

TeamsCommunityDay

Microsoft Teams Community Conference

teamscommunityday.de

[@TeamsDay](https://twitter.com/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](https://registration.teamscommunityday.de)

teamscommunityday.de | @TeamsDay

Central sponsors



INTELLITY



NOOVIC





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



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

Home > msxfaqdev

msxfaqdev | Properties ...
Azure Active Directory

Save Discard | Got feedback?

Overview
Preview features
Diagnose

Manage
User settings
Properties
Security
Roles and adminis
Administrative uni...

Tenant properties

Name *
msxfaqdev ✓

Country or region
Germany

Location
EU Model Clause compliant datacenters

Notification language
English

Organization information

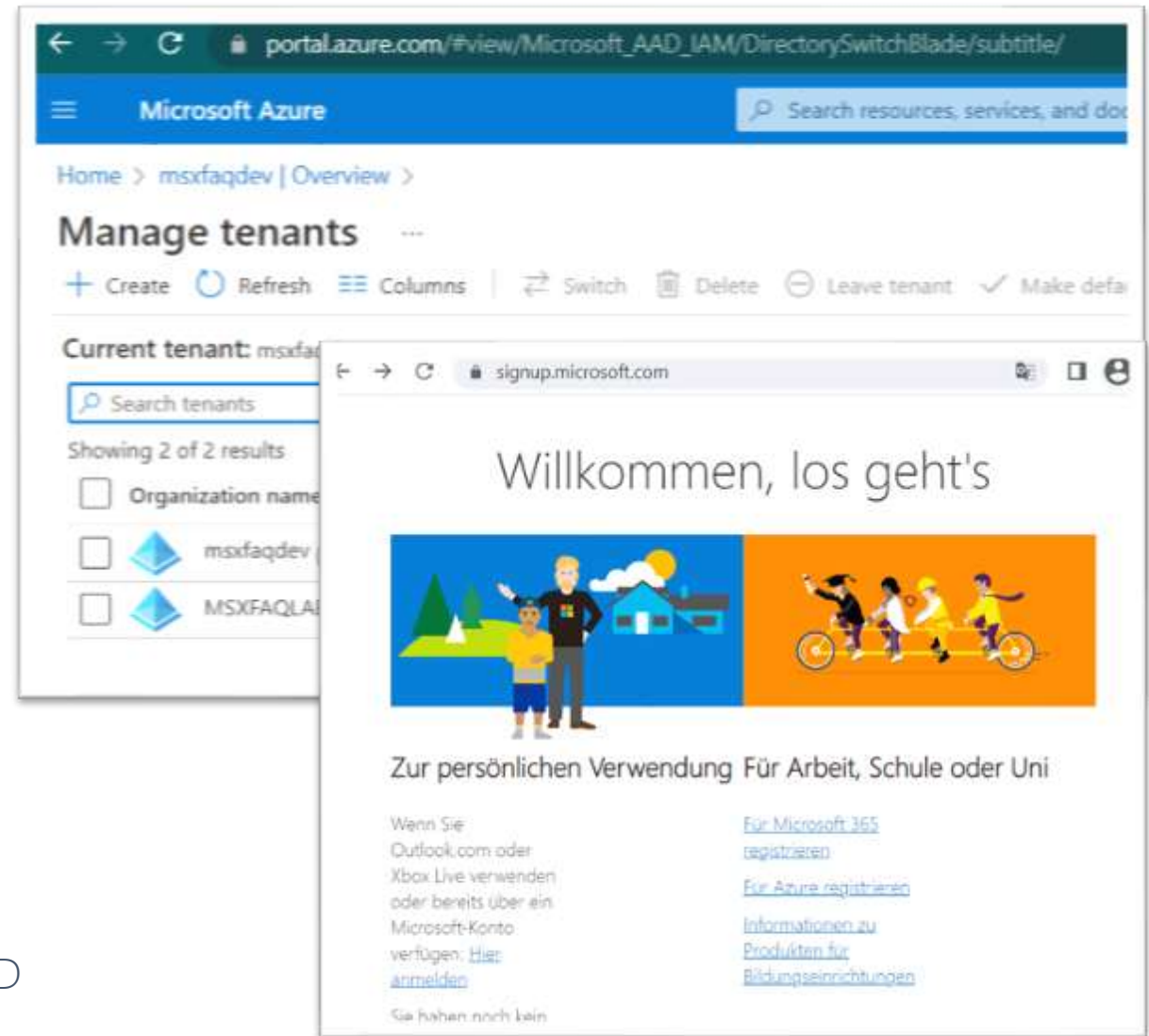
Country or region
Germany

Phone



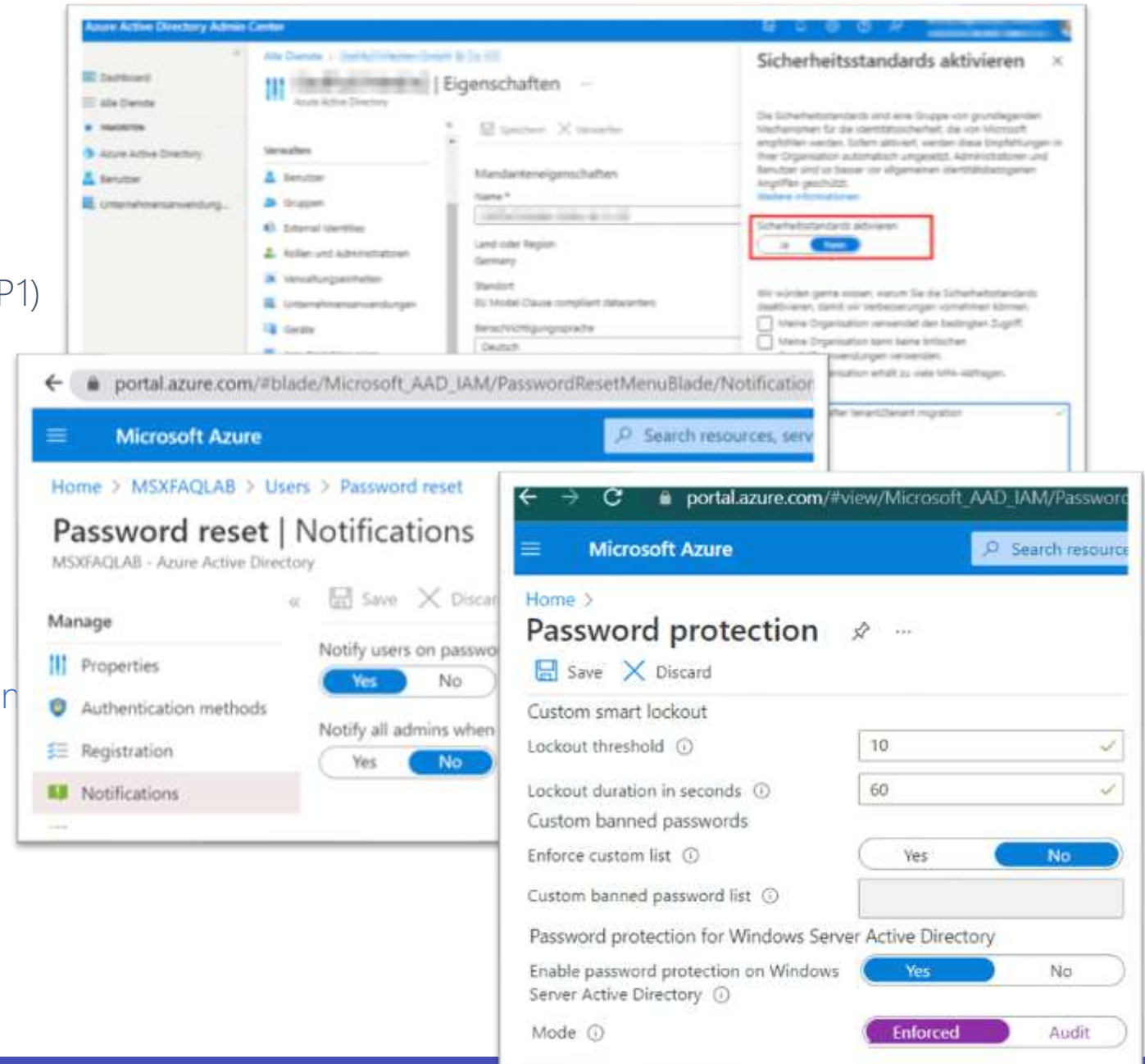
Tenant beantragen

- 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



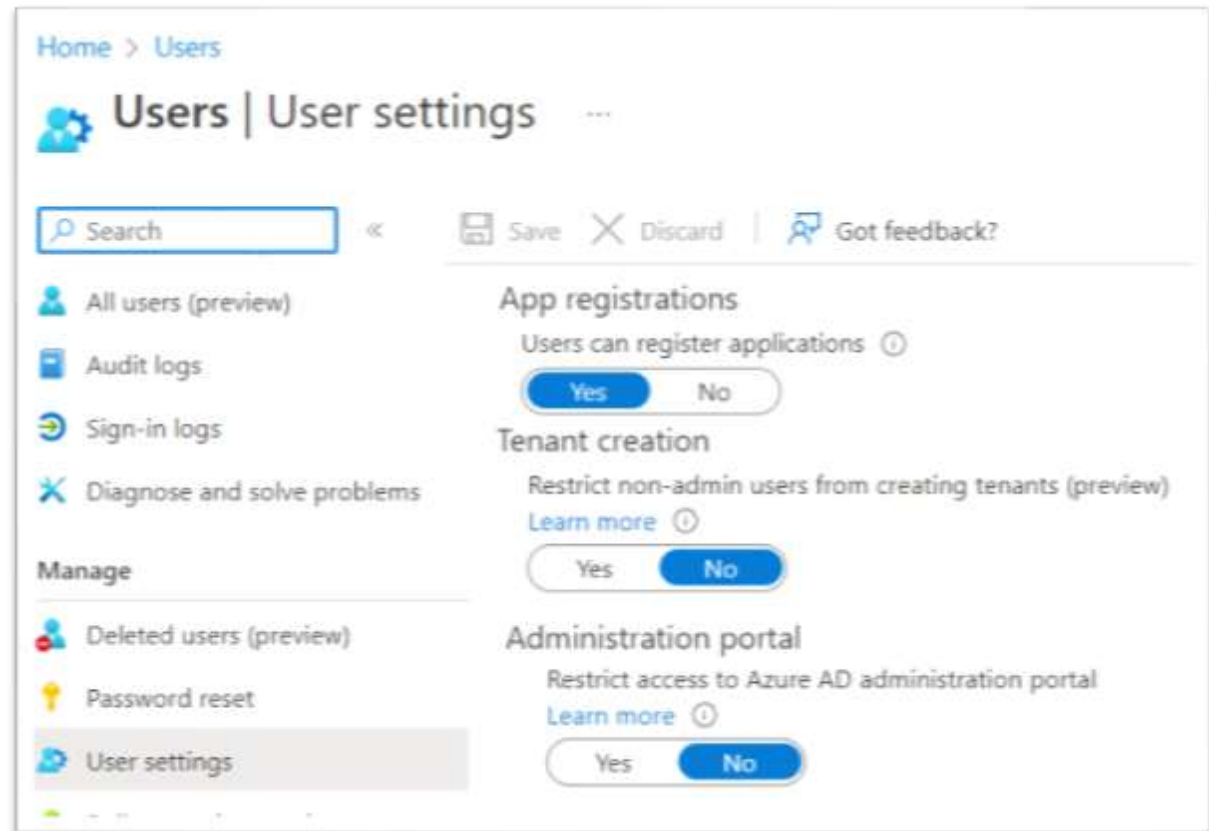
Admin-Konten

