Infinity 365 Conference

Microsoft 365 Tenant Checklist

Kurzvorstellung

Net at Work
Building IT-Excellence.

Infinity 365 Conference

- Frank Carius
  - Microsoft MVP für Office Server Systems
  - Microsoft Certified Master
  - Betreiber von www.msxfaq.de
  - SIP/Mail/Teams: frank.carius@netatwork.de
- Meine Schwerpunkte
  - Unified Communication, (Teams, Exchange SfB)
  - Microsoft 365, Azure, Netzwerk Assessments, Rimscout
  - Identity : AD, AzureAD, ADFS, ADSync
  - Mail Encryption und Signierung, NoSpamProxy
- Net at Work GmbH
  - Gegründet 1995 in Paderborn
  - Ca. 150 Mitarbeiter
  - IT-Systemintegration und Software Development

Microsoft CERTIFIED Master

Microsoft MVP Most Valuable Professional

www.msxfaq.de

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

noSpamproxy

rimscout

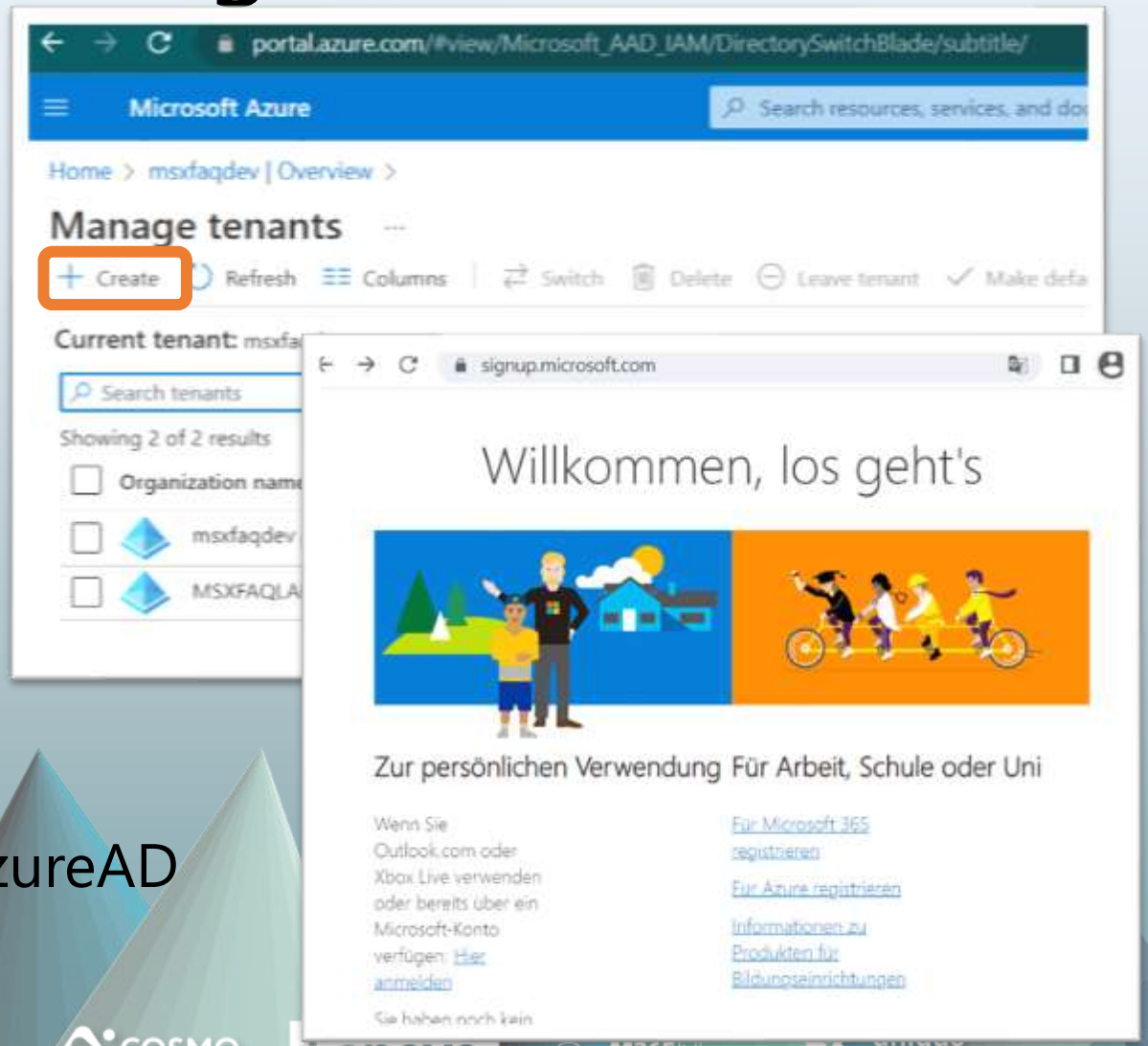
ACP HORNETSECURITY base it ppedv Alight. COSMO CONSULT Lenovo M365 Kaffeepause unique conceptions

Name, Sponsor

- 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!

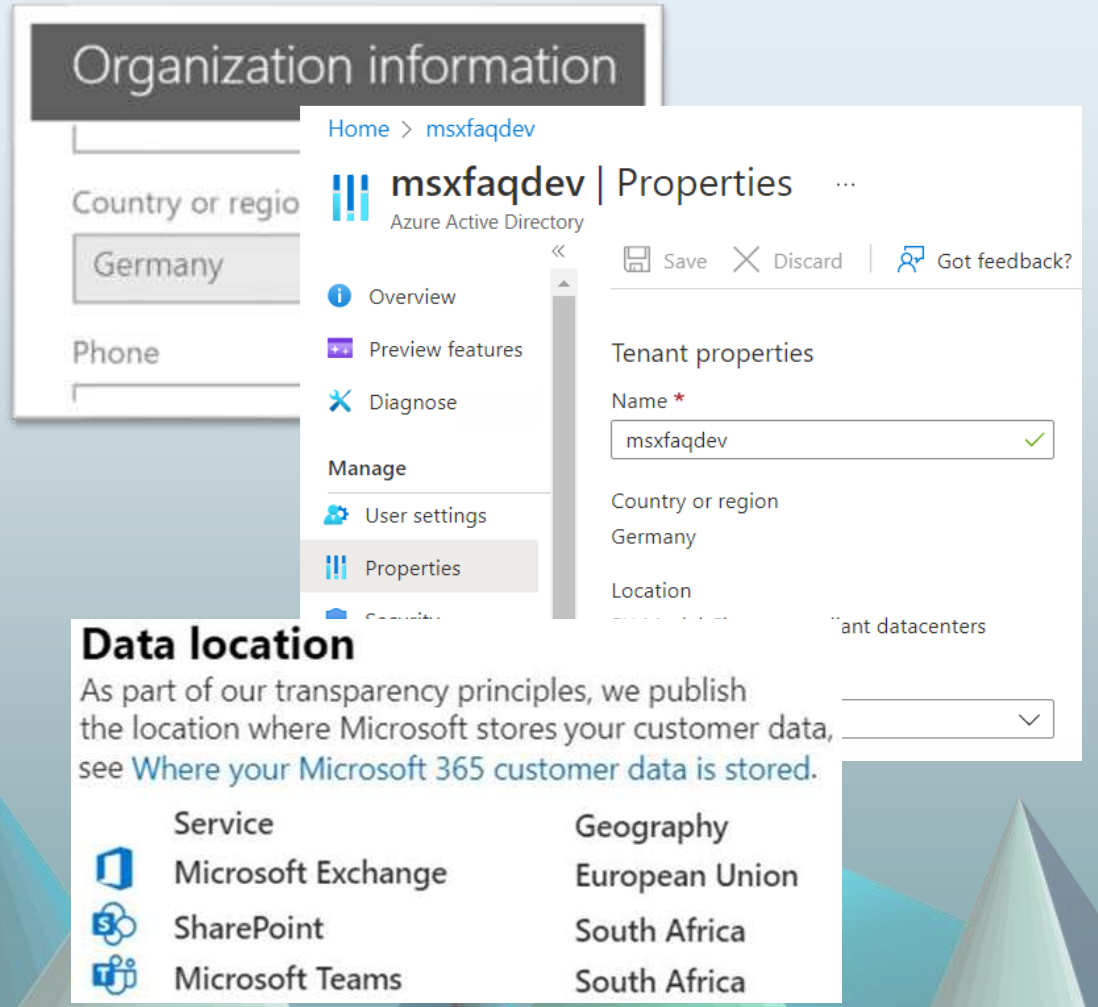
Tenant beantragen

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



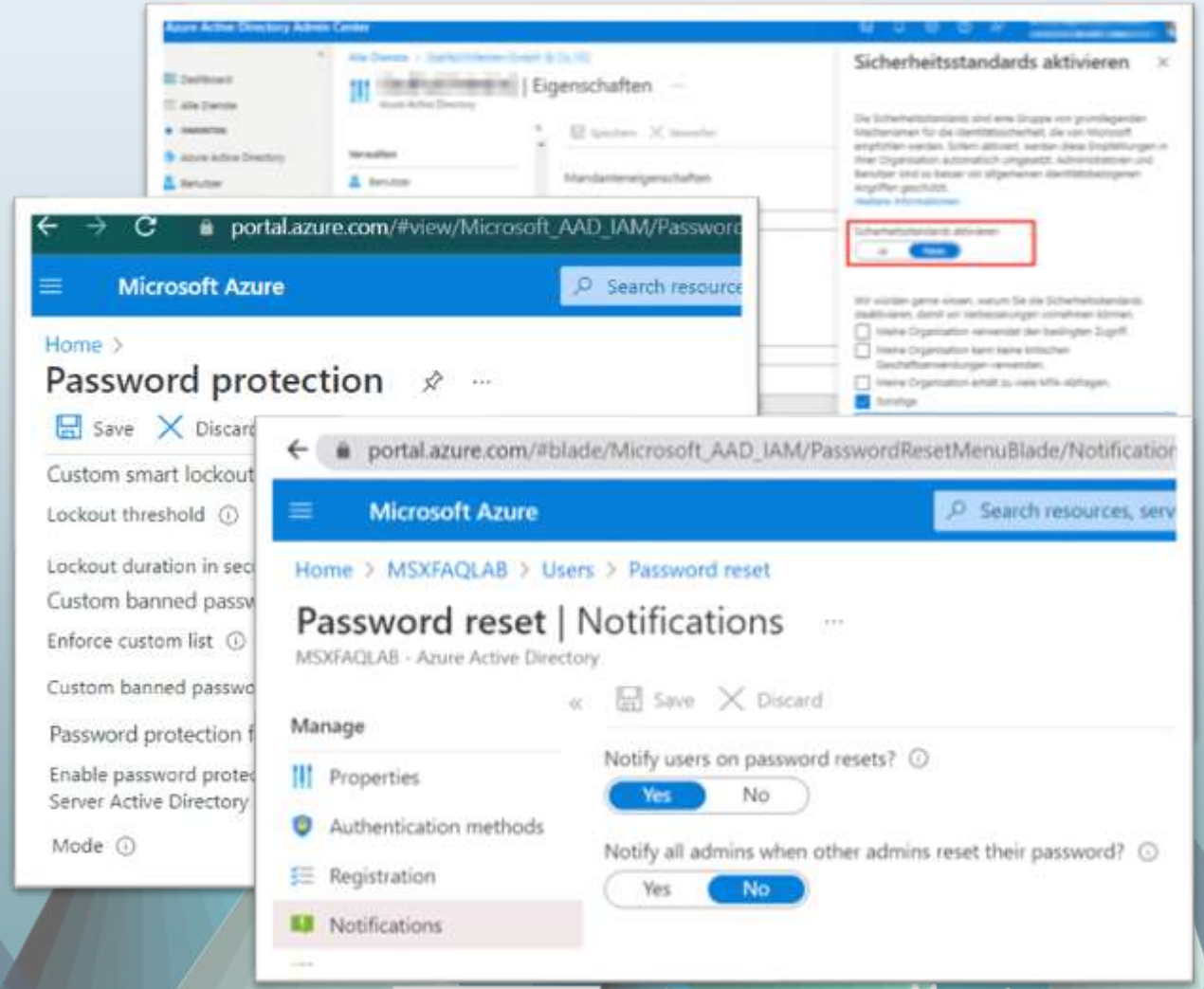
Region, Location, Language

- Country/Region
  - Rechnungsadresse (Umsatzsteuer!)
  - Nicht änderbar
- UsageLocation
  - Pro Benutzer und Global Default
  - für Lizenz-Zuweisung
- Sprache
  - Global oder pro Benutzer, pro Browser
  - Systemnachrichten, Inbox vs. Posteingang
- Preferred Data Location (PDL)
  - Datenspeicherort pro Benutzer
  - MultiGeo Konfiguration



