11.12.2022

Compliance Whitepaper

Microsoft Teams Connect aka shared Channel

Version 4

December 2022

Raphael Koellner
MICROSOFT REGIONAL DIRCTOR, MICROSOFT MVP,
KÖLLNSERVICE GMBH

For Jennifer Köllner

With love and thanks for the support!

Table of contents

1. Versions

Version	Date	Author	Note
0.1	January 2022	Raphael Köllner	Creation start
0.2	April 2022	Raphael Köllner	Familiarization Microsoft product group
1.0	May 2022	Raphael Köllner	Final version 1
1.1	June 2022	Raphael Köllner	Update 2
1.2	June 2022	Raphael Köllner	Update 3
2.0	July 2022	Raphael Köllner	Update
2.1	July 20, 2022	Raphael Köllner	Update after the Inspire and official GA date.
2.5	August 25, 2022	Raphael Köllner	Updates
3.0	September 20, 2022	Raphael Köllner	Updates
3.5	November 12, 2022	Raphael Köllner	Update Conditional Access
4	December 11, 2022	Raphael Köllner	Azure Privacy Update

2. Image credits

3. Usage tips

This document has been created by the community for the community. Commercial use is excluded and prohibited.

Commercial use, requests: raphael.koellner@rakoellner.com

4. Introduction

Microsoft **Teams Connect** aka shared Channel is the third form of a Microsoft Teams channel. This new channel type is the hope of very many companies now to simplify collaboration within the group and with external parties.

The ideas to create another channel after Microsoft Teams private channels comes, as already from private channels, from the Uservoice. The desire of the user group of Microsoft Teams worldwide is to improve collaboration with external parties without having to change the tenant and accordingly receive notifications. Basically, these wishes come from the limitations

5. Summary

5.1. General

As of early July 2022, Microsoft Teams Connect does not yet meet "Enterprise Ready" status. It is expected that even after the "GA" status, there will also be further improvements until the architecture is rebuilt to provide the function as companies need it.

Currently, the function is only being used productively by a few companies, especially Microsoft. In Germany in particular, enterprise companies are still hesitant, but are testing the function extensively. However, many smaller companies are already using the function and are testing it on a living object, so to speak. Among Microsoft partners in Germany, the opinion is very divided, especially with regard to adoption (e.g. unclear display in the own team) and compliance issues show greater challenges for companies.

5.2. Teams Connect status

	Status
Status of the development of Teams Connect	GA
Available in which tenants	1. Business 2. Enterprise 3. EDU (partial) "Shared channels don`t support class teams yet. This capability is on our backlog. We call it out here https://docs.microsoft.com/en-us/microsoftteams/teams-channels-overview#channel-feature-comparison. But we will also include it in the Shared channels dedicated page." 4. Gov (no) 5. Teams Free/ Teams Community (no)

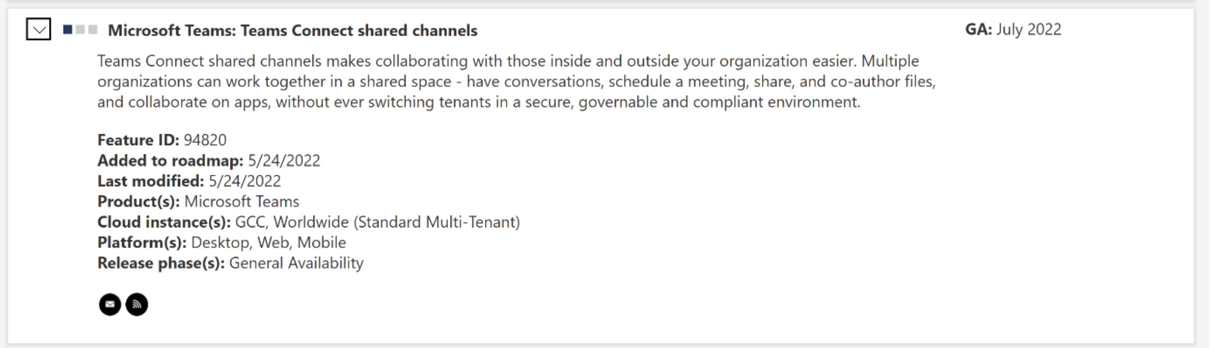
"Shared channels, rolled out in a public preview this March 2022, and as a result, we saw a range of customers adopting the feature to enable frictionless collaboration within their organizations. We are excited to announce that shared channels is moving into general availability. We expect to complete the rollout by mid-August." [1]

This means that the preview will now end in July 2022 and the GA rollout of shared Channels will begin and be completed by mid-August.

6. Roadmap

In the Microsoft 365 Roadmap, Microsoft publishes the current status of new functions and also of Teams Connect shared Channels.

Microsoft 365 Roadmap Status



Microsoft Teams: Teams Connect shared channels **GA:** 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: 5/24/2022
Product(s): Microsoft Teams
Cloud instance(s): GCC, Worldwide (Standard Multi-Tenant)
Platform(s): Desktop, Web, Mobile
Release phase(s): General Availability

[2]

Current: GA July 2022

As of July 2022, Teams Connect GA is now to go live, which means that the function will be officially included in the Microsoft Teams portfolio. This has the consequence that the SLA of Microsoft 365 also applies to the function and can be claimed. This will now also be the case with the rollout until mid-August.

But ATTENTION shared Channels is unlike Lists not to be found in the Productterms, because it belongs to Microsoft Teams.

6.1. Status of the recommendation of the deployment

Deployment is allowed with GA status and under SLA.

**Productive use in
selected scenarios with TOMs**

6.2. What is the market doing?

Initially, the function was tested in a private preview with selected companies and selected users such as some MVPs. From the public preview at the end of April, the test group was greatly expanded and many companies are already using Teams Connect. The expected challenges are changing, so that it can already be seen that the function is deactivated again after the test in the productive environment. The main challenges mentioned are:

[1] https://techcommunity.microsoft.com/t5/microsoft-teams-blog/microsoft-teams-connect-shared-channels-is-moving-into-generally/ba-p/3568000 ,retrieved 20/07/2022.

[2] https://www.microsoft.com/de-de/microsoft-365/roadmap?filters=&searchterms=Teams%2CConnect.

1. B2B users must be uninvited and re-invited as B2B direct
2. Governance tools cannot handle B2B direct yet
3. We do not trust the foreign identity enough.
4. Effort to manage is too great.
5. Adoption: The explanation for the users is too complex. Misunderstandings during use are high.
6. Compliance: challenges too high

It is interesting to note that as of GA in November, some automakers are relying very heavily on teams shared channel and thus also getting their suppliers to use this technology. This is currently leading to many discussions.

3rd Party Governance Provider

In addition, the first providers of governance software for Microsoft Teams want to extend their solutions to shared channels. I am in talks with **solution2share and their Teams Manager, for example,** and am pleased that suggestions are to be taken up and implemented here in order to enable the lowest possible risk operation for the mass of tenants in Germany.

Furthermore, **Rencore** has also announced to address the issue and incorporate this into their product.

7. Focus around Teams Connect

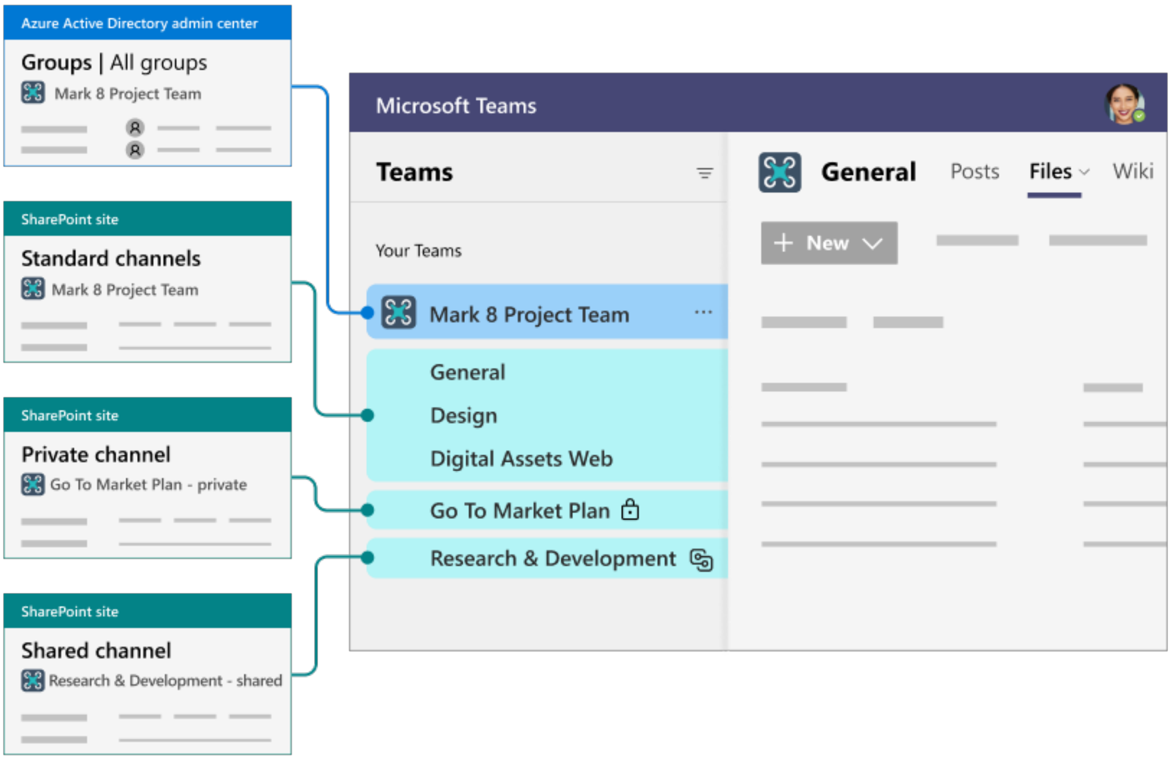
In the context of dealing with Microsoft Teams Connect, topics lend themselves to writing an entire book or a very large chapter in an 800-page reference book. In the context of this larger white paper, the topic of **compliance, including governance and data protection, is** addressed in particular.

7.1. Teams Connect aka shared Channels - What is this?

Microsoft Teams Connect is a new variant of the Microsoft Teams channel type.

Channel types

1. Normal / General (deault channel)
2. Private / private channels (private channels)
3. Shared / Teams Connect (shared Channels)



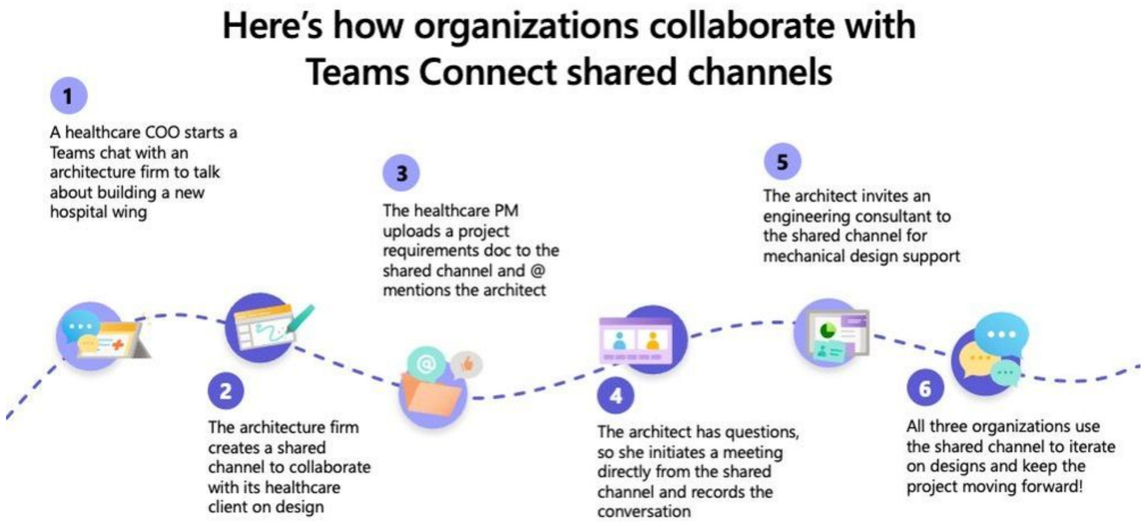
[3] Channel overview

7.1.1. shared Channels process from Microsoft

An interesting new graphic now appeared in the GA announcement of the feature on 20/07/2022.

This unfortunately does not yet include my suggestions that came from my direction in previous versions of this paper and in webinars and architecture sessions with the product group. For now, it's just about the function and not about the use in the context of compliance with lower risk.

[3] https://docs.microsoft.com/en-us/sharepoint/teams-connected-sites, accessed 06/20/2022.



Here's how organizations collaborate with Teams Connect shared channels

1 A healthcare COO starts a Teams chat with an architecture firm to talk about building a new hospital wing

2 The architecture firm creates a shared channel to collaborate with its healthcare client on design

3 The healthcare PM uploads a project requirements doc to the shared channel and @ mentions the architect

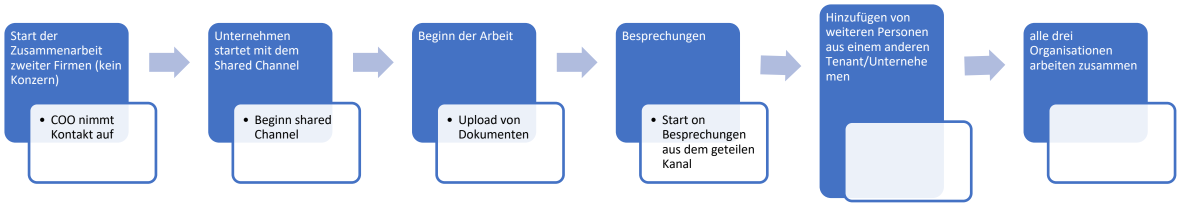
4 The architect has questions, so she initiates a meeting directly from the shared channel and records the conversation

5 The architect invites an engineering consultant to the shared channel for mechanical design support

6 All three organizations use the shared channel to iterate on designs and keep the project moving forward!

Figure 1 https://techcommunity.microsoft.com/t5/microsoft-teams-blog/microsoft-teams-connect-shared-channels-is-moving-into-generally/ba-p/3568000

In German:



Start der Zusammenarbeit zweiter Firmen (kein Konzern)
- COO nimmt Kontakt auf

Unternehmen startet mit dem Shared Channel
- Beginn shared Channel

Beginn der Arbeit
- Upload von Dokumenten

Besprechungen
- Start on Besprechungen aus dem geteilen Kanal

Hinzufügen von weiteren Personen aus einem anderen Tenant/Unternehemen

alle drei Organisationen arbeiten zusammen

7.1.2. Architecture

The architecture of Teams Connect shared channels is not special if you have already dealt with private channels. The shared channels are just an evolution of the private channels with a new identity (B2B direct) and the consequences that follow.

