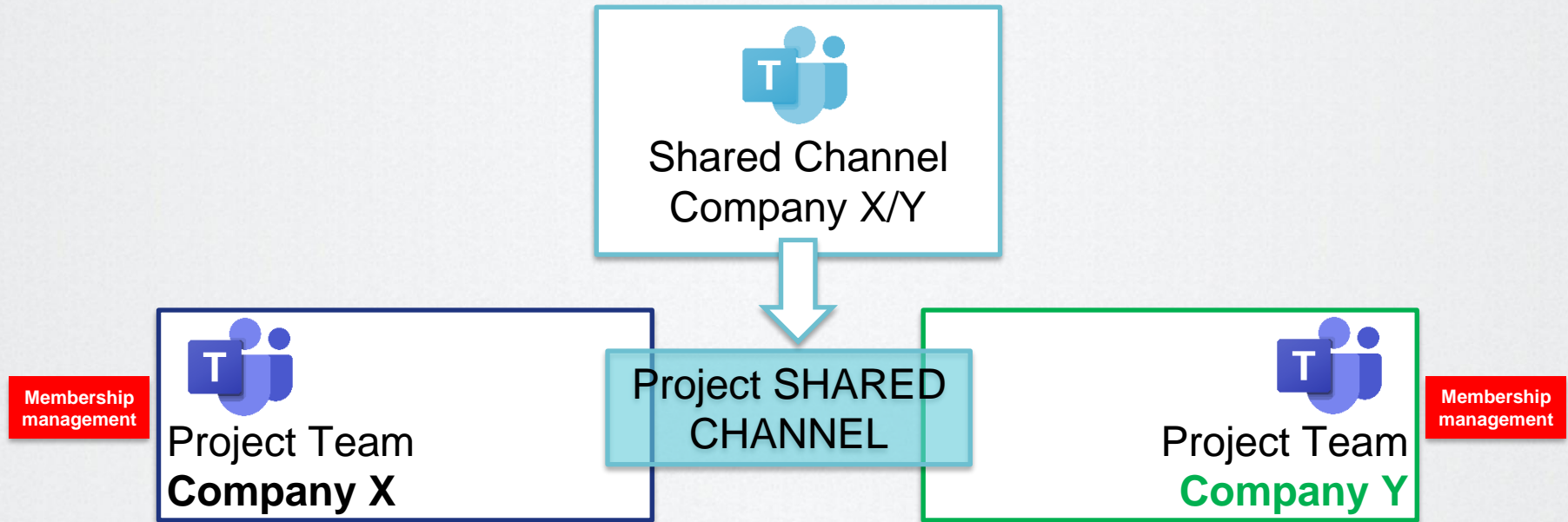
Some use cases for shared channels



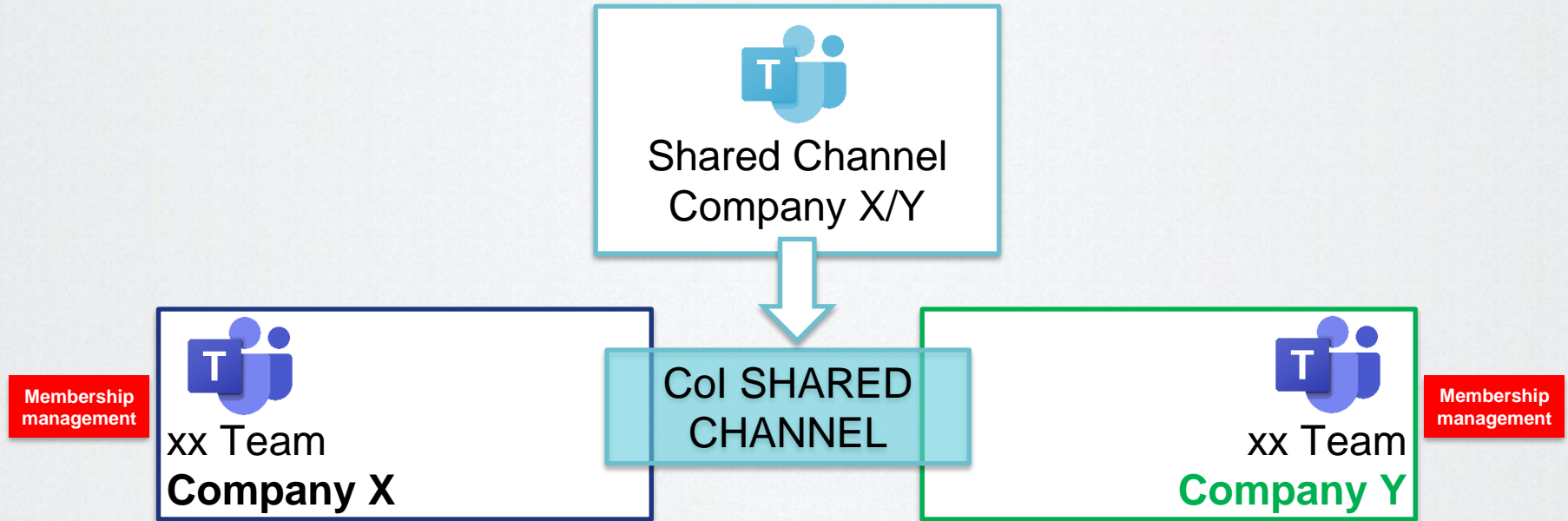
Connect departments from different organizations