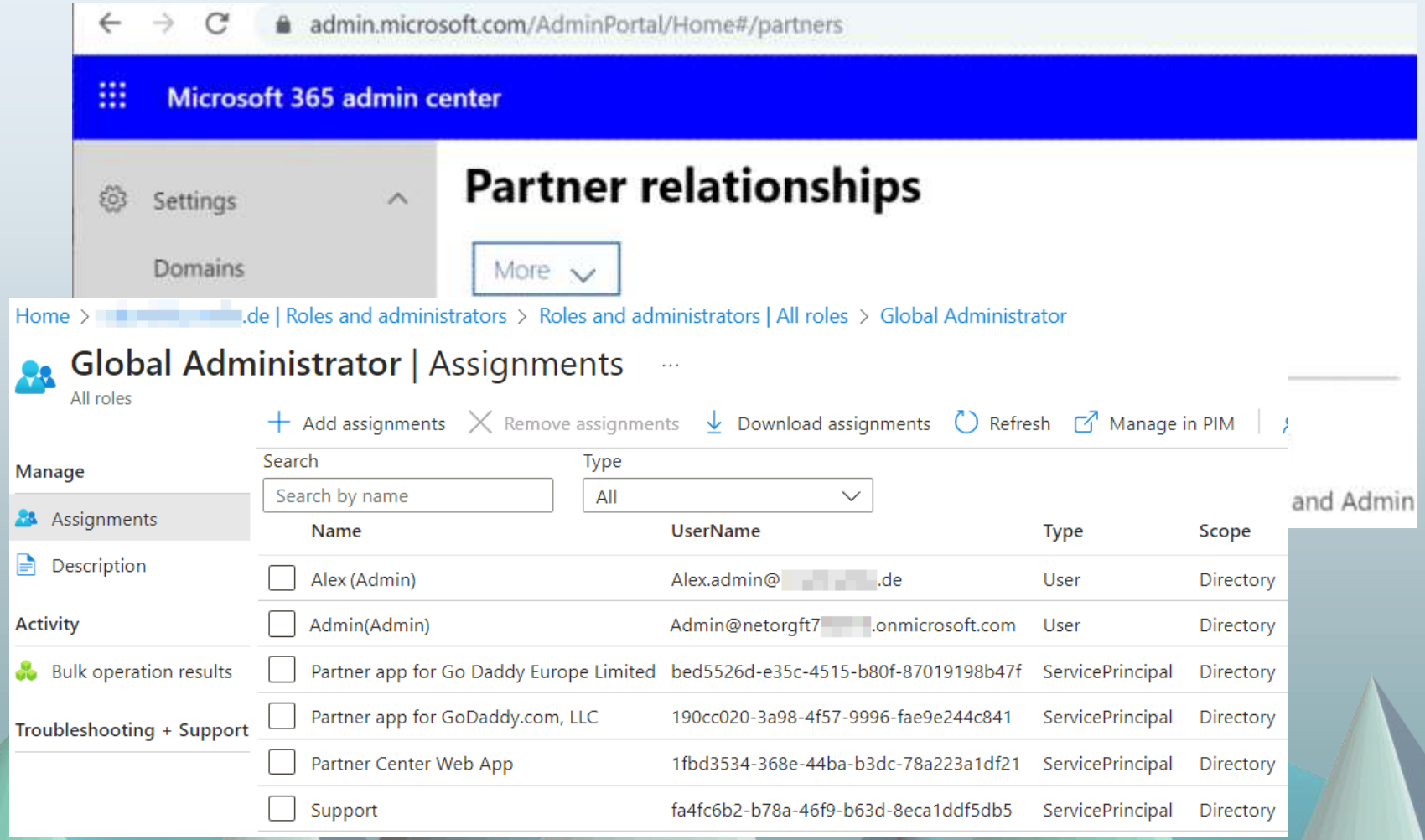
Admin-Konten

- Einer ist zu wenig, weniger ist mehr
- Vorsicht mit „ADFS“ und ADSync
- MFA/Security Defaults
  Eventuell sogar SecureLoginOnly
- Conditional Access (Azure AD P1)
- Später PIM (Azure AD P2)
- Kennwortrichtlinien
  - nur für Cloud-Konten, nicht PHS
  - Password Reset Meldung
- Admins brauchen keine Lizenz
  - und kein Postfach!, Mailadresse reicht
- „Breaking glass admin“



Unerkannte Admins

- GDAP
- Partner-Admin
- Gast-Admins
- GoDaddy Admin

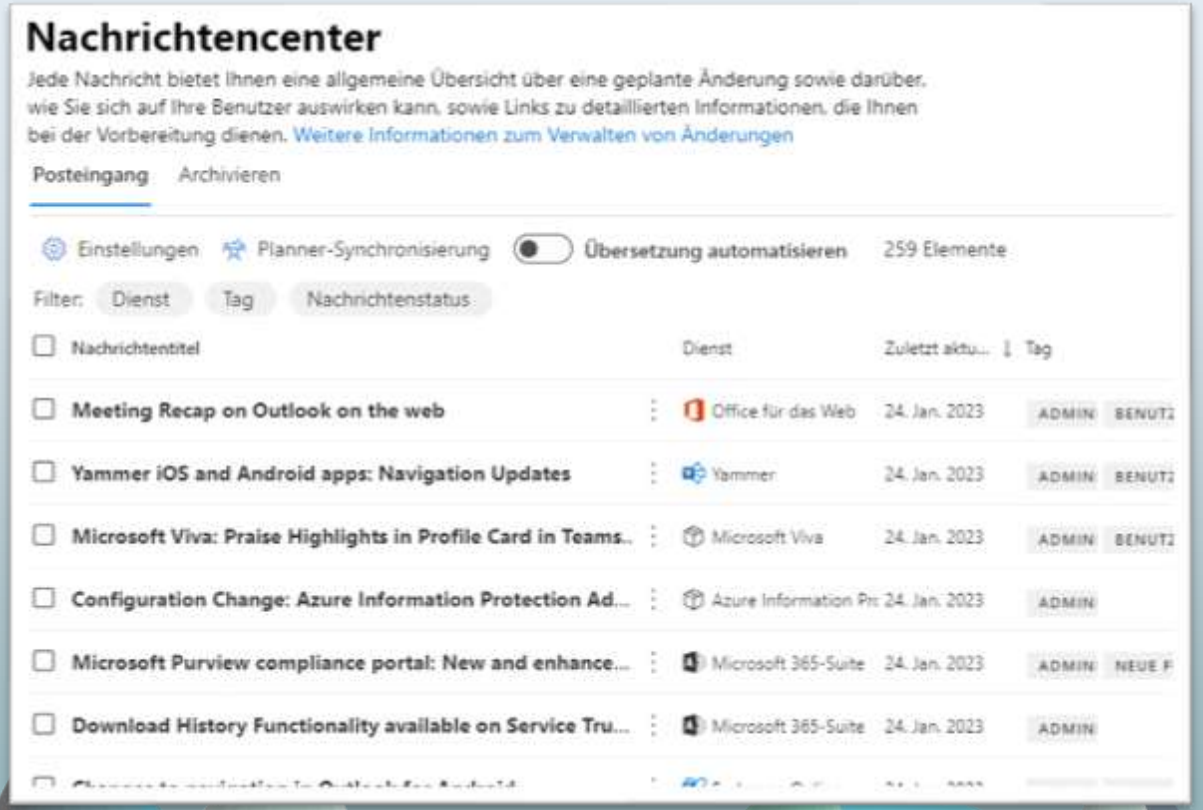


Domains einrichten

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

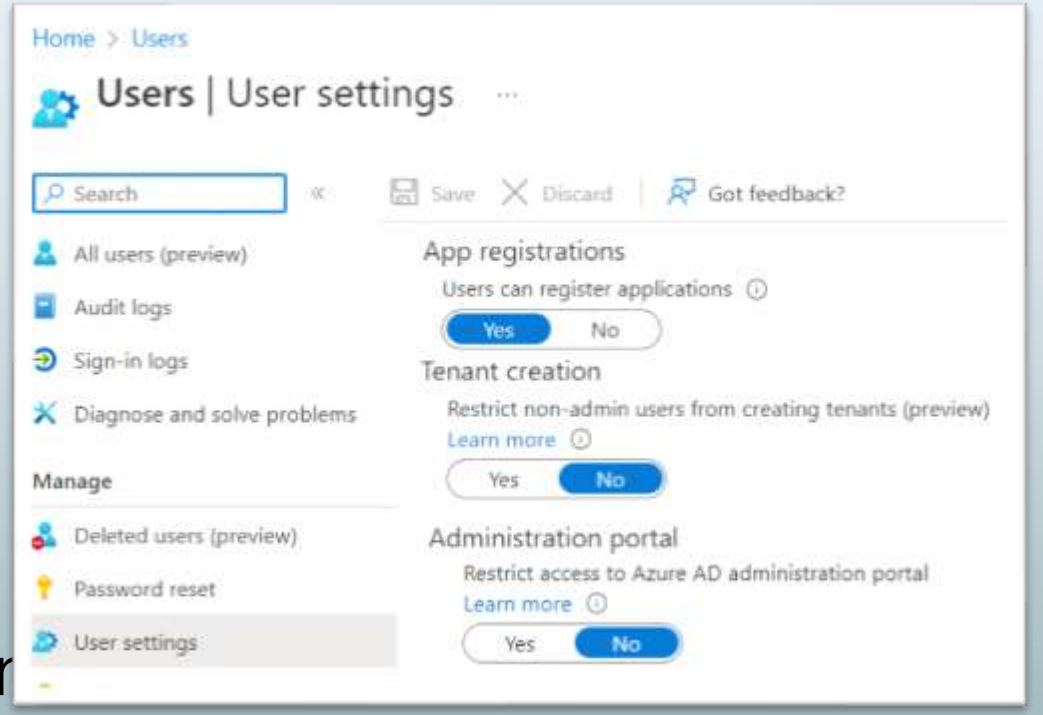
Message Center

- Wichtige Informationen zum Tenant
  - „Never loose a message“
- Zugriff
  - Administratoren (Mailadresse)
  - MessageCenterReader-Rolle
    Achtung: Portalzugriff enthalten
- Tip1: „Einstellungen“
  - Ein Admin trägt Funktionsmailadresse ein
  - z.B. Teams Kanal
  - z.B. Ticketsystem
- Tip2: „Planner-Synchronisierung“
  - Synchronisierung mit Planner/Tasks
- Tip3: „Change Management“
  - Azubis stellen Änderungen vor