Below comes an overview of Microsoft's various channels:

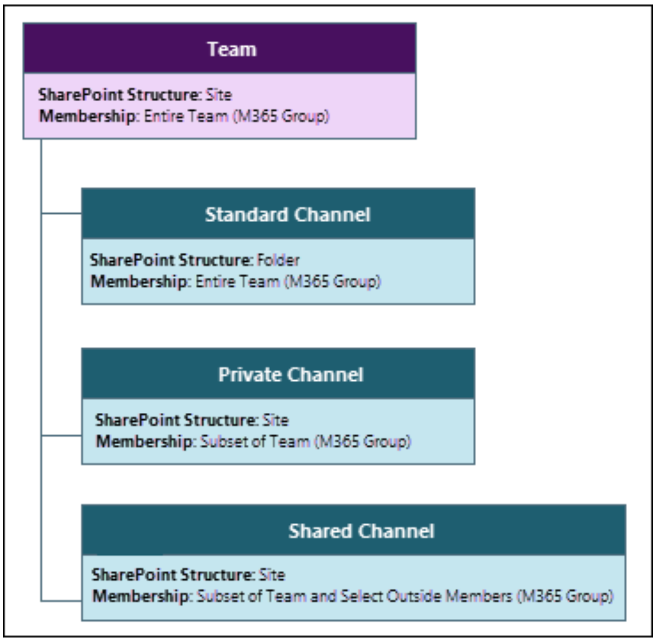

Team
SharePoint Structure: Site
Membership: Entire Team (M365 Group)
Standard Channel
SharePoint Structure: Folder
Membership: Entire Team (M365 Group)
Private Channel
SharePoint Structure: Site
Membership: Subset of Team (M365 Group)
Shared Channel
SharePoint Structure: Site
Membership: Subset of Team and Select Outside Members (M365 Group)

Figure 2 Architecture

From this, you can see the previously mentioned evolution towards shared channels.

7.1.2.1. Key points of the architecture

- **SharePoint / File Storage**
  - New SharePoint Online site for each shared channel
- **Identities**
  - Subset of the team / internal / team members (tenant)
  - B2B direct members / external
  - None B2B External
- **Channel email / group mailbox**
  - Not available

7.1.2.2. B2B direct - Identities

The B2B direct identities are a new development and shows that the topic of shared channels did not come from the Microsoft Teams team, but was driven by the Identity Team (AAD). This is how this new possibility of identities was created and also the appropriate portal to manage them including PowerShell scripts and hints.

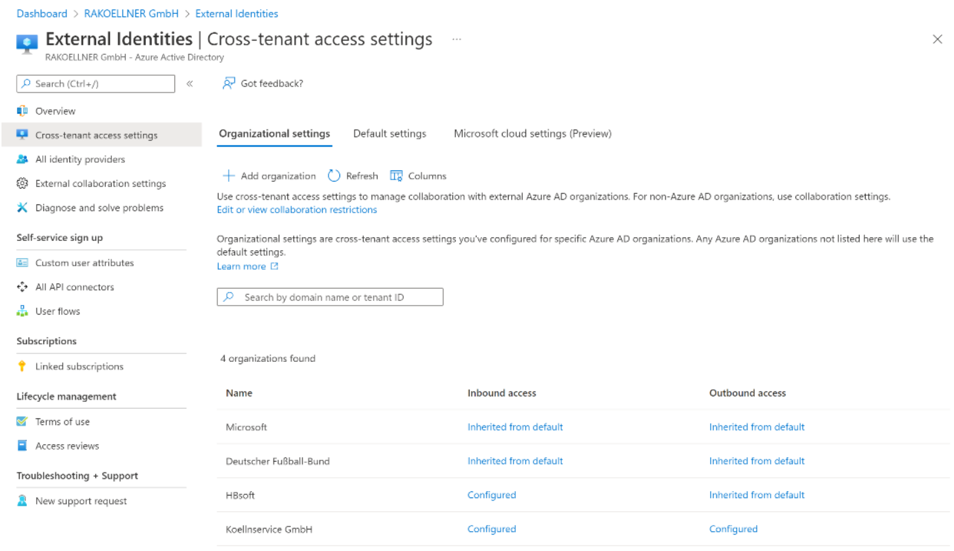
B2B direct briefly explained

B2B direct means the possibility to bring external identities into the own tenant. These are no B2B users (ext.) in the own AAD structure and no anonymous users, as in Microsoft Teams meetings.

The identities now taken from the foreign AAD structure bring the ID object with them into their own tenant and at the same time also their MFA (2FA) and if it is a B2B.

Management Portal - External Identities

The new External Identities Portal is shown below. In this portal, the connections between tenants are controlled and groups or individual users are allowed to act in other tenants.



External Identities | Cross-tenant access settings

RAKOELLNER GmbH - Azure Active Directory

Use cross-tenant access settings to manage collaboration with external Azure AD organizations. For non-Azure AD organizations, use collaboration settings.
Edit or view collaboration restrictions

Organizational settings are cross-tenant access settings you've configured for specific Azure AD organizations. Any Azure AD organizations not listed here will use the default settings.
Learn more

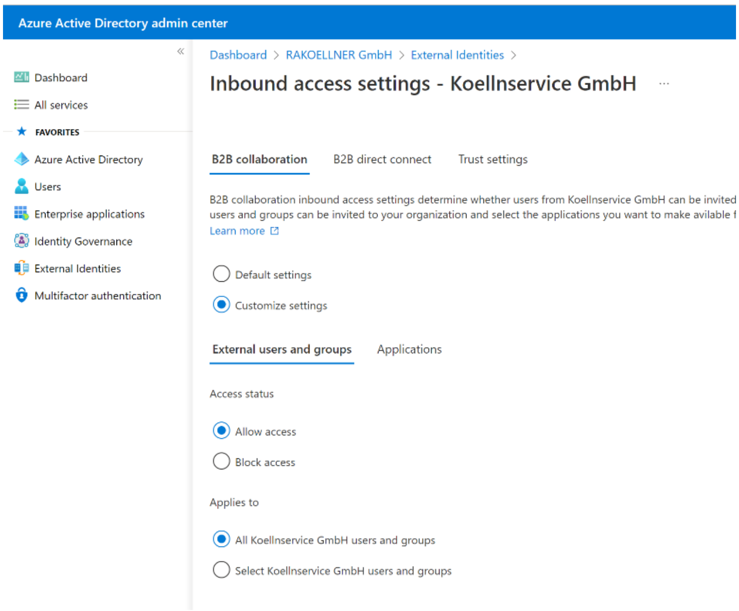
4 organizations found

Name	Inbound access	Outbound access
Microsoft	Inherited from default	Inherited from default
Deutscher Fußball-Bund	Inherited from default	Inherited from default
HBsoft	Configured	Inherited from default
Koellnservice GmbH	Configured	Configured

In the screenshot above, you can see the connection to various tenants that don't currently need to know about it on the other side. There is no notification when a side wants to establish a connection. Nothing happens for the time being, if the other side does not make a configuration.

You can see this configuration in the next screenshot:

a. B2B
b. B2B direct
c. Trust Settings



Inbound access settings - Koellnservice GmbH

B2B collaboration inbound access settings determine whether users from Koellnservice GmbH can be invited
users and groups can be invited to your organization and select the applications you want to make avilable f
Learn more

○ Default settings
● Customize settings

Access status

● Allow access
○ Block access

Applies to

● All Koellnservice GmbH users and groups
○ Select Koellnservice GmbH users and groups

7.1.2.2.1. B2B direct

B2B direct is the new identity, rather a shared identity that can be used in your own tenant and also in other tenants.

B2B direct options

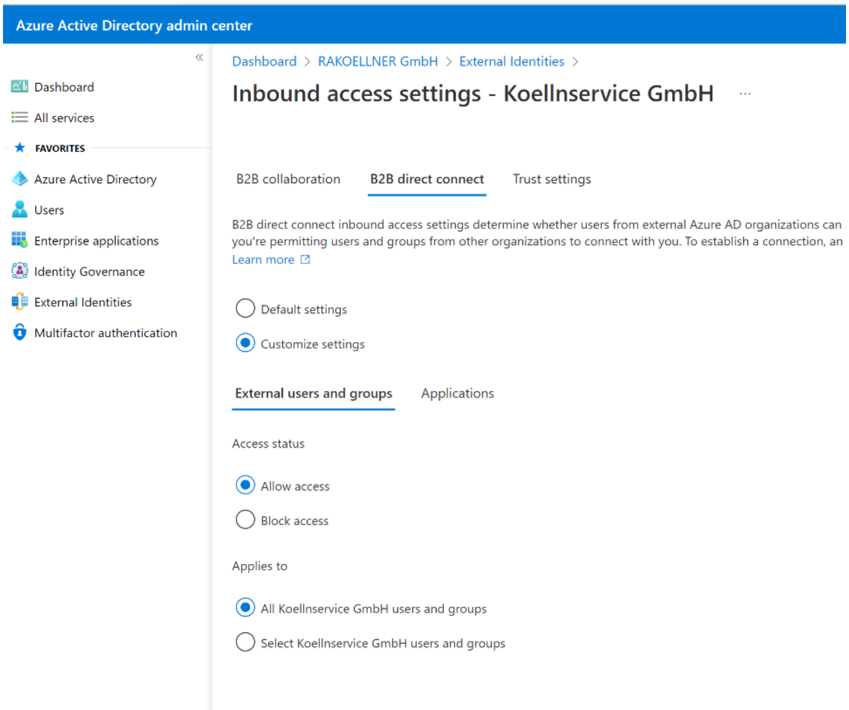
- Identity of the source tenant in a foreign tenant
- Configuration
    - Limitation to one user, group or tenant
    - In foreign tenants
    - And invite to own tenant
- Use
    - Don't: Email distributors, can't assign admin or other rights, no custom MFA.
- Supervision / Monitoring
    - No not in your own tenant in the audit logs
    - Manual monitoring
- Trust settings from the source tenant
    - MFA
    - Device information, compliance status
    - Hybrid join of the device
    - Note: Microsoft is currently working on being able to pass on more information and display parameters from the other tenant.

Identity product group

The product group in question, which came up with the new B2B direct identity and designed its use, is always open to requests and functional enhancements.

Screenshot from my testtenant, Rakoellner GmbH

In the following screenshot you can see the configuration of the foreign tenant (KöllnService GmbH) in my test environment (Rakoellner GmbH). Important to know is that I did not get any feedback as Tenant Admin when a tenant is added and configured in another one. This is a problem.



Inbound access settings - Koellnservice GmbH

B2B direct connect inbound access settings determine whether users from external Azure AD organizations can you're permitting users and groups from other organizations to connect with you. To establish a connection, an Learn more

○ Default settings
● Customize settings

Access status

● Allow access
○ Block access

Applies to

● All Koellnservice GmbH users and groups
○ Select Koellnservice GmbH users and groups

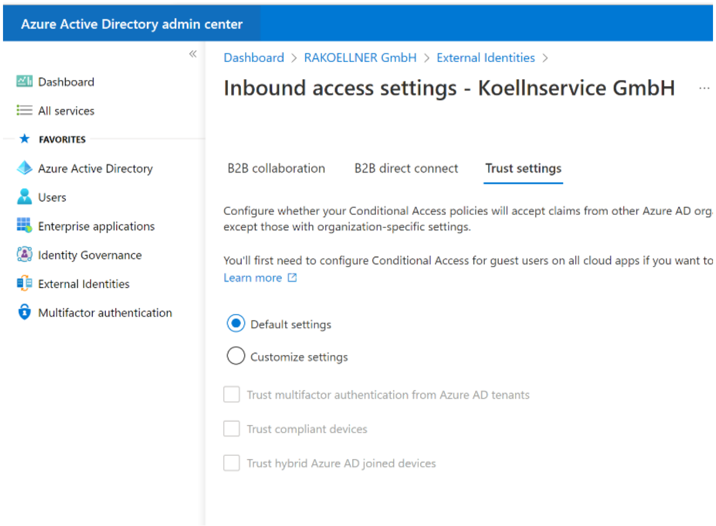
But you can also see that you can either use the default settings, everything blocked to start (Privacy by Design principle) or choose your own settings per company/connection. I can also only recommend this and not to work with the default settings at first.

As an admin, you then select whether you want to have the entire tenant as a B2B direct identity in your tenant (inbound access) or whether your own identities may also be invited into this foreign tenant (exbound access). Of course, it is recommended to limit this to individual users or groups (departments). It is a question of governance.

Ultimately, you also have to approve Applications for Microsoft Teams. Later, there will be more and more services that can be released individually. However, today it is only Microsoft Teams.

7.1.2.2.2. Trust Settings / Trust Settings

A very important setting besides the limitation of the user:s are the "Trust Settings", i.e. the settings for the trust position with the foreign tenant.



Dashboard > RAKOELLNER GmbH > External Identities >

Inbound access settings - Koellnservice GmbH ...

B2B collaboration | B2B direct connect | Trust settings

Configure whether your Conditional Access policies will accept claims from other Azure AD org except those with organization-specific settings.

You'll first need to configure Conditional Access for guest users on all cloud apps if you want to Learn more

● Default settings

○ Customize settings

□ Trust multifactor authentication from Azure AD tenants

□ Trust compliant devices

□ Trust hybrid Azure AD joined devices

As you can see in the screenshot, please select the Customize Settings here as well, although a default setting would simplify things here as well.

Possible:

- **Trust multifactor authentication from Azure AD tenants**
  - MFA of the foreign tenant
  - Microsoft MFA[4] / no third party MFA solution
- **Trust compliant devices**[5]
  - EndPoint Manager rule
  - Compliant with the tenant's rules (source)
- **Trust hybrid Azure AD Joined devices**[6]
  - Device of the organization / no BYOD
  - Integrated with local AD and Azure AD, and requires logging in to the device with the organization account

It is important to know that the three parameters cannot be influenced and must be adopted 1 to 1 by the foreign organization. Information about a detailed configuration, e.g. what compliant devices means, must be requested from the foreign tenant admin or organization.

It is **not possible to** give e.g. own MFA rules to the B2B direct users. This also includes monitoring them. With these shared identities, the configuration and hardening of the foreign tenant must be trusted.

[4] https://docs.microsoft.com/de-de/azure/active-directory/authentication/concept-mfa-howitworks, accessed 04/15/2022.

[5] https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started, accessed 04/15/2022.

[6] https://docs.microsoft.com/en-us/azure/active-directory/devices/concept-azure-ad-join-hybrid, accessed 07/20/2022.

In addition, **3rd party mechanisms or products** such as MobileIron or OneTrust MFA are not recognized and cannot be transferred from the source tenant. Whether this will happen at all is currently questionable. This means that both sides must move in the Microsoft 365 universe with the corresponding products.

https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/cross-tenant-access-settings-for-secure-collaboration-now/ba-p/3575844

7.1.3. Comparison of usage scenarios

The different scenarios are interesting. Some are recommended and some are not. You also have to evaluate this in each case according to company and risk.

The following list is only a small selection of scenarios:

Scenario	**Default (B2B)**	**Private (B2B)**	**Shared (B2B direct)**	
Group subsidiaries	X	X	X	
Parent company and subsidiary	X	X	X	
External service providers (e.g. architects)	X			
Third-party IT service providers	X			
Association or foundation of the company			X	X

7.1.4. Desire of the users / challenges

Many users have expressed their desire to work better and more effectively with external parties using Microsoft Teams via various submissions under Uservoices for Microsoft Teams, as well as via Account Managers.

