TeamsCommunityDay

Microsoft Teams Community Conference

teamscommunityday.de

@TeamsDay

#TeamsCommunityDay 2022

TEAMS COMMUNITY DAY since 2017

28. Januar 2022

Microsoft Teams content by our Teamsheroes

Berlin, Bochum, Bremen, Darmstadt, Dresden, Emden, Finnland, Graz, Hamburg, Hannover, Heilbronn, Karlsruhe, Köln, Lüdinghausen, Lingen, Madrid, München, Münster, Nürnberg, OWL, Saarbrücken, Trier, Wien

Registration.teamscommunityday.de

teamscommunityday.de | @TeamsDay

Central sponsors

COMMUNARDO INTELLITY VALPROVIA IN2SUCCESS NiCE

Powell Software noovic ScriptRunner Jabra GN SOLUTIONS 2SHARE

Microsoft 365 Tenant Checklist

Frank Carius

Kurzvorstellung

- Net at Work GmbH
  - Standort Paderborn
  - Gegründet 1995
  - 125+ Mitarbeiter
  - IT-Systemintegration und Software Development
- Schwerpunkte
  - UC: Exchange, Skype for Business, Teams
  - SharePoint, Office 365, Microsoft 365
  - Infrastruktur: AD, ADFS, ADSync, Netzwerk
  - Security: Mail Encryption und Signierung, NoSpamProxy
- Frank Carius
  - Microsoft MVP für Office Server Systems
  - Microsoft Certified Master Lync 2010
  - Betreiber von www.msxfaq.de

Net at Work
Building IT-Excellence.

Microsoft Solutions Partner
Modern Work
Specialist
Adoption and Change Management
Calling for Microsoft Teams
Teamwork Deployment

noSpamproxy®

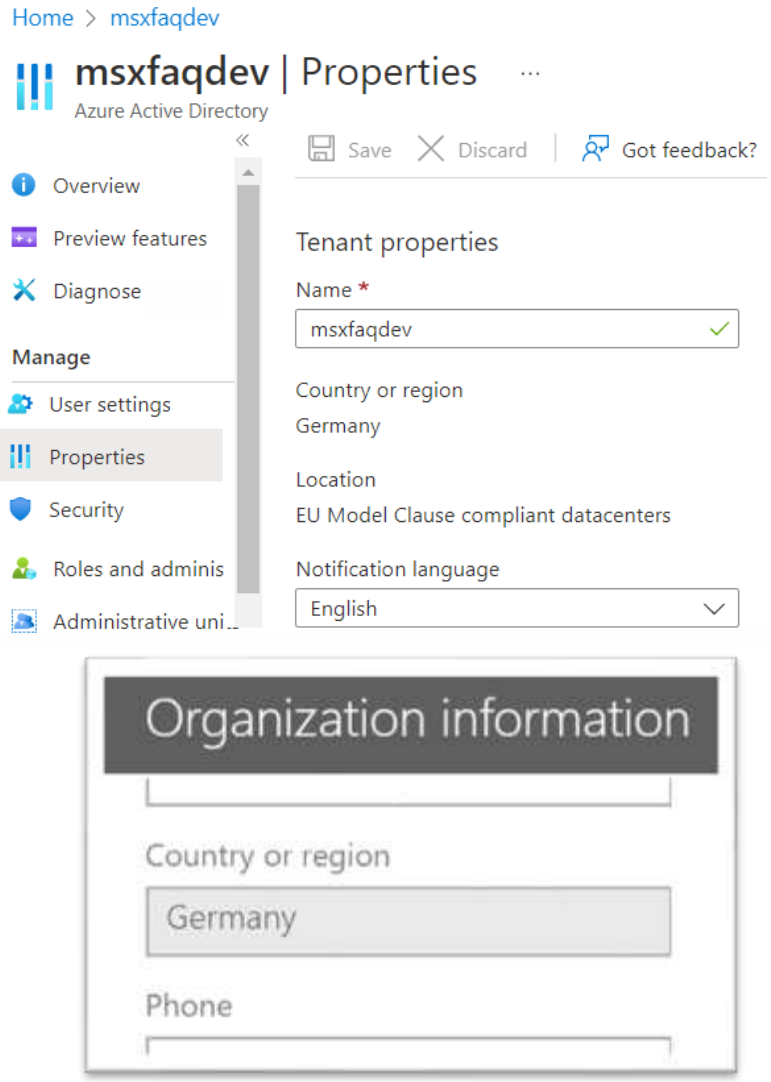
Microsoft CERTIFIED Master

MVP Microsoft® Most Valuable Professional

www.msxfaq.de

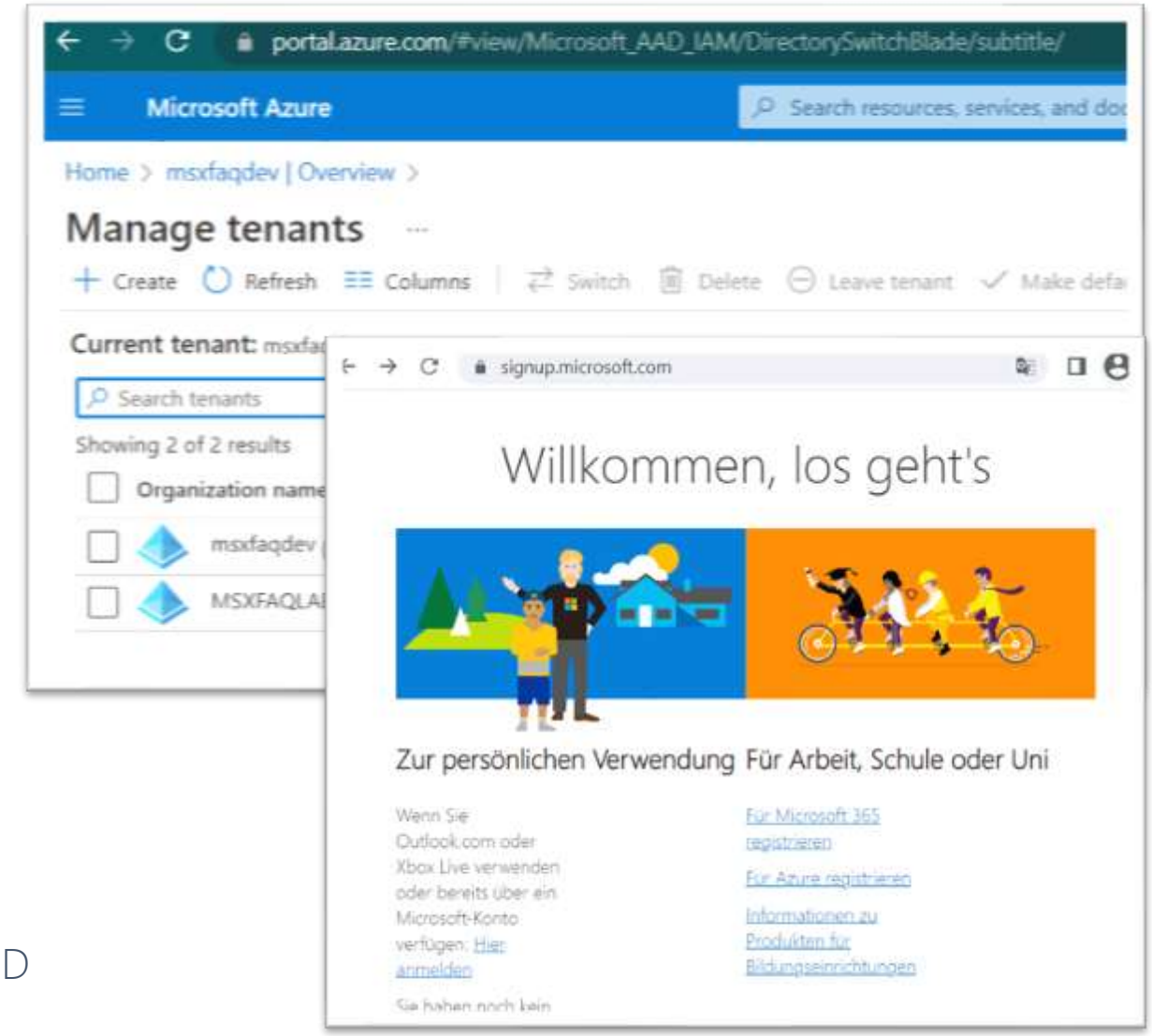
Name, Sponsor, Region

- Bedeutung des Namens
  - SharePoint-URL <tenantname>.sharepoint.com
  - OneDrive-URL <tenantname-my>.sharepoint.com
  - Noch einige andere Admin-Portale (immer weniger)
  - Ist der Name noch frei? (DNS, OAUTH)
- Sponsor
  - Keine Lizenz -> Daten nach 30-90 Tagen gelöscht
  - Lizenzierung, Beschaffung, Bezahlung überwachen!
- Sprache und Region
  - Region = Rechnungsadresse (Umsatzsteuer!) Nicht änderbar
  - UsageLocation: für Lizenz-Zuweisung
  - Sprache: pro Benutzer einstellbar
  - Preferred Data Location: Datenspeicherung, MultiGeo-Option