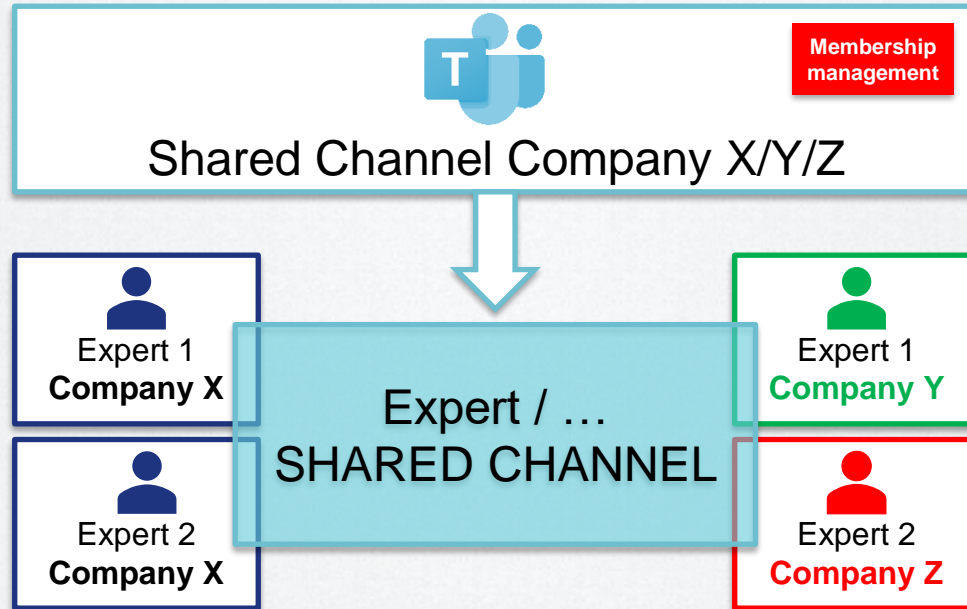
Start a "multi-company" project



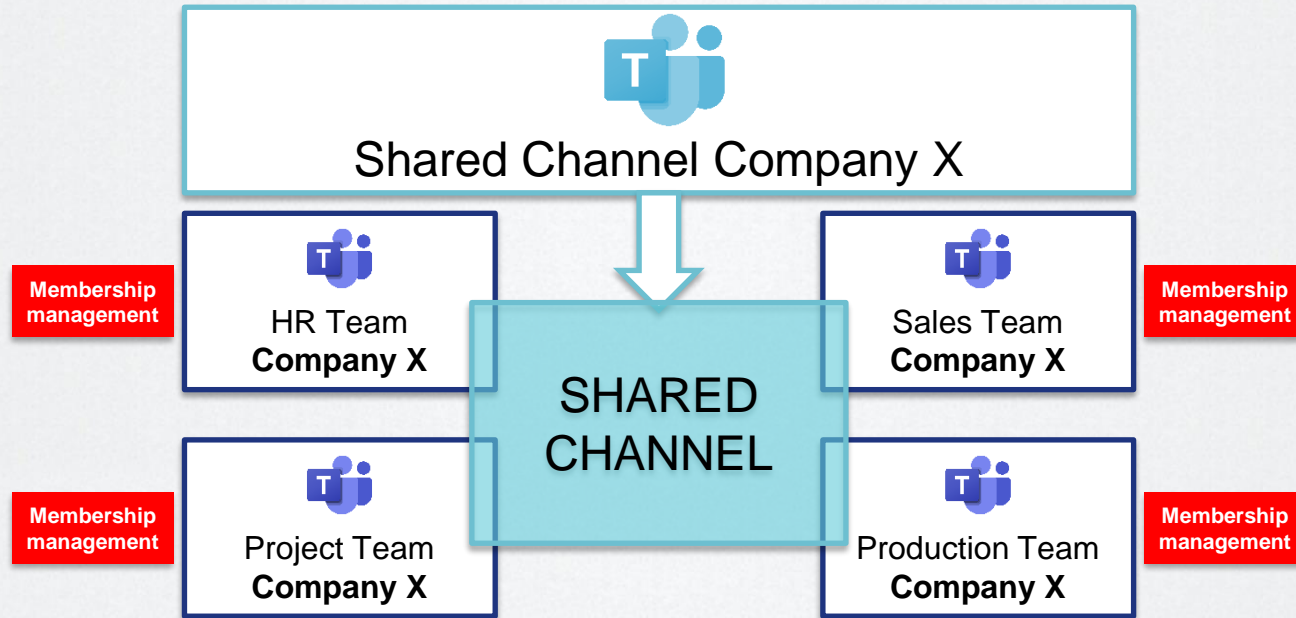