Main points of criticism

i. Change of tenant to external and the consequences of this (interruption of meetings, no notifications, long duration, additional registration, etc.)
ii. B2B user in external tenant that does not allow OneDrive sync.
iii. External is user 2nd class in foreign tenant (functional scope)

Challenges for Microsoft

The architecture of Microsoft Teams and the channels brings some challenges. These main criticisms mentioned above are technical limits that cannot be easily overcome. It has to do with the identity in the form of member and B2B external user, which is also linked to notifications and the fact that you cannot continue a meeting because you change the identity from Xy@domain.de to xy.domain.de@ext.onmicrosoft.com in the other tenant.

This is how the Identity team, and later the Microsoft Teams team, started working over 1.5 years ago to meet customer needs.

The result was **B2B direct**, a new form of identity.

7.1.5. B2B direct as a solution

B2B direct is a new identity in the Microsoft universe. With B2B direct the user:in brings the identity with him into the foreign Microsoft environment. This means that the external user does not get his own identity in the foreign environment. The identity with all its advantages and disadvantages is brought from the foreign environment.

7.2. Governance

In the context of using Microsoft Teams Connect, the topic of governance and management is even more important. It counts as a technical-organizational measure directly on data protection and also on topics such as IT security.

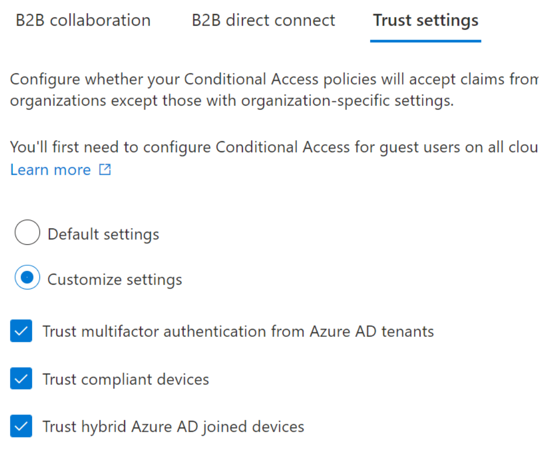
7.2.1.Basics

There are a number of things to consider in the governance of shared channels. In the basics, we will take a look at these and list them.

7.2.2. Governance of the third-party tenant/ cooperation + MFA

B2B Direct Identities bring their own identity with them and can thus work in a foreign team channel (shared channel) without having to change the tenant. Of course, it is advisable to activate MFA as well, but this always comes from your own tenant.

Accept MFA of the foreign tenant



B2B collaboration | B2B direct connect | **Trust settings**

Configure whether your Conditional Access policies will accept claims fron
organizations except those with organization-specific settings.

You'll first need to configure Conditional Access for guest users on all clou
Learn more

○ Default settings

● Customize settings

☑ Trust multifactor authentication from Azure AD tenants

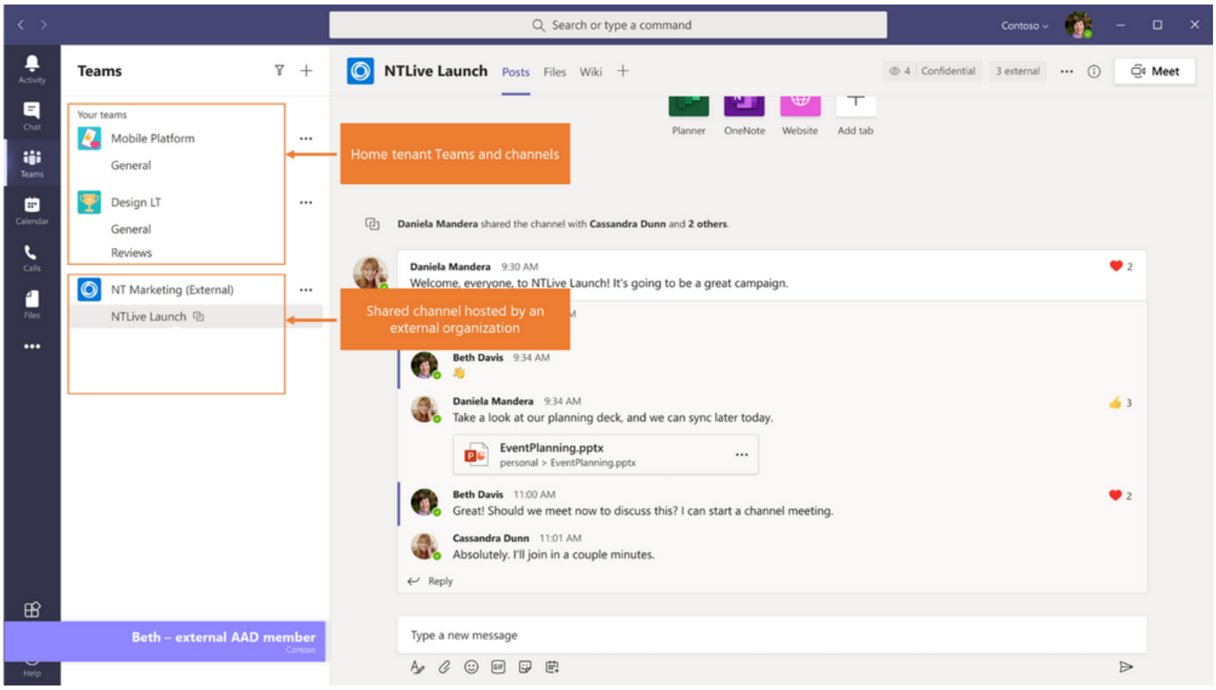
☑ Trust compliant devices

☑ Trust hybrid Azure AD joined devices

Figure 1 Inbound access settings

7.2.3. Channels names

The first issue is the names of the channels. Here you have to think more about shared channels than you did with classic channels or private channels. But what is different now?



Daniela Mandera shared the channel with Cassandra Dunn and 2 others.

Daniela Mandera 9:30 AM
Welcome, everyone, to NTLive Launch! It's going to be a great campaign.

Beth Davis 9:34 AM

Daniela Mandera 9:34 AM
Take a look at our planning deck, and we can sync later today.

EventPlanning.pptx
personal > EventPlanning.pptx

Beth Davis 11:00 AM
Great! Should we meet now to discuss this? I can start a channel meeting.

Cassandra Dunn 11:01 AM
Absolutely. I'll join in a couple minutes.

Source: MS[7]

7.2.3.1. Challenge

The name of the shared channel is displayed and above it the name of the team from which the channel originates. Both must be unique, so that e.g. no users post data to the wrong channel.

Here come once both views:

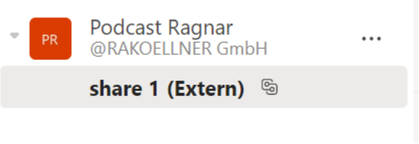

PR
Podcast Ragnar
@RAKOELLNER GmbH
share 1 (Extern)

Figure 2 Screenshot from the External Team

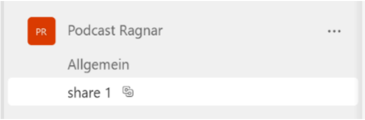

PR
Podcast Ragnar
Allgemein
share 1

Figure 3 Screenshot from the source tensor

In addition, the names of the channels can currently be changed later, but the SharePoint site in the background does not yet follow suit. Microsoft is currently working on this.

7.2.3.2. Possible solutions

To get a handle on the names you could use the following solution:

Team name: Company Project Team

Channel name: Company-Partner

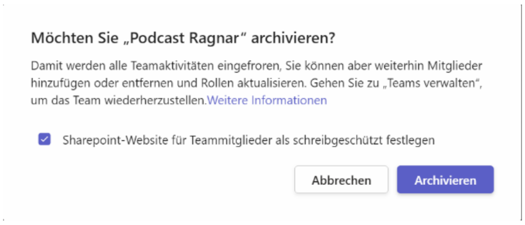
[7] https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/cross-tenant-access-settings-for-secure-collaboration-now/ba-p/3575844 , accessed 07/22/2022.

This leads to the fact that in the own tenant, in the foreign tenant and also in the Windows Explorer/Mac the folders and channels are correctly known and all know how to behave.

7.2.4. Microsoft Teams - Archive Function

It is questionable what the effect of a Microsoft Teams shared channel with the archive function will be. The owner of a team can archive it and thus also archive the shared channel.

Archive the team



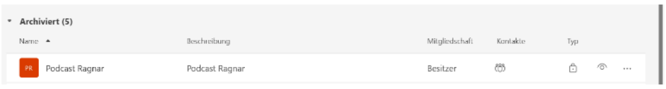
Möchten Sie „Podcast Ragnar" archivieren?

Damit werden alle Teamaktivitäten eingefroren, Sie können aber weiterhin Mitglieder hinzufügen oder entfernen und Rollen aktualisieren. Gehen Sie zu „Teams verwalten", um das Team wiederherzustellen. Weitere Informationen

☑ Sharepoint-Website für Teammitglieder als schreibgeschützt festlegen

Figure 4 Archive team screenshot

Sequence of archiving in the origin tant



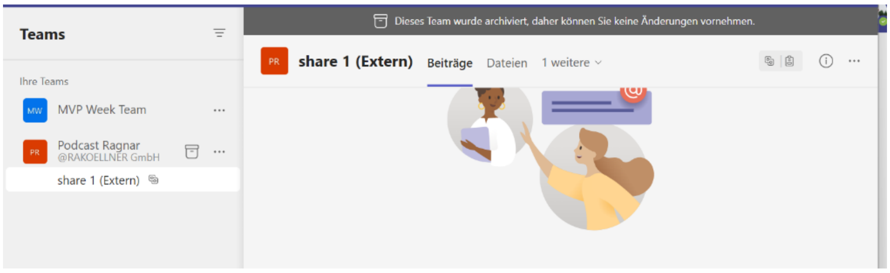
Archiviert (5)

Name	Beschreibung	Mitgliedschaft	Kontakte	Typ
PR Podcast Ragnar	Podcast Ragnar	Besitzer		

Figure 5 Screenshot archived team

This means that the team disappears from the search and GAL and the members can no longer work in the team. The SharePoint Online is now in read-only mode, so users can only read files.

Archived team at the external



Dieses Team wurde archiviert, daher können Sie keine Änderungen vornehmen.

Figure 6 Archived team at the external

This means that the archive icon is also visible here, but the channel is still present. So it remains present in the list and does not disappear, as it does for users from their own team.

However, changes cannot be made by the external party.

The way back is also possible!

After the user in the source tenant has restored the team, the external user can also use it again to its full extent:

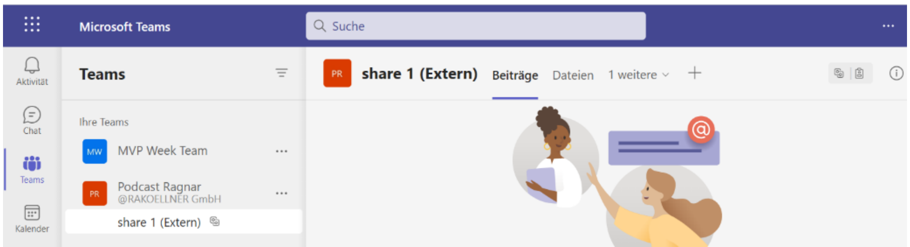


Figure 7 Screenshot restored team

7.2.5. Microsoft Teams - EXIT Policy

In Microsoft Teams it is possible to use an EXIT policy. This enables the automated deletion of orphaned teams.[8] This includes that the owner of the team gets a message 10,15 and 1 day before the end and can keep the team.

This also affects teams with shared channels. In my test it happened that the team was deleted without extension.

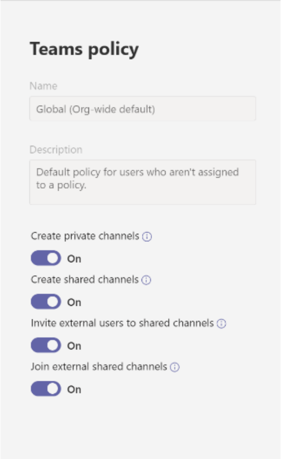
This also means that the channel is removed from the external tenant. The external user then also no longer has access or a view in the team.

7.2.6. Creating shared channels

The creation of shared channels must first be allowed in the Teams Admincenter. For this purpose, you can enable the possibility to create shared channels for a few or all users in the tenant.

As a rule, either all or a "Premium Teams User2, who then also gets this policy, in addition to teams recording function and transcription.

Here you can see the Teams Policy in the Microsoft Teams Admincenter:



Teams policy

Name

Global (Org-wide default)

Description

Default policy for users who aren't assigned to a policy.

Create private channels ⓘ

On

Create shared channels ⓘ

On

Invite external users to shared channels ⓘ

On

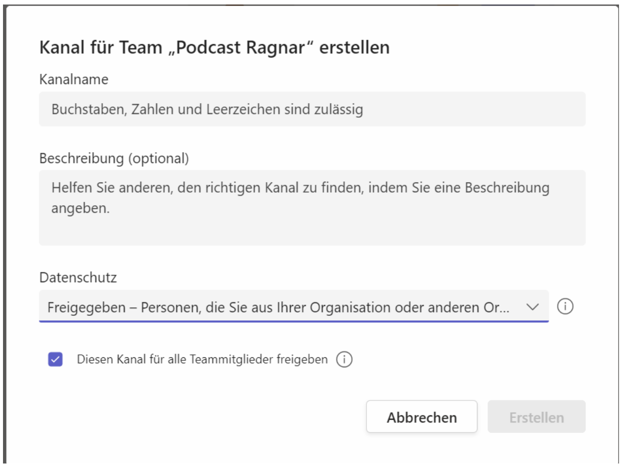
Join external shared channels ⓘ

On

Figure 8 Teams Policy screenshot

[8] https://learn.microsoft.com/en-us/microsoftteams/team-expiration-renewal

Users with these rights can then create a channel in their team:



Kanal für Team „Podcast Ragnar" erstellen

Kanalname

Buchstaben, Zahlen und Leerzeichen sind zulässig

Beschreibung (optional)

Helfen Sie anderen, den richtigen Kanal zu finden, indem Sie eine Beschreibung angeben.

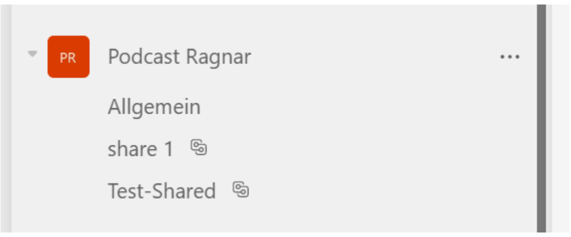
Datenschutz

Freigegeben – Personen, die Sie aus Ihrer Organisation oder anderen Or...

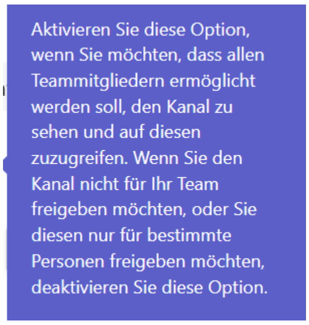
☑ Diesen Kanal für alle Teammitglieder freigeben

Figure 9 Create shared channel screenshot

This then appears normally in the team.



