



Microsoft Entra ID

Der praktische Leitfaden für Administratoren

- Benutzer- und Gäste-Management konfigurieren
- Zugriffsverwaltungen verstehen und definieren
- Das Entra ID härten und absichern



Über den Autor

Aaron Siller

Als ich 2014 als IT-Dienstleister startete, stand ich vor denselben Herausforderungen, mit denen heute viele meiner Kunden zu mir kommen: Komplexe Microsoft-Systeme, ständig neue Security-Anforderungen und nie genug Zeit, um alles richtig zu konfigurieren.

Was als klassische IT-Beratung begann, entwickelte sich schnell zu einer klaren Mission: **Microsoft 365**

Umgebungen sicherer machen, ohne dass Admins dafür Wochenenden opfern müssen.



Heute werde ich von führenden Instituten wie der Heise Academy und Golem Karrierewelt als Trainer für Microsoft 365 Security eingesetzt. Meine Expertise bestätigt sich in der Zusammenarbeit mit Unternehmen vom handwerklichen Mittelstand bis hin zu internationalen Konzernen. Schau Dir gerne meine Referenzen auf meiner Website an.

 E-MAIL aaron@siller.consulting

 WEBSITE siller.consulting

 LINKEDIN [Aaron-Siller](https://www.linkedin.com/in/aaron-siller/)

 YOUTUBE [Aaron-Siller-YT](https://www.youtube.com/c/Aaron-Siller-YT)

Inhaltsverzeichnis

Einleitung	6
Kapitel 1: Grundlagen und Ausgangslage – Aufbau einer hybriden Identitätsinfrastruktur	7
Kapitel 2: Synchronisierungsserver, Staging und Fallback-Konzepte	9
Kapitel 3: Vorbereitung des lokalen Verzeichnisses und Identitätsbereinigung.....	10
Kapitel 4: Standardkonten, Namenskonventionen und Absicherung administrativer Benutzer..	11
Checkliste: Sicherer Breaking Glass Account	13
Breaking Glass Accounts – Früher vs. Heute.....	14
Best Practices für administrative Konten in Microsoft Entra ID.....	15
Kapitel 5: Konsolidierung und Struktur – Herausforderungen bei hybriden Identitäten	16
Kapitel 6: Staging Server und Stammdatenpflege – Grundlagen für eine stabile Synchronisierung	17
Kapitel 7: Verlässlichkeit von Entra ID Connect und Rolle der Microsoft 365 Gruppen	18
Kapitel 8: Passwort-Hash-Synchronisierung und Lizenzverwaltung in Entra ID.....	20
Microsoft 365 Lizenzübersicht (Auswahl)	22
Beispielhafte Conditional Access Richtlinien	23
Kapitel 9: Passthrough-Authentifizierung als moderne Alternative zum klassischen SSO	24
Kapitel 10: Föderierte Authentifizierung – Active Directory Federation Services (AD FS)	26
Vergleichstabelle: Authentifizierungsmodelle in Entra ID	28
Kapitel 11: Architektur und Funktionsweise von Entra ID Connect.....	29
Kapitel 12: Nützliche Ressourcen und Lizenzübersichten für Entra ID	30
Kapitel 13: Einrichtung der lokalen Active Directory-Struktur und Vorbereitung der Synchronisierung.....	33
Kapitel 14: Benutzeranlage und Verzeichnisbereinigung mit IDFix	38
Kapitel 15: Installation und Konfiguration von Microsoft Entra ID Connect.....	40
Auswahl der Authentifizierungsmethode in Microsoft Entra ID Connect	42
Password Hash Synchronization (PHS).....	42
Pass-through Authentication (PTA)	43
Federation with AD FS.....	44
Federation with PingFederate.....	45

Do Not Configure	46
Kapitel 16: Synchronisationsüberwachung und Verwaltung von Gastzugriffen im Entra ID	57
Kapitel 17: Verwaltung und Kontrolle von Gastbenutzern	60
Access Reviews: Automatische Überprüfung	61
Kapitel 17: Protokollanalyse und Sicherheitskonfigurationen im Microsoft Entra ID.....	64
Kapitel 18: Gruppenverwaltung, Berechtigungen und Lifecycle Management in Microsoft Entra ID und Microsoft Teams	69
Teams-Besitzer und deren Bedeutung.....	70
Lifecycle Management aktivieren	70
Teams-Onboarding gezielt steuern	71
Kapitel 19: Geräteverwaltung im Microsoft Entra ID – Best Practices und Konfiguration.....	72
Wie du ungewollte Registrierungen unterbindest.....	75
Ein Registry Key als Schutzmaßnahme.....	76
Achtung bei Terminalservern und Mehrfachanmeldungen.....	76
Geräteeinstellungen in Entra ID – Sicherheit durch klare Konfiguration.....	76
Kapitel 20: Microsoft 365 Installationsoptionen.....	77
So findest du die relevante Einstellung.....	77
Gerätezugriff über Intune einschränken	78
Gerätebereinigung und automatisierte Entfernung veralteter Objekte	80
Kapitel 20: Kontrolle über Benutzereinwilligungen und Applikationsberechtigungen.....	81
Kapitel 21: Externe Identitäten und Zusammenarbeit sicher steuern.....	84
Kapitel 22: Gasteinstellungen in SharePoint und OneDrive sinnvoll konfigurieren.....	85
Kapitel 23: Mandantenübergreifende Zugriffseinstellungen – Kontrolle über eingehende und ausgehende Einladungen	86
Kapitel 24: Identity Protection und Sicherheitsbewertung – Risikoanalysen verstehen und nutzen	88
Kapitel 25: Einstieg in den Bedingten Zugriff (Conditional Access)	90
Namenskonventionen	90
1. Richtlinie: Zugriff aus bestimmten Ländern einschränken.....	90
Technische Umsetzung: 1. Richtlinie Länderblockierung.....	91

Technische Umsetzung: 2. Richtlinie Legacy Authentication	96
Technische Umsetzung: 3. Richtlinie Unsupported Devices	97
Technische Umsetzung: 4. Richtlinie Device Code Flow	99
Technische Umsetzung: 5. Richtlinie Session Lifetime.....	101
Technische Umsetzung: 6. Richtlinie Require MFA Member	104
Technische Umsetzung: 7. Richtlinie Require MFA Device	105
Überprüfung von Richtlinien mit „What-If“ und Anmeldeprotokollen.....	106
Kapitel 26: Hybrid Azure AD Join & MFA bei Geräteregistrierung	107
Vorbereitung für Hybrid Azure AD Join.....	108
Richtlinie: Gruppenrichtlinie zur automatischen MDM-Registrierung (MDM-Join).....	110
Schritt-für-Schritt-Anleitung zur Erstellung der MDM-Join-GPO	110
Schlusswort: Dein Weg zu einer sicheren Microsoft 365 Umgebung.....	116

Einleitung

Microsoft 365 ist ohne Schutz anfällig für Angriffe. Dieser Leitfaden erklärt, wie man Zugriffsrechte kontrolliert, Daten sichert und Geräte schützt. Ein ganzheitlicher Sicherheitsansatz ist entscheidend, um Bedrohungen abzuwehren.

Microsoft 365 ist ein mächtiges Werkzeug. Doch ohne Absicherung wird es schnell zur Einfallstür für Hacker, Datenlecks und Chaos. Die Bedrohungen sind vielfältig: Angriffe auf Benutzerkonten, Malware, Datenverluste.

Das Problem?

Microsoft 365 ist keine einfache Plattform. Es ist ein komplexes System mit zahllosen Stellschrauben – und wer denkt, dass Microsoft die Sicherheit komplett übernimmt, liegt falsch. Die Realität: Dein Tenant ist ohne offen wie ein Scheunentor – wenn du nichts tust.

Genau deshalb habe ich diesen Guide geschrieben.

In den folgenden Kapiteln lernst du:

- wie du Zugriffsrechte kontrollieren und Missbrauch verhinderst.
- wie du Benutzerdaten sichern und Angreifern keine Chance gibst.
- wie du externe Freigaben sinnvoll einschränken und Datenlecks vermeidest.
- wie du Geräte sicher verwalten und klare Regeln für BYOD einführst.

und vieles mehr.

Besonders wichtig?

Microsoft 365 erfordert einen *ganzheitlichen* Sicherheitsansatz.

Ob Benutzerkonfigurationen, Gerätesicherheit, Datenklassifizierung oder Gastzugriffe: Nur durch die Kombination dieser Maßnahmen entsteht eine Umgebung, die sowohl interne Fehler als auch externe Bedrohungen effektiv abwehrt.

Wir fokussieren uns auf den folgenden Seiten primär auf Entra ID. Den Umfang von Entra ID darf man jedoch nicht unterschätzen.

Legen wir los!

Kapitel 1: Grundlagen und Ausgangslage – Aufbau einer hybriden Identitätsinfrastruktur

Zu Beginn einer jeden Planung zur Implementierung von Microsoft Entra ID in einer bestehenden IT-Umgebung ist es essenziell, sich mit den grundlegenden Konzepten der hybriden Identitätsinfrastruktur auseinanderzusetzen. Zentraler Bestandteil dieser Überlegungen ist die Frage, welche technischen Möglichkeiten Entra ID beziehungsweise das ehemals unter dem Namen Azure Active Directory bekannte System bietet und wie sich diese in bestehende Umgebungen integrieren lassen.

Im Kontext dieser ersten Analyse stellen sich für dich insbesondere folgende zentrale Fragen:

- Welche Topologien und Konfigurationsmöglichkeiten sind für eine hybride Identitätsverwaltung überhaupt gegeben?
- Wie viele Mandanten können mit wie vielen Konnektoren verknüpft werden?
- Wie viele lokale Umgebungen lassen sich über einen oder mehrere Dienste mit der Cloud verbinden?
- Was kann synchronisiert werden? Welche Attribute und Objekte sind für die Synchronisation zulässig und relevant?

Ein klassisches Einstiegsszenario bildet die Anbindung eines lokalen Active Directory an einen einzelnen Microsoft-365-Mandanten. Diese Standard-Topologie nutzt in der Regel Entra ID Connect – ein Agent, der auf einem lokalen Server installiert wird, welcher sowohl Zugriff auf das lokale Verzeichnis als auch eine Verbindung zur Cloud besitzt. Über diesen Dienst erfolgt die Synchronisation lokaler Identitäten in die Cloud.