Start a "multi-company" community of interest



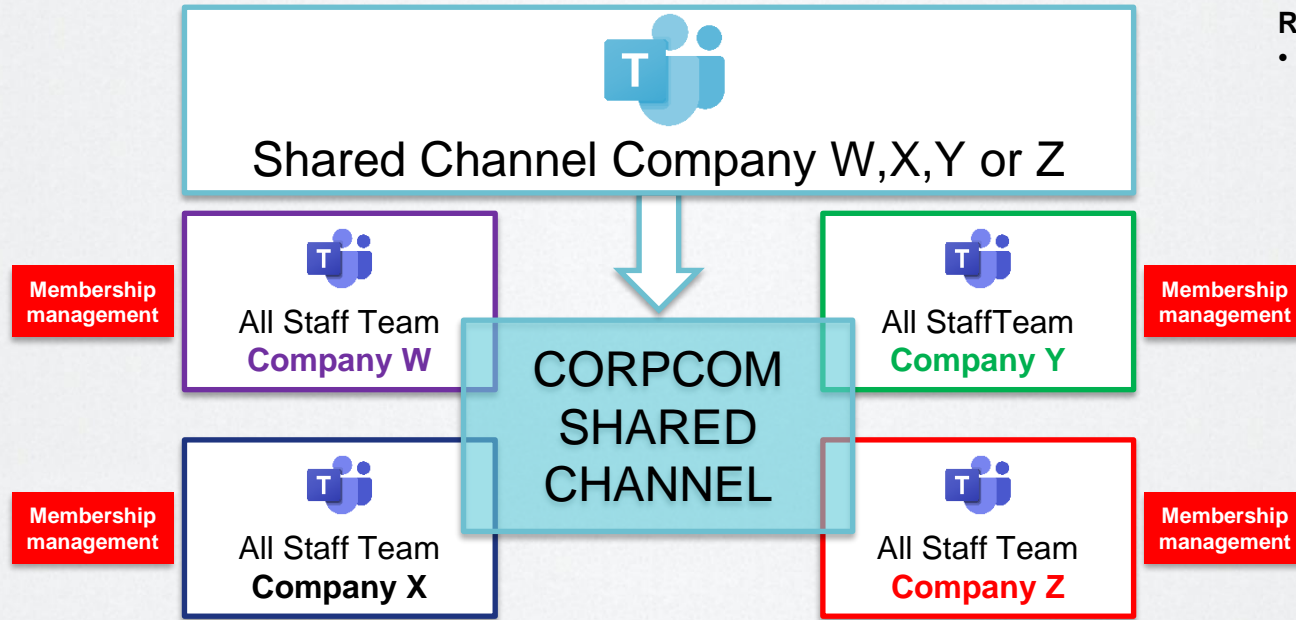
Connect the experts of different organisations