It is important if you want to have all team members directly in the shared channel or if you want to separate them. Then you have to uncheck the lower checkbox "Share this channel with all team members".



Aktivieren Sie diese Option, wenn Sie möchten, dass allen Teammitgliedern ermöglicht werden soll, den Kanal zu sehen und auf diesen zuzugreifen. Wenn Sie den Kanal nicht für Ihr Team freigeben möchten, oder Sie diesen nur für bestimmte Personen freigeben möchten, deaktivieren Sie diese Option.

Figure 10 Screenshot sharing with team members

7.2.7. Manage and administer shared channels

The exciting topic for operations is the management of shared channels.

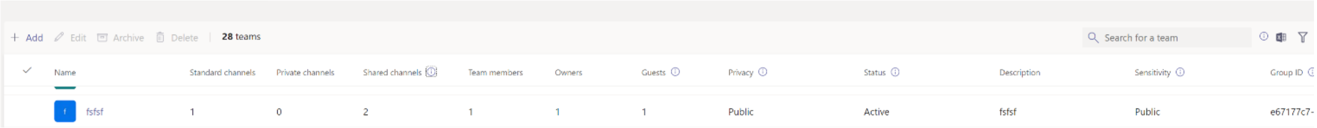
Manage and works in:

- Public teams
- Private teams

Not in: org-wide teams.

7.2.7.1. Microsoft Teams Admin Center

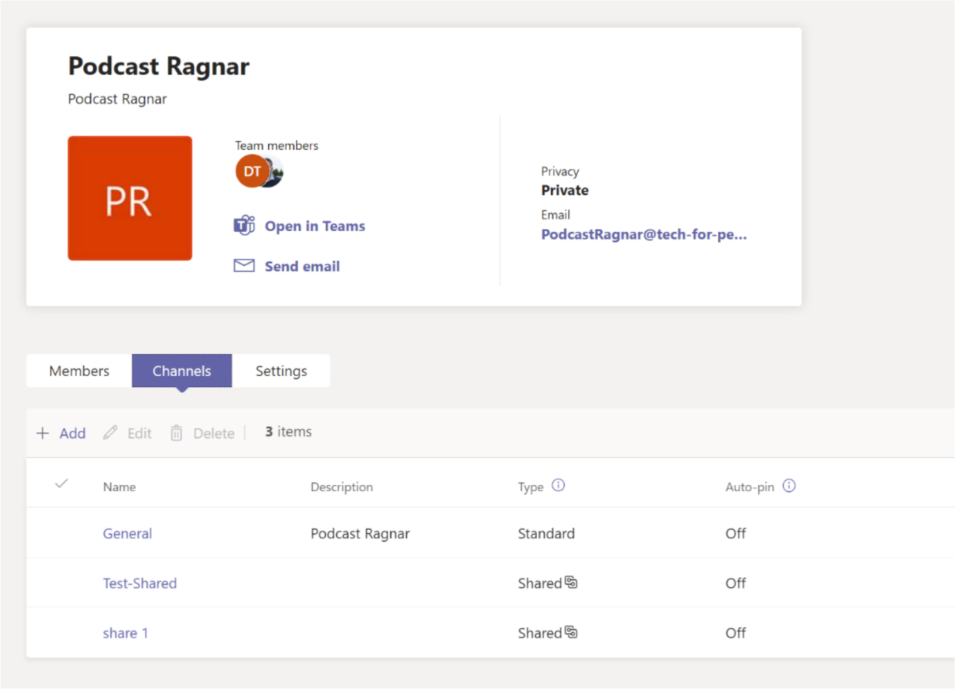
In the Microsoft Teams Admincenter under "Manage Teams" the teams and shared channels can be seen. Here administrators can see the number and in which team they are.



Name	Standard channels	Private channels	Shared channels	Team members	Owners	Guests	Privacy	Status	Description	Sensitivity	Group ID
fsfsf	1	0	2	1	1	1	Public	Active	fsfsf	Public	e67177c7-

Figure 11 Screenshot from the Teams Admincenter

This also applies to the detailed view:



Podcast Ragnar

Podcast Ragnar

Privacy
Private

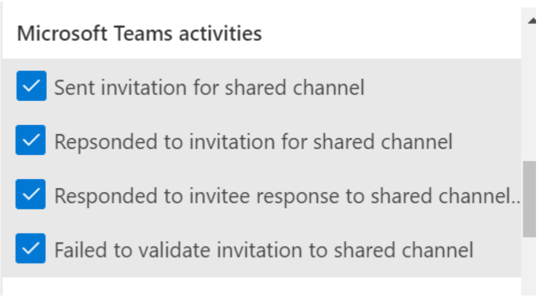
Email
PodcastRagnar@tech-for-pe...

Name	Description	Type	Auto-pin
General	Podcast Ragnar	Standard	Off
Test-Shared		Shared	Off
share 1		Shared	Off

Figure 12 Screenshot detail view Microsoft Teams Team

7.2.7.2. Audit logs

The audit logs have the following values:



Microsoft Teams activities

- ☑ Sent invitation for shared channel
- ☑ Repsonded to invitation for shared channel
- ☑ Responded to invitee response to shared channel..
- ☑ Failed to validate invitation to shared channel

Figure 13 Screenshot of audit logs for shared channels

These audit logs can also be transferred to a SOC SIEM. I have tried it myself with Azure Sentinel and Splunk and the values arrived there as well.

7.2.7.3. Shared channels and dynamic teams

There is also the question of whether shared channels can be filled with dynamic groups so as not to have to intervene manually.

Dynamic teams from dynamic Security Groups are supported for membership in shared channels. So, you could create an Azure AD dynamic group with a filter to find all licensed user accounts and enable the group as a team. The downside is that Azure AD dynamic groups require Azure AD Premium P1 licenses, which may or may not be an issue for the organization.

7.2.7.4. PowerShell

PowerShell and specifically the Microsoft Teams Module also allows you to view, create and also delete the teams with the shared channels.

Example: Creating a Shared Channel via PowerShell[9]

```
New-TeamChannel -GroupId <id of the Team> -DisplayName <shared channel display name> -
MembershipType Shared
```

7.2.8.Identity / Cross-Tenant

For Teams Connect, the new variant of B2B direct identities including a new tool has been introduced. In addition to identities in the tenant, B2B guests, B2B externals, B2B direct (identity from an AAD) are now also possible.

7.2.8.1. B2B and B2B direct

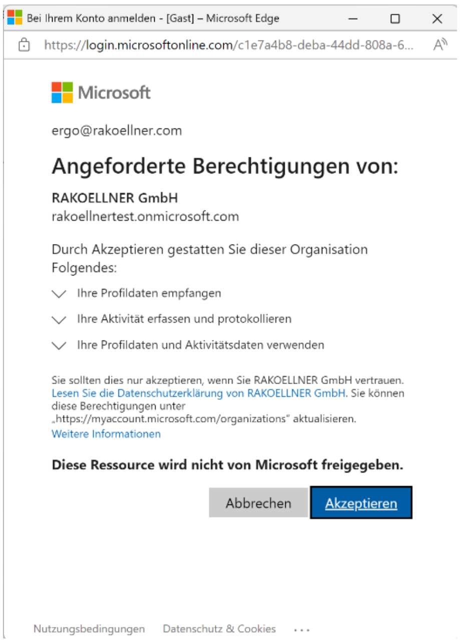
B2B direct is the new form of identity and allows you to take your own identity with you into a foreign tenant.

Comparison within a table

<table>
<tr><th colspan="2"></th><th>B2B</th><th>B2B direct</th></tr>
<tr><td>External identity in own tenant (ext.)</td><td>Yes</td><td colspan="2">No</td></tr>
<tr><td>External identity is brought into the own tenant</td><td>No</td><td colspan="2">Yes</td></tr>
<tr><td>External identity management possible</td><td>Yes</td><td colspan="2">No</td></tr>
<tr><td>Assignment of rights and licenses to the external identity</td><td>Yes</td><td colspan="2">No</td></tr>
<tr><td>Inclusion of the external identity in mail distribution lists</td><td>Yes</td><td colspan="2">No</td></tr>
</table>

The following permissions are required:

[9] https://learn.microsoft.com/en-us/powershell/module/teams/new-teamchannel?view=teams-ps


Bei Ihrem Konto anmelden - [Gast] – Microsoft Edge
https://login.microsoftonline.com/c1e7a4b8-deba-44dd-808a-6...
Microsoft

ergo@rakoellner.com

Angeforderte Berechtigungen von:

RAKOELLNER GmbH
rakoellnertest.onmicrosoft.com

Durch Akzeptieren gestatten Sie dieser Organisation Folgendes:

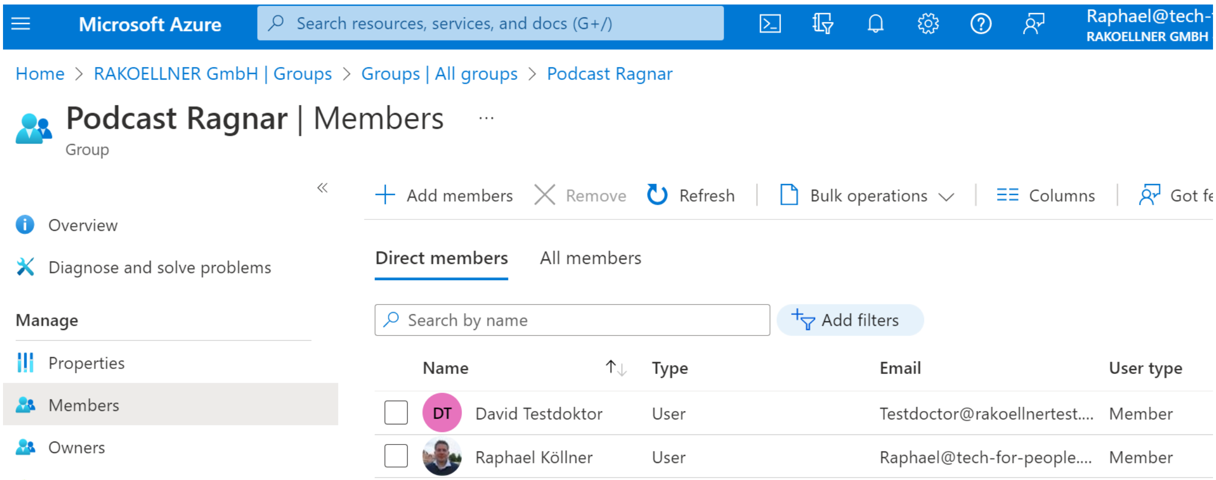
- Ihre Profildaten empfangen
- Ihre Aktivität erfassen und protokollieren
- Ihre Profildaten und Aktivitätsdaten verwenden

Sie sollten dies nur akzeptieren, wenn Sie RAKOELLNER GmbH vertrauen. Lesen Sie die Datenschutzerklärung von RAKOELLNER GmbH. Sie können diese Berechtigungen unter „https://myaccount.microsoft.com/organizations" aktualisieren.
Weitere Informationen

Diese Ressource wird nicht von Microsoft freigegeben.

Figure 14 Permissions screenshot

Let's take a look at the Azure AD of the tenant and the group that invited the B2B direct identities.

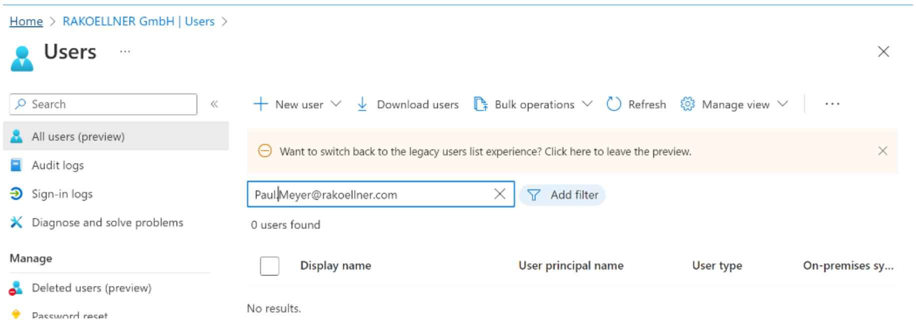


	Name	Type	Email	User type
□	DT David Testdoktor	User	Testdoctor@rakoellnertest....	Member
□	Raphael Köllner	User	Raphael@tech-for-people....	Member

Figure 15 Azure AD Group Member screenshot

This is correct, because in the team "Podcast" Ragnar is only the two people from my tenant. The shared channel is not shown here, which still contains an external B2B direct.

Then let's take a look at the AAD users and look for the B2B direct user:



Want to switch back to the legacy users list experience? Click here to leave the preview.

PaulMeyer@rakoellner.com

0 users found

Display name	User principal name	User type	On-premises sy...

No results.

Figure 16 Screenshot search for B2B direct user

As expected, the B2B direct user cannot be found here, because no identity is created in the tenant as in B2B.

As a result, identity cannot be managed in our tenant, nor can a SOC SIEM or other capabilities such as MFA.

7.2.8.2. Cross Tenant

Collaboration across tenants is extremely important. B2B direct is designed to provide another solution for working together without having to change tenants.

Link: https://docs.microsoft.com/en-us/azure/active-directory/external-identities/cross-tenant-access-overview

7.2.8.3. B2B direct

B2B Direct is the new variant of identities. Currently, these can only be used for shared channels and beyond with the safeguards, such as MFA from the origin tester.

Documentation https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-direct-connect-overview

7.3. Privacy

With shared channels, data protection is an extremely important issue. On the one hand, externals come into one's own channel, but with an identity that cannot be managed or data extracted, but only from the urtenant. In addition, data can quickly leak out and provoke improper use.

In addition, there is the question of:

- Order data processing
- Privacy policy
- Risk Assessment,
- Amendment of the DSFA and adaptation of the processing directory

7.3.1.Protection goals and risks

For each scenario, I recommend a closer look based on risk.

7.3.1.1. Protection goals of data processing according to Art. 5 (1) lit. f DSGVO

7.3.1.1.1. Integrity Art. 5 para. 1 lit. f DSGVO

"Integrity" would be best translated as "intactness", to use a term from the German language (BMJ marg. no. 68). IATE documents besides "intactness" and "integrity" also "unalteredness" and "completeness". Rec. 39 p. 12 refers to "security and confidentiality", which includes "(...) that unauthorized persons have no access to the data and cannot use the data or the devices with which they are processed". With the term "integrity" it can be specifically expressed that accesses do not necessarily have to be unauthorized further processing, but that also a change - i.e. falsification, addition, restriction - of the data by third parties must be excluded; this obligation is directed at the responsible party, regardless of the prohibition directed at the third party, which is also sanctioned by criminal law. In this respect, the controller is subject to the protective obligation of a guarantor to avert risks to the data; to this end, measures must be taken against processing by third parties and against damaging events (Reimer in Sydow DS-GVO Art. 5 marginal no. 47 et seq.). Third parties are persons who are not authorized to process data, i.e. also those who are active within a company entrusted with data processing without being responsible for the specific data processing. Therefore, the controller also has an obligation within the company to secure the data against unauthorized access."[10]

7.3.1.1.2. Confidentiality , Art. 5 para. 1 lit. f DSGVO

The principle of integrity and confidentiality provides that personal data shall be processed in a manner that ensures appropriate security of the data. This data must be protected against accidental loss , accidental destruction or accidental damage by appropriate technical and organizational measures.