Dabei ist zu beachten, dass Microsoft Entra ID und das Azure-Portal denselben Identitätsverwaltungsdienst nutzen. Das bedeutet, unabhängig davon, ob es sich um eine Microsoft-365-Subscription (z. B. Business Premium, E1, E3, E5) oder ein separates Azure-Konto handelt (z. B. über ein Pay-as-you-go-Modell), die zugrundeliegende Architektur bleibt konsistent. Die Mandantenstruktur erlaubt in beiden Fällen eine zentrale Benutzerverwaltung – vorausgesetzt, die Benutzerobjekte sind eindeutig.

Ein häufiger Fehler bei der Synchronisierung ist das sogenannte “Duplicate Attribute Match”, das auftritt, wenn Benutzerkonten mit identischen UPNs (User Principal Names) mehrfach in der lokalen Gesamtstruktur existieren. Dies unterstreicht die Notwendigkeit einer klaren, konsolidierten Struktur auf Seiten des lokalen Active Directoys, bevor eine Synchronisation erfolgt. Jedes Benutzerobjekt darf nur einmalig und eindeutig vorhanden sein, um Konflikte und Synchronisierungsfehler zu vermeiden.

Ein weiteres häufig genutztes, jedoch mit Vorsicht zu betrachtendes Szenario ist die Expressinstallation von Entra ID Connect. Diese Konfiguration synchronisiert das vollständige lokale Verzeichnis ohne

manuelle Selektion. Zwar stellt diese Methode einen schnellen Einstieg dar, jedoch bringt sie erhebliche Risiken mit sich: Auch Servicekonten, gelöschte Benutzer oder administrative Objekte können unbeabsichtigt in die Cloud synchronisiert werden. In der Praxis empfiehlt sich daher eine gezielte Auswahl synchronisierter Objekte – beispielsweise durch organisatorische Einheiten (OUs) und Gruppenfilter – um die Cloud-Umgebung bewusst zu härten und nicht benötigte Konten auszuschließen. Objekte, die im Rahmen einer Expressinstallation fälschlicherweise in Entra ID übernommen wurden und keinen produktiven Zweck erfüllen, müssen nach der Synchronisierung manuell gelöscht oder über entsprechende Filterregeln aus der Synchronisation ausgeschlossen werden, um eine saubere und sichere Mandantenstruktur zu gewährleisten.

Von besonderer Bedeutung ist in diesem Kontext auch die Trennung von Administratorkonten. Lokale Administratoren sollten nicht mit den Cloud-Administrationskonten synchronisiert werden. Stattdessen ist eine klare Trennung der Zuständigkeiten auf lokaler und cloudseitiger Ebene sicherzustellen, um sowohl Sicherheitsaspekte als auch organisatorische Verantwortlichkeiten abzubilden.

Das bevorzugte Synchronisierungsmodell bei dieser Art von hybrider Anbindung ist die sogenannte Kennworthashsynchronisierung. In diesem Szenario verwenden Benutzer dasselbe Passwort und denselben Benutzernamen sowohl lokal als auch in der Cloud. Im Gegensatz zu Pass-Through Authentication oder Single Sign-On erfolgt hier keine direkte Authentifizierung über den lokalen Domain Controller, sondern über die in die Cloud synchronisierten Hashwerte.



Bild 1: Unterstützte Topologien Entra ID

Kapitel 2: Synchronisierungsserver, Staging und Fallback-Konzepte

In hybriden Identitätsinfrastrukturen mit Microsoft Entra ID (vormals Azure Active Directory) ist die Art und Weise, wie die Synchronisation zwischen lokaler Umgebung und Cloud-Diensten erfolgt, von zentraler Bedeutung. Dabei ist zu beachten, dass bestimmte Konstellationen technisch nicht umsetzbar sind. Eine typische Fehlannahme besteht darin, mehrere aktive Synchronisierungsserver gleichzeitig auf eine einzige Entra ID-Instanz synchronisieren zu lassen. Diese Konfiguration funktioniert nicht und führt zu Konflikten.

Dahingegen funktioniert der Einsatz eines sogenannten Staging Servers. Eine übliche Architektur in komplexeren Umgebungen umfasst mehrere lokale Active Directories, die in einem gemeinsamen Forest integriert sind. Diese können untereinander synchronisiert sein und ihre Synchronisierung auf mehrere Server verteilen. Dennoch darf stets nur eine dieser Instanzen aktiv sein – alle übrigen müssen in den Staging-Modus versetzt werden, um Konflikte bei der Synchronisation zu vermeiden. In diesem Modus bezieht der Server Änderungen sowohl aus dem lokalen Active Directory als auch aus der Cloud mit einem Versatz zum Aktiven, exportiert diese jedoch nicht aktiv. Der Staging Server fungiert als passiver Spiegel der aktiven Synchronisierungsinstantz und dient als Fallback-System, sollte der primäre Server ausfallen.

Ein zentraler Aspekt in der Planung von Synchronisierungsszenarien ist die Frage, was passiert, wenn der aktive Server ausfällt und kein Staging Server konfiguriert wurde, der dessen Aufgaben übernehmen kann. Diese Situation muss unbedingt im Rahmen der Ausfallsicherheit und Notfallplanung berücksichtigt werden.

Ein typisches Anwendungsszenario ergibt sich im Rahmen der Kennworthashsynchronisierung, bei der identische Benutzeranmeldeinformationen lokal und in der Cloud verwendet werden. Im Falle eines Ausfalls des aktiven Synchronisierungsservers ist ein sofortiger Systemstillstand nicht zu erwarten. Benutzer können sich weiterhin anmelden und produktiv arbeiten, da der Hash bereits in der Cloud gespeichert ist. Änderungen an Benutzerobjekten, wie Namens- oder Kennwortänderungen, werden jedoch erst dann problematisch, wenn keine Synchronisierung mehr erfolgen kann.

Dies ist bei den Konfigurationen mit Pass-through Authentication (PTA) oder Single Sign-On (SSO) anders. In diesen Szenarien ist ein funktionierender Synchronisierungsserver zwingend erforderlich, da die Authentifizierung über Kerberos-Tickets erfolgt. Fällt die Tokenweitergabe aus, schlägt auch die Authentifizierung fehl. In solchen Fällen muss ein manueller Fallbak in die Kennworthashsynchronisierung erfolgen, der über PowerShell-Befehle eingeleitet werden kann. Dieser Vorgang sollte im Rahmen einer Notfallplanung dokumentiert und regelmäßig getestet werden.

Ein oft gestellter Praxisfrage betrifft die Verzögerung der Synchronisation durch den Staging Server. Microsoft gibt hier eine Synchronisationsverzögerung von rund 60 Sekunden im Vergleich zur aktiven Instanz an. Der Staging Server wird allerdings nicht automatisch aktiviert, sondern muss manuell aus dem passiven Modus in den aktiven Betrieb überführt werden. Das setzt voraus, dass Administratoren den Ausfall des primären Servers zeitnah erkennen. Monitoringlösungen wie PRTG oder der Connected Health-Dienst von Microsoft 365 können hierbei unterstützend wirken, indem sie frühzeitig entsprechende Warnmeldungen generieren.

Die Konfiguration eines Staging Servers erfolgt über eine Checkbox innerhalb des Entra ID Connect-Assistenten, die explizit aktiviert werden muss. Erst dann ist der Server bereit, im Bedarfsfall als Ersatzinstanz zu fungieren.

Unterstützte Topologien Entra ID

- ▶ Einzelne Gesamtstruktur, mehrere Synchronisierungsserver zu einem Azure AD-Mandanten:
 - ▶ Es ist nicht möglich, mehrere Azure AD Connect-Instanzen mit einem Azure Mandanten/Tenant zu verbinden
 - ▶ Es ist erforderlich, dass alle Domänen in der Gesamtstruktur über eine einzelne Azure AD Connect-Instanz erreichbar sind
 - ▶ Der Betrieb von Staging-Servern ist möglich

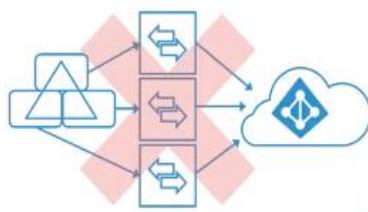


Bild 2: Unterstützte Topologien Entra ID mehrere Server

Kapitel 3: Vorbereitung des lokalen Verzeichnisses und Identitätsbereinigung

Die Synchronisierung mehrerer Gesamtstrukturen (Forests) mit einem zentralen Entra ID Mandanten ist grundsätzlich möglich, sofern ein aktiver Synchronisierungsdienst vorhanden ist. Eine entscheidende Voraussetzung für ein funktionierendes Szenario dieser Art ist jedoch die eindeutige Identifizierbarkeit aller Benutzerobjekte. Gerade in historisch gewachsenen IT-Infrastrukturen kommt es häufig vor, dass Benutzerattribute wie SMTP-Adressen oder UPNs mehrfach vergeben wurden – beispielsweise bei unterschiedlichen Benutzertypen. Während dies lokal in vielen Fällen unproblematisch ist, führt es bei der Synchronisation in die Cloud regelmäßig zu Konflikten.

Vor der erstmaligen Einrichtung von Entra ID Connect ist es daher unerlässlich, das lokale Active Directory umfassend zu bereinigen. Dies betrifft insbesondere veraltete, ungenutzte oder fehlerhaft konfigurierte Benutzer- und Objektinformationen. Die Realität zeigt, dass viele Unternehmen kein durchgehend gepflegtes AD besitzen – sei es aufgrund historischer Entwicklungen, fehlender Ressourcen oder unterschiedlicher administrativer Zuständigkeiten. Diese Gegebenheiten stellen jedoch keine unüberwindbare Hürde dar, sofern entsprechende Vorbereitungsmaßnahmen getroffen werden.

Ein zentrales Hilfsmittel in diesem Kontext ist das Tool „IDFix“, das gezielt Inkonsistenzen, doppelte UPNs, fehlerhafte SMTP-Adressen und andere potenzielle Probleme identifiziert, die bei einer Synchronisierung zu Fehlern führen könnten. Erst wenn die Konsistenz und Eindeutigkeit der Objekte sichergestellt ist, sollte mit der Konfiguration von Entra ID Connect begonnen werden.