Share within the internal organization



Connect ALL employees of all organisations



Remark:

- Use **dynamic groups** for the all staff teams as ORG-Wide teams are not supported (and give you no control on membership) ☺

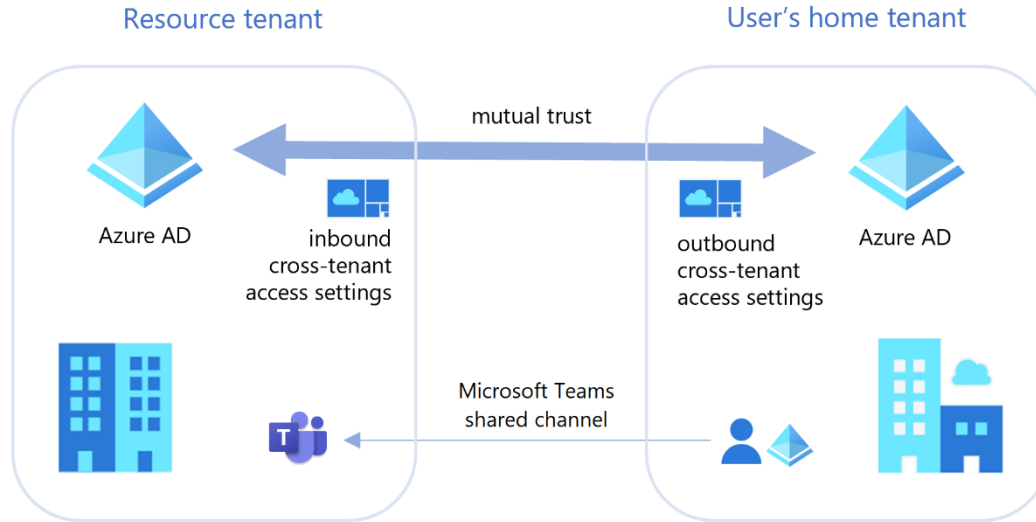
Bonus opportunities



- How about using the **SharePoint site** of the Shared Channel (group news?, usefull links etc?)
- What about "cross-tenant SMTP domain sharing"