7.3.1.1.3. Accuracy , Art 5. para. 1 lit. d DSGVO

The accuracy of the IT systems means that the personal data must be factually correct and, where necessary, kept up to date by the IT system. All reasonable measures must be taken to ensure that personal data which are inaccurate in relation to the purposes of their processing are erased or rectified without delay.

7.3.1.1.4. Purpose limitation , Art. 5 para. 1 lit. b DSGVO

"The purpose legitimizes the processing of the data. It is the linchpin, also in view of necessity, adequacy, completeness and duration of the processing. The purpose can be the aim, reason and essence of the processing. Accordingly, the purpose limitation principle refers specifically and traditionally to data

[10] DS-GVO Art. 5 Principles for the processing of personal data, Frenzel I Paal/Pauly, DS-GVO BDSG 3rd edition 2021.

protection."[11] Processing takes place only for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes (prohibition of coupling).

7.3.1.2. Data minimization , Art. 5 para. 1 lit c DSGVO

"Data minimization" from Article 5 (1) (c) of the GDPR combines three interrelated requirements under the term "data minimization". Data must be qualitatively and quantitatively limited in terms of purpose limitation. They must be significant and proportionate to the achievement of the purpose."[12]

7.3.1.3. Legitimacy t, processing in good faith, transparency, Art. 5(1)(a) GDPR

The processing of personal data must be carried out in a lawful manner, in good faith and in a way that is comprehensible to the data subject.

7.3.1.4. Availability

Availability refers to the specific, flawless availability of an IT system. This must be available for the intended use and function properly. There must be no hindrance to the data subject's access to his or her personal data.

7.3.1.5. Overview of the risks from the hazards

The risks arising from the various hazards, including existing or potential risk mitigation factors, are described below.

7.3.1.5.1. *List of hazards*[13]

- Access by US authorities and consequences of the ECJ Schrems ruling 2
- Discrimination
- Damage to reputation
- Reputational damage
- Financial damage
- Obstruction of the exercise of data subject rights
- Unauthorized cancellation of pseudonymization
- Obstruction of the control of personal data
- Profiling
- Identity Theft
- Violation of professional secrecy
- Other economic or societal disadvantages (not relevant/considered).
- Other (not relevant/not considered)

For example, a consideration of an intra-group shared channel use between group subsidiaries:

Description of the risks	

[11] Frenzel, in Paal/Pauly, DSVGO Commentary, 3rd edition 2021, Art 5, para. 23.
[12] Frenzel, in Paal/Pauly, DSVGO Commentary, 3rd edition 2021, Art 5, para. 34-35.
[13] DSK KPNr 5 Datenschutz-Folgenabschätzung Lizenzvermerk (datenschutzkonferenz-online.de); The concept of protection goals and the standard data protection model (datenschutz-berlin.de)

Damage category	Probability of occurrence	Risk
Preventing data subjects from controlling their own data	with some effort	middle
Identity theft or fraud	Almost impossible	Low
Damage to reputation	Almost impossible	Low
Violation of professional secrecy	with some effort	middle
Obstruction of the exercise of rights of persons concerned	Almost impossible	Low
Unauthorized cancellation of pseudonymization	with some effort	middle
Financial loss	Almost impossible	Low
Profiling through evaluation of personal aspects	Almost impossible	Low

Risk-increasing factors Description of the risk factors	
Special categories of data	No
Large amounts of data	No
Persons in need of protection	Yes, apprentices

7.3.2. Risk assessment and risk matrix

The respective risk resulting from the protection goals per hazard scenario is displayed in a risk matrix corresponding to this one. The results per hazard scenario are condensed into an overall view.

Effects from the perspective of those affected	aximum	hedium	hedium	high	Very high
	tantially	hedium	hedium	hedium	high
	stricted	low	hedium	hedium	medium
	gligible	low	low	hedium	medium
	negligible	restricted	bstantially	maximum	
	bability of occurrence				

The example of shared channels within a corporate group with the TOMs (next chapter) then results in an evaluation:

Effects from the perspecti	ximum	hedium	hedium	high	Very high

ve of thos e affe cted								
	antially	medium	edium	edium	high			
	stricted	red Channel	edium	medium				
	gligible	low	low	edium	medium			
					egligible	restricted	bstantially	aximum
					ability of occurrence			

7.3.3.Risks and TOMs for shared channels

OM	Risk	Explanation
Training Deep Dive	Minimizing the risk: Data outflow	Only people with training are allowed to create and manage Teams Connect channels.
Training Microsoft Teams	Minimizing the risk: • Data outflow • Legality • Copyrights improper use	Only people who have received training and have been informed of the risks of data leakage are allowed to use the channels.
MIP Label for the channel, default Label for DokumentenLib	Minimizing the risk: Data outflow	Using a dynamic group for the label and the channel is difficult, because B2B direct cannot be included. However, documents can be protected against unauthorized access.
Change DSFA	Regulatory compliance	The DSFA needs to be adjusted with this change in risk.
Change of the privacy policy	Comply with Art 13 GDPR	
Modification of the terms of use	Minimizing the risk: Data outflow	
Disable participation in external teams Connect	Minimizing the risk:	Activation only if the other tenant is configured accordingly DSGVO compliant.

	• Data outflow Data protection violations	
B2B direct limit to one Security Group	Minimizing the risk: • Data outflow Data protection violations	The entire tenant must never be released.

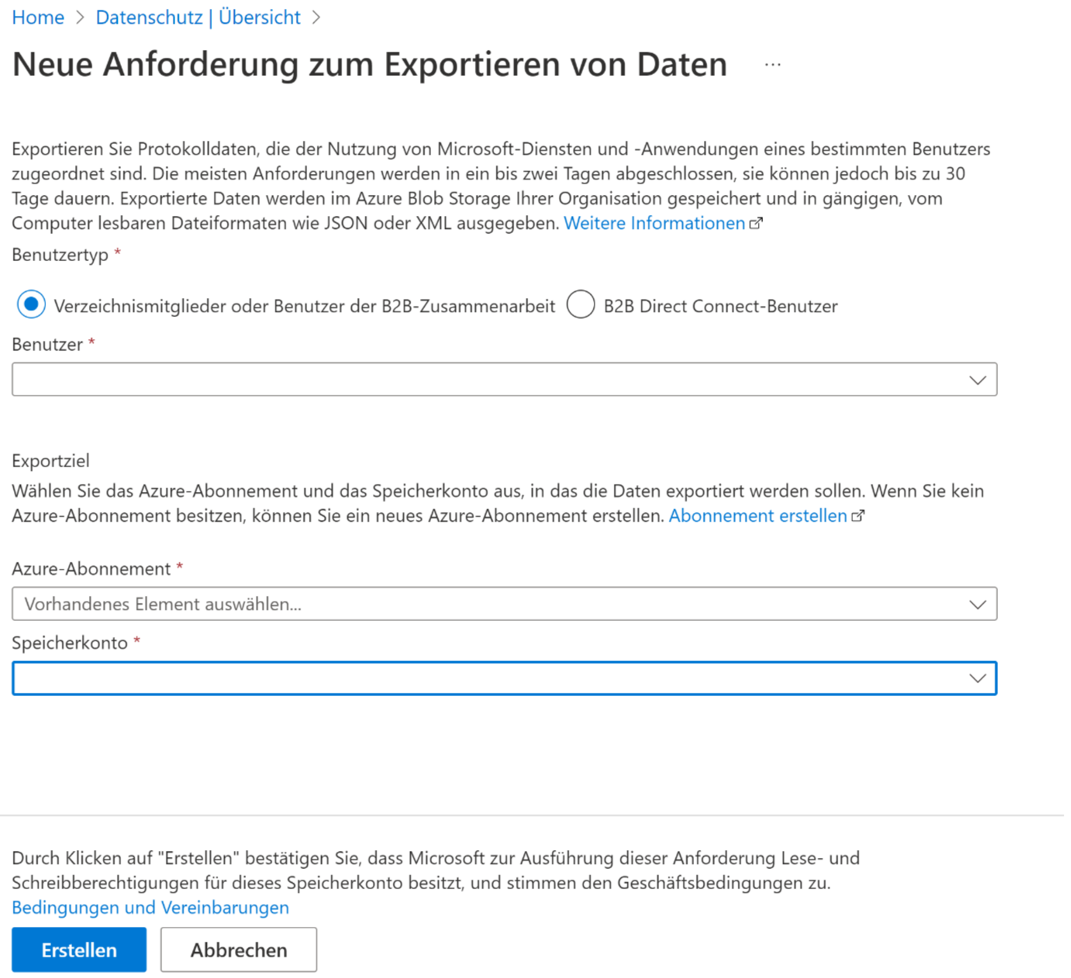
7.3.4. Legal basis

In this point we consider the legal bases for processing personal data.

Processing	Legal basis	Justification
Employees of the company	Art. 6 para. 1 lit. b DSGVO, in conjunction with § 26 BDSG	The processing is carried out via the standard legal basis on the basis of the employment contract. Likewise, the identity also belongs to the area of implementation of stable and secure operation (lit f).
External B2B direct	**External / service provider** Art. 6 para. 1 lit b DSGVO **External** Art. 6 para. 1 lit f DSGVO	Service provider: As a rule, the identity and related information of the data subject is processed for the performance of the contract. In the case of external parties, e.g. from foundations or corporate sponsorships, the basis is the balance of interests, which is decisive for the tenant operating company for reasons of stable and secure operation.
External B2B direct - MFA query	**External** Art. 6 para. 1 lit f DSGVO In her tenant: Art. 6 para. 1 lit. f or b) DSGVO with § 26 BDSG or BV	MFA is used for safe operation.
External B2B direct - hybrid join, device compliance status	**External** Art. 6 para. 1 lit f DSGVO In her tenant: Art. 6 para. 1 lit. f or b) DSGVO with § 26 BDSG or BV	MFA is used for safe operation.

7.3.5. Export functions in Azure

Since the beginning of December 2022, the export functions for B2B Direct Connect users have appeared in the data protection area in Azure. These allow the extraction of personal data of these users into an Azure Blog Storage.



Home > Datenschutz | Übersicht >

Neue Anforderung zum Exportieren von Daten ...

Exportieren Sie Protokolldaten, die der Nutzung von Microsoft-Diensten und -Anwendungen eines bestimmten Benutzers zugeordnet sind. Die meisten Anforderungen werden in ein bis zwei Tagen abgeschlossen, sie können jedoch bis zu 30 Tage dauern. Exportierte Daten werden im Azure Blob Storage Ihrer Organisation gespeichert und in gängigen, vom Computer lesbaren Dateiformaten wie JSON oder XML ausgegeben. Weitere Informationen

Benutzertyp *

● Verzeichnismitglieder oder Benutzer der B2B-Zusammenarbeit ○ B2B Direct Connect-Benutzer

Benutzer *

Exportziel

Wählen Sie das Azure-Abonnement und das Speicherkonto aus, in das die Daten exportiert werden sollen. Wenn Sie kein Azure-Abonnement besitzen, können Sie ein neues Azure-Abonnement erstellen. Abonnement erstellen

Azure-Abonnement *

Vorhandenes Element auswählen...

Speicherkonto *

Durch Klicken auf "Erstellen" bestätigen Sie, dass Microsoft zur Ausführung dieser Anforderung Lese- und Schreibberechtigungen für dieses Speicherkonto besitzt, und stimmen den Geschäftsbedingungen zu. Bedingungen und Vereinbarungen

7.3.6. B2B direct testing

It is important that the tests of the function are also within the regulatory framework and, in this case, data protection. It is also important to involve the works council for a test and to obtain a release for the testing employees.

Clearances required:

- IT Security
- Privacy
- Works Council

Recommendation/ Procedure

It is worthwhile for the test to use for example two Microsoft 365 Developer Tenant[14] or other existing possibilities of test tenants. These are usually already filled with test data and set up the connection with B2B direct and also add AAD P1 to run all tests.

The **recommendation** is that first all functions are configured openly, and then you start to restrict more and more. Example: all users -> later only one AD group -> later only one person

7.4. Compliance and other regulatory topics

This section discusses individual areas of regulation.

7.4.1. Act on the Protection of Business Secrets (GeschGehG)[15]

The outflow of data with B2B direct and thus with shared channels is only slightly increased due to the missing labels for these users and the existing DLP effect, if the foreign tenant has been checked beforehand.

Recommendation: 1. tenant verification schemes 2. NDA for users 3. Microsoft Information Protection deployment to protect accidental data landing in the shared channel.

7.4.2. Example MaRisk[16]

The minimum requirements for risk management in the financial sector (banks) also contain parameters that could be related to shared channels. These need to be examined:

Relevant

- AT 8.1, AT 8.2
- AT 4.1
- AT 4.3.4
- AT 4.4.2

7.4.3. Example: TISAX[17]

In the area of automotive production, TISAX is a set standard. A large part of the testing is also already done for shared channels through the use of Microsoft Teams/Microsoft 365; here it is only necessary to check whether the data center region is already certified. This can be done in the Microsoft Trust Center.

An important check is a checklist for the foreign tenant so that it also meets the security settings according to TISAX and optimally the environment is also TISAX certified after shared channels have been introduced.

[14] https://docs.microsoft.com/en-us/office/developer-program/microsoft-365-developer-program , accessed 07/13/2022.

[15] https://www.gesetze-im-internet.de/geschgehg/index.html#BJNR046610019BJNE000400000

[16] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html

[17] Example . https://portal.enx.com/en-us/tisax/

7.5. Contracts

Within the framework of the contract construct with the service provider, Microsoft and also the external parties, there is a complex set of contracts. In this whitepaper, we will limit ourselves to the B2B direct connection and only show the excerpt.

7.5.1. Contracts required before setting up shared channel

The following contracts secure the operation of shared channels:

- Secrecy /NDA
- Agreement on the use of shared channels and processes with the IT team and specialist department. (e.g., directory assistance process, MFA configuration).
- Commissioned data processing Art. 28 GDPR or joint responsibility Art. 28 GDPR depending on interpretation

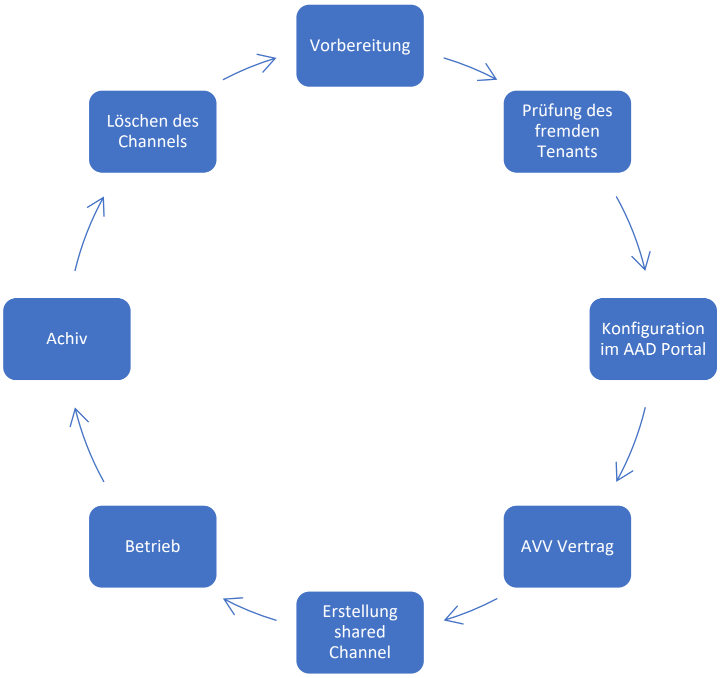
In addition to the knowledge

- Privacy policy of the hosting tenant
- Terms of use of the hosting tenant

Unfortunately, the privacy policy and terms of use of the hosted tenant are not displayed under myaccounts. This is because there is no section for them in your own tenant. Here I am currently working with the product group on the setting.