- 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 AD Sync-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

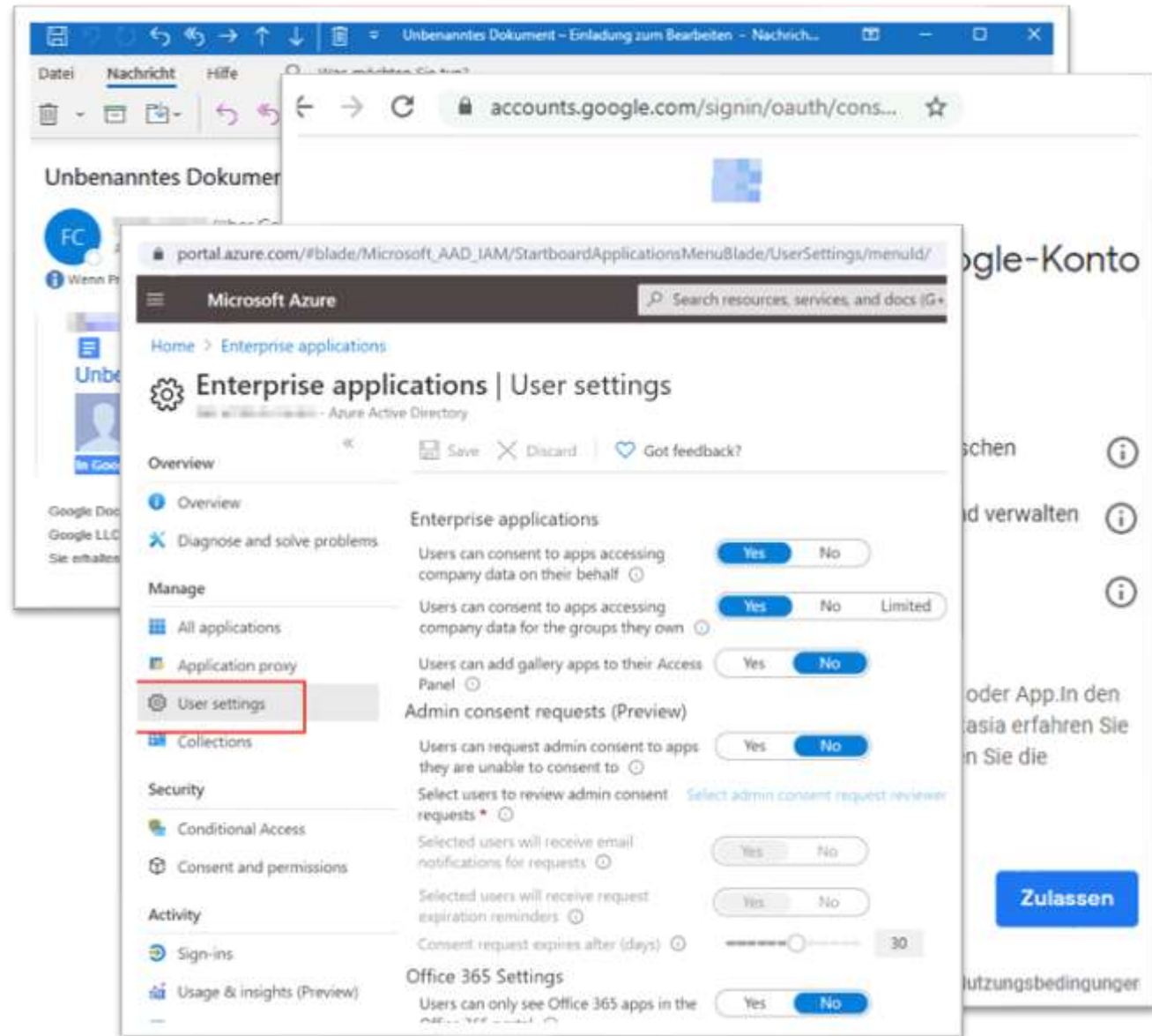
The image displays two screenshots from the Microsoft Azure portal. The top screenshot shows the 'Devices | Device settings' page for an Azure Active Directory tenant. It features a left-hand navigation pane with options like 'Overview', 'All devices', 'Device settings', 'Enterprise State Re', 'BitLocker keys (Pre)', and 'Diagnose and solv'. The main content area is titled 'Devices | Device settings' and includes a 'Save' button, a 'Discard' button, and a 'Got feedback?' link. Below this, there are three settings sections: 'Users may join devices to Azure AD' with a radio button set to 'All', 'Users may register their devices with Azure AD' with a radio button set to 'None', and 'Require Multi-Factor Authentication to register or join devices with Azure AD' with a radio button set to 'No'. A warning icon and the text 'Maximum' are visible at the bottom of this section.