Die Bereinigung des lokalen Verzeichnisses stellt somit eine der grundlegenden Vorbereitungsmaßnahmen dar, die vor dem Aufbau der Synchronisierungsstruktur abgeschlossen sein sollte. Nur auf dieser Basis kann eine stabile und wartungsarme Synchronisierung gewährleistet werden. Wird dieser Schritt ausgelassen oder unvollständig durchgeführt, führt dies häufig zu nachgelagerten Problemen und erhöhtem Administrationsaufwand. Es empfiehlt sich daher, systematisch vorzugehen: erst das lokale Verzeichnis in einen konsistenten Zustand bringen, anschließend die Synchronisierung mit Entra ID einrichten.



Bild 3: Unterstützte Topologien Entra ID einzelner AD Mandant

Kapitel 4: Standardkonten, Namenskonventionen und Absicherung administrativer Benutzer

In Microsoft Entra ID-Umgebungen basiert die Kontenstruktur in der Regel auf einem definierten Standardmodell. Jeder Benutzer verfügt über ein eigenes Konto, mit dem er aktiv arbeitet. Dieses Benutzerobjekt kann dabei mit einem primären Postfach sowie mehreren sekundären SMTP-Adressen ausgestattet sein. Eine Lizenzierung ist für die reine Synchronisation des Kontos mit Microsoft Entra ID zunächst nicht erforderlich. Wird keine benutzerdefinierte Domäne zugewiesen, so erhält das Objekt automatisch eine standardisierte „.onmicrosoft.com“-Adresse. Diese wird jedem Tenant bei der Registrierung mitgegeben und ist daher in der Praxis weit verbreitet. Jedes Benutzerkonto besitzt folglich neben der eigentlichen Domäne stets auch eine „.onmicrosoft.com“-Alias-Adresse.

Diese Adressen sind vor allem im administrativen Bereich von Bedeutung. In vielen Umgebungen ist es gängige Praxis, administrative Konten mit einer solchen Adresse zu betreiben. Ergänzend hierzu kommt häufig ein konsistentes Namensschema zum Einsatz – beispielsweise durch Anhänge wie „-adm“ oder ähnliche Muster. Diese Vorgehensweise birgt allerdings Risiken. Sollte es im Rahmen eines Sicherheitsvorfalls zu einem erfolgreichen Angriff auf die Entra ID-Instanz kommen, zählt die Identifikation privilegierter Konten zu den ersten Maßnahmen eines potenziellen Angreifers. Ein leicht durchschaubares Namensschema begünstigt dabei die gezielte Kompromittierung administrativer Zugänge.

Administrative Konten sollten grundsätzlich durch eine moderne und vor allem phishingresistente Multi-Faktor-Authentifizierung (MFA) geschützt werden. Klassische Verfahren wie SMS-Codes oder App-basierte Bestätigungen (z. B. über Microsoft Authenticator) gelten heute als nicht mehr ausreichend sicher, da sie potenziell durch sogenannte MFA-Bypass-Techniken kompromittiert werden können.

Ein konkreter Fall aus dem Jahr 2023 zeigt die Gefahr: Ein Benutzer gibt seine Anmelde Daten ein, erhält die MFA-Abfrage – bestätigt diese jedoch nicht. Dennoch kann durch die erzeugte Session- oder Cookie-ID ein Angreifer, sofern keine weiteren Schutzmechanismen aktiv sind, einen eigenen zweiten Faktor registrieren und sich erfolgreich am Konto anmelden. Die eigentliche MFA-Prüfung wird somit umgangen, obwohl sie aktiviert war.

Der wirksamste Schutz gegen solche Angriffe sind phishingresistente MFA-Methoden, wie etwa FIDO2-Keys oder zertifikatsbasierte Anmeldeverfahren, da sie keine klassischen Weiterleitungsszenarien zulassen und auf kryptographischen Prüfungen beruhen.

Darüber hinaus sollte die administrative Kontenstruktur überdacht werden. Viele setzen noch auf einfache Benennungsschemata wie vorname-adm@domain.de – das macht es jedoch für potenzielle Angreifer leicht, privilegierte Konten zu identifizieren. Eine Möglichkeit, die Sicherheit zu erhöhen, ist die Anonymisierung administrativer Logins, etwa durch kryptische Kombinationen aus Buchstaben und Zahlen (a7bx-dk93@domain.de). Dies erfordert allerdings eine konsequente Umsetzung im gesamten Verzeichnis.

Eine alternative Herangehensweise wäre, administrative Konten zwar mit Klarnamen zu versehen, aber diese intern mit nicht offensichtlichen Namen zu kombinieren – z. B. aus „Aaron ADM“ wird „Maximilian Mundt“. Für das IT-Team nachvollziehbar, für externe Beobachter jedoch schwer zuzuordnen. Wichtig ist, dass diese Maßnahmen immer Teil eines umfassenden Sicherheitskonzepts sind, das u. a. auch Privileged Identity Management (PIM) und Conditional Access berücksichtigt.



```
*Unbenannt - Editor
Datei Bearbeiten Format Ansicht Hilfe
aaron.siller
adm.siller
aaron.admin
admin.aaron.siller

aaron.adm
DE98817

aaron.adm
Maximilian.Mundt|
```

The screenshot shows a Windows Notepad window with the title "*Unbenannt - Editor". The menu bar includes "Datei", "Bearbeiten", "Format", "Ansicht", and "Hilfe". The content area lists several user accounts:
- aaron.siller
- adm.siller
- aaron.admin
- admin.aaron.siller
- aaron.adm (with value DE98817)
- aaron.adm (with value Maximilian.Mundt) - this entry is partially typed and ends with a cursor.
The status bar at the bottom displays "Zeile 11, Spalte 17", "100%", "Windows (CRLF)", and "UTF-8".

Bild 4: Beispiel Admin Benennung

Ein weiterer relevanter Aspekt betrifft die Handhabung sogenannter „Breaking Glass Accounts“. Ein Breaking Glass Account muss vollständig von allen automatisierten Richtlinien und Schutzmechanismen ausgenommen sein – also keine Conditional Access Policies, kein Privileged Identity Management, keine Session Controls. Der Fokus liegt auf garantierter Zugänglichkeit im Notfall. Gleichzeitig gelten verschärzte Anforderungen an die Kennwortsicherheit: Ein komplexes Passwort mit mindestens 16 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen ist verpflichtend. Zusätzlich sollte auch dieser Account mit einem phishingresistenten zweiten Faktor abgesichert werden, um Missbrauch zu verhindern.

Checkliste: Sicherer Breaking Glass Account

Punkt	Empfehlung
🔒 MFA aktiviert	Ja, unbedingt! Nur phishingresistente Methoden wie FIDO2-Keys oder zertifikatsbasierte Verfahren verwenden.
🚫 Ausschluss aus Richtlinien	Der Account muss vollständig von Conditional Access, PIM und anderen automatisierten Kontrollen ausgenommen sein.
📝 Passwortkomplexität	Mindestens 16 Zeichen, inkl. Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen.

 Individuell statt Shared	Kein Shared Account! Jeder Admin sollte ein eigenes Konto mit klarer Nachvollziehbarkeit haben.
 Protokollierung und Nachvollziehbarkeit	Auch Notfallzugriffe sollten audierbar sein – Logging aktivieren.
 Getrennte Speicherung von Anmelddaten	Zugangsdaten sicher und außerhalb der Umgebung speichern (z. B. in einem versiegelten Safe oder einem Offline-Passwortmanager).
 Dokumentation	Account-Konfiguration, Zugriffsvoraussetzungen und Testverfahren regelmäßig prüfen und dokumentieren.

Tabelle 1: Checkliste Breaking Glass Account

Breaking Glass Accounts – Früher vs. Heute

Aspekt	Früher	Heute (Best Practice)
MFA-Nutzung	Meist deaktiviert , um jederzeit Zugriff zu garantieren	Aktiv , aber phishingresistent (z. B. FIDO2-Key, Zertifikat)
Conditional Access / PIM	Teilweise aktiv	Vollständig ausgeschlossen , um Zugang jederzeit zu gewährleisten
Passwortanforderungen	Standardkennwort-Richtlinie	Mindestens 16 Zeichen , hoher Komplexitätsgrad
Nutzeridentität	Häufig Shared Accounts (z. B. „admin01“)	Personalisierte, dedizierte Konten
Sicherheit vs. Verfügbarkeit	Fokus auf schnelle Verfügbarkeit	Balance zwischen sicherem Zugriff und Ausfallschutz
Kontrollmechanismen	Minimal oder nicht vorhanden	Ergänzt durch regelmäßige Tests , Dokumentation und Zugriffsprotokollierung

Tabelle 2: Vergleich früher vs. Heute Breaking Glass Account

Ein häufig diskutiertes Thema ist die Verwendung von Shared Admin-Konten, bei denen mehrere Personen ein und denselben administrativen Login nutzen. Diese Praxis ist aus heutiger Sicht nicht mehr empfehlenswert, da sie die Nachvollziehbarkeit und Verantwortlichkeit massiv einschränkt. Moderne Sicherheits- und Compliance-Anforderungen setzen auf personalisierte, klar zuordnbare Konten mit entsprechender Protokollierung – auch und gerade im Admin-Bereich.

Für reguläre Admin-Konten gilt ebenfalls: MFA ist Pflicht – und zwar möglichst phishingresistent. Während für Daily-Admin-Konten oft noch auf App-basiertes Number Matching zurückgegriffen wird, um den Alltag praktikabel zu halten, sollte bei privilegierten Notfallkonten keine Kompromisslösung mehr zum Einsatz kommen. Nur so lässt sich eine effektive, zukunftssichere Absicherung gewährleisten.

Insbesondere bei kleinen und mittelständischen Unternehmen ist die vollständige Umsetzung dieser Maßnahmen nicht immer sofort realisierbar. Budgetäre, personelle und organisatorische Rahmenbedingungen führen oft zu priorisierten Umsetzungsplänen. Dennoch sollte eine schrittweise Modernisierung der Kontostrukturen und Absicherungsmechanismen erfolgen – nicht zuletzt im Hinblick auf steigende regulatorische Anforderungen und eine zunehmend professionelle Bedrohungslage.

Best Practices für administrative Konten in Microsoft Entra ID

1. Benennung neutral halten

Sprechende Namen wie max.admin oder m.mustermann-adm vermeiden. Stattdessen generische oder anonymisierte Aliasnamen, z. B. mxm-5291 oder „nicht zuordenbare“ Kombinationen aus Vor- und Nachnamen nutzen.