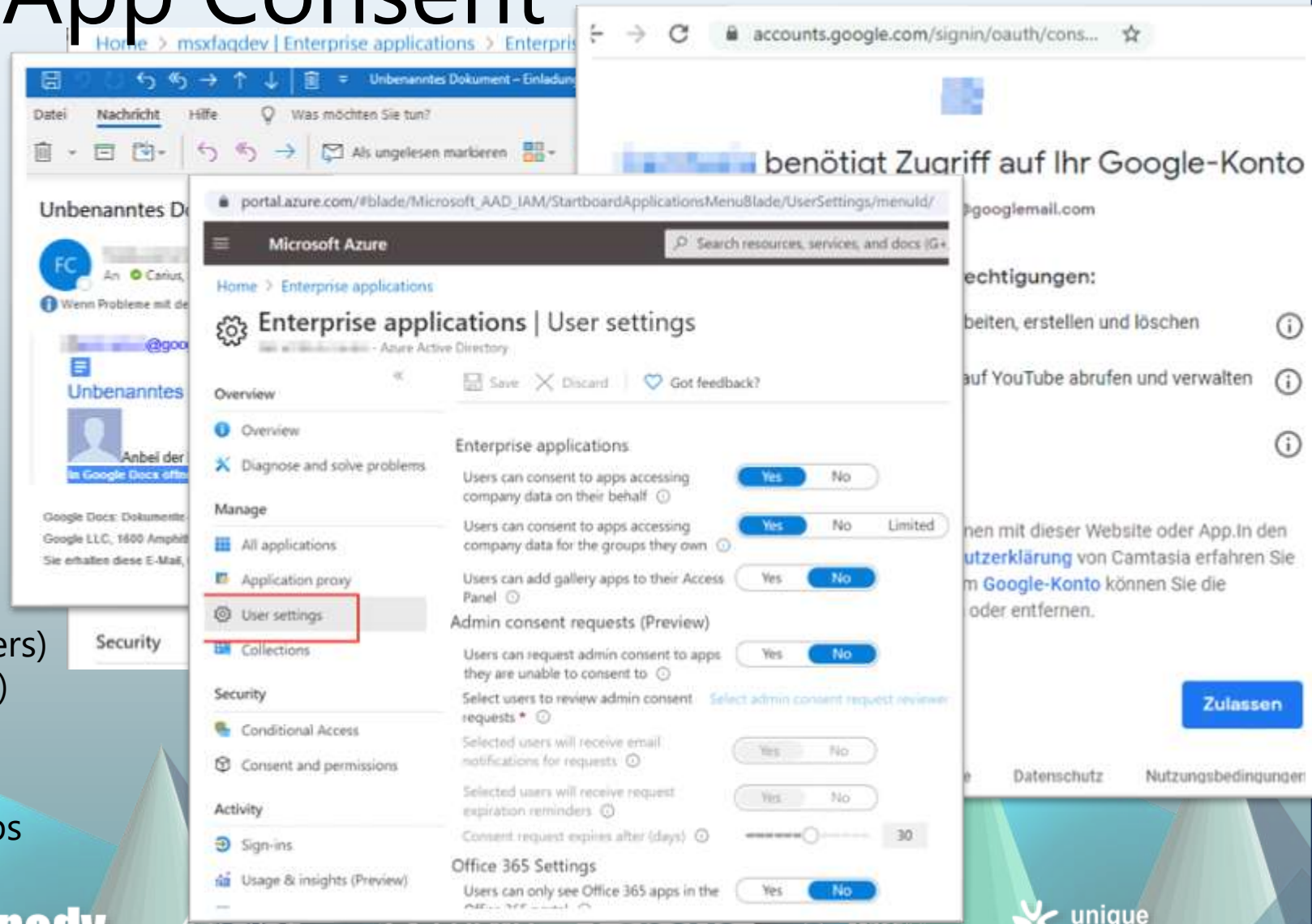
Benutzer beschränken

- Wer darf Apps registrieren?
  - Default: „Alle“!
- Wer darf weitere Tenants anlegen?
  - Default: „Alle“!
- Wer darf auf http://portal.azure.com?
  - Default: „Alle“!
- Wer darf Teams/Office Groups anlegen?
  - Default: „Alle“!
- Wer darf …



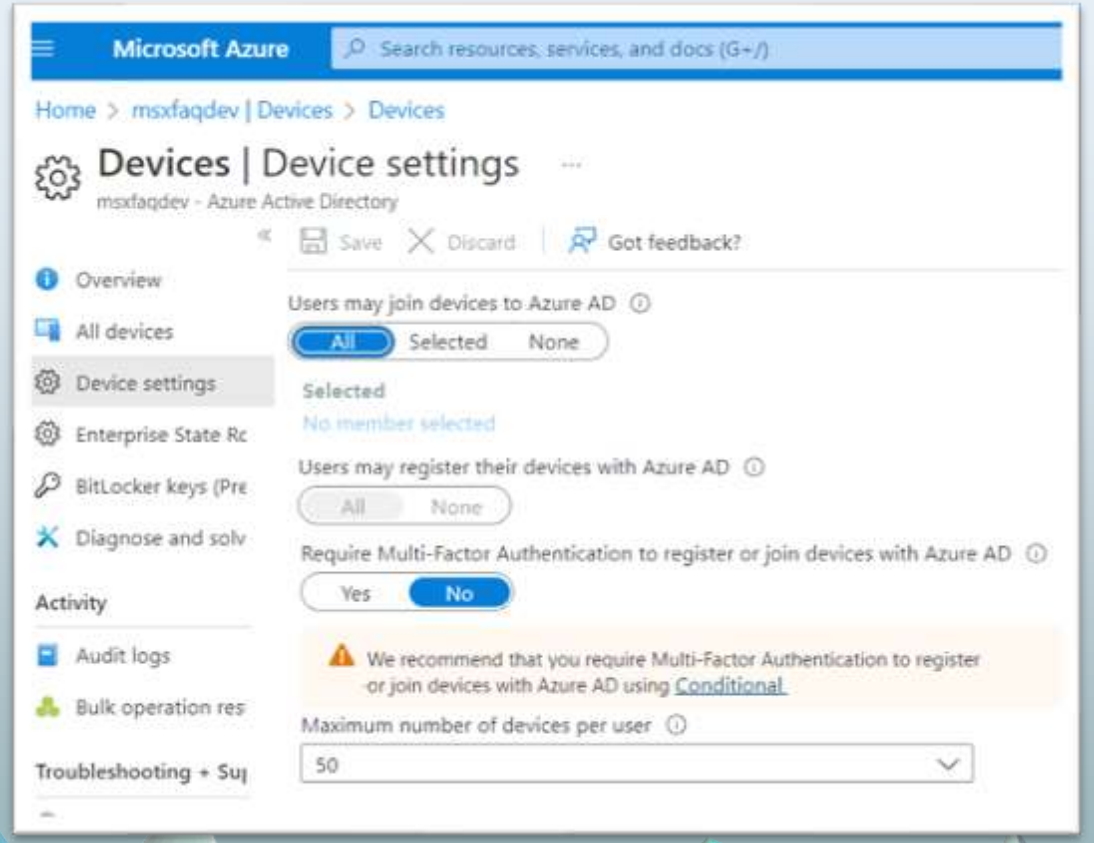
App Consent

- 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



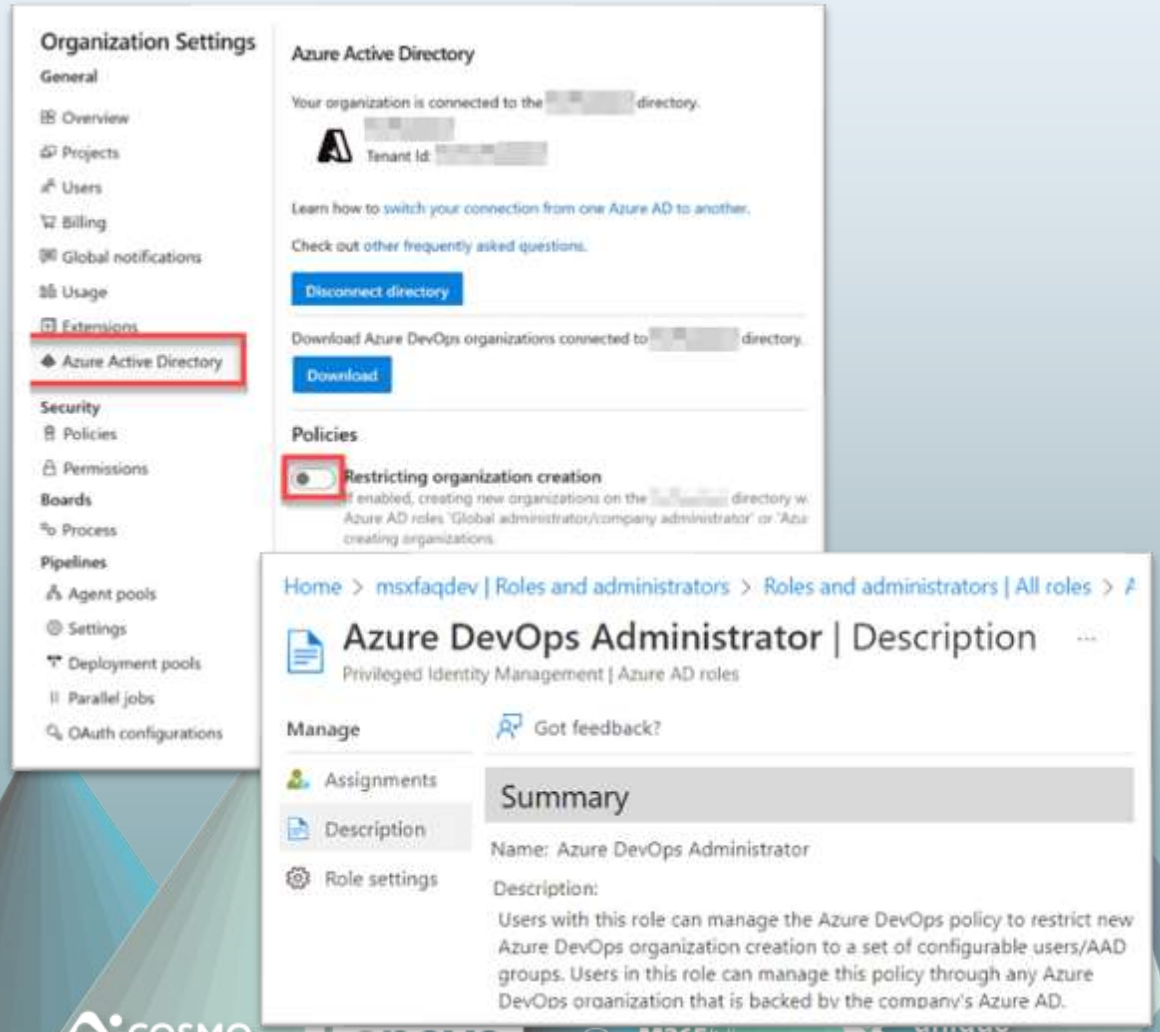
AzureAD Devices

- Benutzer kann Computer addieren
  - Lokales AD: bis zu 10 Geräte
  - AzureAD: bis zu 50 Geräte
- Empfehlung
  - Geräte werden durch ADSync oder Device-Administratoren addiert
- Device Konzept erstellen
  - Hybrid-Joined
  - AzureAD Joined
  - AzureAD Registered
  - Unknown
- Lokaler Admin für AzureAD Joined Devices vorgeben