The bottom screenshot shows the 'Device Administrators | Description' page. It includes a 'Diagnose' button and a 'Summary' section. The summary text reads: 'Name: Azure AD Joined Device Local Administrator', 'Description: Users with this role become local machine administrators on all Windows 10 devices that are joined to Azure Active Directory. They do not have the ability to manage devices objects in Azure Active Directory.' Below the summary, there are sections for 'Manage', 'Assignments', 'Description', and 'Activity'.



„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!

The screenshot shows the Azure portal interface for the 'Azure DevOps Administrator' role. The breadcrumb navigation is 'Home > msxfqdev | Roles and administrators > Roles and administrators | All roles > Azure DevOps Administrator | Description'. The page title is 'Azure DevOps Administrator | Description' with a sub-header 'Privileged Identity Management | Azure AD roles'. The left sidebar contains a 'Manage' section with options: 'Assignments', 'Description' (selected), and 'Role settings'. The main content area is titled 'Summary' and contains the following information:

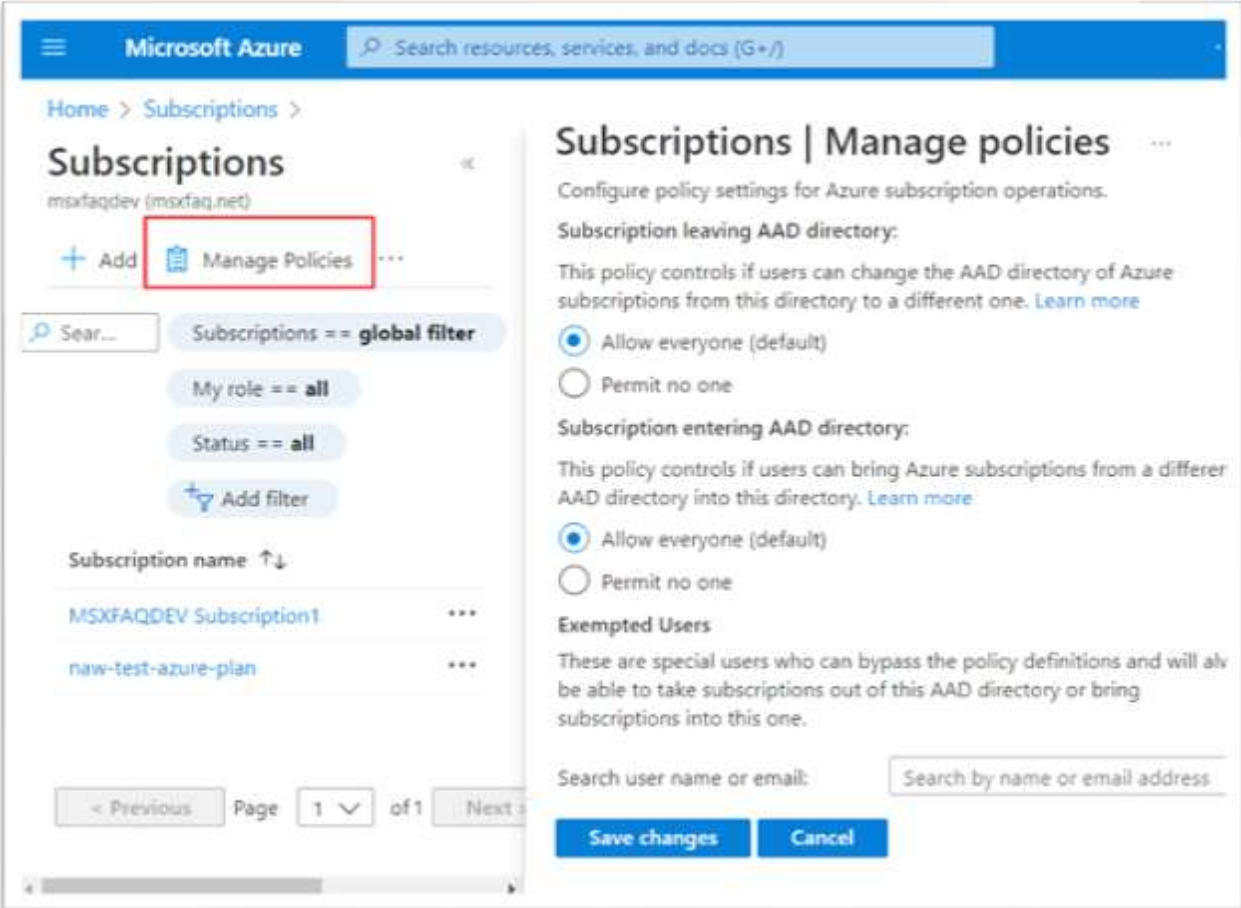
- Name: Azure DevOps Administrator
- Description: Users with this role can manage the Azure DevOps policy to restrict new Azure DevOps organization creation to a set of configurable users/AAD groups. Users in this role can manage this policy through any Azure DevOps organization that is backed by the company's Azure AD.

Below the description, there are sections for 'Global notifications', 'Usage', 'Extensions' (with 'Azure Active Directory' highlighted in a red box), 'Security', 'Policies', 'Permissions', 'Boards', 'Pipelines', 'Agent pools', 'Settings', 'Deployment pools', 'Parallel jobs', and 'OAuth configurations'. The 'Policies' section shows a toggle for 'Restricting organization creation' which is currently turned off (indicated by a red box around the toggle). Below this, there is an 'Allow list' section with a button to 'Add AAD user or group' and a 'Display error message' section with a button to 'Edit display message'.