2. Keine Shared Accounts verwenden

Jeder Administrator sollte ein individuelles, personalisiertes Konto mit eindeutiger Zuordnung erhalten – keine Sammelkonten.

3. MFA ist Pflicht – phishingresistent bevorzugt

Auf moderne MFA-Verfahren wie FIDO2-Sicherheitsschlüssel oder zertifikatsbasierte Authentifizierung setzen. Schwächere Methoden wie SMS oder App-Code, wo möglich, vermeiden.

4. Breaking Glass Accounts definieren

Mindestens ein Notfallkonto vorhalten, das von Conditional Access und PIM ausgenommen ist – jedoch ebenfalls mit starkem Passwort und MFA geschützt ist.

5. Dokumentation und Rollenklärung sicherstellen

Namenskonventionen, Konto-Zuordnungen und Berechtigungen sollten zentral dokumentiert und regelmäßig überprüft werden.

6. Sichtbarkeit reduzieren

Administrative Konten in öffentlichen Verteilern oder allgemeinen Adressbüchern sichtbar zu machen, sollte vermieden werden. Einschränkungen über Exchange oder Entra ID sind möglich.

Unterstützte Topologien

Entra ID

► Standardkonfiguration der Azure AD Connect-Synchronisierung:

- Jeder Benutzer hat nur ein einziges aktiviertes Konto, und die Gesamtstruktur, in der sich dieses Konto befindet, wird verwendet, um den Benutzer zu authentifizieren.
- Jeder Benutzer hat nur ein Mailpostfach.
- Sind diese zwei fundamentalen Bedingungen nicht gegeben, werden Benutzer nicht oder fehlerhaft Synchronisiert (*.onmicrosoft.com-Adresse)

Kapitel 5: Konsolidierung und Struktur – Herausforderungen bei hybriden Identitäten

In vielen IT-Infrastrukturen finden sich nicht selten mehrere, teils voneinander getrennte lokale Active-Directory-Strukturen. Häufig steht hinter jeder Struktur ein eigener AD-Server, der wiederum mit einem separaten Azure AD Connect (bzw. Microsoft Entra Connect) Synchronisierungsserver gekoppelt ist. In der Praxis wird dabei oft versucht, diese voneinander isolierten Umgebungen in einen zentralen Microsoft Entra ID-Mandanten zusammenzuführen – in der Hoffnung, dass sich die Daten automatisch oder zumindest reibungslos konsolidieren lassen.

Doch genau hier liegt eine der größten Stolperfallen hybrider Identitätsmodelle: Eine direkte Konsolidierung logisch getrennter AD-Strukturen innerhalb des Entra-Mandanten funktioniert in der Regel nicht zuverlässig. Die parallele Synchronisation unterschiedlicher Quellen in einen zentralen Mandanten führt häufig zu Inkonsistenzen, insbesondere bei der eindeutigen Benutzeridentifikation.

Stattdessen empfiehlt es sich, die Konsolidierung auf lokaler Ebene zu priorisieren. Das Ziel muss sein, bereits vor der Synchronisation eine einheitliche, saubere Datenbasis zu schaffen – also beispielsweise Dubletten aufzulösen, eindeutige Benutzerobjekte zu definieren und Namenskonflikte zu vermeiden. Nur so kann sichergestellt werden, dass der Entra-Mandant später verlässliche Informationen erhält, diese korrekt interpretieren und verarbeiten kann.

Ein unterstützendes Element in diesem Zusammenhang ist das sogenannte Staging. Dabei handelt es sich um eine Art Puffer oder Vorverarbeitungsebene, die eine erste Harmonisierung der Daten vornimmt, bevor sie produktiv in den Mandanten übertragen werden. Insbesondere in komplexen Migrations- oder Fusionsszenarien kann das Staging helfen, potenzielle Probleme frühzeitig zu erkennen und abzufedern.

Zusammengefasst: Eine saubere hybride Identitätsarchitektur steht und fällt mit einer durchdachten Struktur. Die Konsolidierung sollte möglichst vor der Cloud-Anbindung erfolgen. Nur so lässt sich die nötige Datenqualität sicherstellen, die für stabile, skalierbare und sichere Identitäten in Microsoft Entra ID erforderlich ist.

Unterstützte Topologien Entra ID

- ▶ Mehrere Gesamtstrukturen, mehrere Synchronisierungsserver zu einem Azure AD-Mandanten:
 - ▶ Die Verbindung mehrerer Azure AD Connect-Synchronisierungsserver aus verschiedenen lokalen Verzeichnissen in einen Tenant wird nicht unterstützt
 - ▶ Es gibt keine „Abgleichung“ der Synchronisierungs-Instanzen

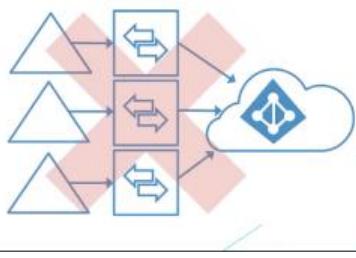


Bild 6: Mehrere Gesamtstrukturen, mehrere Synchronisierungsserver

Kapitel 6: Staging Server und Stammdatenpflege – Grundlagen für eine stabile Synchronisierung

Ein zentraler Bestandteil beim Aufbau einer zuverlässigen Synchronisationsarchitektur ist der sogenannte Staging Server. Dieser arbeitet in der Regel mit dem klassischen Synchronisierungszyklus von 30 Minuten – zeitlich versetzt um 60 Sekunden zum aktiven Server. An der grundlegenden Konfiguration oder der grafischen Oberfläche des Systems ändert sich durch den Einsatz eines Staging Servers nichts. Wichtig ist jedoch zu wissen, dass ein solcher Server nicht automatisch in den aktiven Betrieb übergeht: Er muss manuell von einem Administrator aktiviert werden. Diese bewusste Umschaltung bietet einerseits Sicherheit, erfordert andererseits aber auch ein hohes Maß an Verantwortungsbewusstsein bei der Handhabung.

Bei der Konfiguration von Entra ID Connect – wie wir sie in den nächsten Abschnitten noch näher betrachten werden – spielt insbesondere das Thema OU-Filterung eine zentrale Rolle. Dabei ist die Auswahl der zu synchronisierenden Objekte über Organisationseinheiten (OUs) nach wie vor die gängigste Methode, da sie in der Praxis eine einfache und effektive Möglichkeit zur Steuerung und Pflege der Stammdaten bietet. Alternativ lassen sich Filterungen auch auf Gruppenbasis oder über spezifische Attribute realisieren, was in komplexeren Umgebungen Vorteile bieten kann.

Besonders hervorzuheben ist, dass die Pflege der Stammdaten im lokalen Active Directory den Grundstein für eine saubere und funktionale Synchronisation mit Entra ID legt. Die Qualität und Struktur dieser Daten entscheidet maßgeblich darüber, wie stabil, transparent und sicher die gesamte hybride Identitätsinfrastruktur funktioniert. Eine sorgfältige Planung und klare Richtlinien für die Stammdatenpflege sind daher unerlässlich – sowohl im produktiven Betrieb als auch in der Notfallabsicherung.

Unterstützte Topologien Entra ID

► Nutzung des Staging-Servers:

- Azure AD Connect unterstützt die Installation eines zweiten Servers im *Stagingmodus*
- Ein Server in diesem Modus liest Daten aus allen verbundenen Verzeichnissen, schreibt jedoch nicht in diese (Keine Import-Funktionalitäten)
- Der Staging-Server verwendet den normalen Synchronisierungszyklus

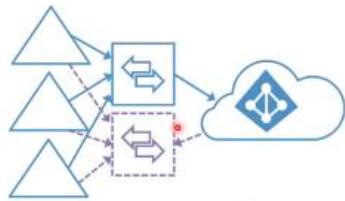


Bild 7: Staging Server

Kapitel 7: Verlässlichkeit von Entra ID Connect und Rolle der Microsoft 365 Gruppen

Ein zentraler Bestandteil einer hybriden Identitätsinfrastruktur ist die stabile Funktionsweise von Entra ID Connect. In der Praxis erweist sich dieser Dienst nach erfolgreicher Einrichtung in der Regel als äußerst zuverlässig und störungsarm. Fälle von Ausfällen sind selten, dennoch sollte bedacht werden, dass ein potenzielles Failover manuell durchgeführt werden muss. Ein konkretes Beispiel eines großflächigen Problems ereignete sich Anfang 2024, als es seitens Microsoft zu einer Störung kam, die hauptsächlich KMUs im europäischen Raum betraf. Infolge dieser Störung konnten vorübergehend keine Synchronisierungen oder Änderungen über Entra ID Connect durchgeführt werden.

Im Standardfall erfolgt die Verwaltung der Identitäten – also von Benutzerkonten, Gruppen und Geräten – lokal. Die Synchronisierung in die Cloud dient hauptsächlich der Bereitstellung von Lizenzen und zusätzlichen Cloud-Funktionalitäten. Es existieren jedoch Mechanismen wie der Password Writeback, über die bestimmte Änderungen aus der Cloud zurück ins lokale Active Directory geschrieben werden können. Dennoch bleibt das Grundprinzip eine Synchronisierung von lokal nach cloudbasiert.