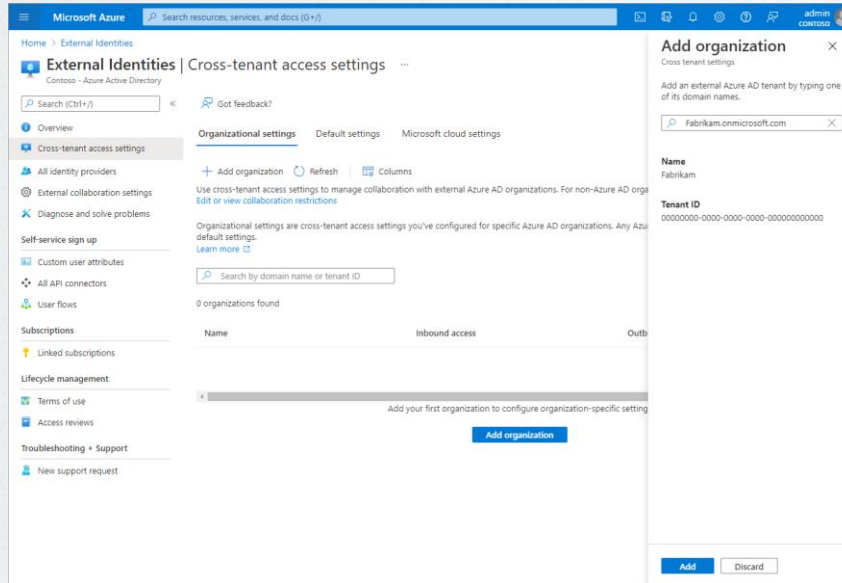
Onboarding = Easy

B2B direct connect

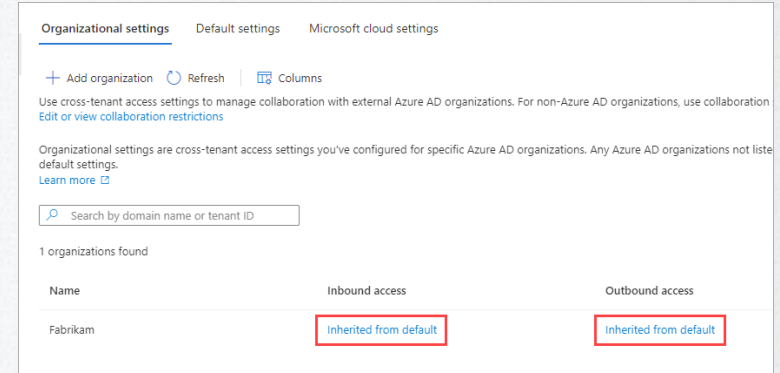


<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-settings-b2b-direct-connect>

Add organization and edit settings



The screenshot shows the Microsoft Azure portal interface. On the left, the 'External Identities' section is expanded, showing 'Cross-tenant access settings'. The main area displays the 'Add organization' dialog box. The dialog has a search bar with 'Fabrikam.onmicrosoft.com' entered. Below the search bar, there are tabs for 'Organizational settings', 'Default settings', and 'Microsoft cloud settings'. The 'Organizational settings' tab is active, showing a table with columns for 'Name', 'Inbound access', and 'Outbound access'. The table is currently empty, with a message '0 organizations found'. A blue 'Add organization' button is at the bottom right of the dialog.



This screenshot shows a detailed view of the 'Add organization' dialog box, specifically the 'Organizational settings' tab. The dialog has a search bar with 'Fabrikam.onmicrosoft.com' entered. Below the search bar, there are tabs for 'Organizational settings', 'Default settings', and 'Microsoft cloud settings'. The 'Organizational settings' tab is active, showing a table with columns for 'Name', 'Inbound access', and 'Outbound access'. The table contains one entry: 'Fabrikam' with 'Inherited from default' in the 'Inbound access' column and 'Inherited from default' in the 'Outbound access' column. The 'Inherited from default' text is highlighted with a red box.

Configure Inbound settings

Inbound access settings - Pink Elephant ...

B2B collaboration **B2B direct connect** Trust settings Cross-tenant sync

B2B direct connect inbound access settings determine whether users from external Azure AD organizations can access your resources without being with you. To establish a connection, an admin from the other organization must also enable B2B direct connect.
[Learn more](#)

- ☐ Default settings
- ☒ Customize settings

External users and groups Applications

Access status

- ☒ Allow access
- ☐ Block access

Applies to

- ☒ All Pink Elephant users and groups
- ☐ Select Pink Elephant users and groups

Inbound access settings - Pink Elephant ...

B2B collaboration B2B direct connect **Trust settings** Cross-tenant sync

Configure whether your Conditional Access policies will accept claims from other Azure AD organizations when external users access your resources. You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multifactor authentication.
[Learn more](#)

- ☐ Default settings
- ☒ Customize settings
- ☒ Trust multifactor authentication from Azure AD tenants
- ☒ Trust compliant devices
- ☐ Trust hybrid Azure AD joined devices

Automatic redemption

- ☒ Check this setting if you want to automatically redeem invitations. If so, users from the specified tenant won't have to suppress the consent prompt if the specified tenant checks this setting for outbound access as well.
[Learn more](#)
- ☒ Automatically redeem invitations with the tenant Pink Elephant.