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

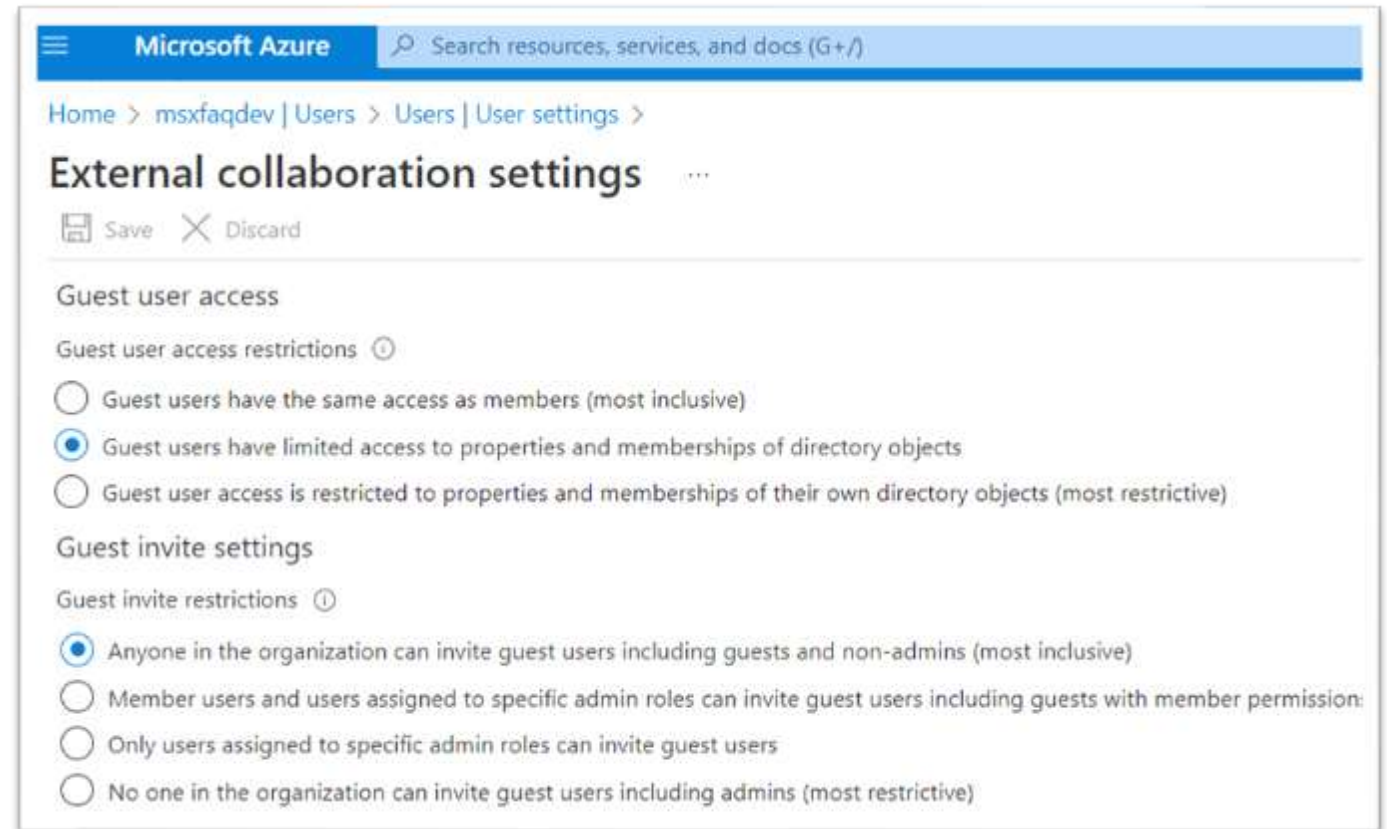


The screenshot shows the Microsoft Azure portal interface. At the top, there is a search bar and navigation links. The main content area is titled 'Subscriptions | Manage policies'. On the left, there is a list of subscriptions with a search bar and filter buttons. The 'Manage Policies' button is highlighted with a red box. The right side of the page shows the policy configuration for 'Subscription leaving AAD directory' and 'Subscription entering AAD directory'. Both policies are set to 'Allow everyone (default)'. There is also a section for 'Exempted Users' with a search field and 'Save changes' and 'Cancel' buttons.



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

Microsoft Azure | Search resources, services, and docs (G+)

Home > msxfaqdev | External Identities > External Identities

External Identities | Cross-tenant access settings

msxfaqdev - Azure Active Directory

Search

Organizational settings | **Default settings** | Microsoft cloud settings

Default settings apply to all external Azure AD organizations not listed on the organizational settings tab. These default settings can be modified but not deleted.

Inbound access settings | Edit inbound defaults

Type	Applies to	Status
B2B collaboration	External users and groups	All allowed
B2B collaboration	Applications	All allowed
B2B direct connect	External users and groups	All blocked
B2B direct connect	Applications	All blocked
Trust settings	N/A	Disabled

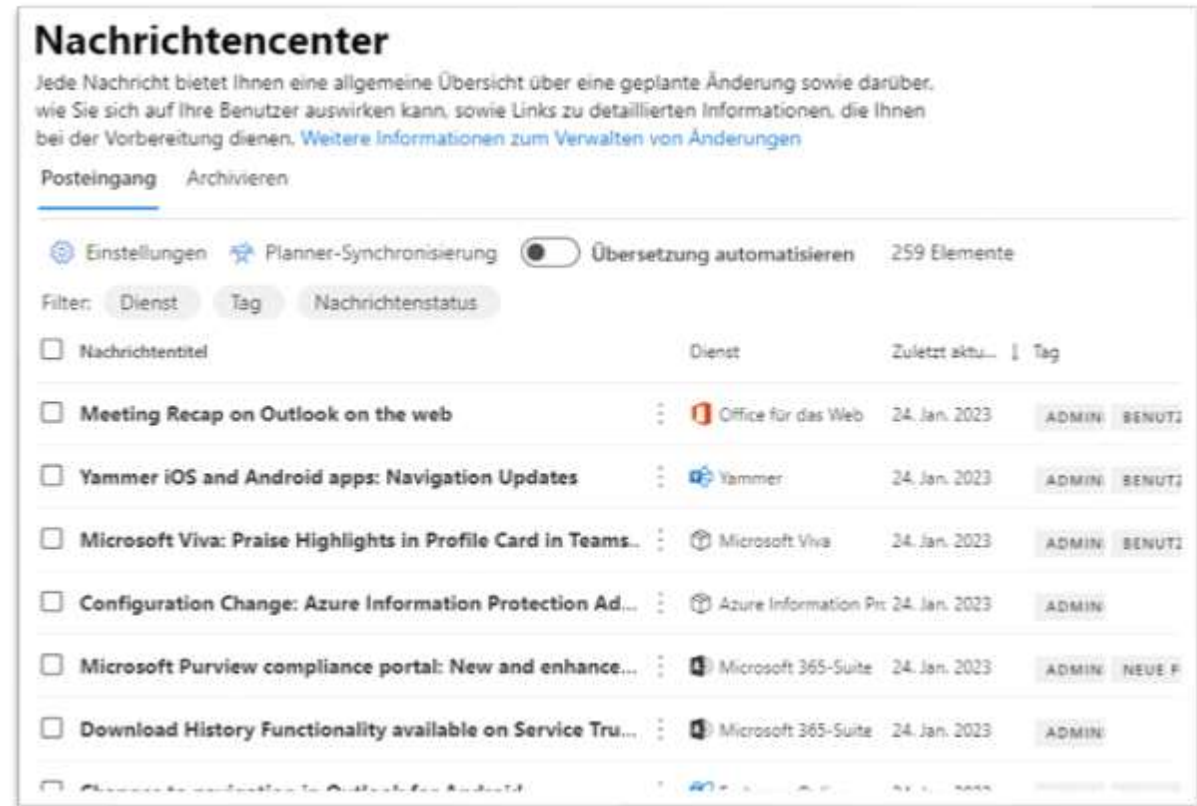
Outbound access settings | Edit outbound defaults