Unterstützte Topologien Entra ID

- ▶ Bei einem notfallbedingten Ausfall des primären Servers kann ein Failover auf den Stagingserver durchgeführt werden.
 - ▶ Der Failover muss manuell durchgeführt werden!
- ▶ Jede am primären Server vorgenommene Konfigurationsänderung muss manuell an den zweiten Server kopiert werden
- ▶ Man kann den Status eines Aktiven- und Staging-Servers jeweils wechseln
- ▶ Es können mehrere Staging-Server verwendet werden

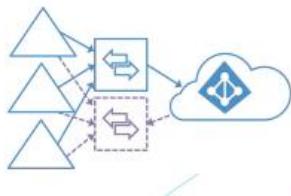
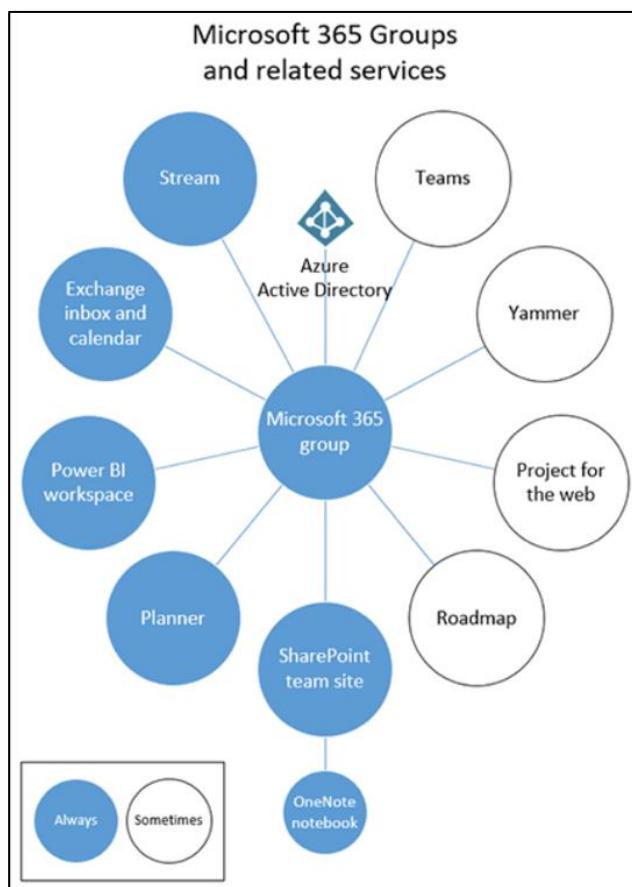


Bild 8: Wofür wird ein Staging Server genutzt?

Ein Spezialfall in der Cloud-Verwaltung betrifft die Microsoft 365 Gruppen. Diese Gruppenform ist nicht mit traditionellen Gruppenarten im lokalen AD vergleichbar, da sie ausschließlich in der Cloud existiert und mit der Nutzung von Microsoft 365-Diensten wie Teams eng verknüpft ist. Wird beispielsweise ein neues Team in Microsoft Teams angelegt, erzeugt Entra ID im Hintergrund automatisch eine Microsoft 365 Gruppe. Dieses Konzept ist technologische Grundlage für zahlreiche weitere Dienste wie Stream, Exchange Online Postfächer mit Kalendern, Power BI Workspaces, Planner, SharePoint Teamseiten sowie OneNote Notizbücher. Die Gruppenform stellt somit eine Art zentrale Organisationsstruktur dar, über die verschiedene Cloud-Dienste miteinander verbunden werden.

Besondere Aufmerksamkeit verdient in diesem Zusammenhang das Speicherplatz-Management, da jede neu erstellte Microsoft 365 Gruppe Ressourcen im SharePoint, Speicher des Tenants beansprucht. Dieser Speicher berechnet sich nach einem Basiswert von einem Terabyte pro Tenant plus zehn Gigabyte pro lizenziertem Benutzer.

Ein Benutzer arbeitet dabei ganz normal mit Kanälen, Chats und Dateien innerhalb von Teams, ohne zu merken, dass all diese Inhalte auf einer Microsoft 365 Gruppe basieren. Diese Tatsache zeigt deutlich, dass Entra ID zwar die zentrale Identitätsplattform darstellt, jedoch zahlreiche Abhängigkeiten und



Integrationen mit anderen Diensten innerhalb von Microsoft 365 bestehen. Daher sollte im Unternehmen regelmäßig hinterfragt werden, wie die Teams-Erstellung geregelt ist: Dürfen alle Benutzer selbständig neue Teams anlegen? Oder erfolgt dies zentral über Administratoren oder autorisierte Poweruser?

Bild 9: Microsoft Groups Quelle: Microsoft Learn

Hintergrund dieser Überlegung ist, dass mit jeder Teams-Erstellung automatisch eine Microsoft 365 Gruppe generiert wird, die wiederum ein SharePoint-Teamsite erzeugt und somit Ressourcen im unternehmensweiten Tenant beansprucht. Diese Gruppen tauchen anschließend auch in der Verwaltung innerhalb von Entra ID auf.

Neben der reinen Erstellung sollten auch weitere Aspekte der Governance berücksichtigt werden, z. B. Lebensdauer von Teams, Regelungen zum Gastzugriff oder die automatisierte Archivierung. Wichtig ist in diesem Zusammenhang auch, dass

der Großteil der Microsoft 365 Gruppen – in über 90 % der Fälle – direkt durch die Nutzung von Microsoft Teams entsteht. Ein fundiertes Verständnis über Ursprung und technische Hintergründe dieser Gruppen ist somit essenziell für eine strukturierte Administration in Entra ID.

Kapitel 8: Passwort-Hash-Synchronisierung und Lizenzverwaltung in Entra ID

Ein essenzieller Bestandteil der hybriden Identitätsinfrastruktur ist die Passwort-Hash-Synchronisierung. Diese Methode ermöglicht es, Benutzerkonten aus dem lokalen Active Directory in die Cloud zu synchronisieren und dabei deren Passworthashes sicher zu übertragen. Dadurch können sich Benutzer sowohl lokal als auch in der Cloud mit dem gleichen Benutzernamen und Passwort authentifizieren. Die technische Umsetzung erfolgt über Entra ID Connect, welches als Brücke zwischen der lokalen Infrastruktur und der Microsoft-Cloud agiert.

Sobald ein Benutzer in der Cloud verfügbar ist, kann ihm über Entra ID eine Microsoft 365-Lizenz zugewiesen werden. Dies ermöglicht den Zugriff auf die ihm zugeordneten Cloud-Dienste. Dabei ist zu beachten, dass – sofern keine gezielte Konfiguration erfolgt – standardmäßig alle enthaltenen Services der Lizenz aktiviert werden. Besonders bei umfangreichen Lizenzpaketen wie Microsoft 365 Business Premium, E3 oder E5 umfasst dies eine Vielzahl von Anwendungen und Diensten. In einem E5-Plan können dies über 50 verschiedene Services sein.

Die Entscheidung, welche Services für den Endnutzer tatsächlich sinnvoll und erforderlich sind, sollte wohlüberlegt sein. Nicht jeder Benutzer benötigt beispielsweise Zugriff auf Applikationen wie Microsoft Sway, insbesondere wenn sie im Unternehmen nicht aktiv genutzt oder angefragt werden. Eine detaillierte Lizenzoptimierung kann nicht nur die Übersichtlichkeit verbessern, sondern auch potenzielle Sicherheitsrisiken verringern.

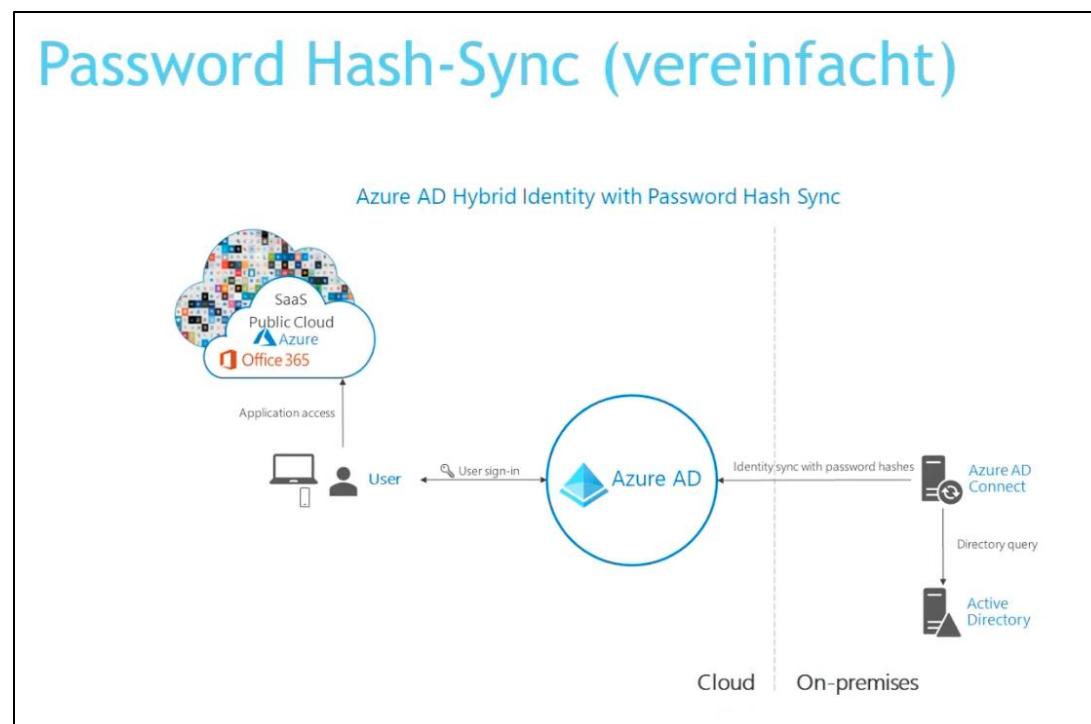


Bild 10: Password Hash-Sync

Ein weiterer Sicherheitsaspekt betrifft die Anmeldung aus verschiedenen Netzwerken. Durch die Passwort-Hash-Synchronisierung ist der Login sowohl innerhalb des Unternehmensnetzwerks als auch extern möglich. Um diese Zugriffsmöglichkeiten gezielt zu kontrollieren, kommt Conditional Access zum Einsatz. Dieses Tool innerhalb von Entra ID ermöglicht die Definition von Richtlinien, um Zugriffe abzusichern, Risiken zu minimieren und unautorisierte Anmeldungen zu verhindern.

Im weiteren Verlauf werden empfohlene Conditional-Access-Richtlinien vorgestellt, die sich in der Praxis bewährt haben. Diese können direkt mit bestehenden Regelwerken im eigenen Unternehmen abgeglichen und angepasst werden, um das Sicherheitsniveau der Entra ID Umgebung systematisch zu erhöhen.