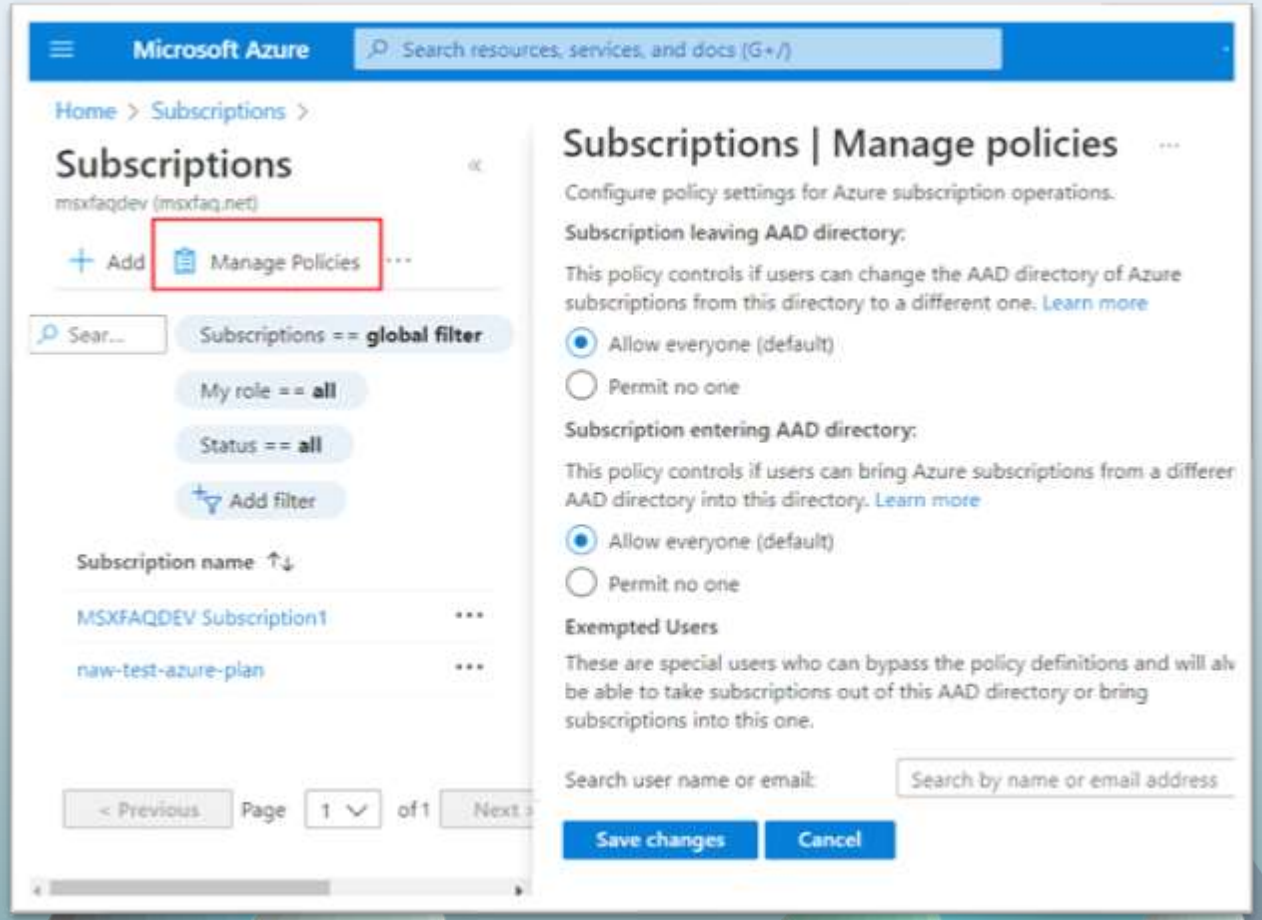
DevOps absichern

- Was ist DevOps?
  - Sourcecode Verwaltung wie GIT
  - Planungswerkzeuge
  - https://dev.azure.com/ u.a.
  - kostenfrei- > SchattenIT
  - DevOps ist mit AzureAD verbunden
- Wer darf DevOps verbinden?
  - Default: „Jeder“!
- Wer DevOps Orgs anlegen
  - Default: „Jeder“!



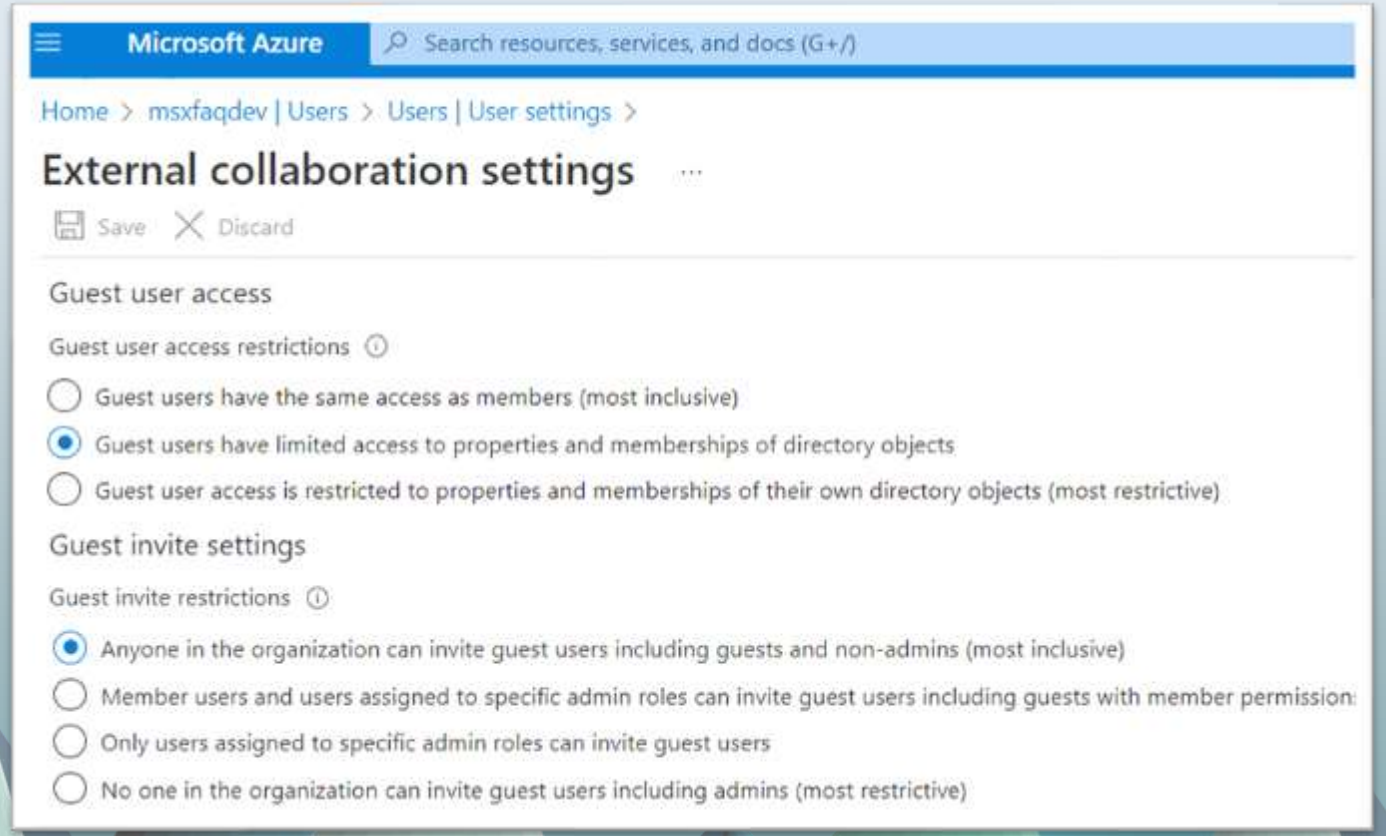
Azure Subscriptions

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



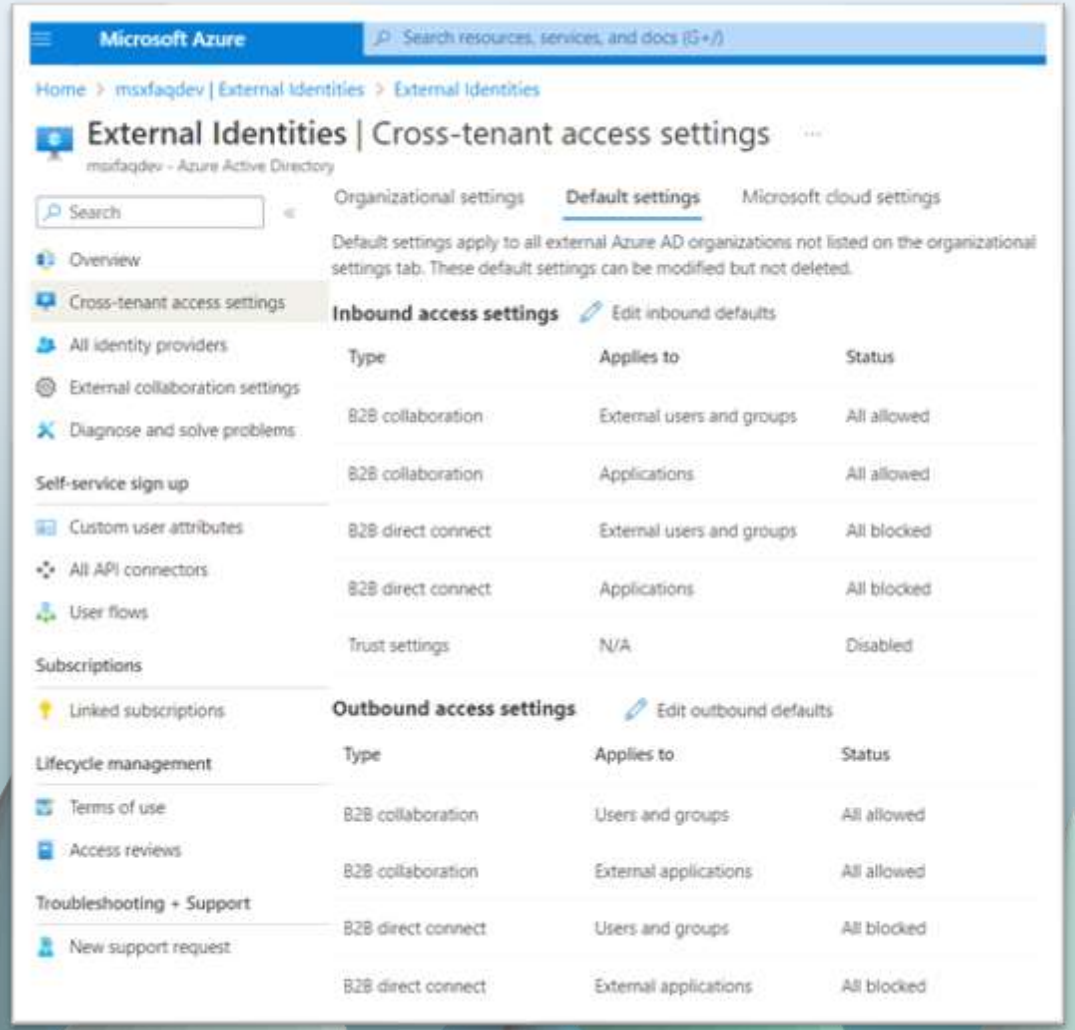
Gäste und external Identites

- Wer darf Gäste einladen
  - Default: Jeder kann einladen
- Gäste können
  - Gruppen lesen
  - Mitglieder lesen
  - Auch rekursiv
- Guest Life cycle
  - Beantragungsprozess
  - Inaktive Gäste erkennen
  - Deaktivieren/Löschen
- Bitte einschränken wenn möglich