Type	Applies to	Status
B2B collaboration	Users and groups	All allowed
B2B collaboration	External applications	All allowed
B2B direct connect	Users and groups	All blocked
B2B direct connect	External applications	All blocked



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

Microsoft 365 apps-Installationsoptionen

Featureupdates Installation

Wählen Sie aus, wie oft Ihre Benutzer Funktionsupdates für Microsoft 365 apps auf Geräten mit Windows installieren sollen. Ihre Auswahl gilt für neue und vorhandene Installationen. [Weitere Informationen zum Auswählen eines Updatekanals](#)

- Sobald sie bereit sind (aktueller Kanal, empfohlen)** ⓘ
Geräte bleiben bis zum nächsten Update in Version 2212 erhalten.
- Einmal im Monat (Monatlicher Enterprise-Kanal)** ⓘ
Geräte werden bis zu
- Alle sechs Monate (Halbjährlicher Enterprise-Kanal)** ⓘ
Geräte werden bis zu

Microsoft 365 apps-Installationsoptionen

Featureupdates Installation

Microsoft Apps auswählen, die Benutzer auf Ihren eigenen Geräten installieren können

Microsoft 365-Apps, die Benutzer installieren können

Wählen Sie aus, ob Ihre Benutzer Microsoft 365-Apps auf ihren eigenen Geräten installieren können. Wenn Sie dies nicht zulassen, können Sie stattdessen [Apps manuell für Benutzer bereitstellen](#) verwenden.

Apps für Windows und mobile Geräte

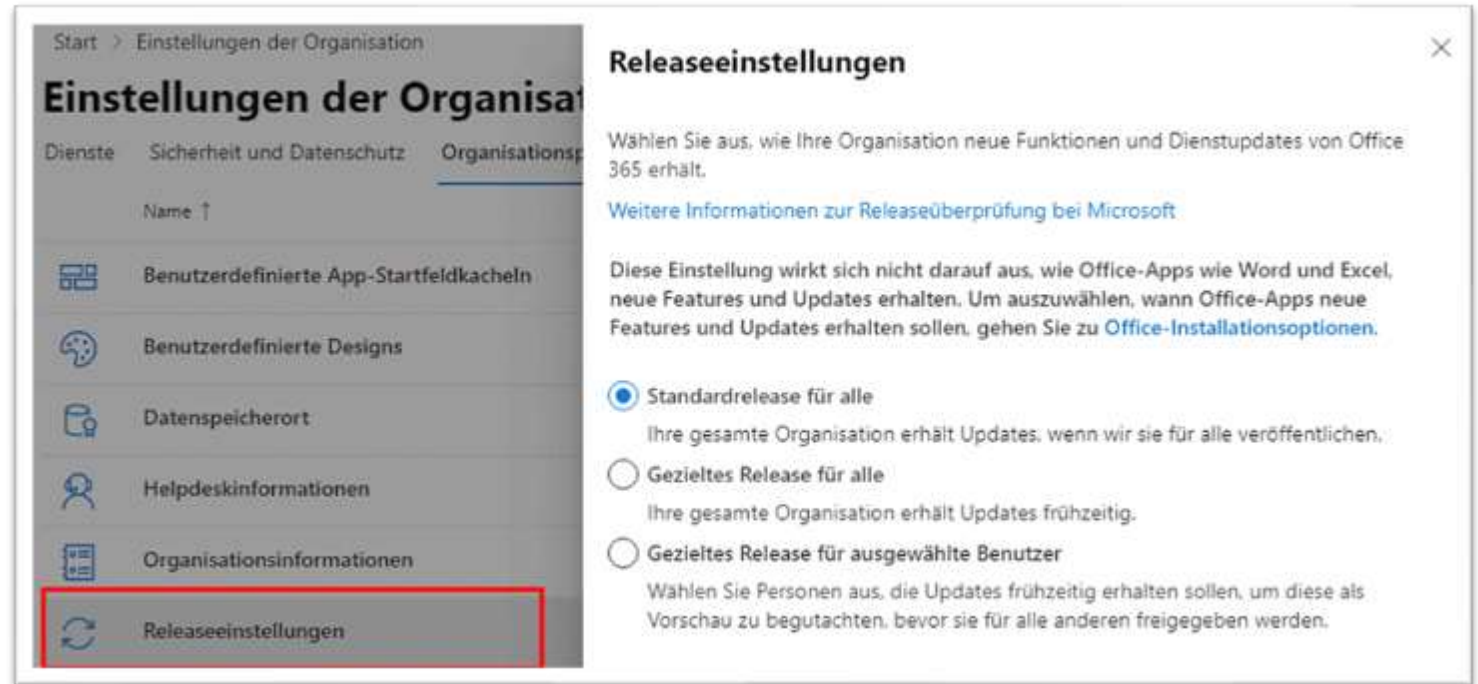
- Office (enthält Skype for Business)
- Skype for Business (eigenständig)

Apps für Mac

- Office
- Skype for Business (X El Capitan 10.11 oder höher)



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.

Apps und Dienste im Besitz des Benutzers

Wählen Sie aus, ob Benutzer in Ihrer Organisation auf die Office Store zugreifen und Microsoft 365 Testkonten erstellen können.