Password Hash-Sync (vereinfacht)

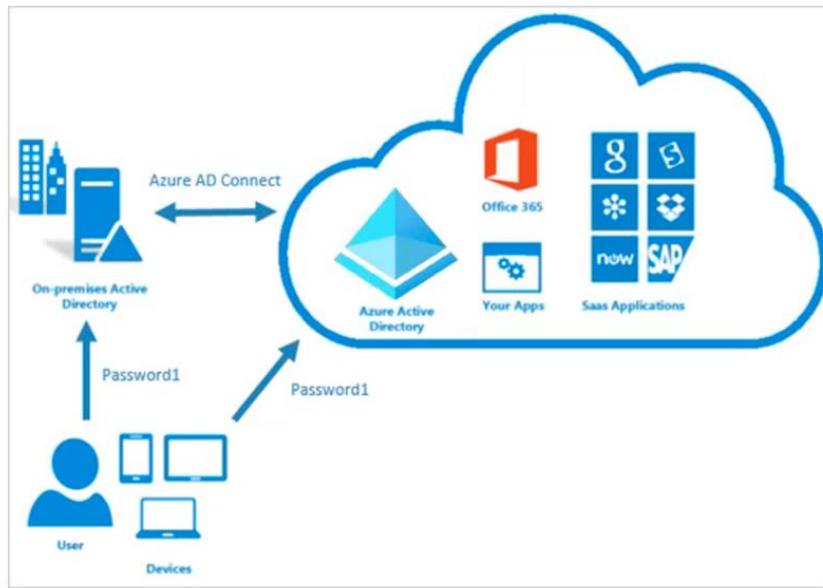


Bild 11: Password Hash Sync vereinfacht

Microsoft 365 Lizenzübersicht (Auswahl)

Lizenztyp	Zielgruppe	Typische Inhalte	Besonderheit
Business Premium	Kleine und mittlere Unternehmen	Outlook, Word, Excel, Teams, Exchange Online, OneDrive, SharePoint	Grundlegende Sicherheitsfeatures, MDM (Intune)
Microsoft 365 E3	Mittelstand, große Unternehmen	Business Apps + erweiterte Verwaltung: Azure AD Premium P1, Microsoft Defender for Office 365	Verbesserte Verwaltung & Reporting
Microsoft 365 E5	Unternehmen mit hohen Sicherheitsanforderungen	E3 + Azure AD Premium P2, Microsoft Defender (vollständig),	Fokus auf Security, Identity Protection & SIEM

		Compliance & Insider Risk Tools	
--	--	---------------------------------	--

Tabelle 3: Lizenzübersicht

Hinweis: Alle Lizenzen aktivieren standardmäßig sämtliche enthaltenen Dienste. Eine gezielte Konfiguration der Serviceverfügbarkeit pro Benutzer ist empfehlenswert.

Beispielhafte Conditional Access Richtlinien

Richtlinie	Ziel/Schutz
MFA für externe Zugriffe	Schutz vor unerlaubtem Zugriff von außerhalb
Blockieren veralteter Clients	Verhindert die Nutzung unsicherer Anwendungen
Zugriff nur aus bestimmten Ländern	Geo-basiertes Sicherheitsfiltering
Zugriff nur von verwalteten Geräten	Sicherstellung von Gerätekontrolle
Risikobasierter Zugriff (Identity Protection)	Automatische Reaktion auf ungewöhnliche Aktivitäten
Blockieren von Legacy-Authentifizierung	Verhindert Angriffe über alte Protokolle

Tabelle 4: Beispiel Conditional Access Richtlinien

Tipp: Conditional Access ist ein zentrales Steuerungsinstrument in Entra ID. Die frühzeitige Planung, Standardisierung und kontinuierliche Optimierung der Richtlinien ist ein zentraler Bestandteil der Cloud-Sicherheitsstrategie.

Kapitel 9: Passthrough-Authentifizierung als moderne Alternative zum klassischen SSO

Seit etwa 2018/2019 stellt Microsoft mit der Passthrough-Authentifizierung (PTA) eine Alternative zur bisherigen Passworthashsynchronisierung bereit. Ziel dieser Methode ist es, Benutzern einen modernen und unkomplizierten Zugang zur Cloud zu ermöglichen – insbesondere unter dem Aspekt des Single Sign-On (SSO). Während viele Unternehmen weiterhin auf die Passwortsynchronisierung setzen, bietet PTA eine wesentlich einfachere Möglichkeit, lokale Anmeldedaten ohne wiederholte Passwortabfragen zu nutzen.

Technisch basiert PTA auf einem Authentication Agent, der innerhalb der lokalen Infrastruktur installiert wird. Dieser übernimmt die Rolle eines Azure Active Directory Federation Services (ADFS) Servers, allerdings ohne den früher notwendigen hohen administrativen Aufwand. Im Gegensatz zu klassischen ADFS-Setups, bei denen vier zusätzliche Server (zwei ADFS-Server plus zwei Web Application Proxies) erforderlich waren, benötigt PTA lediglich einen oder mehrere schlanke Agent-Installationen sowie bestimmte freigegebene URLs in der Firewall.

Ein wesentlicher Vorteil von PTA besteht in der Reduktion der Komplexität: Es gibt keine Notwendigkeit mehr, separate ADFS-Infrastrukturen aufzubauen und zu betreiben, was besonders für kleine und mittelgroße Unternehmen attraktiv ist. Stattdessen wird bei der Anmeldung ein Kerberos-Ticket generiert, das vom Authentication Agent verarbeitet und zur Authentifizierung gegenüber Azure Active Directory (Entra ID) genutzt wird. Der Agent prüft die lokalen Anmeldeinformationen in Echtzeit, ohne dass Passwörter in die Cloud repliziert werden müssen.

Ein Nachteil gegenüber ADFS ist jedoch die sequenzielle Verarbeitung von Authentifizierungsanfragen. Während ADFS mehrere Anfragen parallel bearbeiten kann, arbeitet PTA Schritt für Schritt. In der Praxis bedeutet dies für die Benutzer unter Umständen eine minimale Verzögerung bei der Anmeldung – typischerweise nur ein bis zwei Sekunden, die im Alltag jedoch kaum wahrnehmbar sind.

Pass-through Authentifizierung (vereinfacht)

Azure AD Hybrid Identity with Pass-through authentication

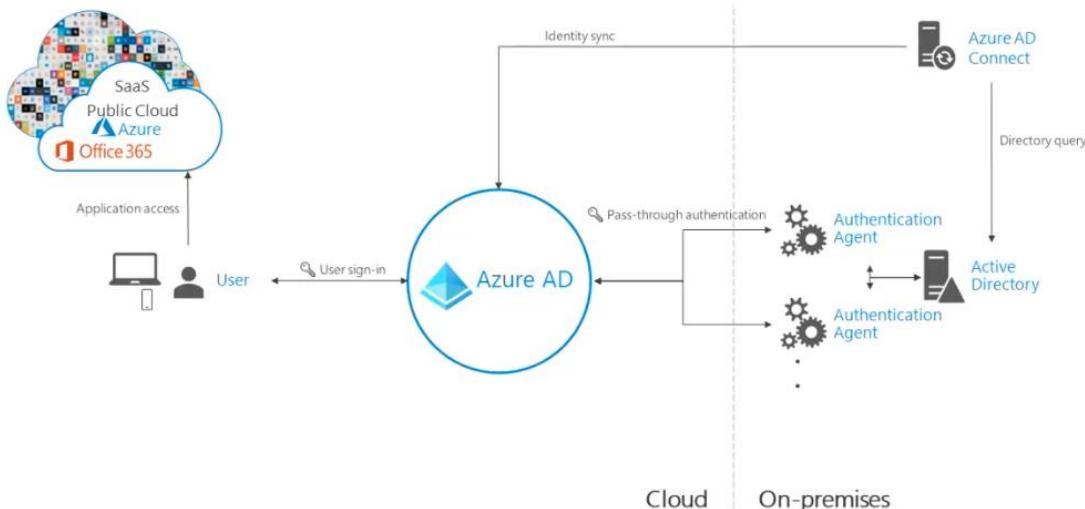


Bild 12: Pass-through Authentifizierung

Microsoft hat die Vorteile von Single Sign-On zunächst vor allem mit dem Argument der **Zeitersparnis** beworben. In entsprechenden Rechenbeispielen wurde aufgeführt, wie viel Zeit und damit Geld eingespart werden könnte, wenn Benutzer ihr Passwort nicht mehr mehrfach täglich eingeben müssten. Diese Argumentation überzeugte viele Unternehmen jedoch nicht nachhaltig.

Die **neue strategische Ausrichtung** von Microsoft rückt nun den **Sicherheitsaspekt** in den Vordergrund. Jede Passworteingabe wird heute als potenzielles Sicherheitsrisiko betrachtet. Jeder Authentifizierungsvorgang – insbesondere bei Verwendung von Password Hash Sync – erzeugt ein neues Token und birgt das Risiko des Abfangens oder der Kompromittierung. Durch PTA mit SSO wird die Anzahl der Passworteingaben reduziert, was wiederum das Abfangen stark erschwert. In Kombination mit **Conditional Access-Richtlinien**, wie dem Ausschluss persistenter Browser-Sessions oder automatischer Abmeldungen nach definierten Zeiträumen, ergibt sich ein deutlich höheres Sicherheitsniveau

Dennoch darf PTA **nicht als universelle Lösung** betrachtet werden. Eine solide Sicherheitsarchitektur erfordert weiterhin **phishingresistente MFA-Verfahren** (z. B. FIDO2-Keys) sowie **fein granulierte Zugriffskontrollen** über Conditional Access Policies. PTA ist somit ein starker Baustein innerhalb eines modernen Identitätsmanagements, ersetzt aber nicht das Gesamtbild einer durchdachten Sicherheitsstrategie.