B2B Connect

- Primär für Microsoft Teams
  - „Shared“ Channels
  - Zugriff ohne Tenant-Wechsel
- Default „off“
  - Pro Domain beidseitig einzustellen
  - Sicher by default
  - Filterung mit AzureAD P1
- Cross-tenant sync
  - Meine Benutzer sind deine Gäste
    … oder external Identites

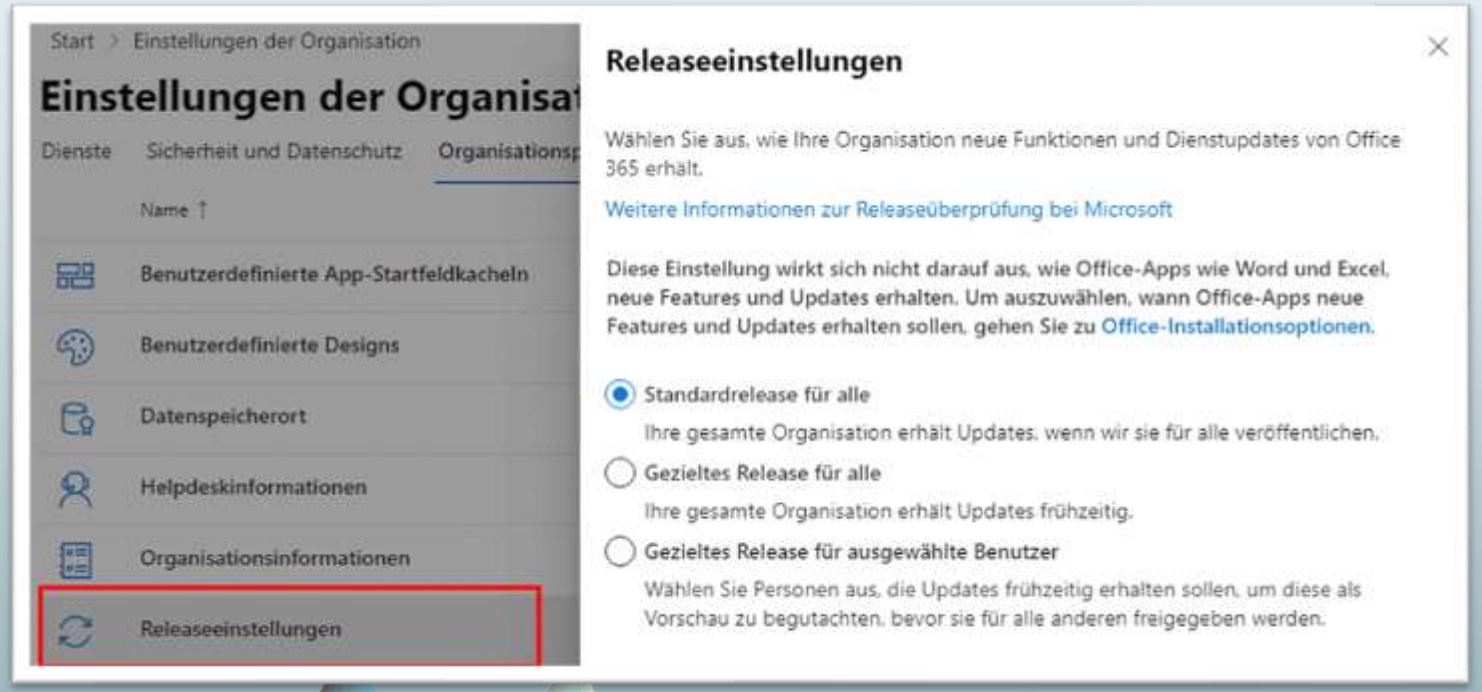


Apps und Features

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

Office Release Einstellungen

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



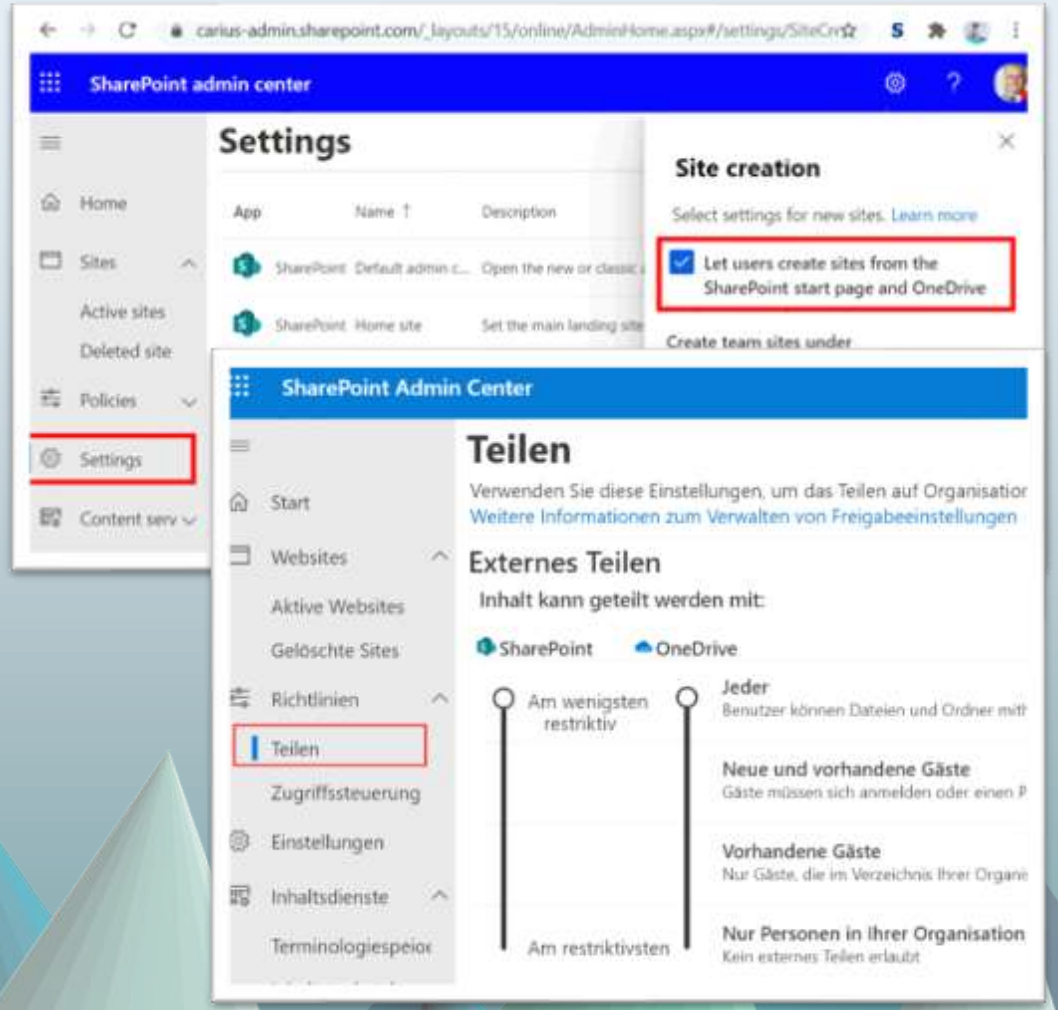
Eval/Trial/Self-Provisioning

- Benutzer können
  - eigenständig „Testversion“ anfordern
  - Wollen Sie das?
- Teams aktuell 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`
}
```

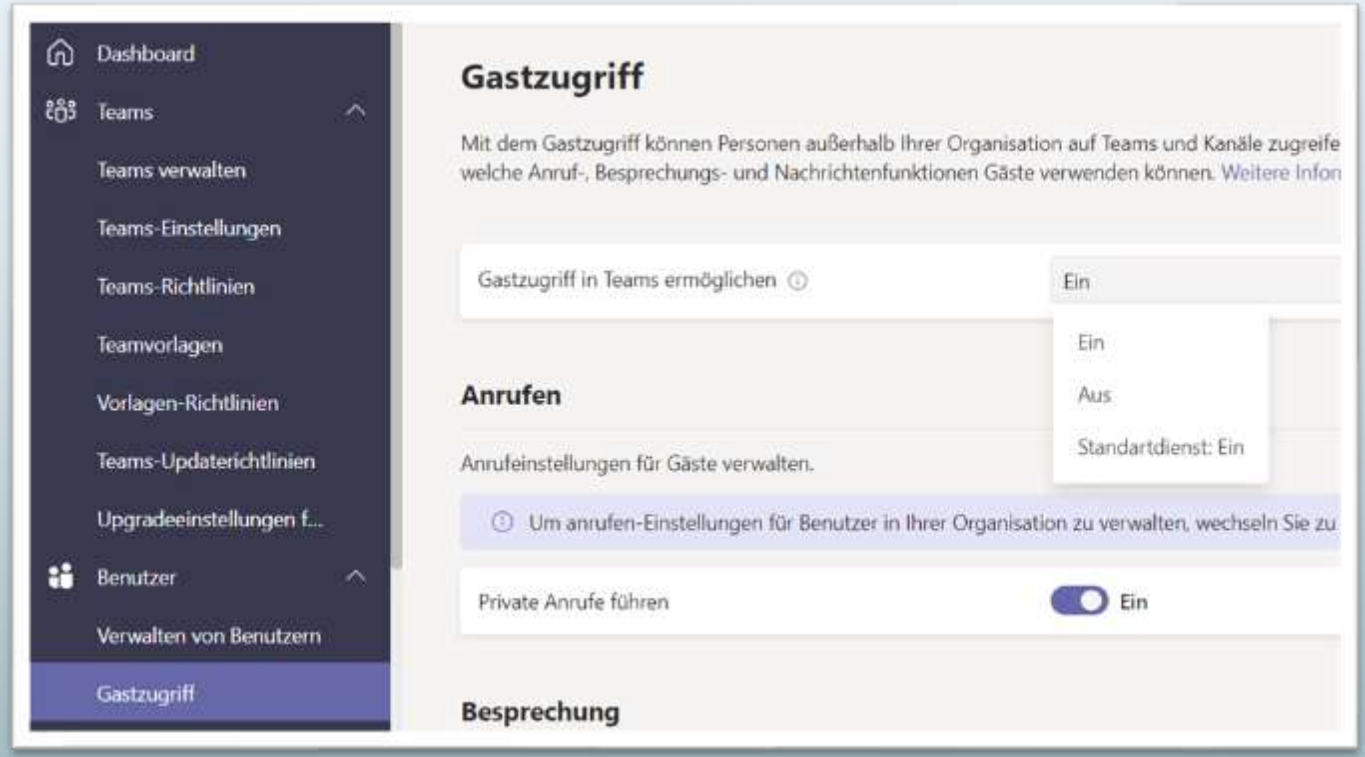
SharePoint

- 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?



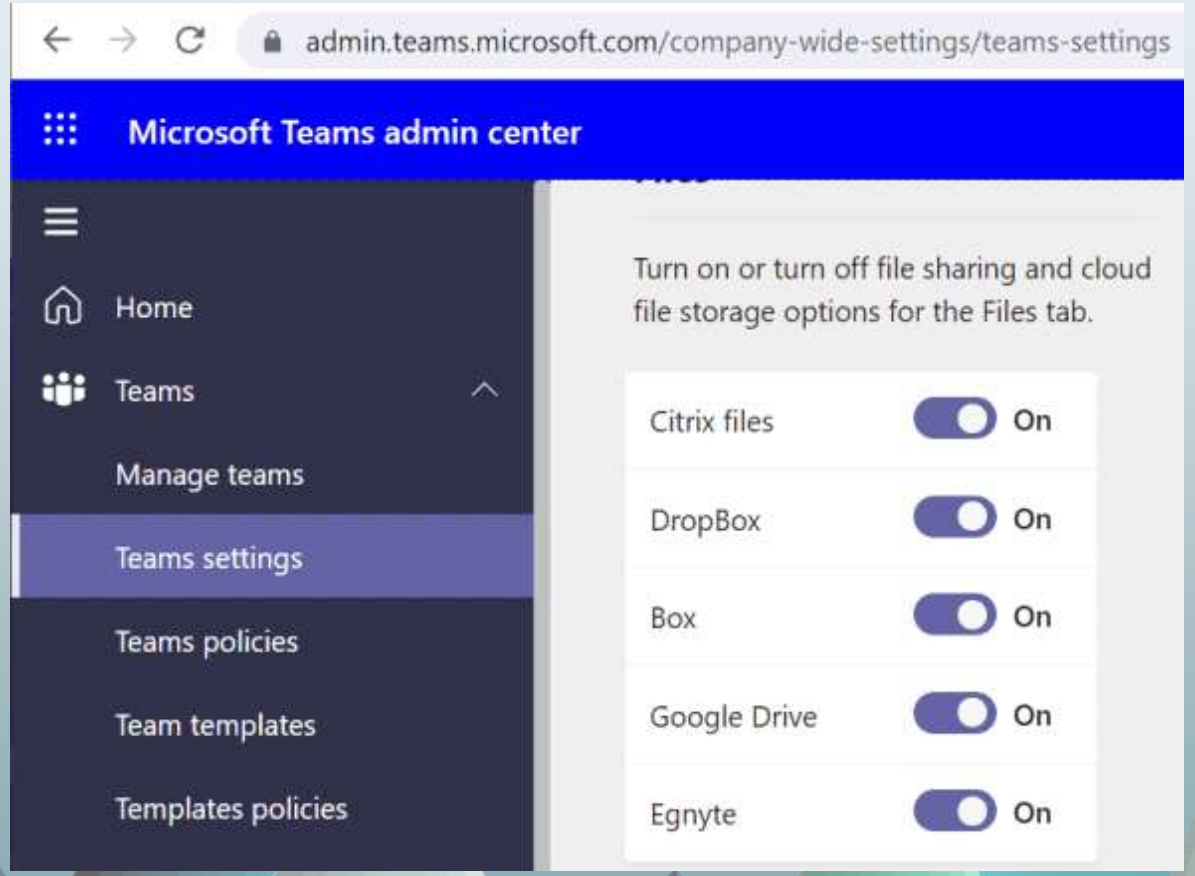
Teams: Management

- Wer darf Teams anlegen
  - Default: Jeder darf anlegen
  - Abschalten per PowerShell
- Teams Gastzugriff
- Teams Shared Channel
- Teams Life Cycle
- Teams „Führerschein“
  - Die Pflichten eines Owners



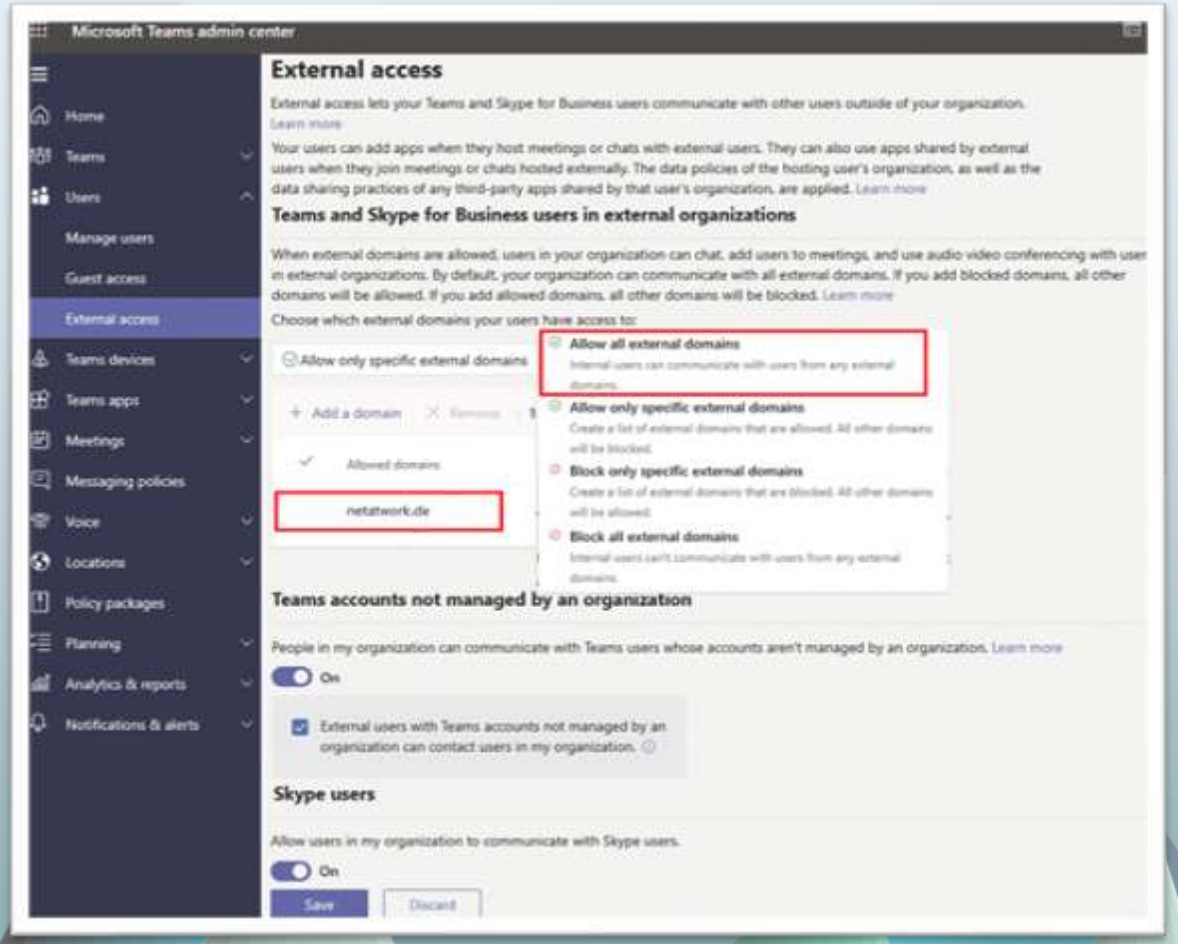
Teams Sharing: neben OneDrive

- Dropbox
- Box
- Google Drive
- …



Teams: Federation

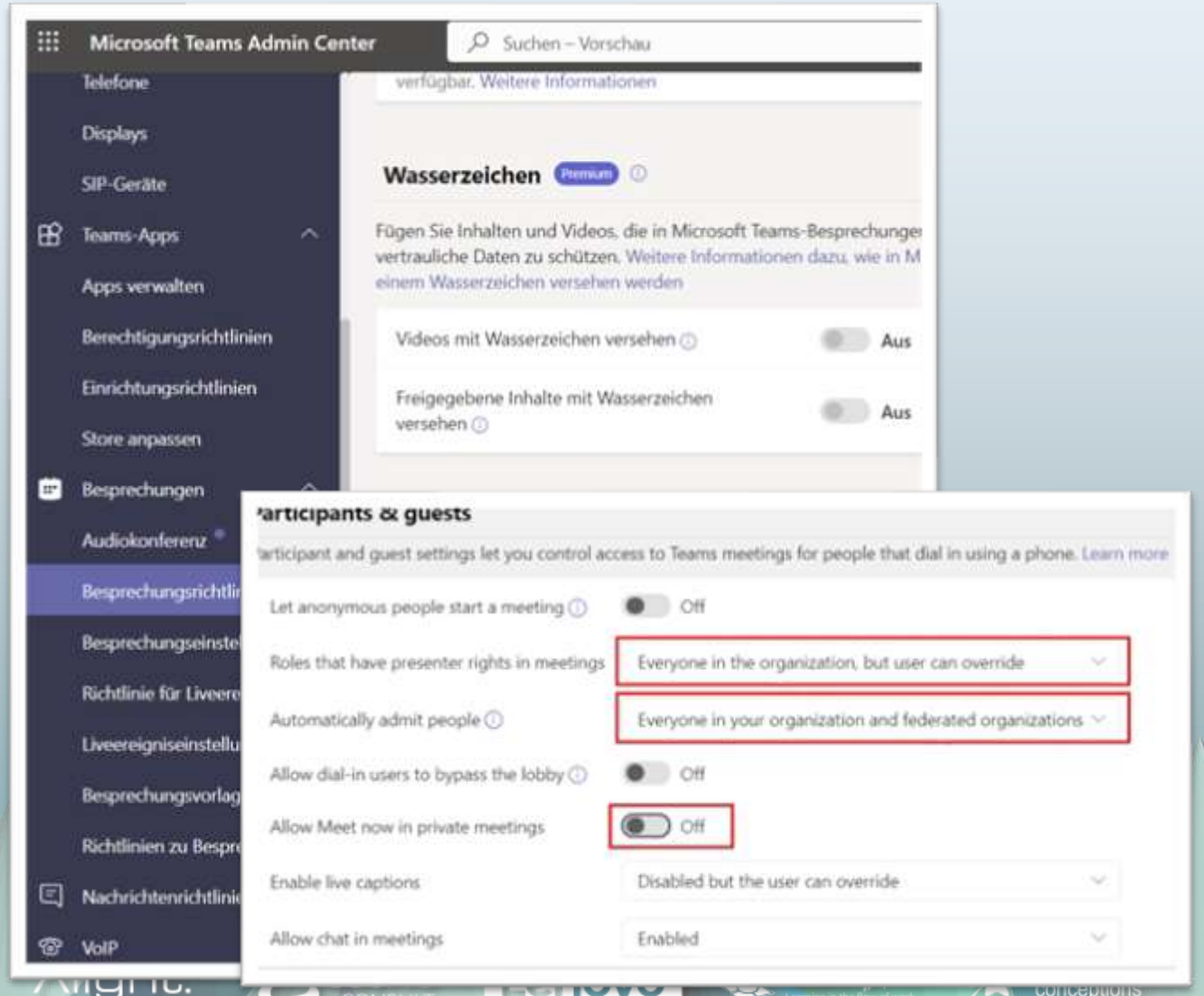
- Federation
  - Andere Tenants: Default: Allow
  - Skype: Default: Aktiv
- Risiken
  - Direkte Ansprache des Mitarbeiters
  - Direkter „Anruf“ auch ohne Headset
  - Externe Präsenzanzeige
  - SPIM, Phishing
- Empfehlung
  - Nie aktivieren ohne Userschulung
  - User Risk Awareness
  - Domain Whitelisting