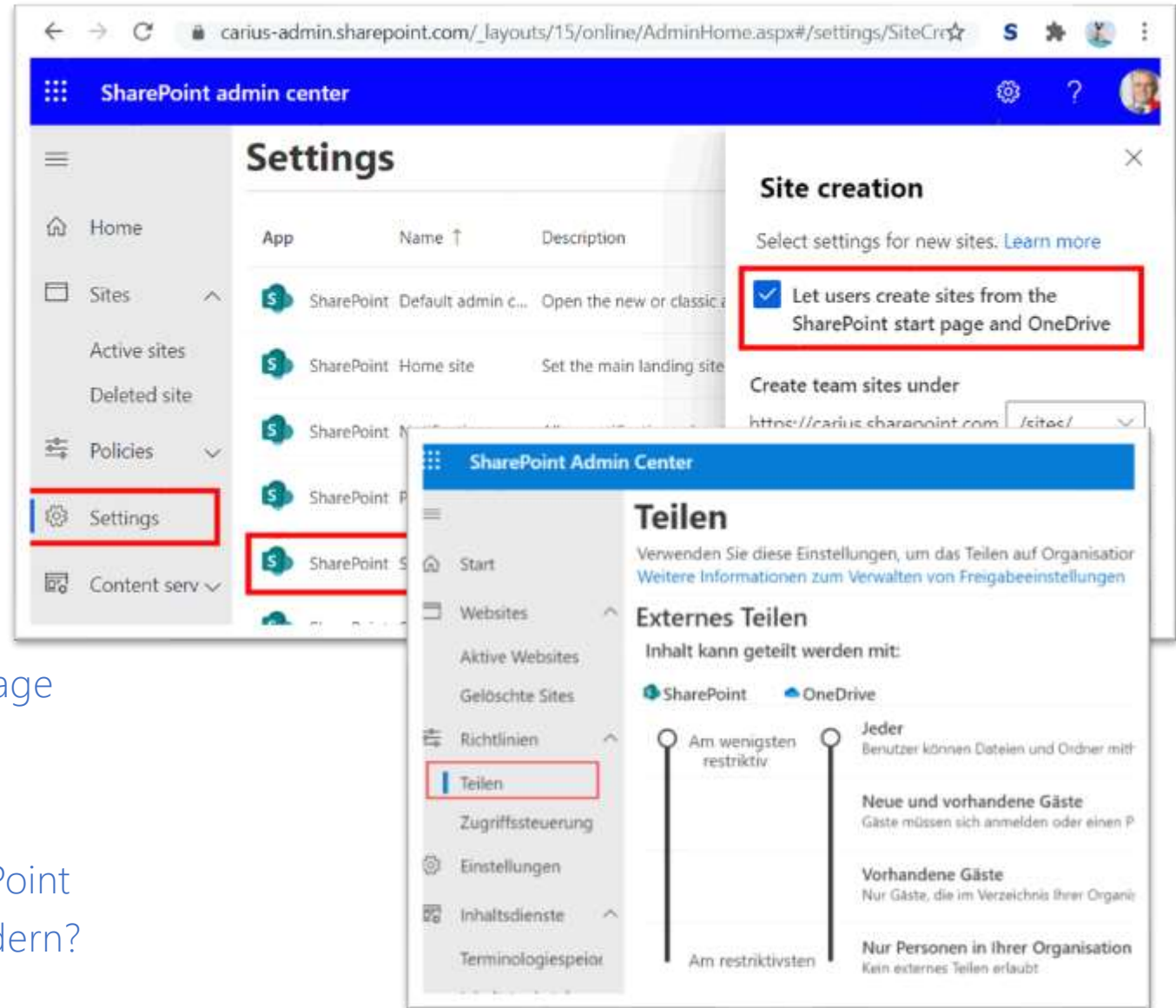
- Benutzern den Zugriff auf den Office Store gestatten
Ermöglichen Sie Personen in Ihrer Organisation, mit ihrem Arbeitskonto auf Office Store zuzugreifen. Der Office Store bietet Zugriff auf Apps, die nicht von Microsoft zusammengestellt oder verwaltet werden.
- Lassen Sie Benutzer Probeläufe im Namen Ihrer Organisation starten
Erlauben Sie Personen in Ihrer Organisation, Testabonnements für Apps und Dienste zu starten, die Tests unterstützen. Admins verwalten die Lizenzen für diese Testversionen auf die gleiche Weise wie andere Lizenzen in Ihrer Organisation. Nur Administratoren können diese Testversionen zu kostenpflichtigen Abonnements aktualisieren, sodass sie keinen Einfluss auf Ihre Abrechnung haben.
- Zulassen, dass Benutzer Lizenzen bei der ersten Anmeldung automatisch anfordern

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



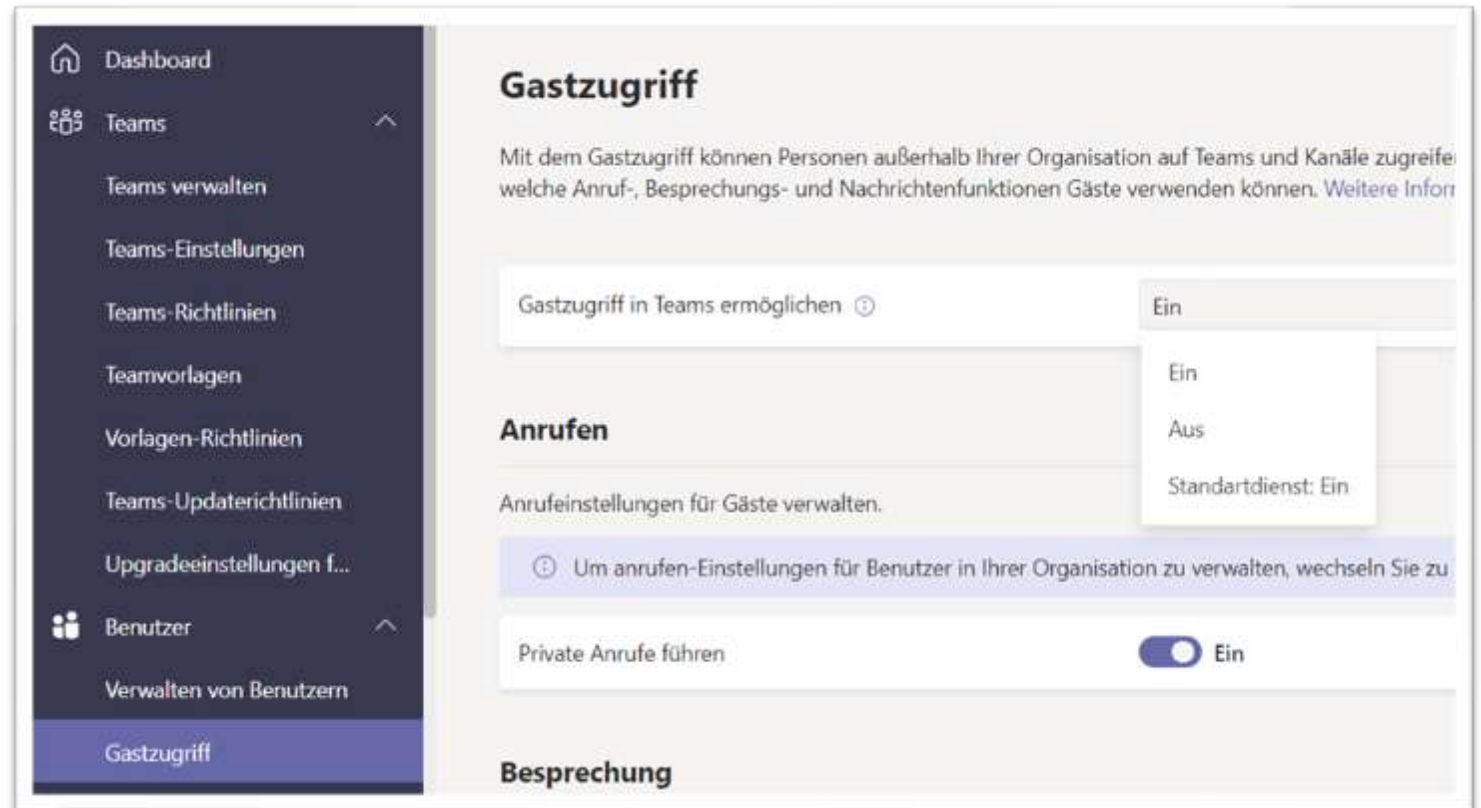
SharePoint

- 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?