Pass-through Authentifizierung (vereinfacht)

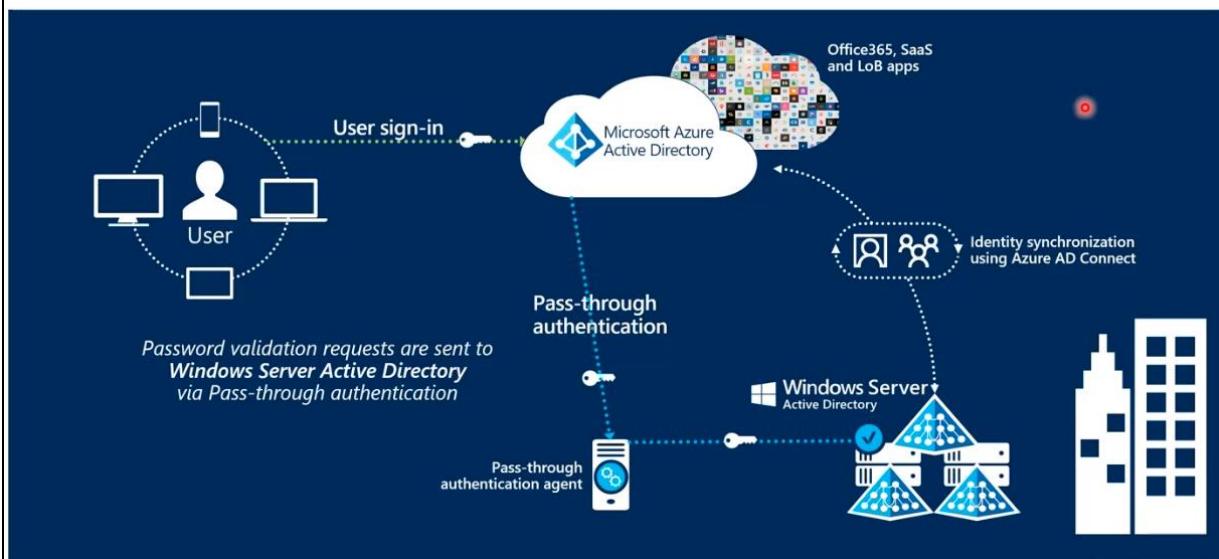


Bild 13: Pass-through vereinfacht

Kapitel 10: Föderierte Authentifizierung – Active Directory Federation Services (AD FS)

Zur Abrundung der Authentifizierungsszenarien in Microsoft Entra ID darf die **föderierte Authentifizierung** mittels **Active Directory Federation Services (AD FS)** nicht fehlen. Diese Lösung ermöglicht eine vollständige Single Sign-On (SSO)-Erfahrung für Benutzer, indem Authentifizierungsanfragen direkt an lokale Federation Server weitergeleitet werden. Damit ist eine zentrale Anmeldung über das lokale Active Directory möglich, ohne dass Passworthashes in die Cloud synchronisiert werden müssen.

Das klassische Szenario umfasst neben dem lokalen Active Directory und Azure AD Connect mindestens vier zusätzliche Serverkomponenten: zwei **Federation Server** und zwei **Federation Proxys**, jeweils redundant ausgelegt für Hochverfügbarkeit und Ausfallsicherheit. Diese Komponenten agieren als Bindeglied zwischen der lokalen Authentifizierungsstruktur und der Cloud, übernehmen das Token-Issuing und stellen sicher, dass Benutzeranmeldungen innerhalb der Organisation verarbeitet werden, ohne dass die Anmeldeinformationen jemals die lokale Umgebung verlassen.

Dieses Modell bringt jedoch einen erheblichen **administrativen und infrastrukturellen Aufwand** mit sich. Neben der initialen Konfiguration müssen Themen wie Zertifikationsmanagement, Hochverfügbarkeit, Monitoring und Security regelmäßig betreut werden. Dieser hohe technische und organisatorische Investitionsaufwand hat dazu geführt, dass viele Unternehmen – auch viele IT-Administratoren – von der Einführung dieser Technologie abgesehen haben.

Stattdessen hat sich in der Praxis die **Passwort-Hash-Synchronisierung** als bevorzugter Standard etabliert. Dieses Verfahren wird auch von Microsoft in offiziellen Empfehlungen häufig als bevorzugtes Authentifizierungskonzept genannt. Bei entsprechender Filterung (z. B. über OUs oder Benutzergruppen) lässt sich so eine robuste und wartungsarme hybride Umgebung realisieren. Aus Sicht der Administration stellt die Hash-Synchronisierung derzeit die **einfachste und gleichzeitig stabile Lösung** für die Mehrheit der Unternehmen dar.

Ein alternativer Sonderfall ist die vollständige Verlagerung in die Cloud, also ein **Cloud-only-Szenario**. In dieser Konstellation werden sämtliche Benutzerobjekte direkt in Entra ID verwaltet, eine Synchronisation mit einem lokalen Active Directory entfällt vollständig. Solche Modelle kommen typischerweise in kleineren Unternehmen oder Startups zum Einsatz. Im Mittelstand oder bei größeren Organisationen dominiert dagegen weiterhin der hybride Ansatz, der die Vorteile beider Welten kombiniert.

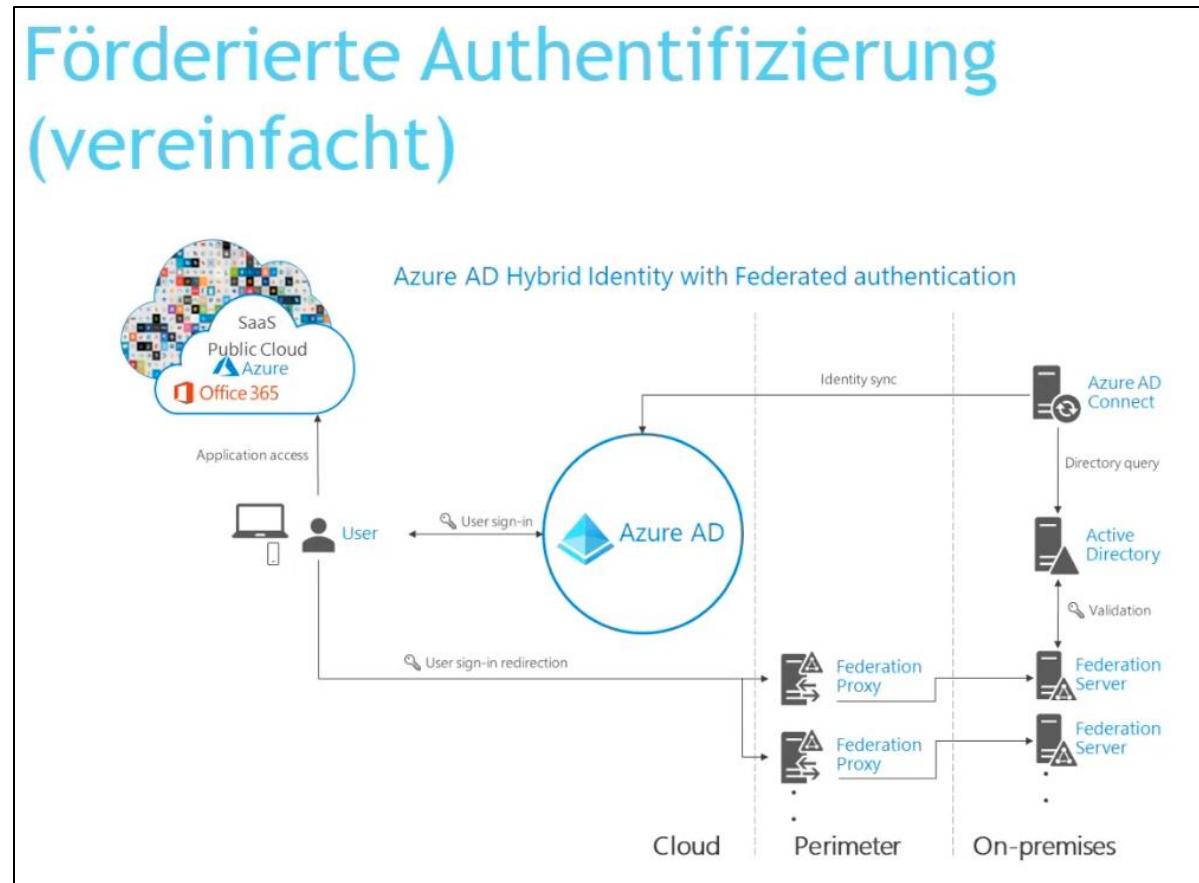


Bild 14: Förderierte Authentifizierung

Vergleichstabelle: Authentifizierungsmodelle in Entra ID

Merkmal	Passwort-Hash-Synchronisierung	AD FS (Föderierte Authentifizierung)	Cloud-only Identitäten
Infrastrukturbedarf	Gering (nur Entra ID Connect)	Hoch (mind. 4 zusätzliche Server nötig)	Kein lokales AD erforderlich
SSO-Funktionalität	Eingeschränkt (kein echtes SSO)	Vollständiges SSO über Kerberos/Token	Ja, für alle cloudbasierten Dienste
Verfügbarkeit bei Ausfall AD	Anmeldung weiterhin möglich	Anmeldung abhängig vom lokalen AD	Unabhängig vom lokalen Netz
Administrative Komplexität	Niedrig	Hoch	Niedrig
Empfohlen für	Standard-Hybridzenarien	Spezielle Compliance-/Sicherheitsanforderungen	Kleine Unternehmen, Startups
Sicherheitsfeatures	Unterstützt Conditional Access	Kombinierbar mit On-Prem Security-Tools	Abhängig von Cloud-Policies
Wartungsaufwand	Minimal	Hoch (inkl. Zertifikatsverwaltung)	Gering
Microsoft-Empfehlung (Standard)	✓	✗ (nur in Sonderfällen)	✓ (je nach Szenario)

Tabelle 5: Vergleich Authentifizierungsmodelle

Kapitel 11: Architektur und Funktionsweise von Entra ID Connect

Ein zentrales Element der hybriden Identitätsinfrastruktur ist **Entra ID Connect** (vormals Azure AD Connect). Diese Komponente stellt die Verbindung zwischen dem lokalen Active Directory und Microsoft Entra ID her und ermöglicht die Synchronisation von Benutzer-, Gruppen- und Geräteobjekten. Um die dahinterliegende Funktionsweise zu verstehen, ist ein Blick auf den technischen Aufbau hilfreich.

Grundsätzlich wird beim Einsatz von Entra ID Connect zwischen zwei Welten vermittelt: dem **lokalen Active Directory Forest** auf der einen Seite und dem **Azure AD Mandanten** auf der anderen. Die Synchronisation erfolgt in beiden Richtungen über klar definierte Mechanismen – primär von lokal in die Cloud, jedoch mit ausgewählten Ausnahmen auch umgekehrt, z. B. für **Passwort-Writeback** oder **Geräterückschreibung**.

Entra ID Connect nutzt intern eine integrierte, sogenannte **SQL Lightweight-Datenbank**, die bei der Installation automatisch mit eingerichtet wird. Darin befindet sich der sogenannte **Connector Space**, der als Zwischenspeicher und Kontrollinstanz für die Synchronisationsprozesse dient. Die Koordination zwischen dem lokalen Verzeichnis und Entra ID erfolgt über einen **Synchronisierungsagenten**, der auf Basis des sogenannten **Metaverse** arbeitet.