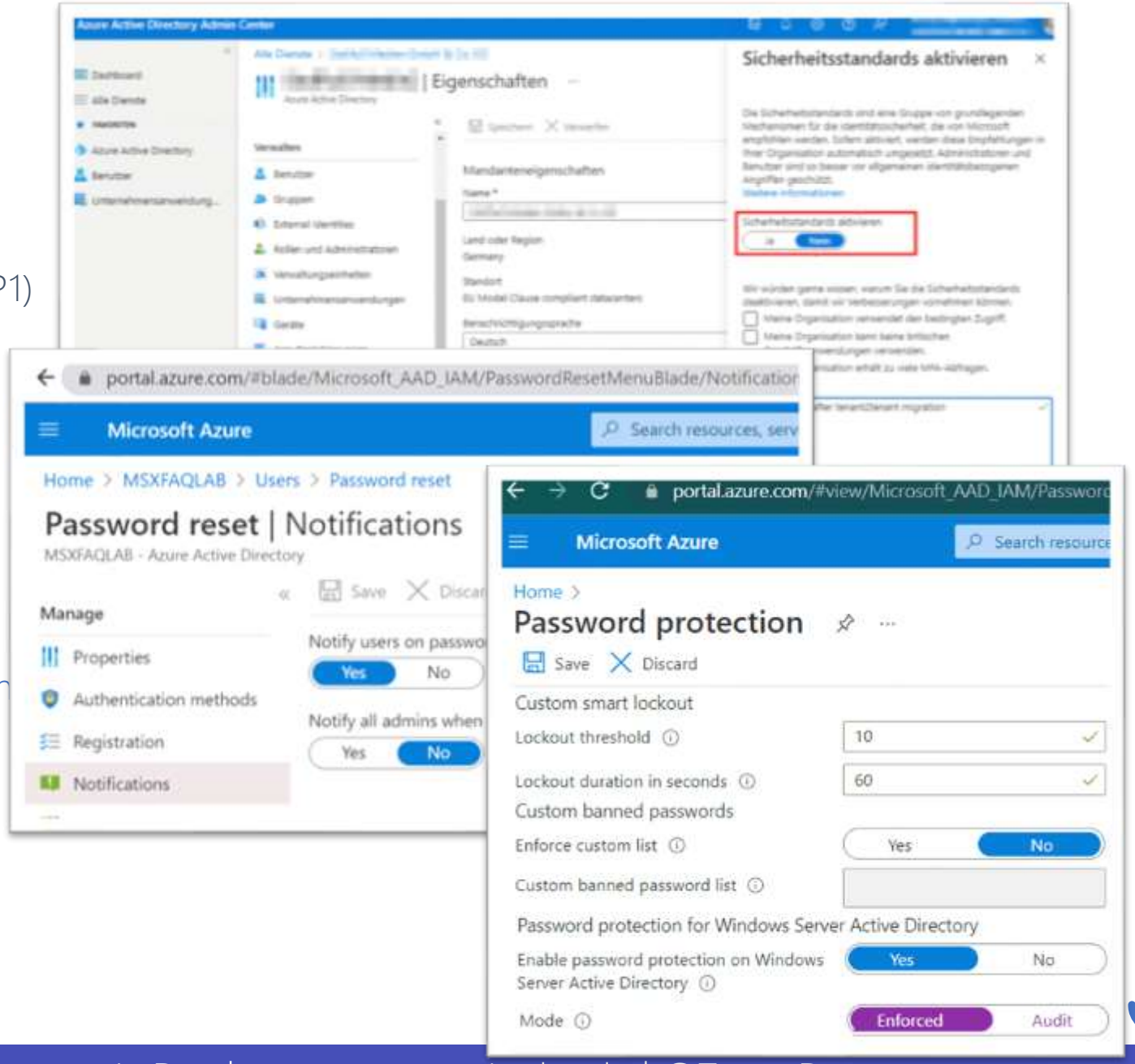
Tenant beantragen

- Wenn Anwender schneller sind
  - Viraler Tenant (PowerBI)
    Admin-Takeover oder Migration
  - Demo/Lab-Tenant
- So starte ich
  - MS-Trial https://signup.microsoft.com/
  - Über Partner (Azure/CSP o.ä.)
- Eigenschaften
  - „Schöner Name“
  - Technischer Ansprechpartner
  - Billing Admin
  - Teams Upgrade blocken
- Hinter einem Tenant steht immer ein AzureAD

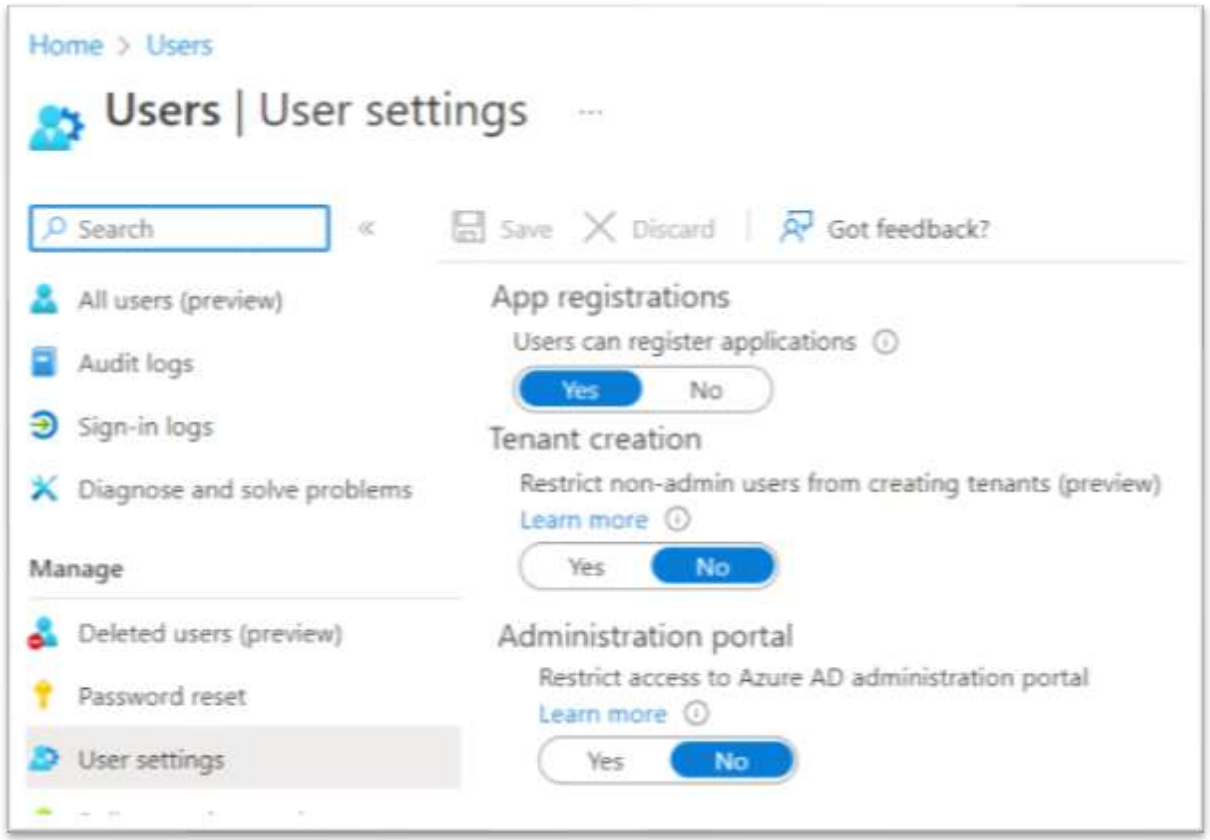


Admin-Konten

- Default: „Security Default“
  - Blockiert SMTP AUTH!
- Optional: Conditional Access (Azure AD P1)
- Admin-Konten
  - Einer ist zu wenig, weniger ist mehr
  - MFA sollte Pflicht sein
  - Ausnahme „Breaking glass admin“
  - DAG/GDAP/PartnerAdmin
  - Später: PIM (Azure AD P2)
  - „Named Admin“ vs „anonymous Admin
  - CloudOnly vs. Dirsync Admin
- Kennwortrichtlinien
  - Default nur für Cloud-Konten,
  - Keine ADSync-Konten