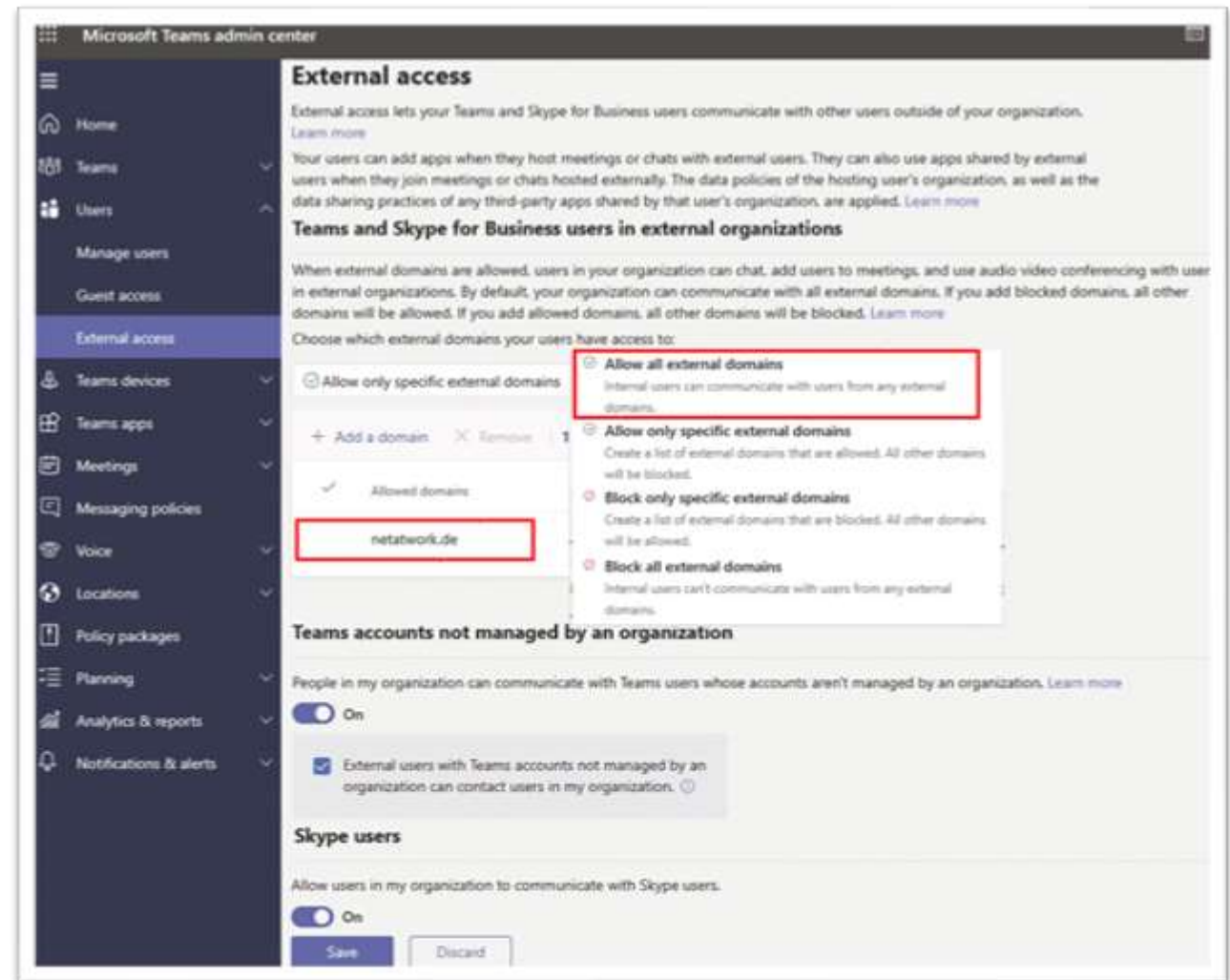
Teams 1

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



Teams 2: Federation

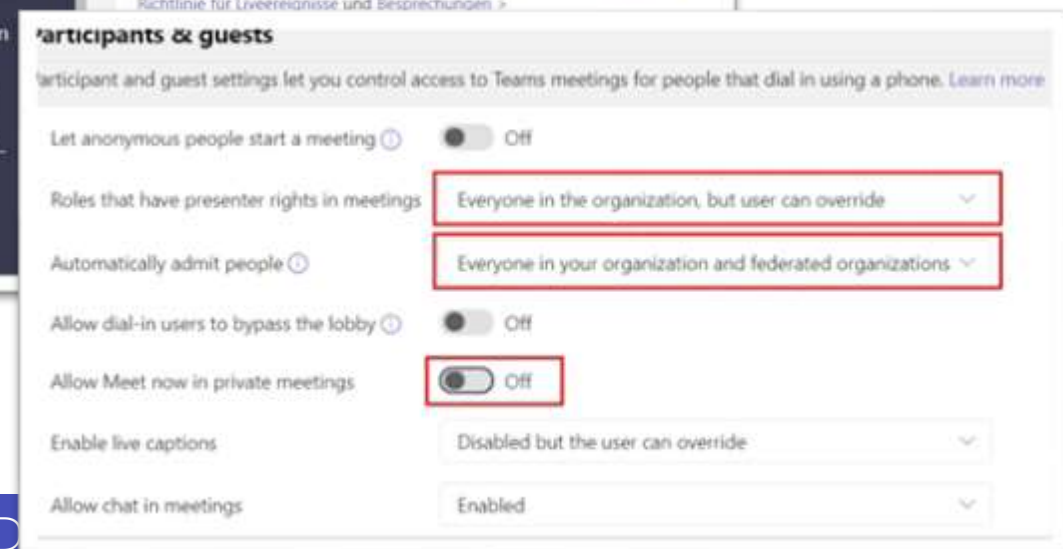
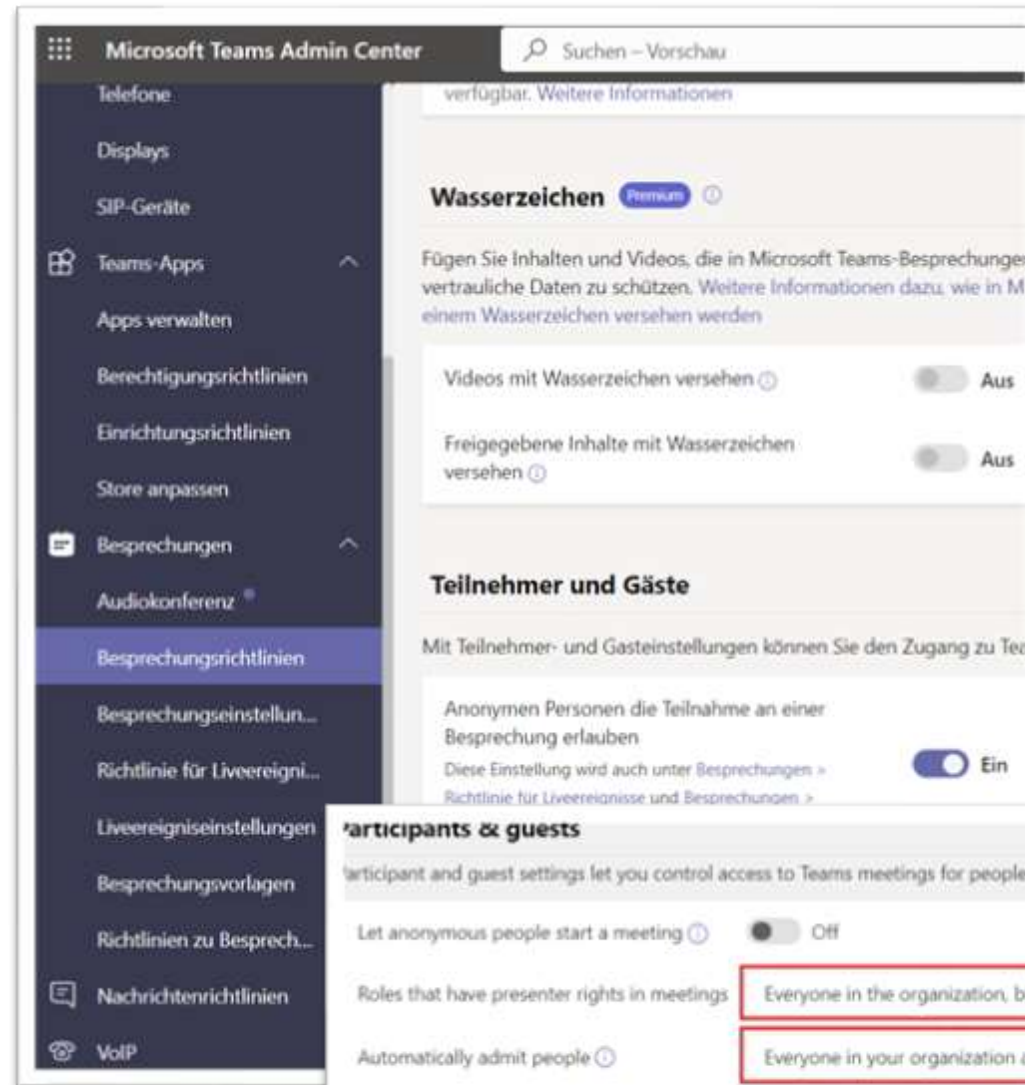
- Federation mit anderen Teams
 - Default: ANY ALLOW
- Federation mit Skype
 - Default: Aktiv
- Risiken
 - Direkte Ansprache des Mitarbeiters
 - Direkter „Anruf“ auch ohne Headset
 - Externe Präsenzanzeige
 - SPIM
 - Phishing
- Empfehlung
 - Nie aktivieren ohne Userschulung
 - User Risk Awareness
 -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