And outbound for connecting tenant

B2B collaboration **B2B direct connect** Trust settings

Outbound access settings determine how your users and groups can interact with apps and resources in external organizations. The settings can be modified but not deleted.
[Learn more](#)

B2B direct connect lets your users and groups access apps and resources that are hosted by an external organization. To establish a limited data about your users is shared with the external organization, so that they can perform actions such as searching for your u
[Learn more](#)

☐ Default settings
☒ Customize settings

Users and groups External applications

Access status

☒ Allow access
☐ Block access

Applies to

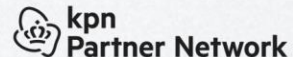
☒ All [redacted] users
☐ Select [redacted] users and groups

B2B collaboration B2B direct connect **Trust settings**

Automatic redemption

☒ Check this setting if you want to automatically redeem invitations. If so, users from this tenant suppress the consent prompt if the specified tenant checks this setting for inbound access as v
[Learn more](#)

☒ Automatically redeem invitations with the tenant Pink Elephant.





Think about....

- Enable **by default** or enable **per tenant**
- Enable for **all users** or for **specific groups**
- **Inbound** and **outbound** access settings should be correct!
- **Conditional Access** policies for your shared Channels (MFA + Device Compliance) and the **B2B Direct Connect TRUST** settings 😊



How shared channels help in raising security standards

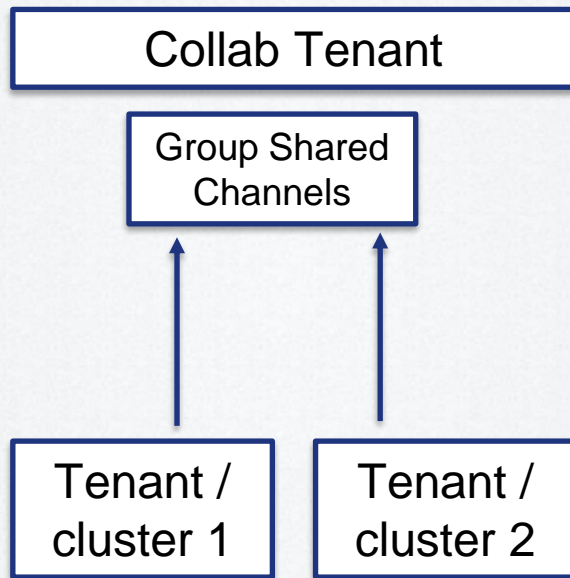
Enforce a security standard with **sensitivity labels** and **conditional access** per channel...