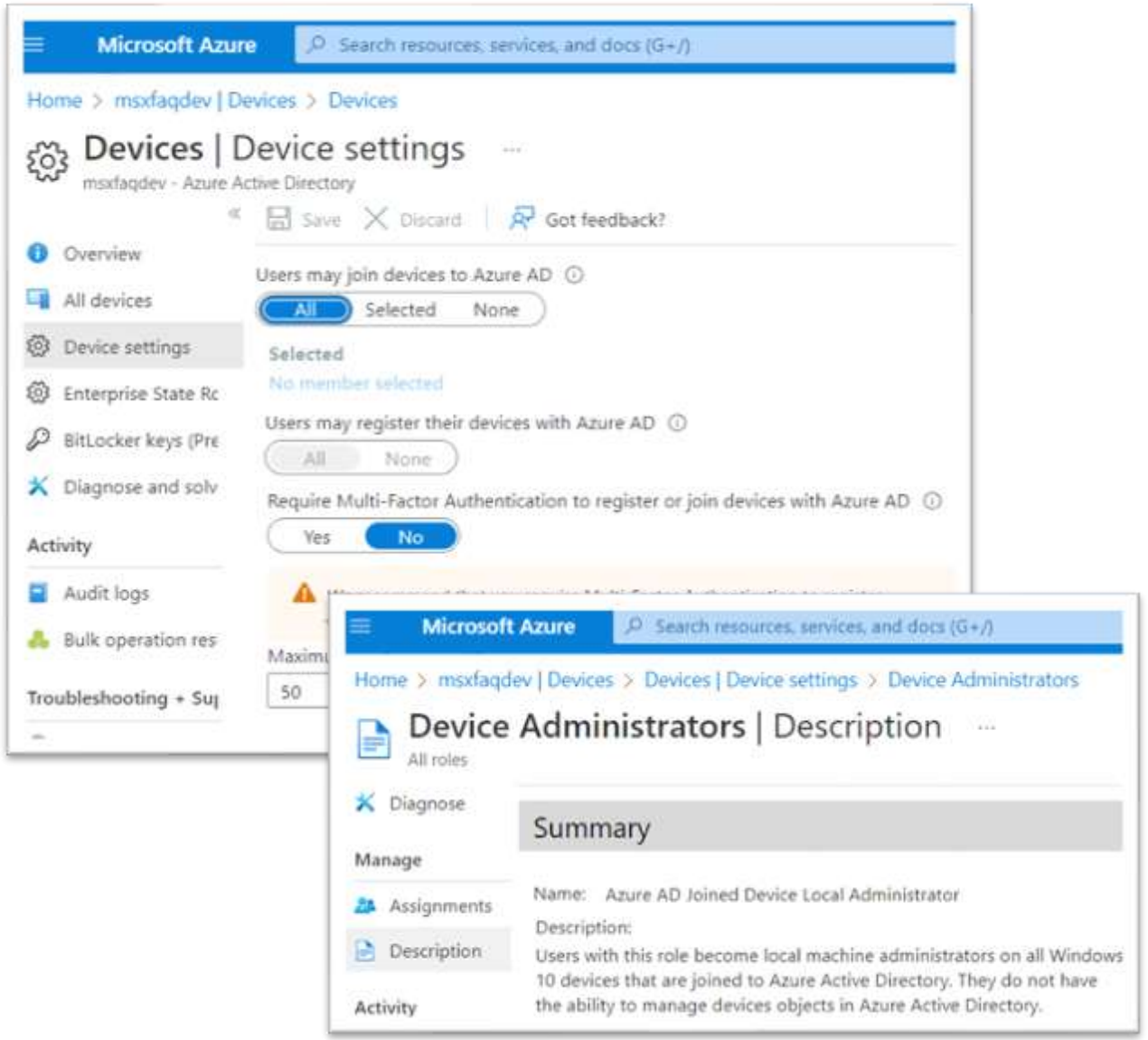
Benutzer beschränken



- Wer darf Apps registrieren?
  - Default Alle
  - Ihre Wahl: _____
- Wer darf Tenants anlegen?
  - Default Alle
  - Ihre Wahl: _____
- Wer darf auf http://portal.azure.com?
  - Default Alle

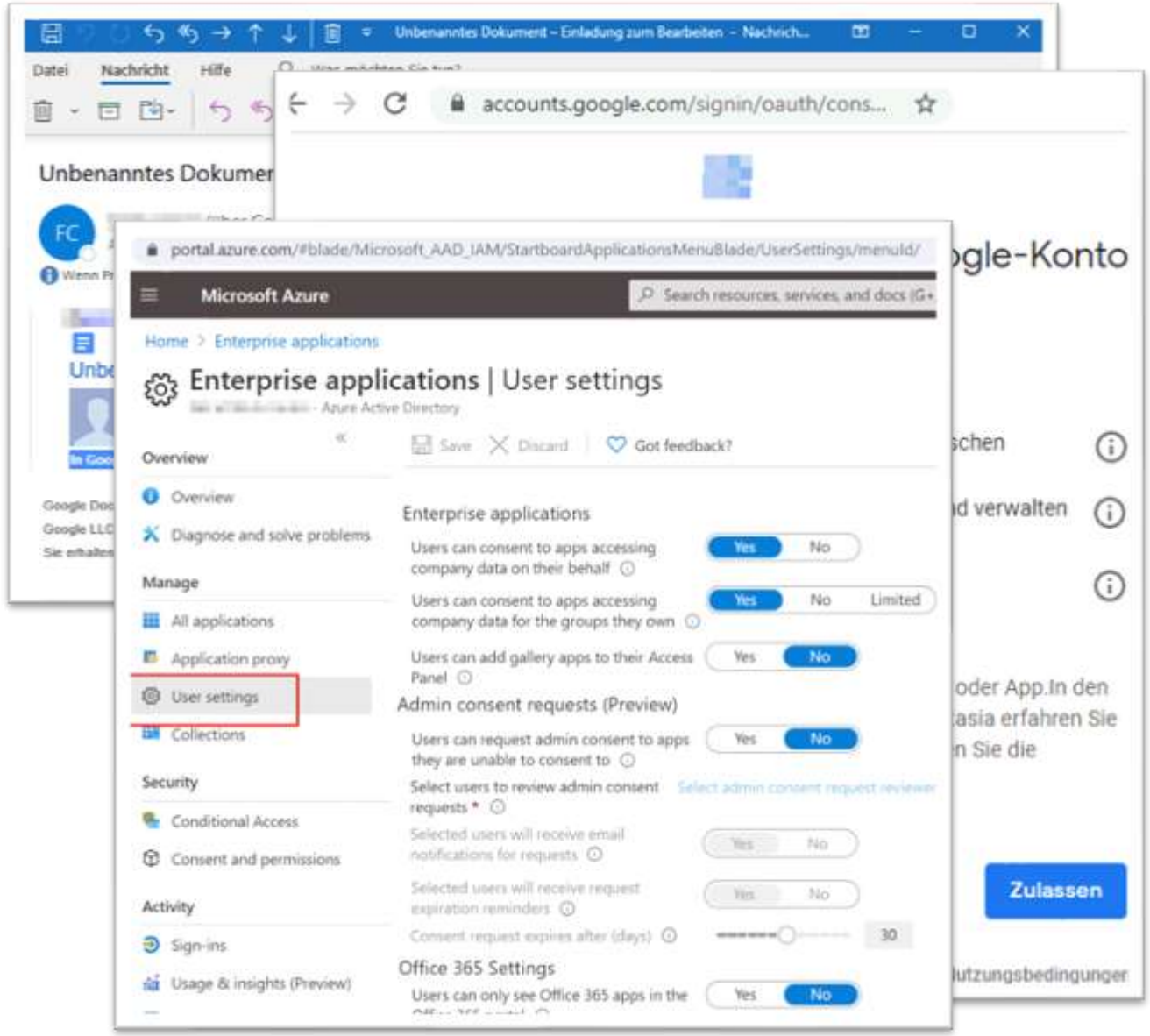
Computerkonten

- Lokales AD
  - Benutzer kann bis zu 10 Geräte addieren
- AzureAD
  - Benutzer kann bis zu 50! Geräte addieren
- Empfehlung
  - Niemand addiert Geräte selbst
- Device Konzept erstellen
  - HybridJoined
  - AzureAD Joined
  - AzureAD Registered
  - Unknown
- Lokaler Admin für AzureAD Joined Devices