  - Max 3000 Domains



Teams: Meetings

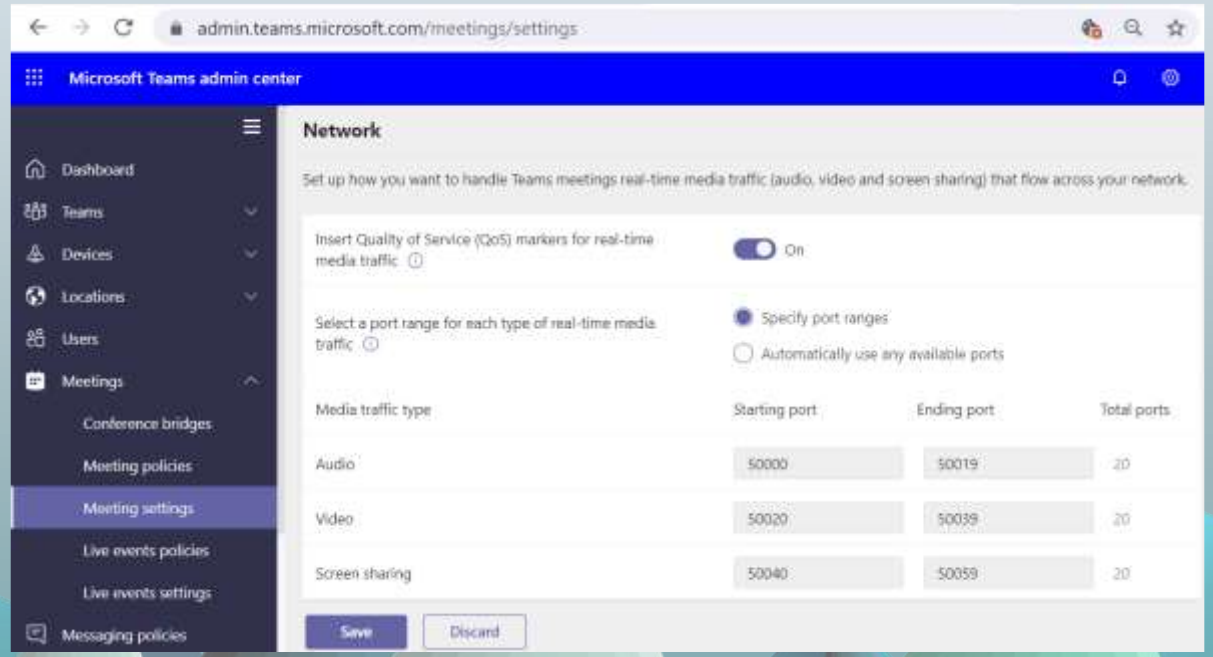
- Audio/Video
  - Default aktiv
- UDP-Portrange
  - Default nicht vorgegeben
- Aufzeichnung in der Cloud
  - Default zugelassen
- Bildschirmfreigabe
  - Default: Voller Bildschirm
  - Default: Fernsteuerung erlaubt
- Präsenter
  - Default: Jeder
- Live Events
  - Default: Jeder

Teams Führerschein !



Teams: Netzwerk

- UDP statt TCP oder HTTP
  - Paketverlust mit TCP -> Stream stoppt bis Retransmit erfolgt
  - UDP: Empfänger kann Sender Qualität per RTCP mitteilen
  - Sender kann reagieren (Mono/Stereo, 1080/720/VGA, Framerate)
- Portrange vorgeben
  - 50000-50019 Audio
  - 50020-50039 Video
  - 50040-50059 Sharing
  - Das sind „SourcePorts !)
  - Blockieren bei Split-VPN
-



Hinweis zu UDP 3478-3481 und TCP443

Firewall and proxy requirements

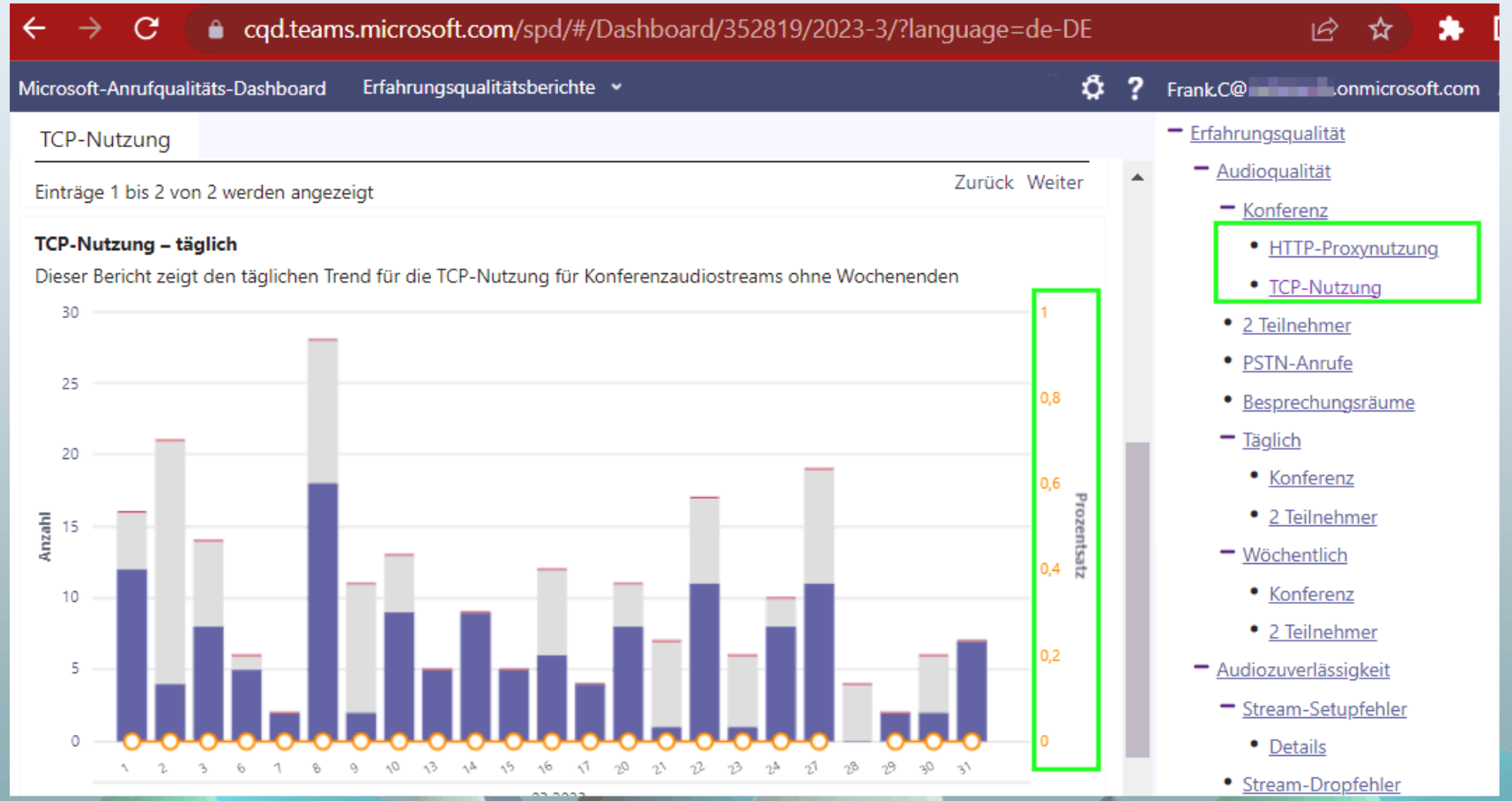
Microsoft Teams connects to Microsoft Online Services and needs internet connectivity for this. For Teams to function correctly, you must open TCP ports 80 and 443 from the clients to the internet, and UDP ports 3478 through 3481 from the clients to the internet. The TCP ports are used to connect to web-based content such as SharePoint Online, Exchange Online, and the Teams Chat services. Plug-ins and connectors also connect over these TCP ports. The four UDP ports are used for media such as audio and video, to ensure they flow correctly.

Opening these ports is essential for a reliable Teams deployment. Blocking these ports is unsupported and will have an effect on media quality.