8. Teams Connect Lifecycle

In this section we have recorded a lifecycle of a shared channel:


Vorbereitung
Prüfung des fremden Tenants
Konfiguration im AAD Portal
AVV Vertrag
Erstellung shared Channel
Betrieb
Achiv
Löschen des Channels

9. Technical measures and products at Teams Connect in detail

In general, it is important to know that compliance and security measures only come from the hosting tenant and are effective. Currently, only three parameters of the foreign tenant are passed on.

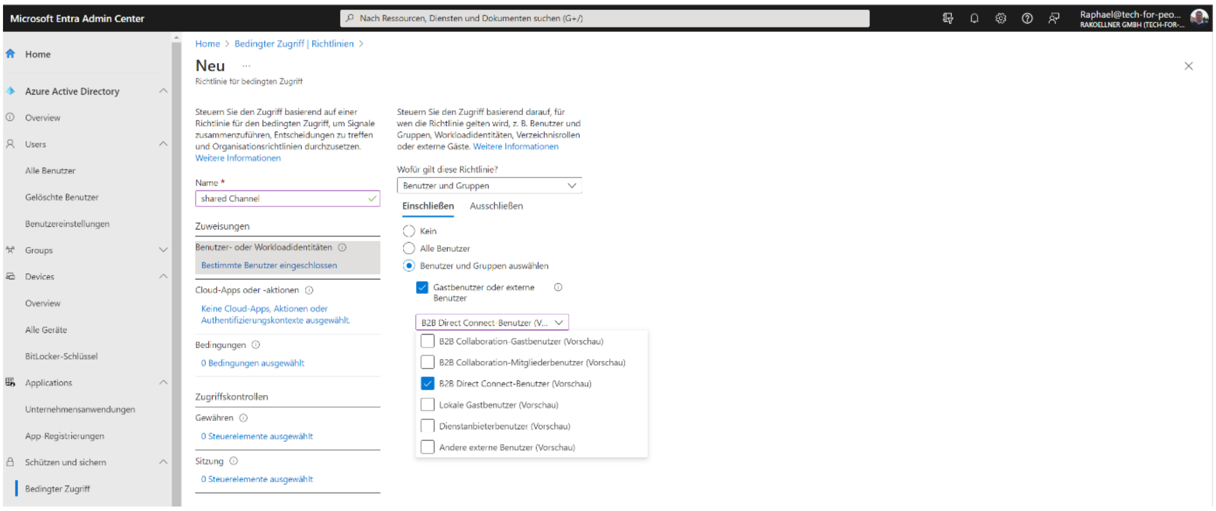
9.1. Identity / Identity Protection

Unfortunately, there is no identity protection or PIM or PAM for B2B direct connect users. Monitoring is also difficult at first, since these identities are not visible in the AAD of the hosting tenant. Here we are working hard on a preview variant in Entra. The desire of the tenants using the system is great.

Only the MFA of the foreign tenant is taken along, which must now also be part of the minimum standard.

9.2. Conditional Access (CA)

In Preview you can now also use CA for B2B direct users from the foreign tenant. You can find it here:



Neu

Richtlinie für bedingten Zugriff

Steuern Sie den Zugriff basierend auf einer Richtlinie für den bedingten Zugriff, um Signale zusammenzuführen, Entscheidungen zu treffen und Organisationsrichtlinien durchzusetzen. Weitere Informationen

Name *: shared Channel

Zuweisungen

Benutzer- oder Workloadidentitäten: Bestimmte Benutzer eingeschlossen

Cloud-Apps oder -aktionen: Keine Cloud-Apps, Aktionen oder Authentifizierungskontexte ausgewählt

Bedingungen: 0 Bedingungen ausgewählt

Zugriffskontrollen

Gewähren: 0 Steuerelemente ausgewählt

Sitzung: 0 Steuerelemente ausgewählt

Steuern Sie den Zugriff basierend darauf, für wen die Richtlinie gelten wird, z. B. Benutzer und Gruppen, Workloadidentitäten, Verzeichnisrollen oder externe Gäste. Weitere Informationen

Wofür gilt diese Richtlinie?: Benutzer und Gruppen

Einschließen | Ausschließen

○ Kein
○ Alle Benutzer
● Benutzer und Gruppen auswählen

☑ Gastbenutzer oder externe Benutzer

B2B Direct Connect-Benutzer (V...

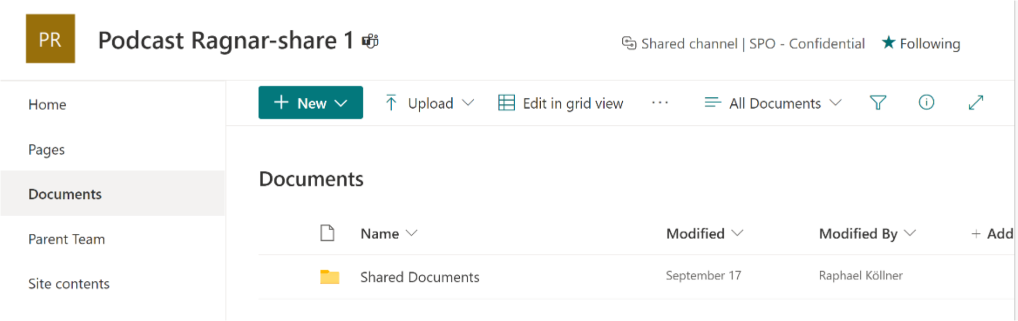
- ☐ B2B Collaboration-Gastbenutzer (Vorschau)
- ☐ B2B Collaboration-Mitgliederbenutzer (Vorschau)
- ☑ B2B Direct Connect-Benutzer (Vorschau)
- ☐ Lokale Gastbenutzer (Vorschau)
- ☐ Dienstanbieterbenutzer (Vorschau)
- ☐ Andere externe Benutzer (Vorschau)

In this way, CA scenarios can also be implemented with B2B direct users, one of the important points of including them in the ZeroTrust concept.

9.3. Information Protection

Microsoft Purview Information Protection also works for shared channels on the channel and also for the SharePoint Online site behind it, e.g. the default label for the document library. These all originate from the hosting tenant.

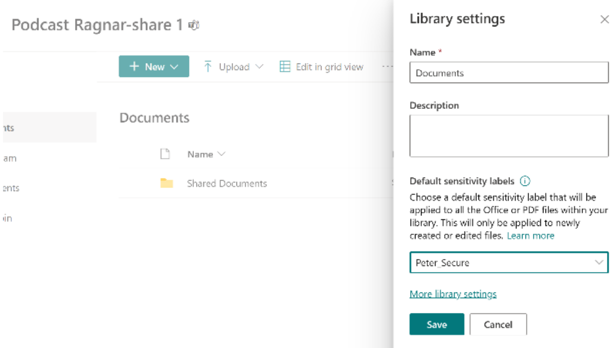
Container MIP Label



Name	Modified	Modified By
Shared Documents	September 17	Raphael Köllner

It is very interesting and also intentional that the labels work to also prevent B2B and B2B direct users from being invited and to enable a lifecycle.

Default library label



Library settings

Name *: Documents

Description

Default sensitivity labels

Choose a default sensitivity label that will be applied to all the Office or PDF files within your library. This will only be applied to newly created or edited files. Learn more

Peter_Secure

Here, as an example, the label "Peter Secure".

Unfortunately, currently the B2B direct users of the foreign tenant cannot yet be members of an email-enable security group or M365 Group to be included in the label. Microsoft is working on this.

MIP Auto labeling

Autolabeling also works for the document library of the shared channel. It was tested with Trainable Classifier and also with Sensitivity Informationtypes.

9.4. Data Life Cycle / Retention

In addition to the MIP labeling, the shared channel lifecycle is important. Unfortunately, the shared channel is not yet displayed in the retention policies.

Retention policies for chat	No
Retention Polcies for the SPO Site	Yes
Retention Label for Files and Items in the SPO Site	Yes

Currently the retention team is working on an extension to automatically delete the chat in the shared channels.

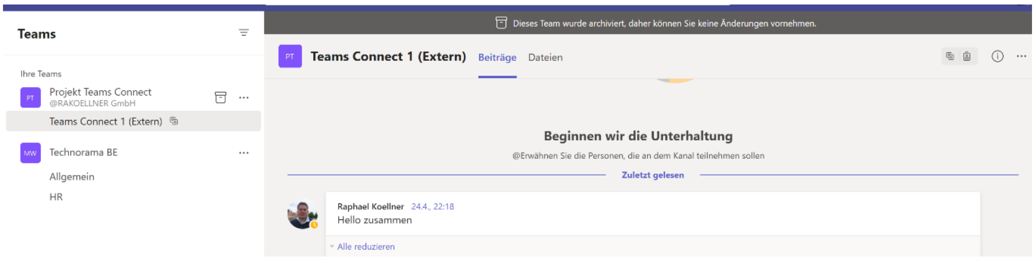
9.5. Archiving and autodelete

9.5.1. Autodelete

Currently, an autodelete for shared channels is not possible. However, the autodelete for the team also takes effect for shared channels, so that these are also removed.

9.5.2. Archiving

Microsoft Teams and therefore also the channels can be archived in the context of this also the shared channel is archived.



Dieses Team wurde archiviert, daher können Sie keine Änderungen vornehmen.

Beginnen wir die Unterhaltung

@Erwähnen Sie die Personen, die an dem Kanal teilnehmen sollen

Raphael Koellner 24.4., 22:18
Hello zusammen

Figure 17 View of an External B2B direct User in his Tenant of an Archived Channel

The users in the foreign tenant then no longer have access to the channel, or only view rights, depending on how you archive or even manually remove all users.

9.6. Information Barriers

Shared channels in Microsoft Teams create areas for collaboration where you can invite people who are not on the team. **Information barriers** are policies that can be implemented to prevent users and groups from communicating with each other inside and outside your organization.

Shared channels are in teams by default. You can choose whether people can create shared channels, whether they can share them with people outside your organization, and whether they can participate in external shared channels by creating a channel policy. If information barrier policies are configured in your organization, checks are run when shared channels are configured to verify that none of the existing channel members and any new users added to the shared channel violate information barrier policy conditions.

Use the following table to understand how information barrier policies can affect communications and result in certain behaviors when configuring shared channels:

Scenario	**Information barrier behavior**
Share a channel with a user in your organization	If the user is not allowed to communicate with member-shared channels per information barrier policy, the user will not appear in the user search and the channel will not be shared with the team. If the user cannot be added by information barrier policy, the following message is displayed: *No matches* were *displayed. Talk to your IT administrator to expand the search scope.*
Share a channel in your organization with another team you own	If the other team has users who are not allowed to communicate with members shared channels through an information barrier policy, the channel will not be shared with the team. If communications are not allowed due to an information barrier policy, the following message is displayed: The channel cannot be *shared with this team. Select another team or contact your administrator for more information.*
Share a channel in your organization with another team that you do not own	If the team owner or users of the other team are not allowed to communicate with other channel members through an information barrier policy, the channel cannot be shared with the team. If communications are not allowed due to an information barrier policy, the following message is displayed: The channel cannot be *shared with this team. Select another team or contact your administrator for more information.*
Adding a new user to the team when the team has shared channels with other teams	If the new user is not allowed to communicate with members of the shared channel team through an information barrier policy, the user cannot be added to the team. When you add a user to a team with six or more shared channels, the user is immediately added to the channel and sharing is supported. Sharing to the team and previously shared channels can be stopped if the new user is determined to be non-compliant with an information barrier policy. If the user cannot be added due to an information barrier policy, the following message is displayed: User cannot be *added* due to an information barrier policy.
Enabling a channel for an external team	Information barrier policies for internal and external clients do not restrict communication between users of the different clients. Shared channels can be shared with external users.

https://docs.microsoft.com/en-us/microsoftteams/information-barriers-shared-channels

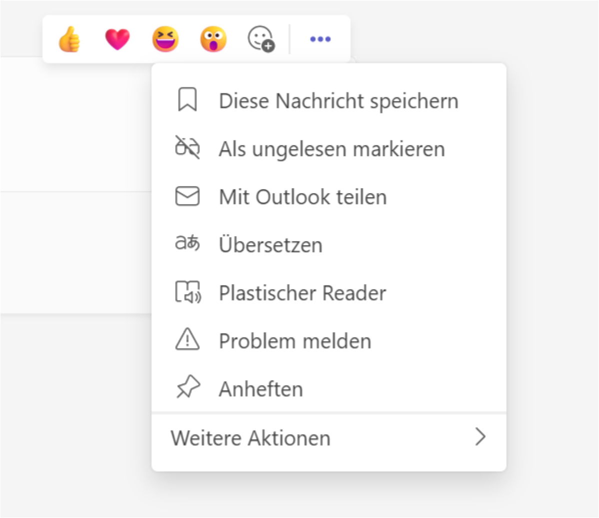
9.7. eDiscovery

eDiscovery and channels in Microsoft Teams has always been an exciting topic, as private channels also appeared quite late in eDiscovery. Initially this was only possible in eDiscovery Advanced and this is now the same for shared channels. Current tests from November show that the chats and data are showing up, but initially only in the Premium Cases. At least you can use eDiscovery for now.

9.8. Communication Compliance / Insider Risk Management

Both Communication Compliance and Insider Risk Management will impact shared channels from December 2022.

Example of reporting a problem from Communication Compliance



9.9. Monitoring and Surveillance / PowerShell

Monitoring is currently possible manually via PowerShell or in the UI, or in the AAD portal. Conditional Access is currently in Public Preview (9.2) and so slowly probably also the B2B direct object will come into the hosting tenant, initially for monitoring.Aut

PowerShell Reporting

I like to refer to my MVP colleague and his report script. This works wonderfully and shows at least some information.

Use the Get-AssociatedTeam Cmdlet to Report Teams Members (office365itpros.com)

AuditLogs

- No audit logs are currently available for B2B direct users.

10.Organizational measures

10.1. Training of employees and externals

Training is a popular means for companies to fulfill a TOM and to explain the framework of use to their employees. In addition to live training sessions in person or via Microsoft Teams, on-demand training is also available in Microsoft Stream, and this training is also available as an option for external participants.