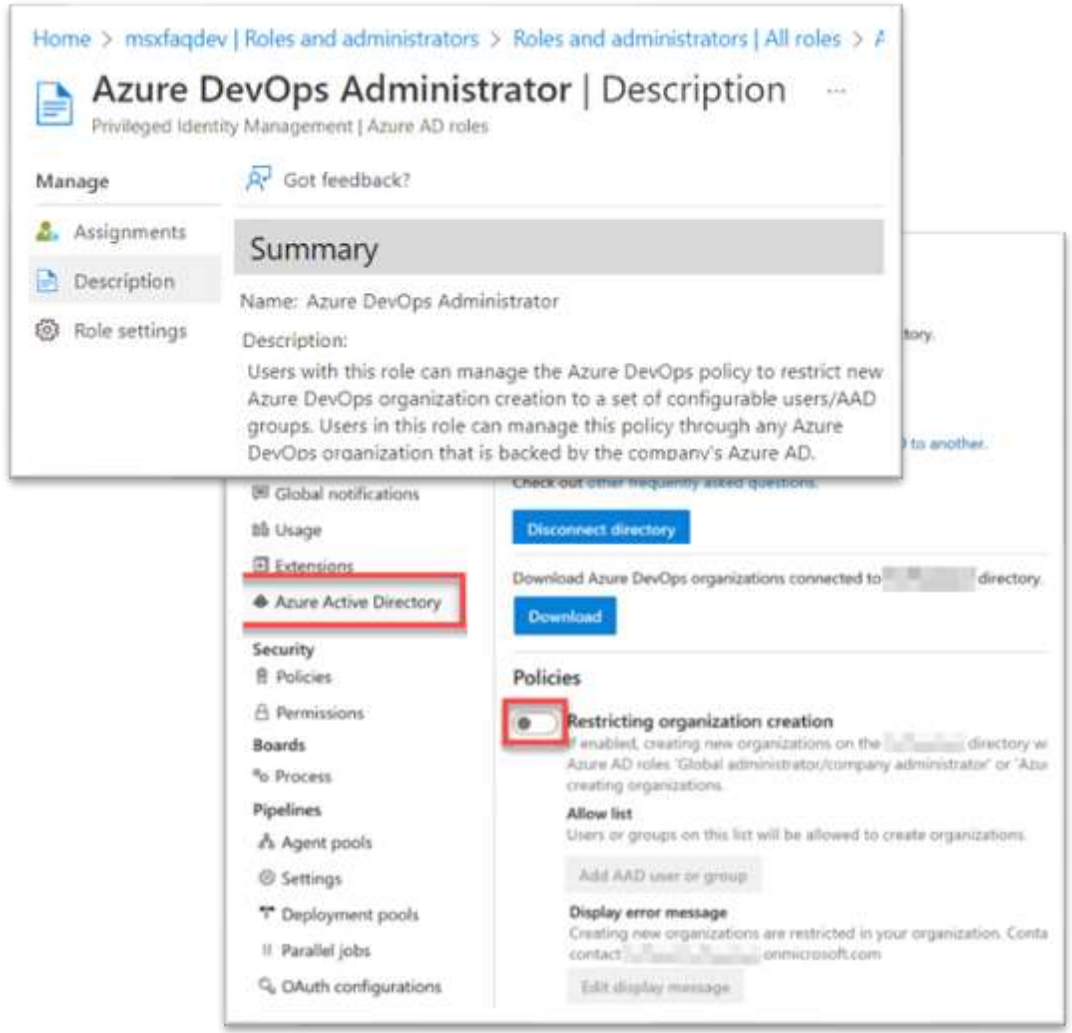
„Consent“

- Modern Auth erfordert
  - Username
  - Kennwort
  - App-Identifikation
  - …
- Application?
  - Microsoft vordefiniert
  - 3rd Party vordefiniert
  - selbst bereitgestellt
  - Definiert „Berechtigungen“
- Berechtigungen
  - Delegated (im Auftrag des Users)
  - App-Permission (durch Admin)
- Risiko
  - App fordert zu viele Rechte
  - Benutzer starten „fremde“ Apps



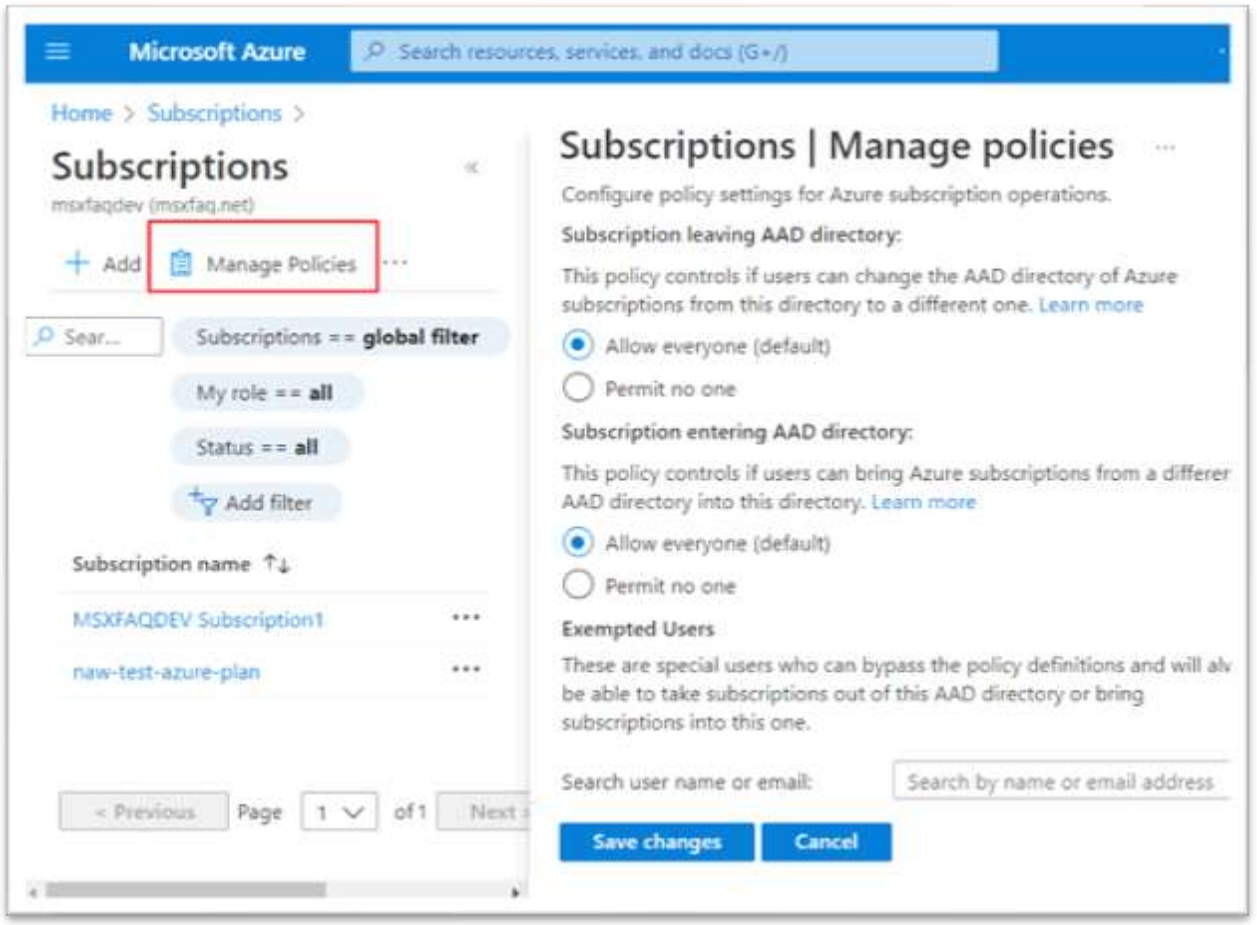
DevOps absichern

- Was ist Devops?
  - Sourcecode Verwaltung wie Git
  - Planungswerkzeuge
  - https://dev.azure.com/
  - U.a.
  - Vieles ist Kostenfrei!
  - Jeder User kann ein Devops anlegen
  - Devops ist mit einem AzureAD verbunden
- Wer darf DevOps verbinden?
  - Default Jeder!
- Wer DevOps Orgs anlegen
  - Default Jeder!

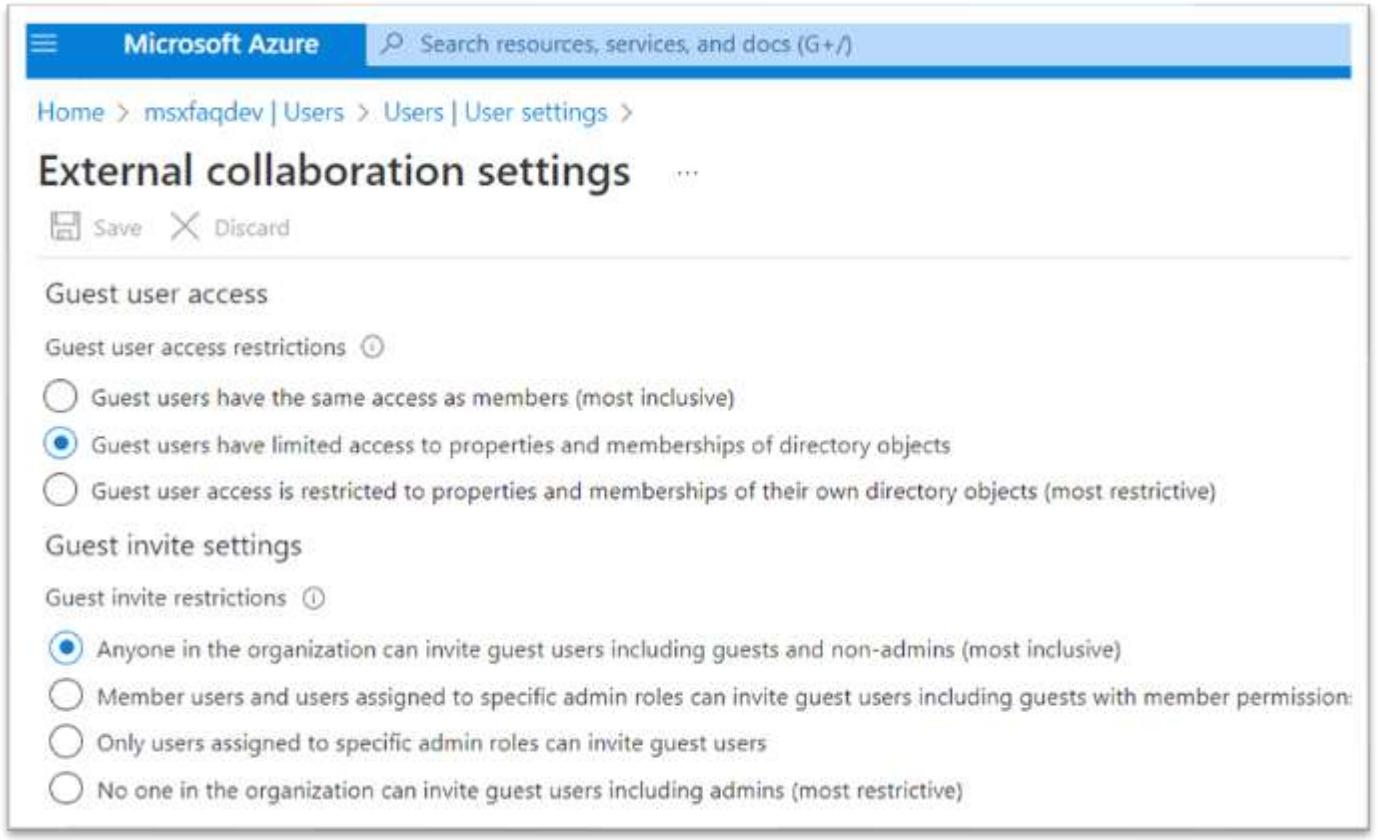


Azure Subscriptions

- Eine Subscription für …
  - VMs
  - Netwerke
  - Azure Functions
  - IP-Adressen
  - Datenbanken
  - ….
  - + Abrechnungsinformation
  - + Berechtigungen
- Enthält keine Identitäten
  - Benutzer, Gruppen
- Jede Subscription ist an ein AzureAD gebunden