Source: https://learn.microsoft.com/en-us/microsoftteams/3-envision-evaluate-my-environment#firewall-and-proxy-requirements

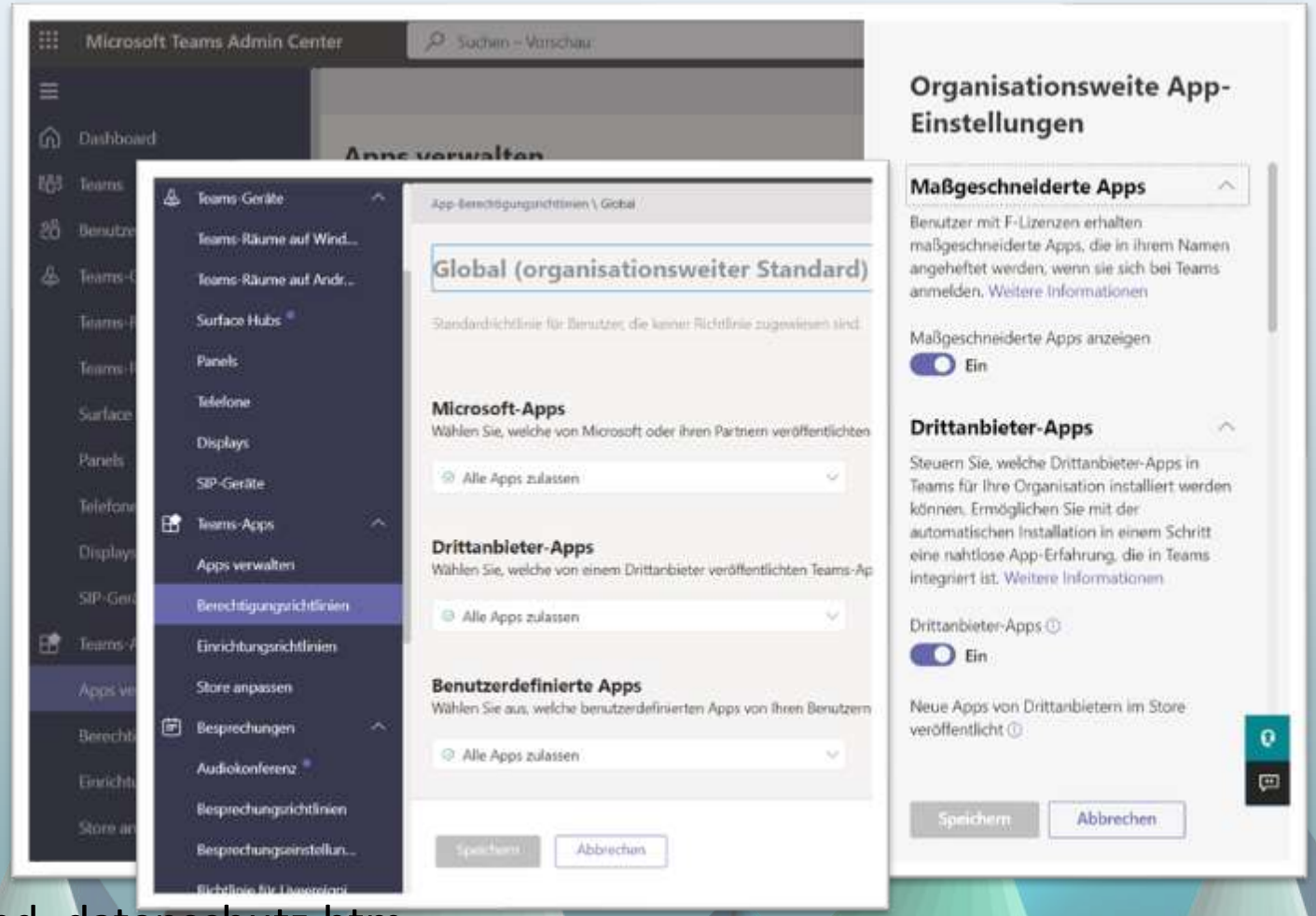
Teams CQD: Wer nutzt TCP oder gar HTTP

- PII Daten!



Teams Apps

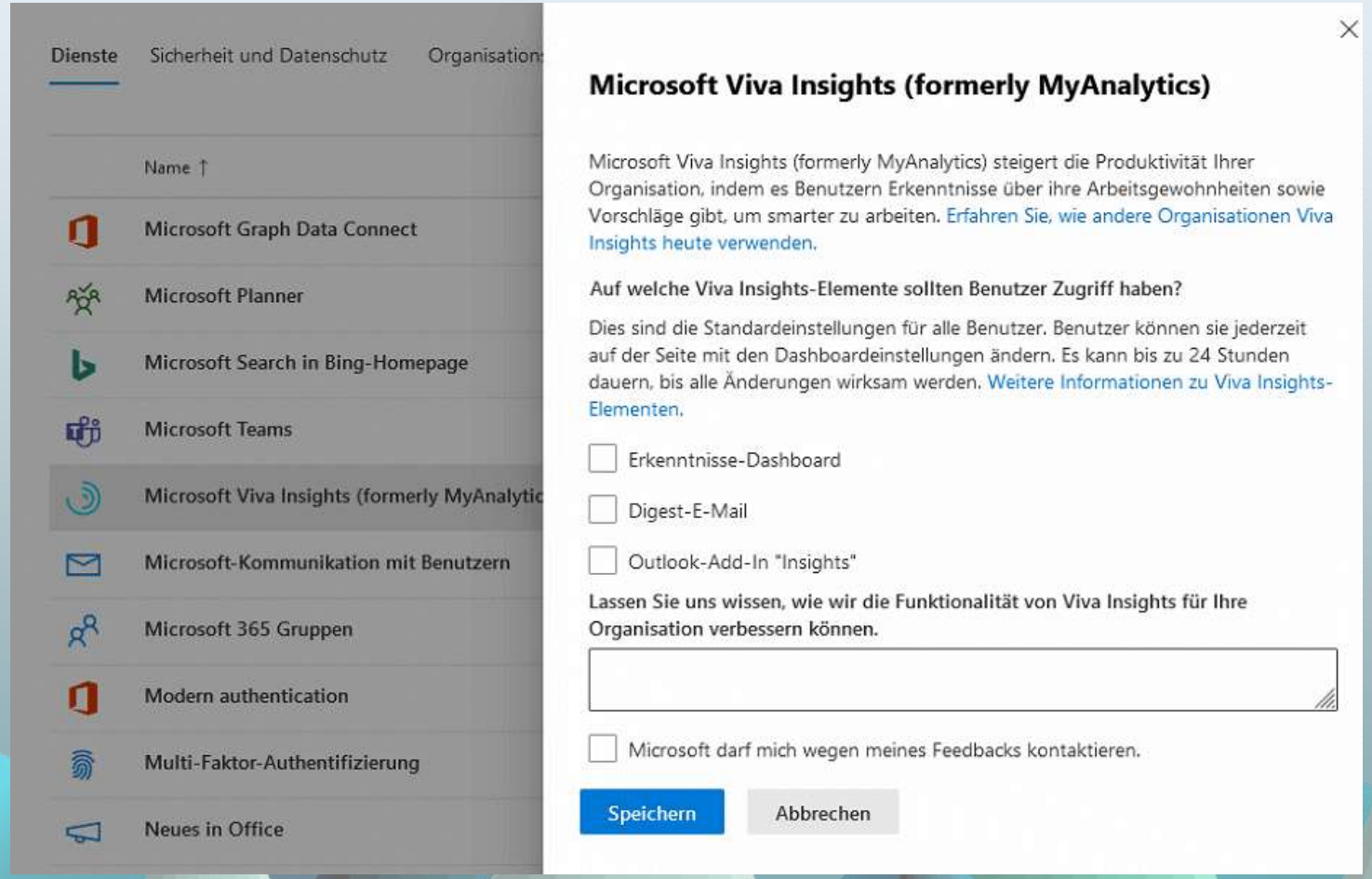
- Default
  - Alle Erlaubt
- Risiken
  - Apps tracken Aktivität (Giphy = Facebook) (Polly = extern)
  - App Consent Erteilung



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

Viva Meldungen ?

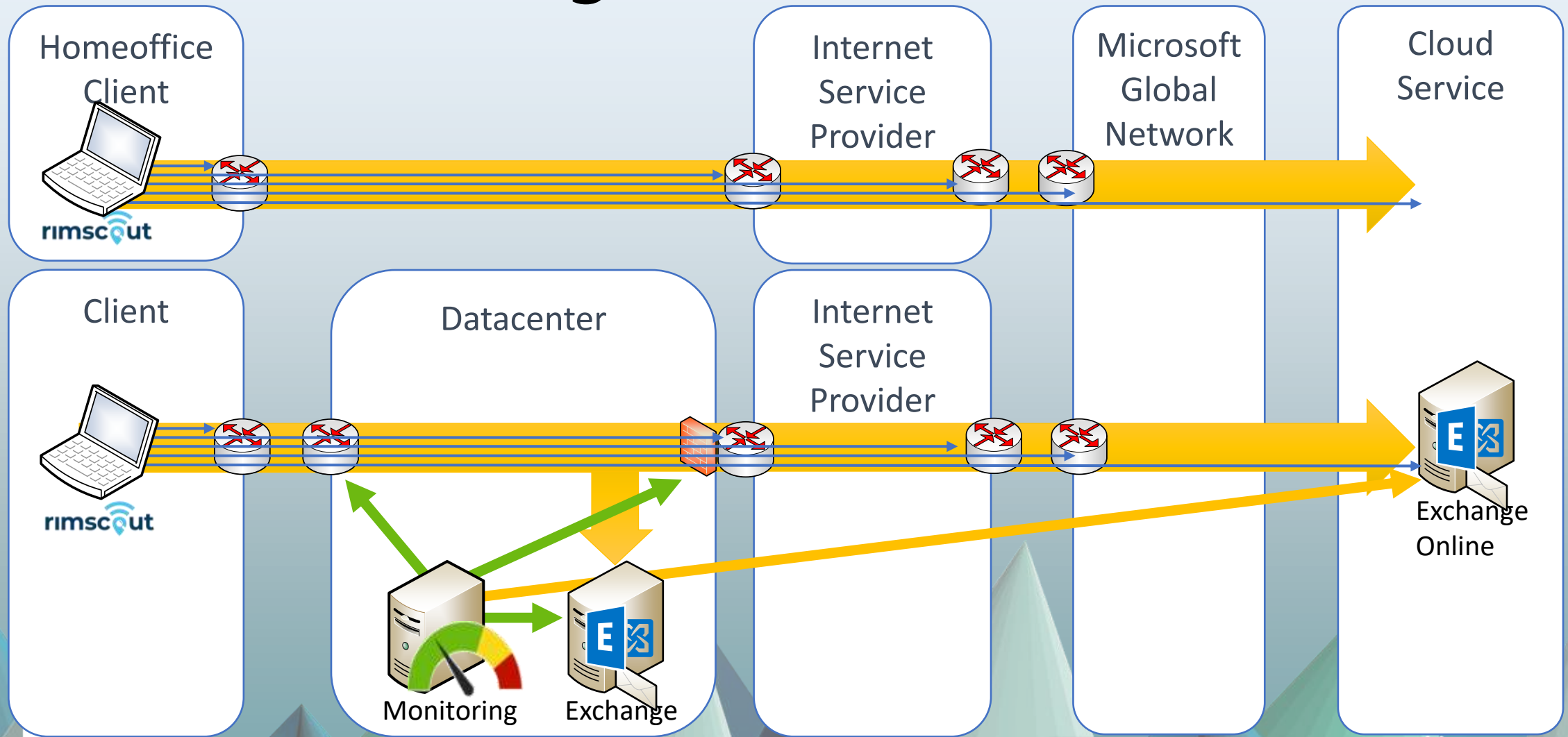
- An oder aus?



Was es sonst noch alles gibt

- Pureview -Einstellungen
- SignIn-Logs -> Sentinel wegen 30 Tage Haltezeit
- Retention, Compliance Labels –Design first
- Reporting und P1-Datenschutz
- Microsoft 365 Apps Telemetrie
- Integration Suche
- Teams QoE-Reporting
- Teams Telefonie-Verbindungsdaten
- Zukünftige Microsoft Produkte

Monitoring bisher und erweitert



Monitoring: Häufige Fehler

- Falsche Gegenstellen
  - Nur LAN, Firewall
  - Untaugliche Cloud-Endpunkte oder APIs
- Latenzzeit vs. Bandbreite
  - 80% Auslastung einer Leitung ist nicht generell schlecht
  - Wenn die Latenzzeit ausreichend niedrig ist
  - Hohe Latenzzeit bedeutet „nicht genug Bandbreite auf einer Teilstrecke“
- Zu große Messintervalle: Minuten statt Sekunden
  - Es reicht nicht aus, einmal pro Minute zu messen
  - RTP ist viel empfindlicher
  - Sekunden oder sogar mehrfach pro Sekunde
- „Durchschnittswerte“ taugen nicht
  - Wie sehen keine „Verteilung“, keine Spikes, keine Aussetzer
  - Besser: Perzentil oder Median

Exchange Online Mailbox Distribution

- Einzelne Exchange Online Mailbox