Mandatory content must be:

(1) Architecture
(2) Usage scenarios (permitted/not permitted)
(3) Process and responsibility of the plant and management
(4) Risks
(5) Data protection and compliance
(6) Questions and answers

10.2. Community / Early Adopter

In addition to the training, it is worth creating an internal community that already exists optimally. The champions/early adopters should contribute the topic to this community and thus serve as supporters in addition to 1st level support and IT.

10.3. Privacy

The topic of data protection is extremely important in the area of shared channels, especially with the B2B direct identities that have now been brought along. The processing of the B2B direct identities now also takes place in the own tenant.

For a complete list, see section 10.3.3.

10.3.1. Update Privacy Policy Art 13 DSGVO

In the context of the use of shared channels, it is mandatory to expand the privacy policy and add a point shared channels. This has to do with the fact that a new interface and a new user format is added and data flows differently than usual.

See appendix of this document under 11.2.

10.3.2. Updating the processing directory Art. 30 GDPR

It is possible to create a new processing or to add to the already existing entries for processing. In addition, there is a new interface and, depending on the foreign tenant, a transfer to the USA.

10.3.3. Update data protection impact assessment Art. 35/36 DSGVO

It is mandatory to update the DSFA before using shared channels. There are also some points or attachments/paperwork in the DSFA:

Paperwork

- Processing
- Extinguishing and blocking concept
- Authorization concept
- Review of a Transfer Impact Assessment (TIA).
  - Especially if the foreign tenant is located in the USA or China, for example.

Update points in the DSFA

- ➢ Risk factors shared channels
  - Examples
    - Data outflow
    - Obstruction of the exercise of data subject rights
    - Financial losses

10.4. User agreement

The user agreement must clarify how the shared channels are to be used.

11. Appendix

11.1. General checklist and checklist for the introduction of Microsoft Teams Connect

This is an excerpt from the test catalog:

ID	Checkpoint	Result
1	Confidentiality agreement in place	
2		
3		
4		
5		
6		

11.2. Compliance checklist for setting up B2B direct with another (third-party) tenant

This is an excerpt from the test catalog:

ID	**Checkpoint**	**Result**
1	Tenant Region	
2	Multi-tenant in use	
3	AD hybrid join method and configuration	
4	Compliance settings for the device	
5	Teams TAP or Preview in use	
6	MFA method and configuration	

11.3. Compliance checklist for users:inside my organization who are invited to other tenants

11.4. Privacy policy excerpt sample supplement

Microsoft Teams section

Shared Channel

They can also work together with us in our tenant with shared channels. This way, they bring their own identity of their Microsoft environment. We only receive the following data:

- First name and last name
- UPN
- E-mail address
- Company
- Hybrid join of the terminal
- Compliance status of the end device
- Multi-factor setting
- Image / Person

Your data will be processed in our environment in the Germany central region (Frankfurt).

11.5. VVT sample (supplement/extract)

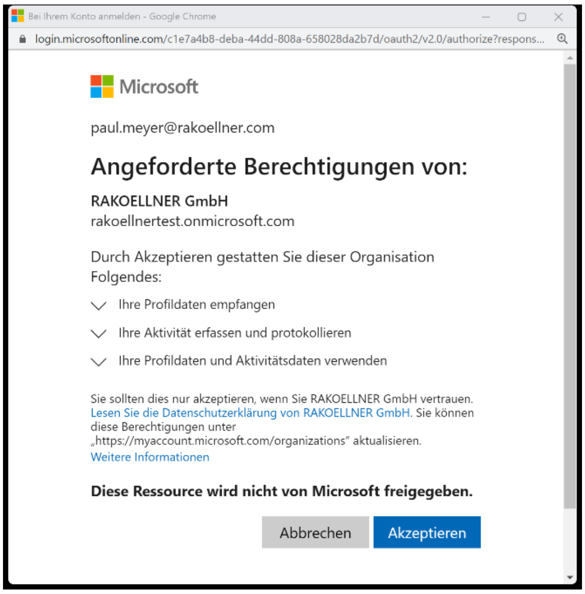
Purpose	**Personal data / categories**	**Protection level**	**Legal basis**	**Deletion reason**	**Deletion period**
Collaboration within the framework of the modern workplace in Microsoft Teams.	➢ First name and last name ➢ UPN ➢ E-mail address ➢ Compliance status of the end device ➢ Multi-factor setting ➢ Image / Person	Level B No Art. 9, 10 GDPR data	**Employees:** Art. 6 para. 1 lit. b DSGVO, in conjunction with. § 26 BDSG (if applicable BV) **External** (depending on) Art. 6. para. 1 lit. b / lit. f) lit. a) DSGVO	Manual deletion after end of purpose Automatic deletion with end of team	End of purpose Audit logs 30 days

Responsible	**Representative of the responsible**	**Measures**	**Recipient of the data**	**Persons authorized to access**	**Information requirements**
➢		➢ Compliance status of	➢ Stranger Tenant:	➢ AAD Group	DSE available at: XXX

		the device ➢ Hybrid Join ➢ Purview Information Protection ➢ Conditional Access ➢ Purview Data Lifecycle Access protection ➢ MFA ➢ User and password	Company Contact Mail ➢ Phone number	➢ Foreign tenant: AAD Group	

11.6. Message in screenshot with MFA

User gets first time invitation for external team via B2B Direct



Bei Ihrem Konto anmelden - Google Chrome

login.microsoftonline.com/c1e7a4b8-deba-44dd-808a-658028da2b7d/oauth2/v2.0/authorize?respons...

Microsoft

paul.meyer@rakoellner.com

Angeforderte Berechtigungen von:

RAKOELLNER GmbH
rakoellnertest.onmicrosoft.com

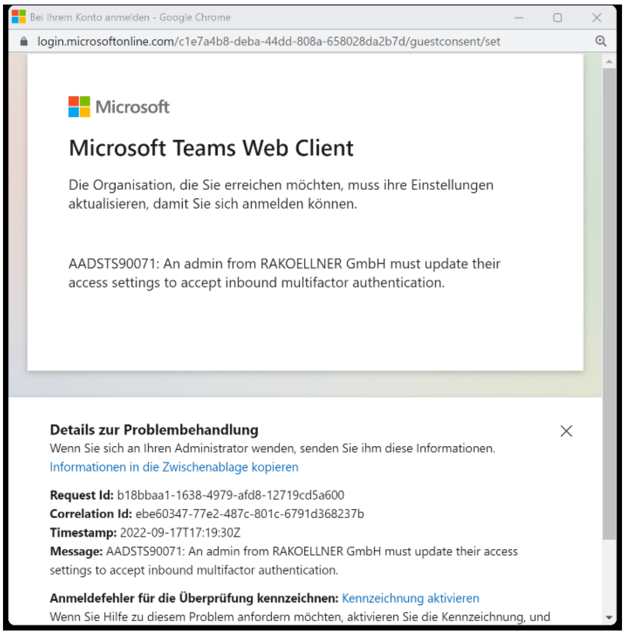
Durch Akzeptieren gestatten Sie dieser Organisation Folgendes:

- Ihre Profildaten empfangen
- Ihre Aktivität erfassen und protokollieren
- Ihre Profildaten und Aktivitätsdaten verwenden

Sie sollten dies nur akzeptieren, wenn Sie RAKOELLNER GmbH vertrauen. Lesen Sie die Datenschutzerklärung von RAKOELLNER GmbH. Sie können diese Berechtigungen unter „https://myaccount.microsoft.com/organizations" aktualisieren.
Weitere Informationen

Diese Ressource wird nicht von Microsoft freigegeben.

Error, since MFA is missing



Bei Ihrem Konto anmelden - Google Chrome

login.microsoftonline.com/c1e7a4b8-deba-44dd-808a-658028da2b7d/guestconsent/set

Microsoft

Microsoft Teams Web Client

Die Organisation, die Sie erreichen möchten, muss ihre Einstellungen aktualisieren, damit Sie sich anmelden können.

AADSTS90071: An admin from RAKOELLNER GmbH must update their access settings to accept inbound multifactor authentication.

Details zur Problembehandlung

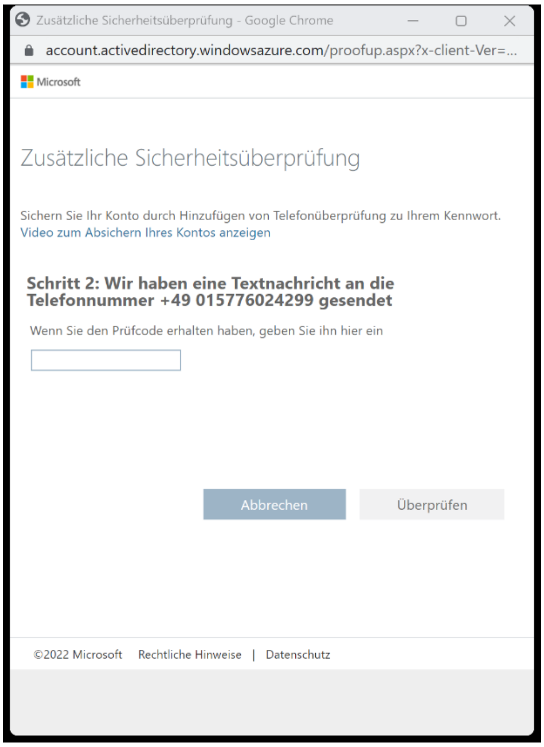
Wenn Sie sich an Ihren Administrator wenden, senden Sie ihm diese Informationen.
Informationen in die Zwischenablage kopieren

Request Id: b18bbaa1-1638-4979-afd8-12719cd5a600
Correlation Id: ebe60347-77e2-487c-801c-6791d368237b
Timestamp: 2022-09-17T17:19:30Z
Message: AADSTS90071: An admin from RAKOELLNER GmbH must update their access settings to accept inbound multifactor authentication.

Anmeldefehler für die Überprüfung kennzeichnen: Kennzeichnung aktivieren
Wenn Sie Hilfe zu diesem Problem anfordern möchten, aktivieren Sie die Kennzeichnung, und

Solution: MFA must be activated in the target tenant, i.e. that the MFA is trusted.

If it is enabled, then:



Zusätzliche Sicherheitsüberprüfung - Google Chrome
account.activedirectory.windowsazure.com/proofup.aspx?x-client-Ver=...
Microsoft

Zusätzliche Sicherheitsüberprüfung

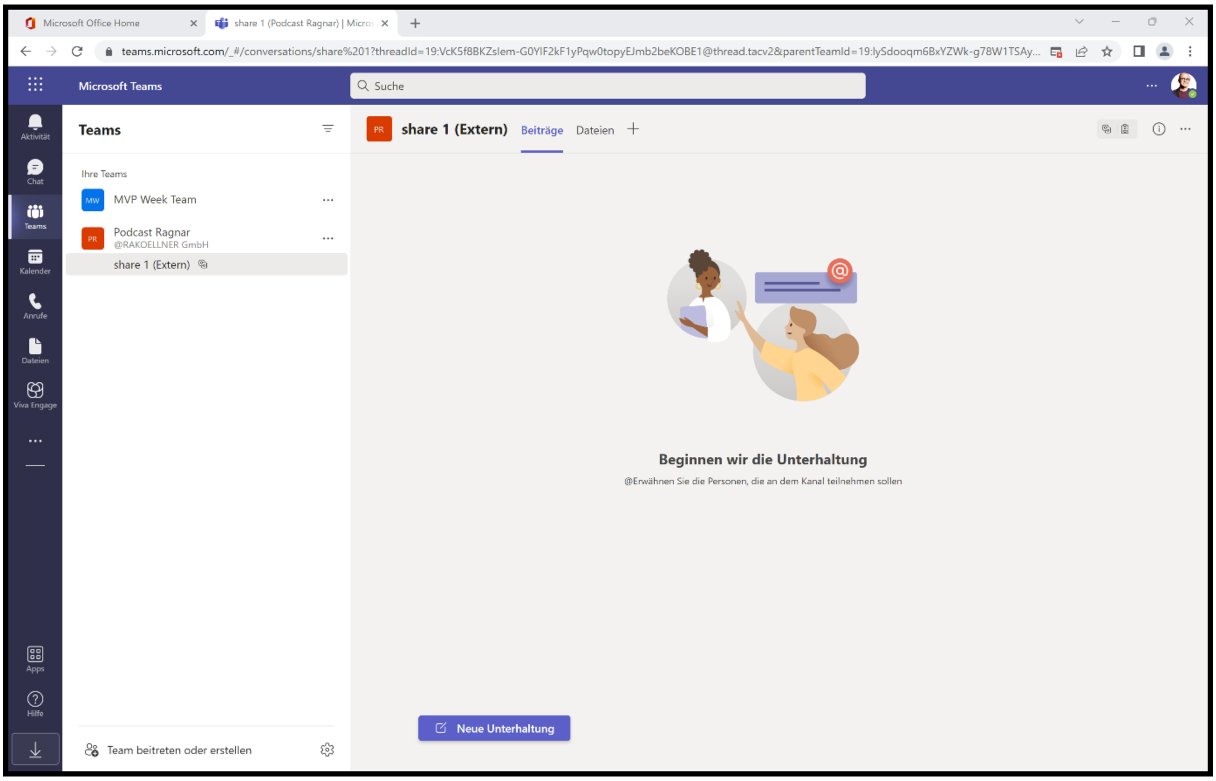
Sichern Sie Ihr Konto durch Hinzufügen von Telefonüberprüfung zu Ihrem Kennwort.
Video zum Absichern Ihres Kontos anzeigen

Schritt 2: Wir haben eine Textnachricht an die Telefonnummer +49 015776024299 gesendet

Wenn Sie den Prüfcode erhalten haben, geben Sie ihn hier ein

Abbrechen
Überprüfen
©2022 Microsoft
Rechtliche Hinweise | Datenschutz

Then the external can write in the channel:

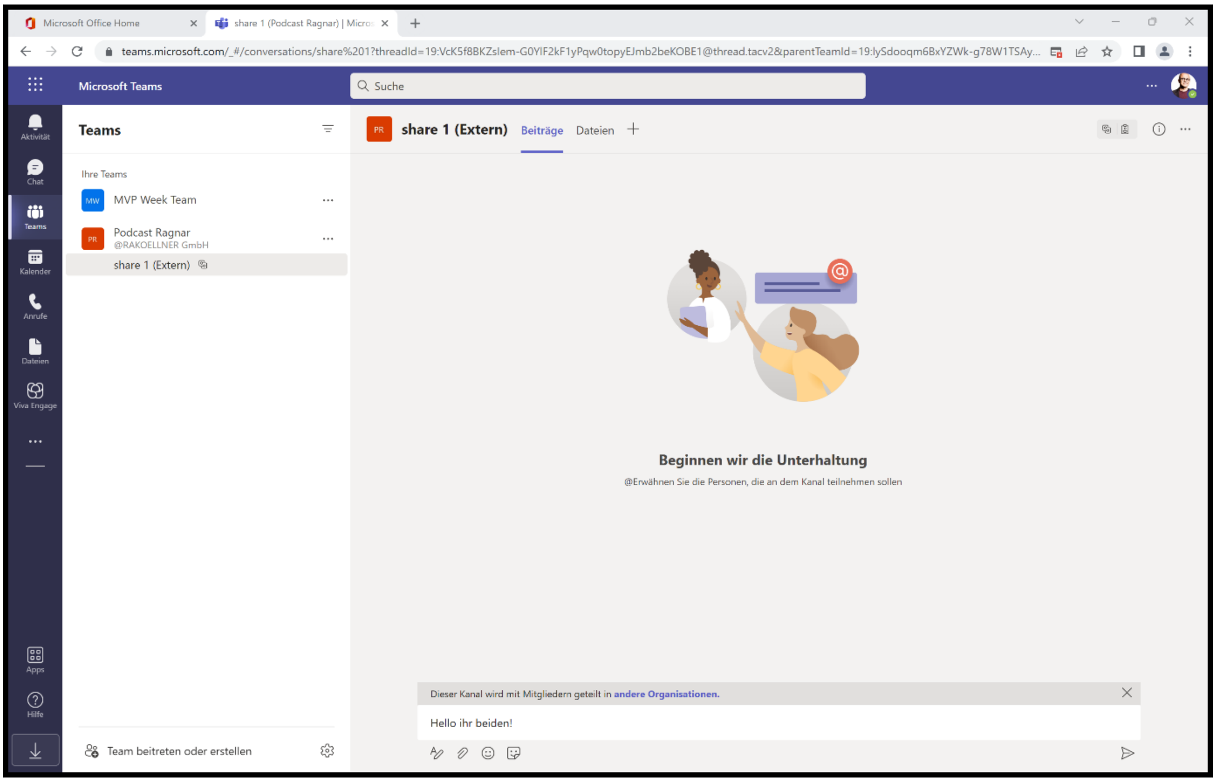


Microsoft Office Home
share 1 (Podcast Ragnar) | Micros
teams.microsoft.com/_#/conversations/share%201?threadId=19:VcK5f8BKZslem-G0YIF2kF1yPqw0topyEJmb2beKOBE1@thread.tacv2&parentTeamId=19:lySdooqm6BxYZWk-g78W1TSAy...
Microsoft Teams
Suche
Aktivität
Chat
Teams
Kalender
Anrufe
Dateien
Viva Engage
Apps
Hilfe
Teams
Ihre Teams
MW
MVP Week Team
PR
Podcast Ragnar
@RAKOELLNER GmbH
share 1 (Extern)
Team beitreten oder erstellen
PR
share 1 (Extern)
Beiträge
Dateien

Beginnen wir die Unterhaltung

@Erwähnen Sie die Personen, die an dem Kanal teilnehmen sollen

11.7. Screenshots work in shared channel in own team


Microsoft Office Home
share 1 (Podcast Ragnar) | Micro
teams.microsoft.com/_#/conversations/share%201?threadId=19:VcK5f8BKZslem-G0YlF2kF1yPqw0topyEJmb2beKOBE1@thread.tacv2&parentTeamId=19:lySdooqm6BxYZWk-g78W1TSAy...
Microsoft Teams
Suche
Aktivität
Chat
Teams
Kalender
Anrufe
Dateien
Viva Engage
Apps
Hilfe
Teams
Ihre Teams
MVP Week Team
Podcast Ragnar
@RAKOELLNER GmbH
share 1 (Extern)
Team beitreten oder erstellen
share 1 (Extern)
Beiträge
Dateien

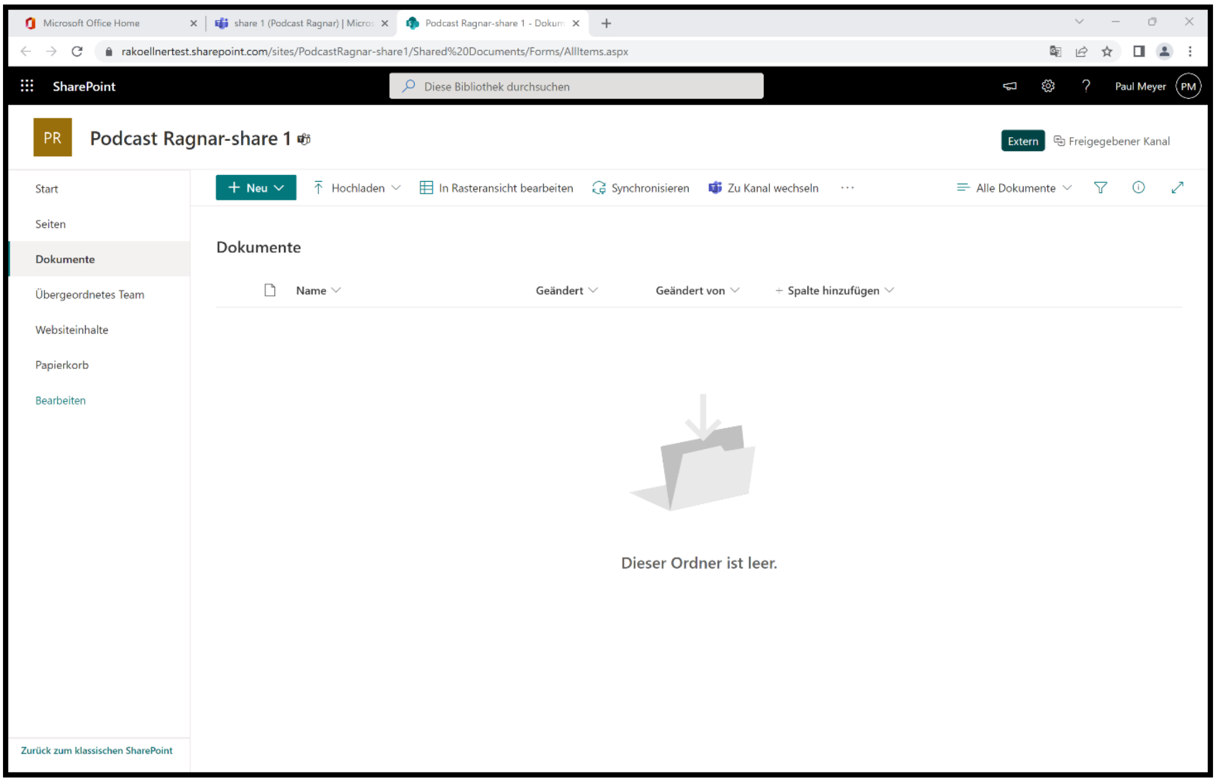
Beginnen wir die Unterhaltung

@Erwähnen Sie die Personen, die an dem Kanal teilnehmen sollen

Dieser Kanal wird mit Mitgliedern geteilt in **andere Organisationen.**

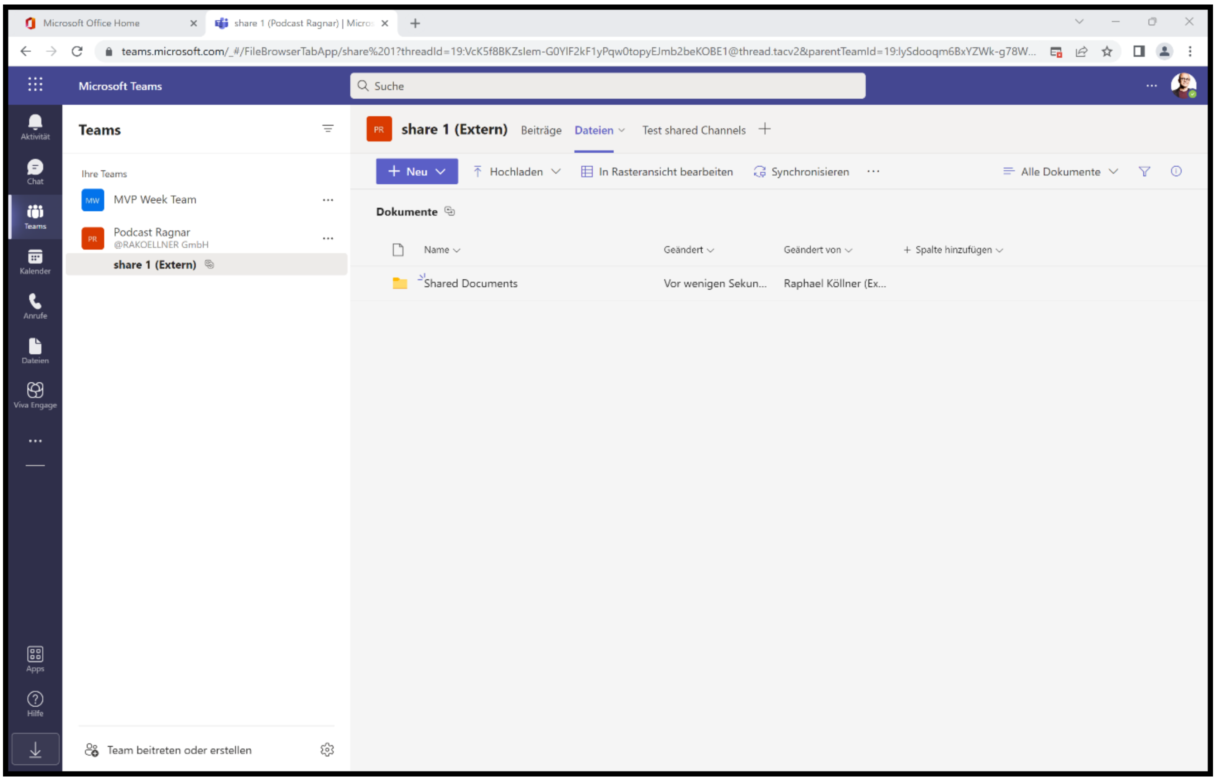
Hello ihr beiden!

SharePoint view of the external



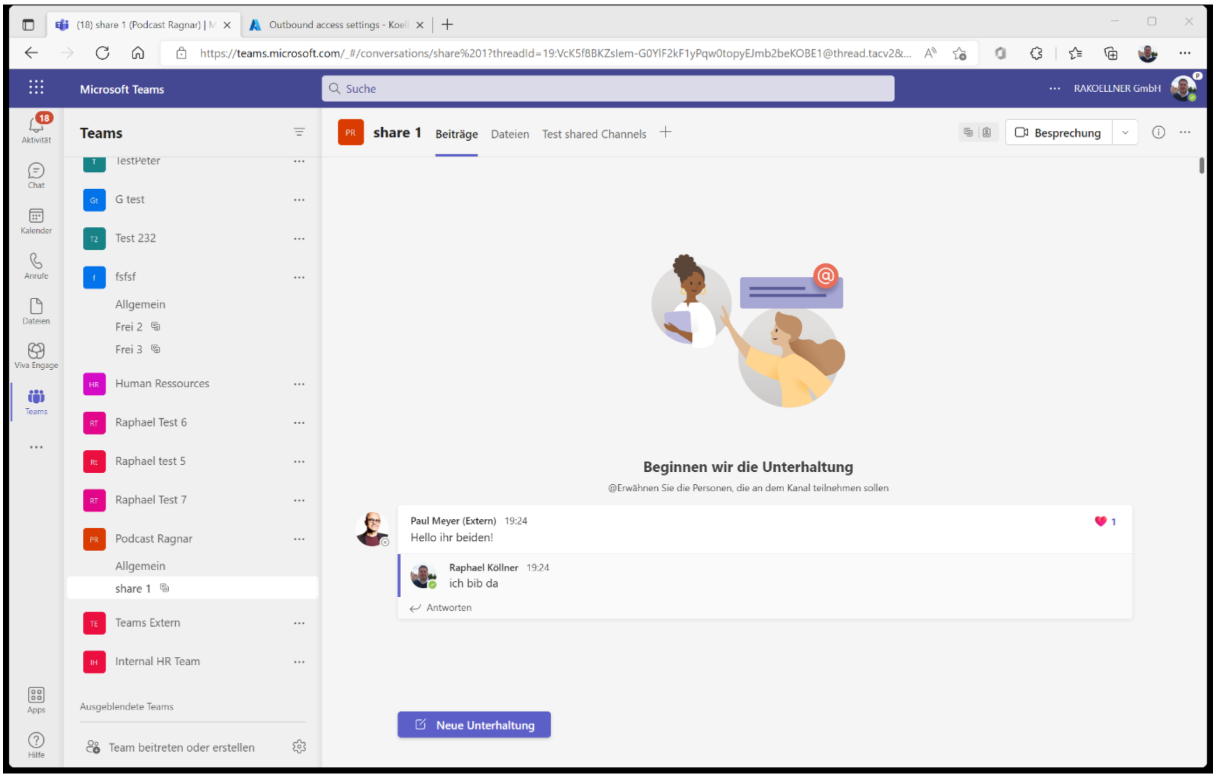
Dieser Ordner ist leer.

Creation of a OneNote folder by the user in his own tenant and view of the external one



Name	Geändert	Geändert von
Shared Documents	Vor wenigen Sekun...	Raphael Köllner (Ex...

View of the user in his own tenant



Paul Meyer (Extern) 19:24
Hello ihr beiden!

Raphael Köllner 19:24
ich bib da

11.8. Link list

11.8.1. Blogpost

Microsoft Teams Connect shared channels is rolling out to public preview - Microsoft Tech Community

https://techcommunity.microsoft.com/t5/microsoft-teams-community-blog/teams-connect-with-your-partners-get-to-know-the-azure-ad-config/ba-p/3267140

https://techcommunity.microsoft.com/t5/microsoft-teams-blog/microsoft-teams-connect-shared-channels-is-rolling-out-to-public/ba-p/3252901?msclkid=66413e22b05611eca8e7bc0fc3457d9a

11.8.2. User

- **Create a shared channel in Teams**
- **Share a channel with people in Teams**
- **Share a channel with a team**
- **Why use a shared channel versus other channel types in Teams?**
- **Guests and shared channels in teams**
- **Shared channel owner and member roles in teams**

11.8.3. Administrators

- **Shared channels in Microsoft Teams (Preview) - Microsoft Teams | Microsoft Docs**
- **Collaborate with external participants in a channel | Microsoft Docs**
- **B2B direct connect overview - Azure AD | Microsoft Docs**
- **Configure B2B collaboration cross-tenant access - Azure AD | Microsoft Docs**
- **Teams and SharePoint integration - SharePoint in Microsoft 365 | Microsoft Docs**
- **Sharing & permissions in the SharePoint modern experience - SharePoint in Microsoft 365 | Microsoft Doc**
- **Get context for your tab - Teams | Microsoft Docs**
- **Teams workflow in Advanced eDiscovery - Microsoft 365 Compliance | Microsoft Docs**
- **Search the audit log for events in Microsoft Teams - Microsoft Teams | Microsoft Docs**
- **Information barriers and shared channels (preview) - Microsoft Teams | Microsoft Docs**
- **Search | Microsoft Docs**
- Created Shared Channel: **https://support.microsoft.com/office/80712457-579e-42b2-b54f-112329578aaa**
- Shared Channel: **https://support.microsoft.com/office/5f60de2d-0080-4e55-b26f-33a9dafa120e**
- Share Channel with Team: **https://support.microsoft.com/office/b2e89992-2708-4583-b11e-bbb6edb4f1c3**

- Why used a shared channel: **https://support.microsoft.com/office/e6ad61d0-6b3f-4e1b-baac-63e2978bd92e**
- Member / Roles: **https://support.microsoft.com/office/75b379f4-8e9c-4202-acf1-6ffc3878a2d7**