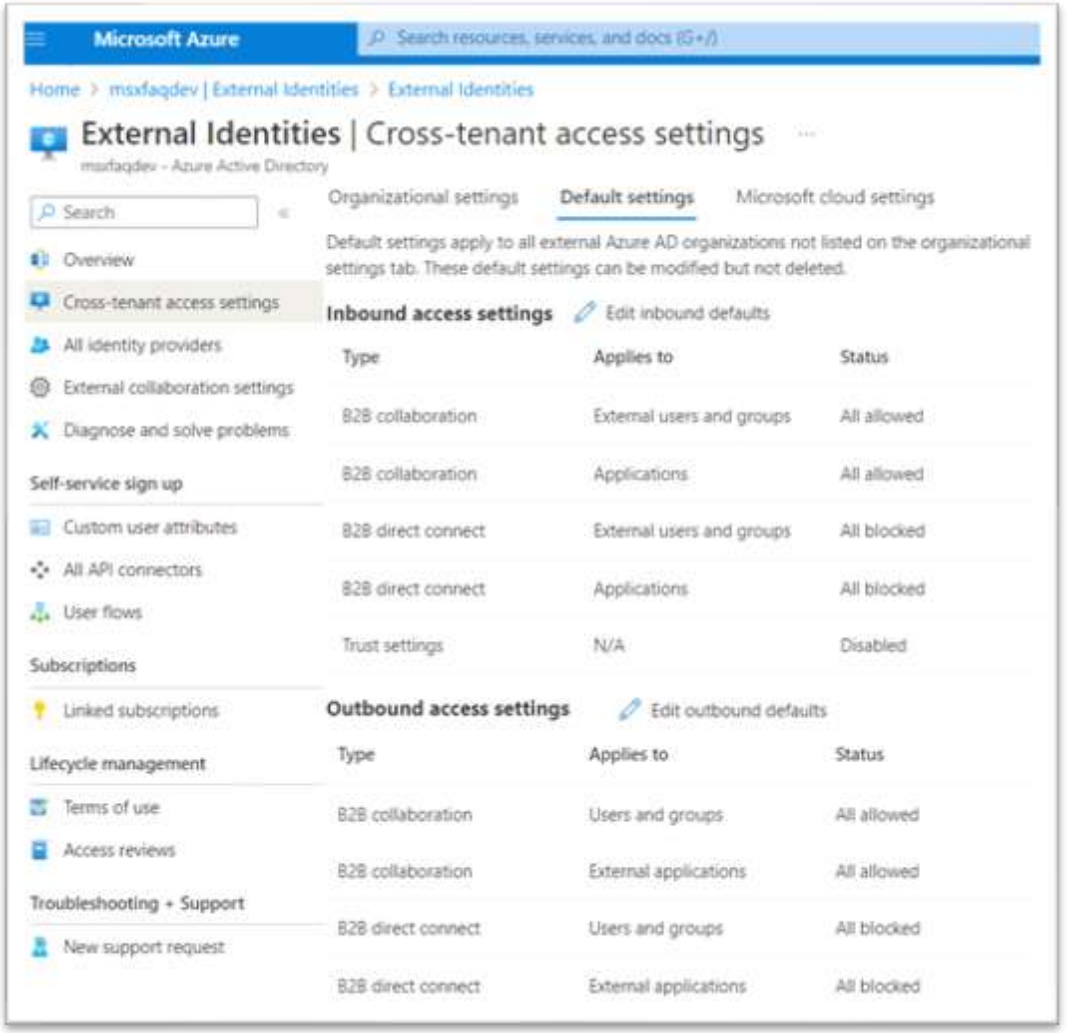
External Access: Gäste



- Wer darf Gäste einladen
  - Default: Jeder kann einladen
- Gäste können ihre Gruppe und Mitglieder lesen
  - Auch rekursiv

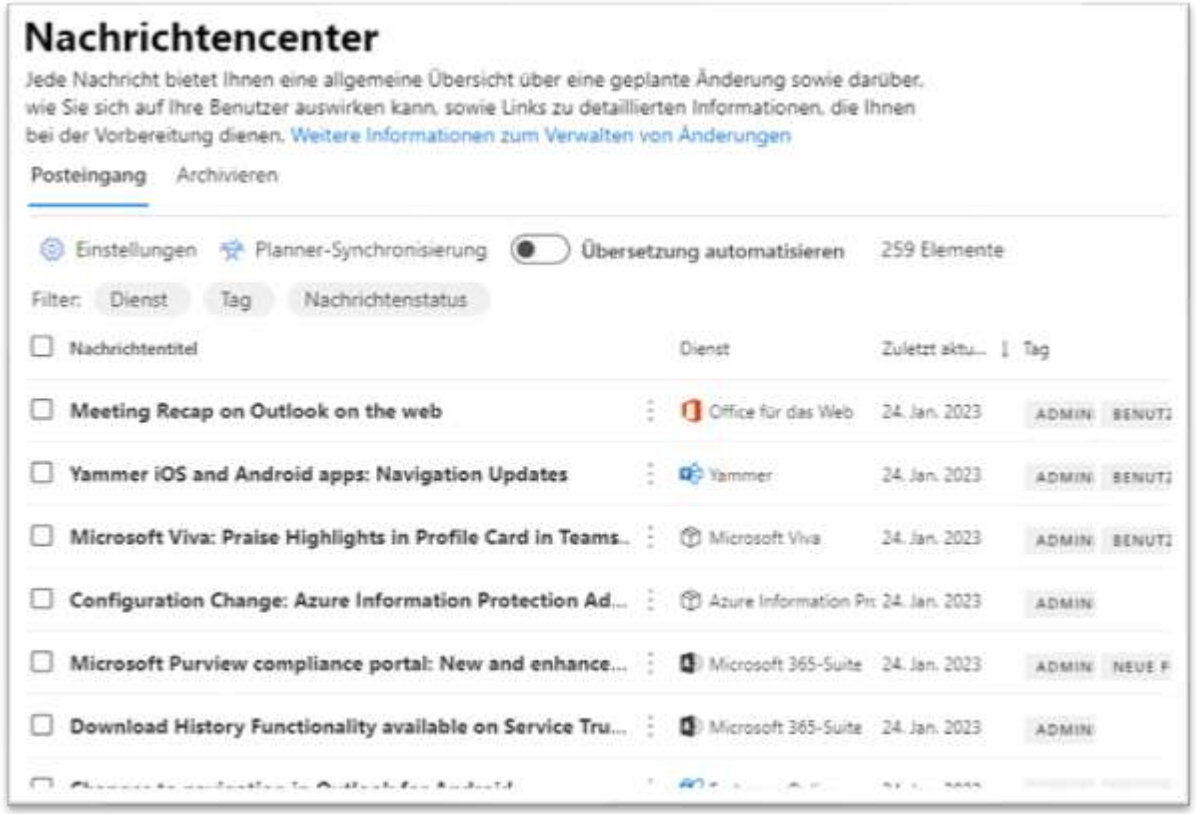
B2B Connect

- Primär für Microsoft Teams
  - „Shared Channels
  - Zugriff ohne Tenantwechsel
- Default „off“
  - Pro Domain beidseitig einzustellen
  - Soweit sicher