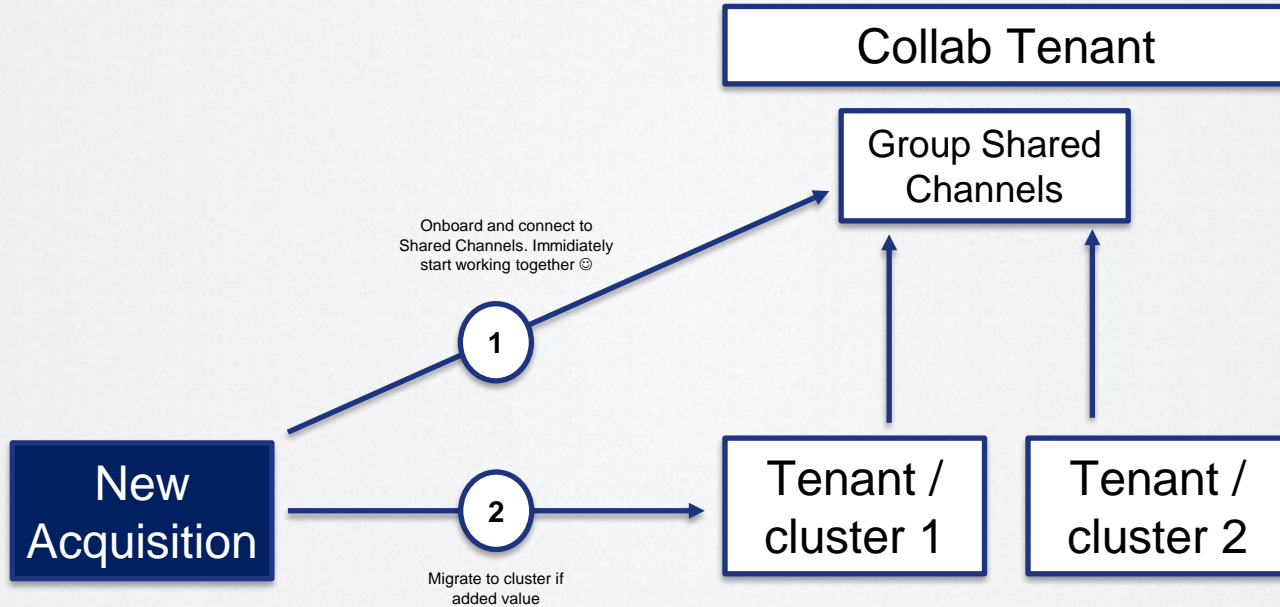
Example controls on data

Controls	Outcome
MFA required	No MFA -> no access
MFA required + Device Compliance required	No MFA -> no access No compliant device -> web access only
MFA required + Device Compliance required	No MFA -> no access No compliant device -> no access