Teams: Meetings

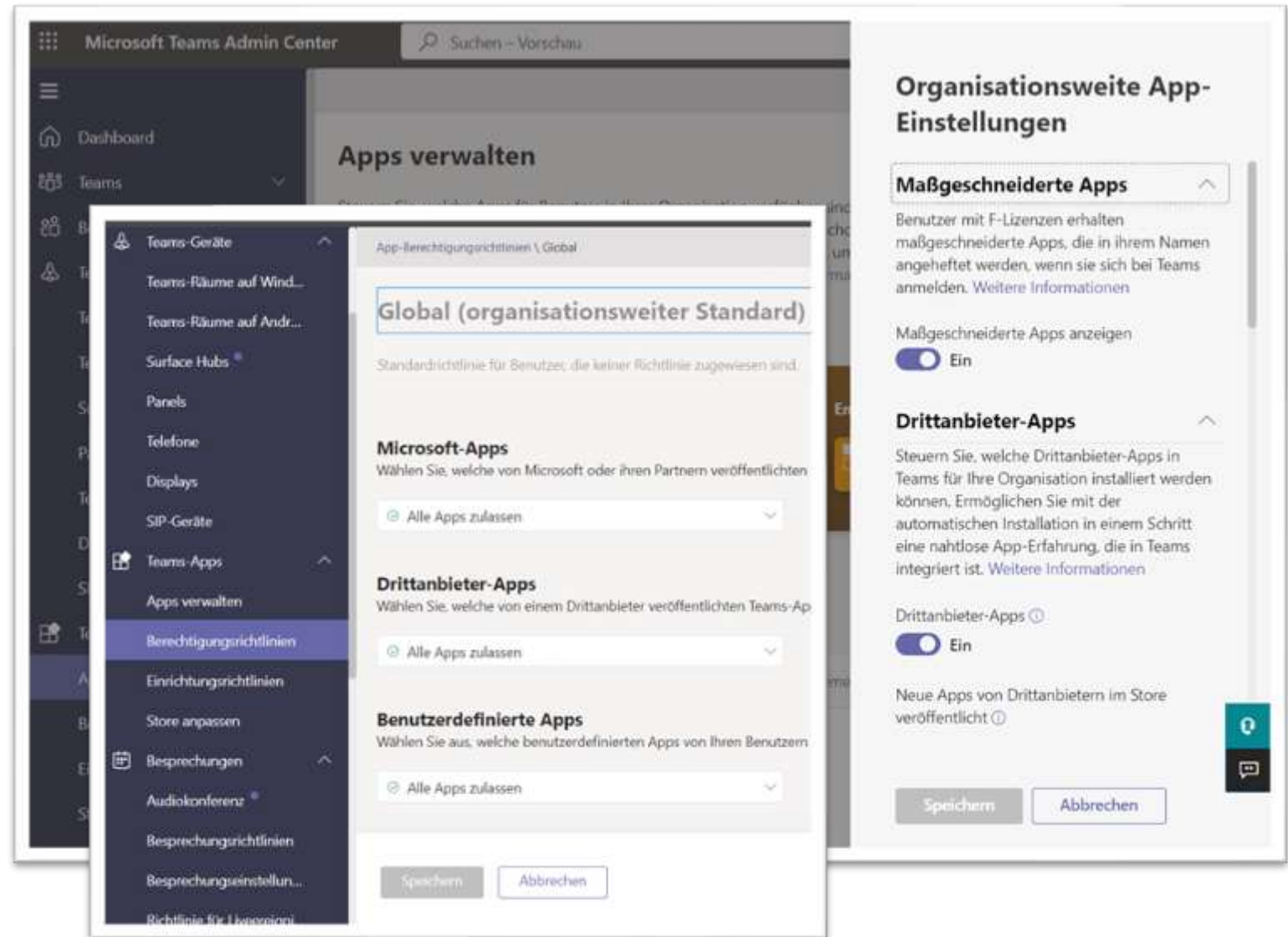
- Audio/Video
 - Default aktiv
- UDP-Portrange
 - Default nicht vorgegeben
- Aufzeichnung in der Cloud
 - Default zugelassen
- Bildschirmfreigabe
 - Default: Voller Bildschirm
 - Default: Fernsteuerung erlaubt
- Präsenter
 - Default: Jeder
- Live Events
 - Default: Jeder

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/>