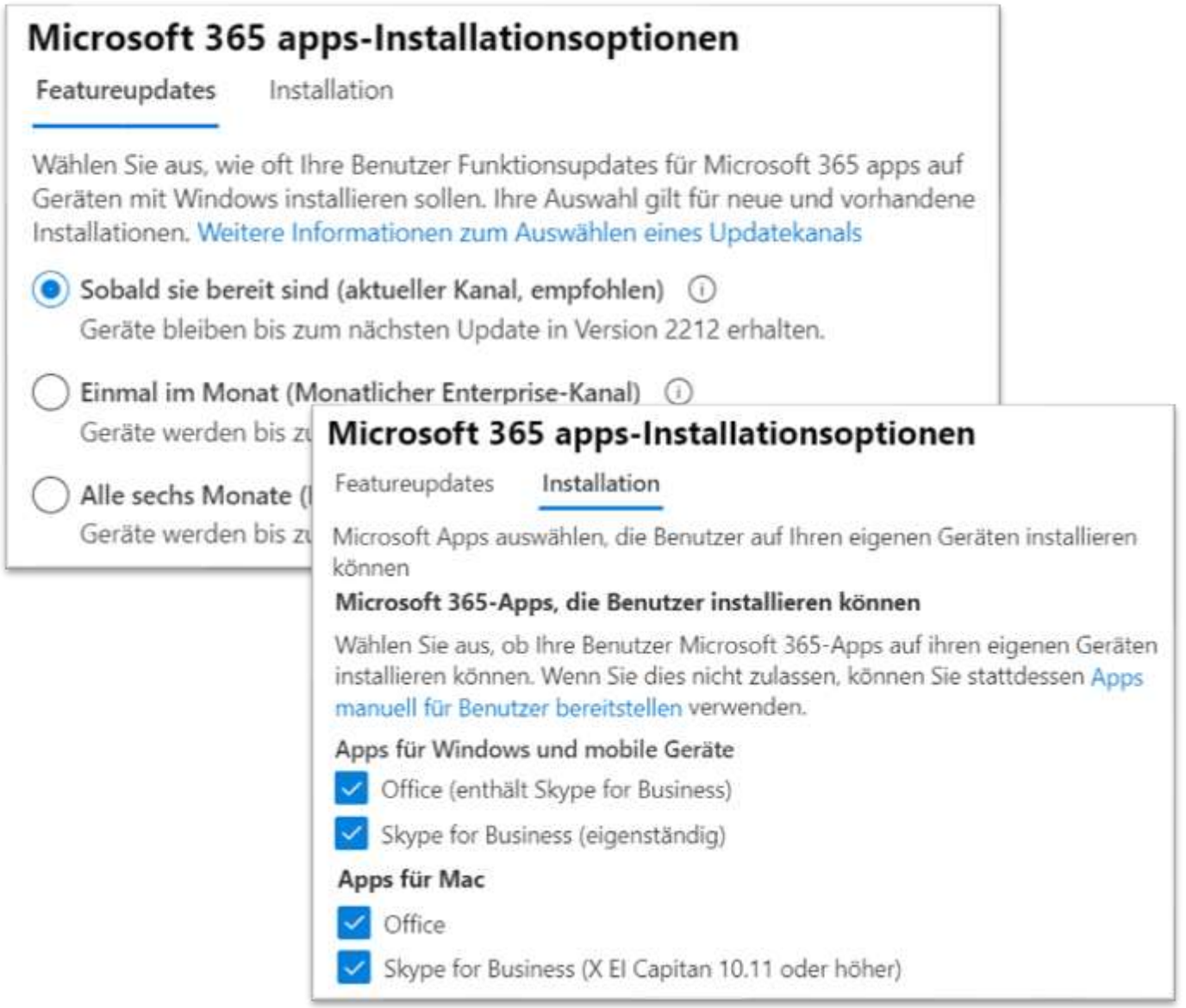
Message Center

- Wichtige Informationen zum Tenant
  - „Never loose a message“
- Zugriff
  - Administratoren
  - Benutzer von „Message Center Reader“!
- Tip1: „Einstellungen“
  - Ein Admin trägt Funktionsmailadresse ein
  - z.B. Teams Kanal sein
  - z.B. Ticketsystem
- Tip2: „Planner-Synchronisierung“
  - Synchronisierung mit Planner/Tasks
- Tip3: „Change Management“
  - Azubis stellen Änderungen vor

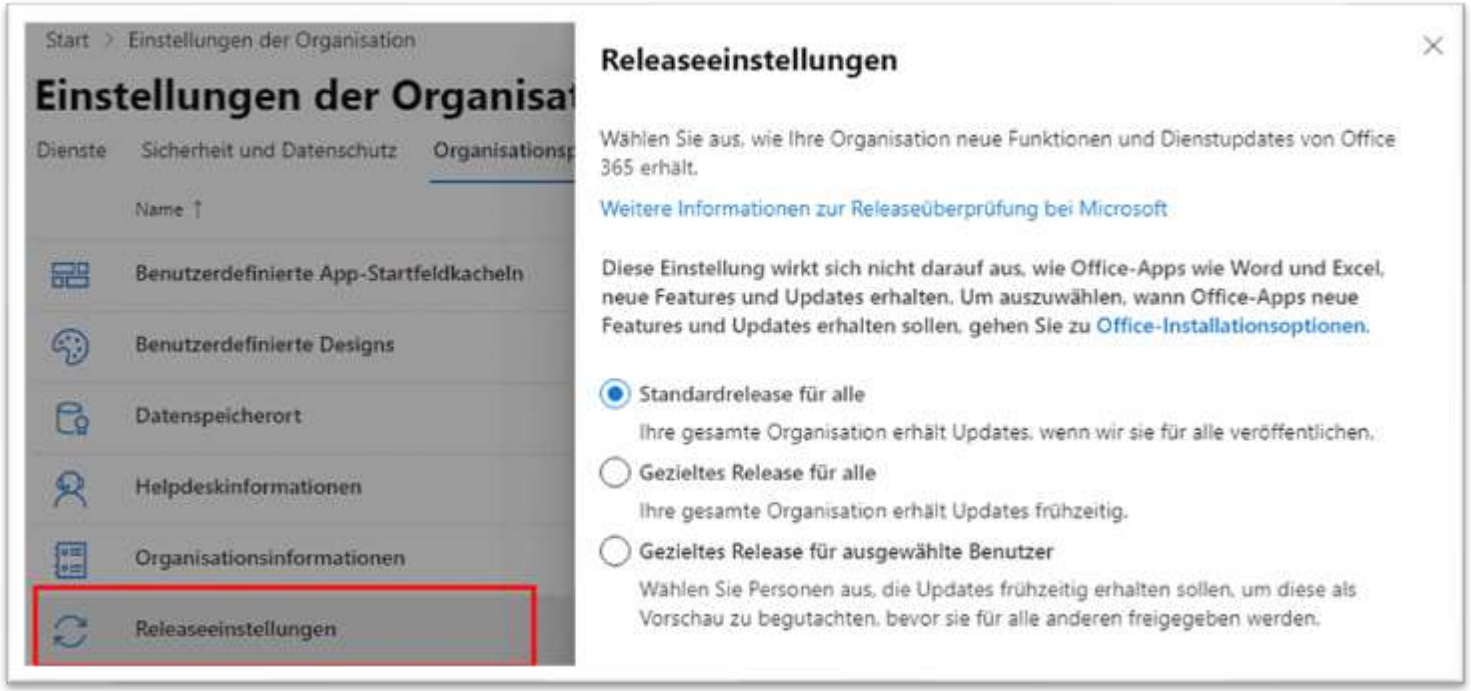


Apps und Features

- Jeder darf Office installieren
  - Kann eigene Verteilung stören
  - Bandbreitenbedarf
- Steuerung des Office Release Zyklus
- Steuerung des Teams Ring
- Steuerung



Office Release Einstellungen



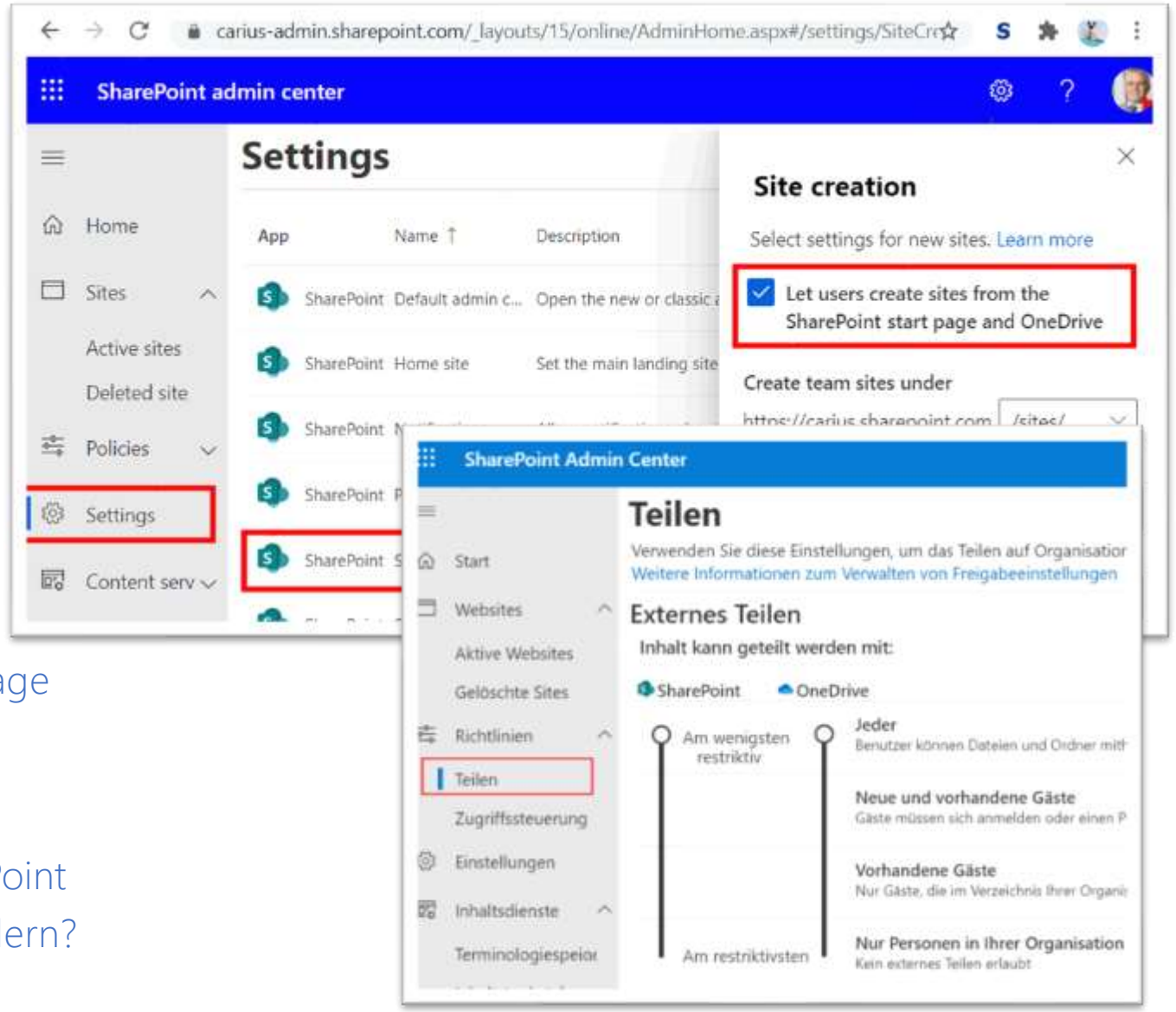
- Default: Standard
  - OK
- Piloten sollten aber „gezielt“ nutzen
  - Funktionsfähigkeit verifizieren
  - Schulungen vorbereiten

Eval/Trial/Self-Provisioning

- Benutzer können eigenständig „Testversion“ anfordern
  - Wollen Sie das?
- Teams wäre einzige App aber es gibt keine Richtlinien
- Achtung: PowerApps u.a.