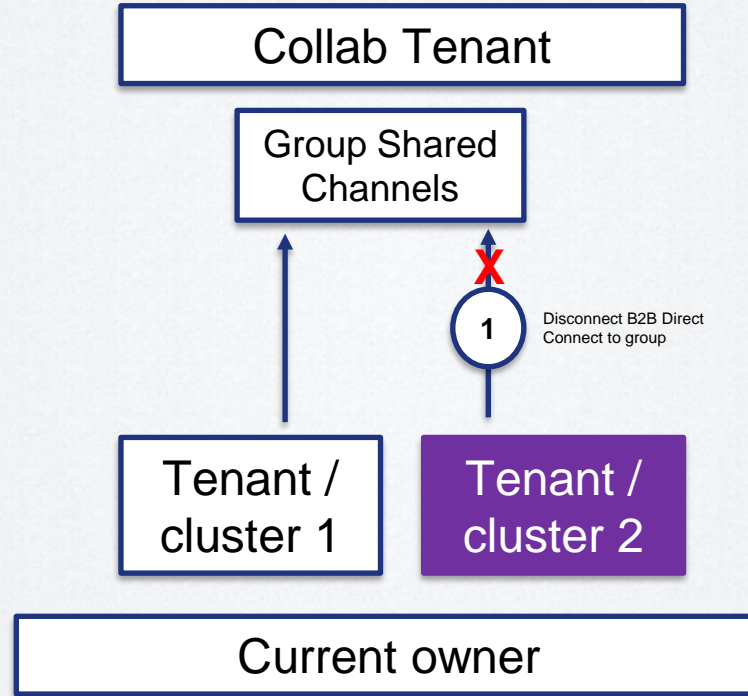
M&A Setup



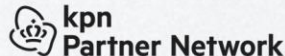
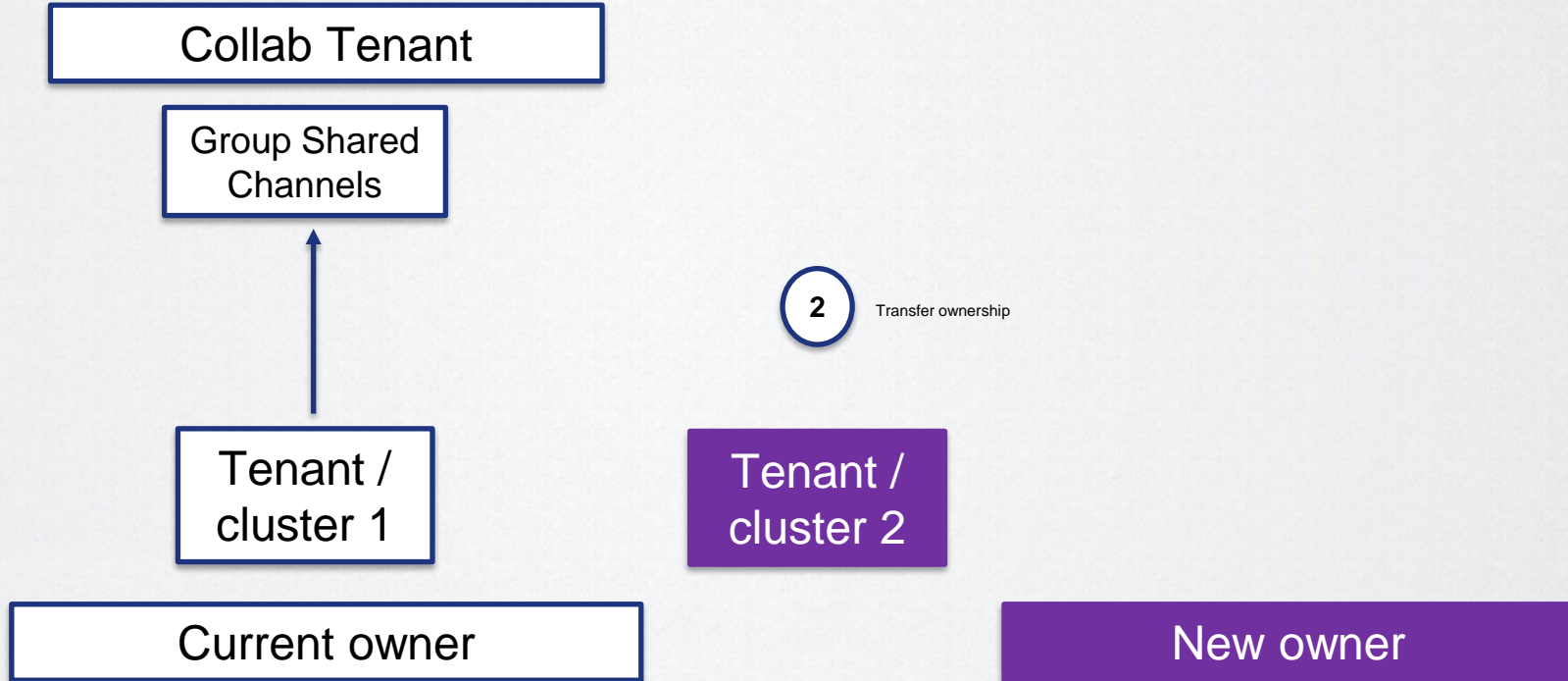
M&A Setup - onboarding



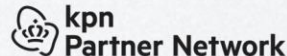
M&A Setup – offboarding



M&A Setup – offboarding



M&A Setup – offboarding





Lessons Learned part 1

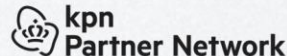
- Group shared channels based on **sensitivity labels** (or future). Sensitivity labels are set on **TEAMS** level. Shared channels inherit them
- Set the **security baseline** wisely. This is a **powerful** tool to enforce a basic security level for the participating organisations and agree on **device compliance levels**





Lessons Learned part 2

- Try to **share** teams “as much” with **teams** instead of individuals (**decentralize user management!**)
- Appoint **owners** and **administer** this per channel 😊
- Think about the **naming convention** within all tenants. Especially for “public” channels (use a **public** team in each tenant, so employees can join it “on demand”)
- Each **Shared Channel** has a **SharePoint** site. This is a bit **buggy** at the moment, but basic functionality works...
(for some webparts a guest account is still required for example....)





And don't forget!

- Only **users** from **within** the tenant **hosting** the shared channels can **manage** the "DIRECT" **members**
- Only **users** from **within** the tenant **hosting** the shared channels can **schedule** channel **meetings**
- **Moderation** is **not** (yet) **available** within shared channels
- Be carefull with the Mention feature! (notification fatigue!)





Summary

1

Shared Channels
are more powerful
than most people
think

Be creative in using it

2

Usability for end-users
and it is increased by at
least **42%**

Reduce MFA registrations in
authenticator! And what about guest
accounts?

3

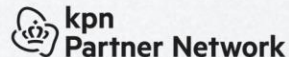
Onboarding and
offboarding is very
simple

And buys time for the
real discussion





Please rate my session in Yellenge





You can find my presentation on



<https://github.com/bzelders/ExpertsLive>