```
PS C:>Get-mailbox -resultsize 1| fl servername,database

ServerName : am0pr08mb2945
Database : EURPR08DG170-db093
```

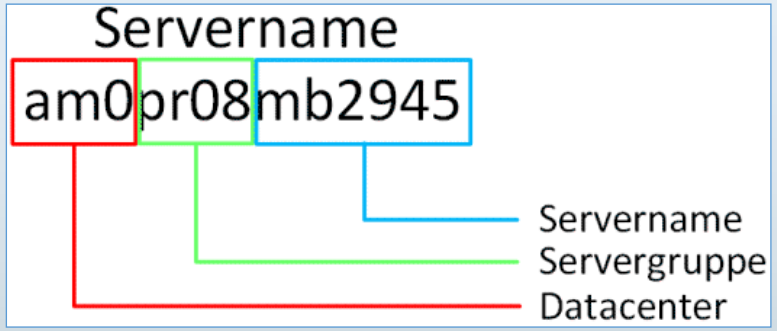
- Beispiel: Tenant mit 35000 Postfächer
- Gruppierung nach Servername: 6982 Server
- Gruppierung nach Datenbankname: 28205 DBs

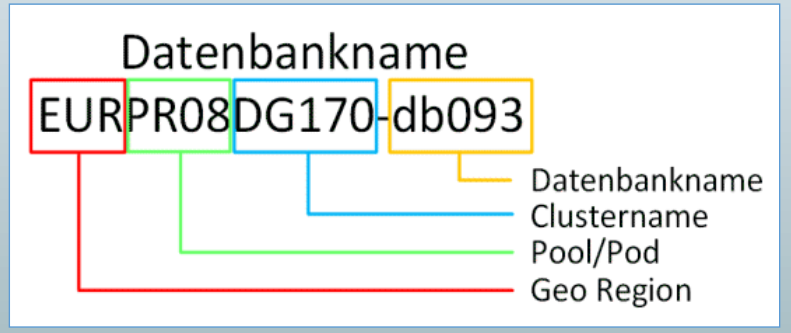
```
PS C:>($mblist.database | group -NoElement).count
28205
```

- Gruppierung nach DG : 473 DAGs (?)

```
PS C:>(($mblist.database).substring(7,5) | group -NoElement).count
473
```

- Server by Location
  - 2 Buchstaben Datacenter
  - 9 Locations and 33 Datacenters





Amsterdam!	am0			am4	am5	am6	am7	am8	am9	
??? !		as1	as2	as4				as8		
Dublin !				db3	db4	db5	db6	db7	db8	db9	dba	dbb
??? !	du0		du2							
Gävle !		gv1	gv2							gvx
Helsinki !		he1								
Paris !				pa4					pav	paw	pax	paz
??? !		ve1								
Wien !		vi1								

Infinity 365 Conference

Q&A

Ich freue mich auf Feedback!

Scan mich!

frank.carius@netatwork.de

https://forms.office.com/e/9k4NqhU2zd

Infinity 365 Conference

Vielen Dank!