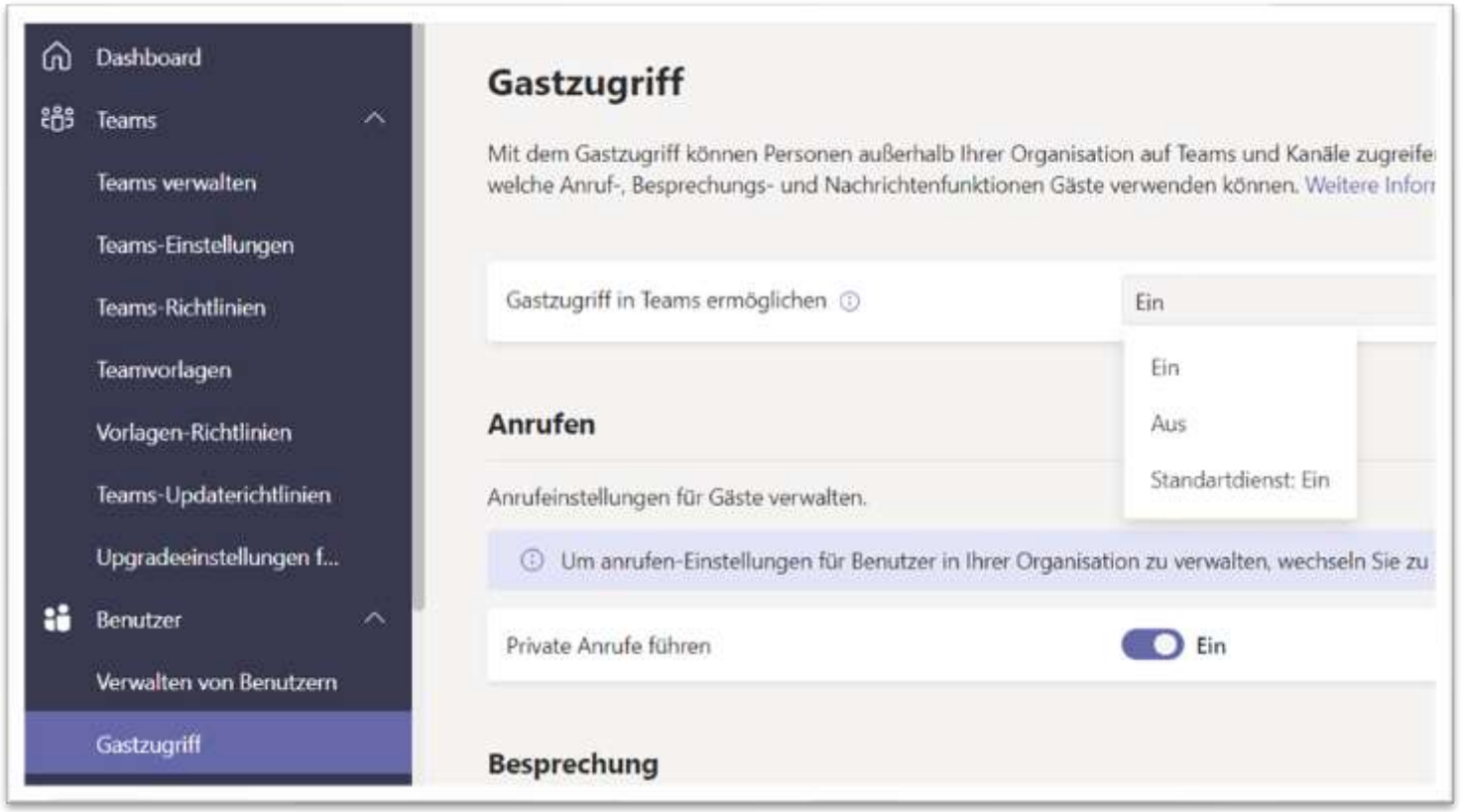
```
Install-Module -Name MSCommerce
Import-Module -Name MSCommerce
Connect-MSCommerce
$product = Get-MSCommerceProductPolicies `
                -PolicyId AllowSelfServicePurchase
$product | %{`
   Update-MSCommerceProductPolicy `
       -PolicyId AllowSelfServicePurchase `
       -ProductId $_.productid `
       -Enabled $false`
}
```

SharePoint



- Neuanlage von SharePoint Sites
  - Default: Jeder darf anlegen
  - Hinweis: Verbunden mit Teams Anlage
- Sharing
  - Default: Mit jedem erlaubt
  - OneDrive kann nie mehr als SharePoint
  - Default anpassen oder pro Site ändern?

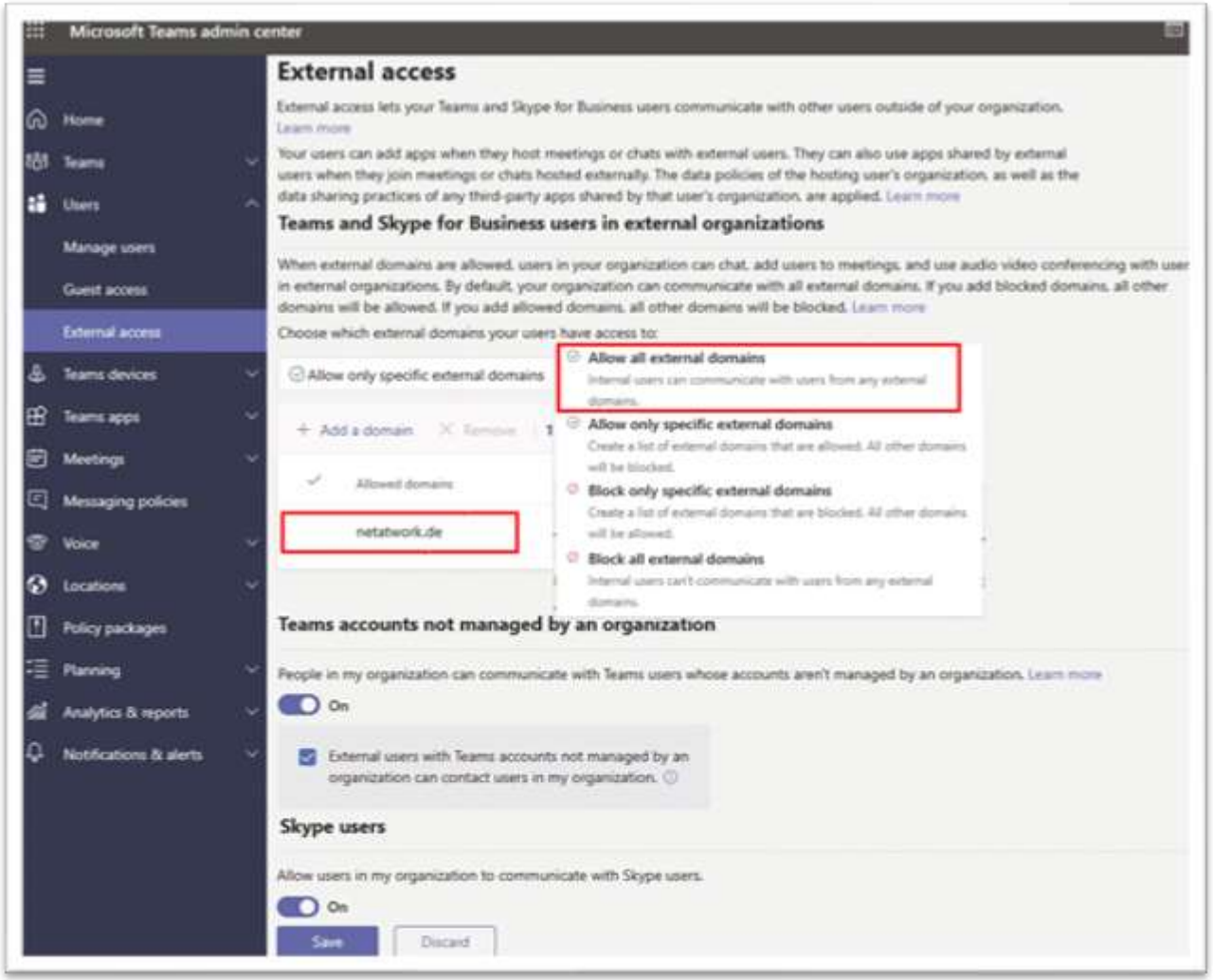
Teams 1



- Wer darf Teams anlegen
  - Default: Jeder darf anlegen
  - Abschalten per PowerShell
- Teams Gastzugriff

Teams 2: Federation

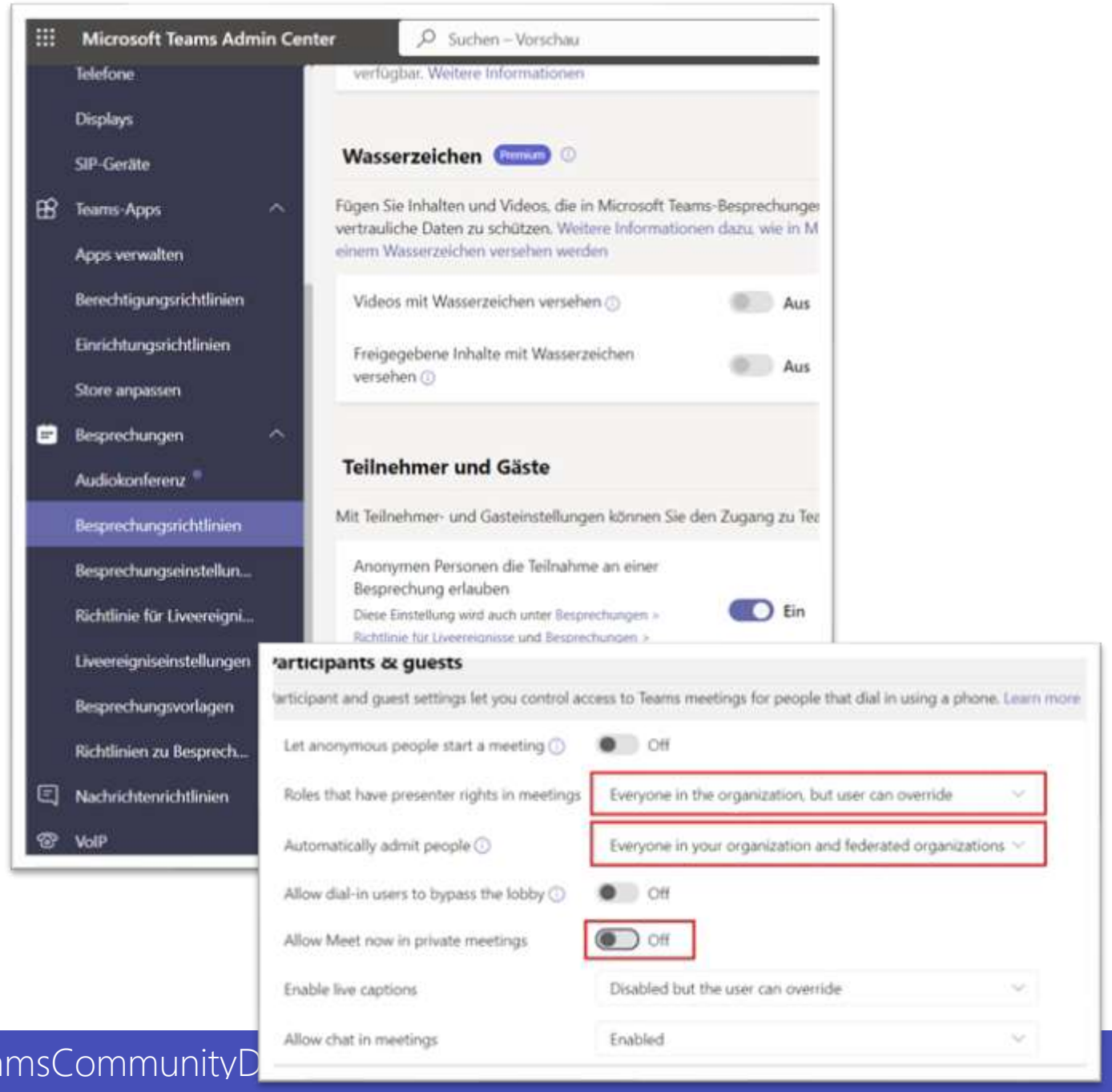
- Federation mit anderen Teams
  - Default: ANY ALLOW
- Federation mit Skype
  - Default: Aktiv
- Risiken
  - Direkte Ansprache des Mitarbeiters
  - Direkter „Anruf“ auch ohne Headset
  - Externe Präsenzanzeige
  - SPIM
  - Phishing
- Empfehlung
  - Nie aktivieren ohne Userschulung
  - User Risk Awareness
  - Domain Whitelisting



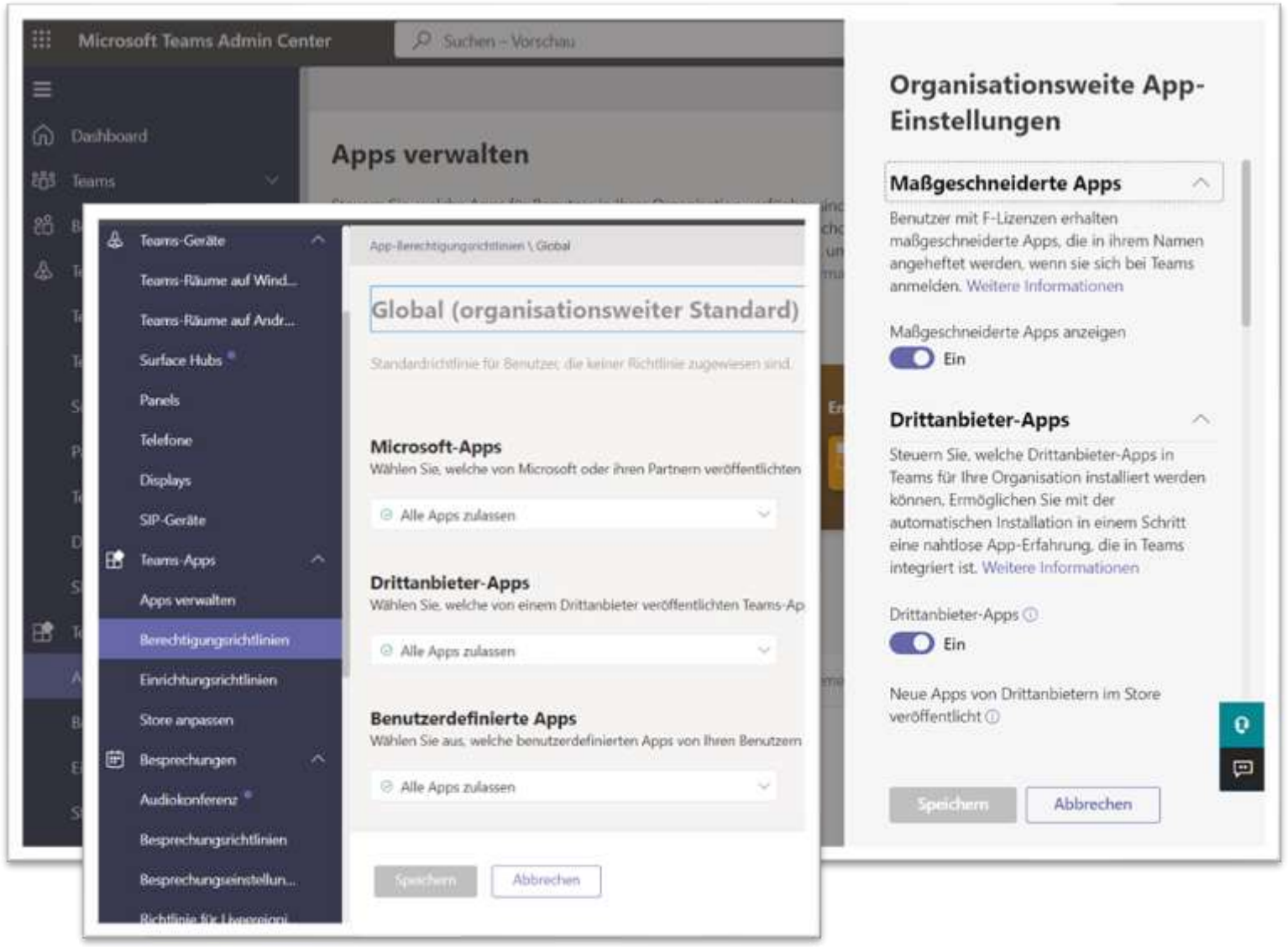
Teams: Meetings

- Audio/Video
  - Default aktiv
- UDP-Portrange
  - Default nicht vorgegeben
- Aufzeichnung in der Cloud
  - Default zugelassen
- Bildschirmfreigabe
  - Default: Voller Bildschirm
  - Default: Fernsteuerung erlaubt
- Präsenter
  - Default: Jeder
- Live Events
  - Default: Jeder

Teams Führerschein !



Teams Apps



- Default
  - Alle Erlaubt
- Risiken
  - Apps tracken Aktivität (Giphy = Facebook) (Polly = extern)
  - Consent Erteilung

https://www.msxfaq.de/teams/apps/polly_und_datenschutz.htm

Domains einrichten

- Finger weg von „onmicrosoft.com
  - Außer für Cloud Only Admins
- Eigene Domains
  - Max 900
  - Verifikation per DNS
- Applikationen
  - Anmeldenamen (UPN)
  - Exchange Accepted Domains und Sonderfall <tenant>.mail.onmicrosoft.com
  - UPN <> AD DNS-Domain !!
- ADSync, AzureAD CloudSync
  - IDFix
  - Lokale Absicherung

Was es sonst noch alles gibt

- Datenschutz
  - Bing Suche
  - Report
  - MyAnalytics/Viva
  - Microsoft 365 Apps Telemetrie
  - Teams QoE-Reporting
  - Teams Telefonie-Verbindungsdaten
  - …
- Zukünftige Produkte

TeamsCommunityDay 2023

Feedback

http://feedback.teamscommunityday.de/