Das **Metaverse** bildet dabei eine zentrale Repräsentation der synchronisierten Objekte und dient als Abgleichsschicht für alle Änderungen. Jedes Attribut, das nach der Installation von Entra ID Connect angepasst wird, wird intern mit einem technischen „Change Flag“ versehen. Dieses signalisiert, dass eine Validierung und ggf. Synchronisierung erfolgen muss.

Die initiale Einrichtung von Entra ID Connect beginnt immer mit einem **Full Sync** (Vollständige Synchronisierung). Dabei wird das gesamte Verzeichnis überprüft und auf Basis der definierten Filterregeln (z. B. OU- oder Gruppenfilter) entschieden, welche Objekte tatsächlich synchronisiert werden sollen. Nach Abschluss dieses ersten vollständigen Abgleichs folgt ausschließlich ein **Delta Sync**, bei dem nur noch die geänderten Objekten übertragen werden.

Technisch betrachtet findet die Synchronisation in mehreren Stufen statt –**Import**, **Export** und **Sync**, jeweils für das lokale AD und für Entra ID. Das ergibt insgesamt **sechs nachvollziehbare Schritte**, die über das integrierte Tool **Synchronization Service Manager** transparent eingesehen und überwacht werden können. Dort lässt sich nachvollziehen, welche Objekte wann geändert, hinzugefügt oder entfernt wurden.

Für spezielle Anforderungen besteht zudem die Möglichkeit, anstelle der integrierten Datenbank eine eigene bestehende SQL-Server-Instanz zu verwenden. Microsoft empfiehlt jedoch den Einsatz der mitgelieferten SQL-Lightweight-Variante, da diese für den Standardbetrieb vollkommen ausreichend ist.

Auch hinsichtlich der Systemanforderungen zeigt sich Entra ID Connect äußerst ressourcenschonend. Unterstützt werden bereits Windows Server 2016, bei minimalen Anforderungen von 4 GB RAM. Damit lässt sich der Dienst problemlos in nahezu jeder Umgebung bereitstellen.

Ein solides Verständnis des Metaverse-Konzepts und der Synchronisationsvorgänge ist essenziell, um Fehlerquellen zu identifizieren, Abläufe zu optimieren und die Integration in komplexe IT-Landschaften kontrolliert umzusetzen. Die Synchronisation bildet das Rückgrat der hybriden Identitätsverwaltung und sollte entsprechend sorgfältig geplant, eingerichtet und überwacht werden.

Azure AD Connect - Komponenten

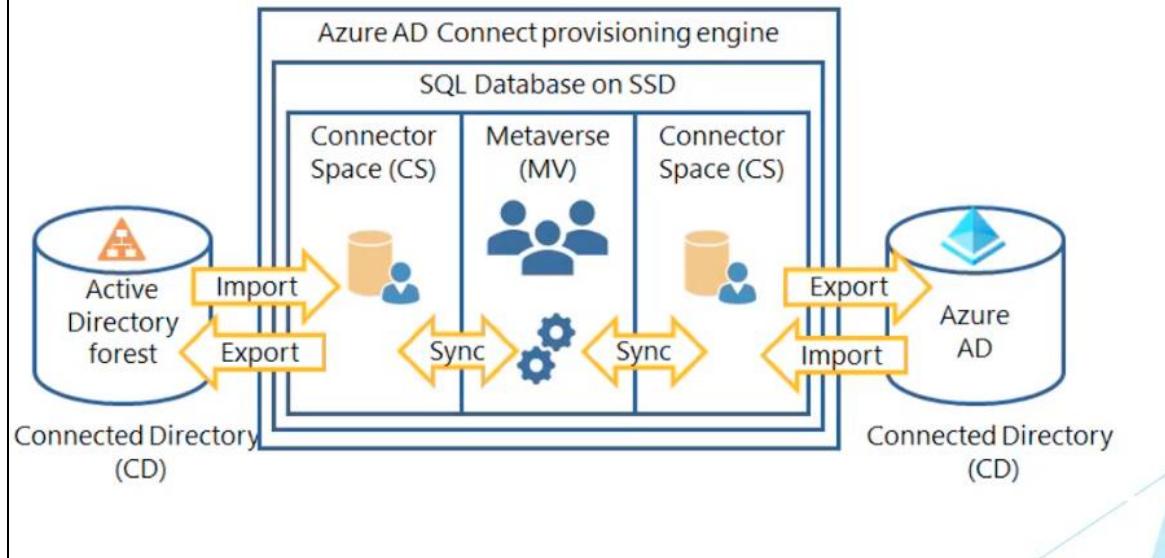


Bild 15: Azure AD Connect Komponenten

Kapitel 12: Nützliche Ressourcen und Lizenzübersichten für Entra ID

Im Rahmen der Verwaltung und Absicherung von Microsoft Entra ID sowie Microsoft 365 insgesamt ist es hilfreich, auf strukturierte, verlässliche Informationsquellen zugreifen zu können. Hierzu gibt es mehrere zentrale Plattformen, auf denen aktuelle Informationen, Lizenzbedingungen und Sicherheitsfunktionen übersichtlich dokumentiert sind.

Eine der empfehlenswertesten Quellen ist die [Microsoft 365 Guidance for Security & Compliance](#). Diese Plattform stellt nicht nur umfassende Informationen zu Microsoft 365-Diensten bereit, sondern deckt auch sicherheitsrelevante Funktionen wie **Entra ID Protection** und **Entra ID Governance** ab. Der Aufbau dieser Seiten ist weitgehend konsistent: Es wird dargestellt, welchen Nutzen ein Dienst bietet, welche Lizenzierungsmodelle unterstützt werden, wie der Dienst bereitgestellt wird (z. B. tenant- oder benutzerbasiert) und in welchen Microsoft-Plänen die jeweilige Funktion enthalten ist. Diese Form der Darstellung eignet sich ideal zur Validierung von Lizenzanforderungen und zur Einschätzung, welche Funktionen in der eigenen Umgebung nutzbar sind.

Microsoft 365 guidance for security & compliance

Article • 03/27/2025 • 23 contributors

 Feedback

In this article

- [Microsoft Entra ID Governance](#)
- [Microsoft Entra ID Protection](#)
- [Compliance Program for Microsoft Cloud](#)
- [Microsoft Defender for Business](#)

[Show 28 more](#)

For the purposes of this article, a tenant-level service is an online service that is activated in part or in full for all users in the tenant (standalone license and/or as part of a Microsoft 365 or Office 365 plan). Appropriate subscription licenses are required for customer use of online services. To see the options for licensing your users to benefit from Microsoft 365 compliance features, download the Microsoft 365 Comparison table for Enterprise and Frontline Workers Plans  or the Microsoft 365 Comparison table for Small and Medium Business  Plans.

Some tenant services aren't currently capable of limiting benefits to specific users. To review the terms and conditions governing the use of Microsoft products and Professional Services acquired through Microsoft Licensing programs, see the [Product Terms](#) .

Bild 16: Microsoft 365 guidance Quelle: Microsoft Learn

Ergänzend zur offiziellen Guidance bietet sich die Nutzung der sogenannten [M365 Maps](#) an. Diese werden von **Aaron Dinnage**, einem Microsoft-Mitarbeiter, regelmäßig aktualisiert und stellen eine inoffizielle, aber weit verbreitete und anerkannte Übersicht über die Lizenzverfügbarkeit von Microsoft 365-Diensten dar. Die M365 Maps bieten zwei zentrale Darstellungen:

1. **Interaktive Matrix-Ansicht**, über die man auf Services wie **Privilege Identity Management**, **Access Reviews**, **Entitlement Management** oder **Entra ID Protection** zugreifen kann. Ein Klick führt dabei direkt zu den zugehörigen offiziellen Learn-Artikeln.

Feature Matrix					
Office 365 Enterprise	E1	E3	E5		
Microsoft 365 Business	Basic	Standard	Premium		
Microsoft 365 Frontline	F1	F3	F5 Sec	F5 Comp	F5 Sec+Comp
Microsoft 365 Enterprise	E3	E5 Sec	E5 Comp	E5	
Microsoft 365 Education	A1 (Legacy)	A1 for Devices	A3	A5 Sec	A5 Comp
					A5
<input checked="" type="checkbox"/> Select All	<input type="checkbox"/> Select None	<input type="checkbox"/> Save Selection		<input type="checkbox"/> Download	<input type="checkbox"/> Export
<input type="checkbox"/> Feature Map	<input type="checkbox"/> New	<input type="checkbox"/> Load	<input type="checkbox"/> Save	<input type="checkbox"/> Close	<input type="checkbox"/> Timeline
<input type="text"/> Search for a feature ...		Office 365		Microsoft 365 Bu	
Feature	E1	E3	E5	Basic	Standard
Office 365	E1	E3	E5		
Activity Reports	✓	✓	✓	✓	✓
Adoption Score	✓	✓	✓	✓	✓
Alert Policies	✓	✓	✓	✓	✓
Audit (premium)			✓		
Audit (standard)	✓	✓	✓	✓	✓
Basic Mobility & Security	✓	✓	✓	✓	✓
Bookings	✓	✓	✓	✓	✓

Bild 17: Feature Matrix Quelle: Aaron Dinnage

2. Tabellarische Feature-Matrix, in der sich verschiedene Microsoft-365-Pläne (z. B. E3, E5, P1, P2, Education) miteinander vergleichen lassen. Diese bietet einen schnellen Überblick, welche Entra-ID-bezogenen Funktionen in welchem Lizenzmodell enthalten sind.

<input type="text"/> Search for a feature ...		Office 365	Microsoft 365 Business	
Feature		E3	E5	Premium
Office 365	E3	E5		
Activity Reports	✓	✓		✓
Adoption Score	✓	✓		✓
Alert Policies	✓	✓		✓
Audit (premium)		✓		
Audit (standard)	✓	✓		✓
Basic Mobility & Security	✓	✓		✓
Bookings	✓	✓		✓
Communication Compliance		✓		
Compliance Manager	✓	✓		✓
Content Search	✓	✓		✓
Copilot Studio for Teams	✓	✓		✓
Customer Key		✓		
Customer Lockbox	✓			

Bild 18: Vergleich E3, E5, Premium Quelle: Aaron Dinnage

Solche Quellen sind insbesondere dann hilfreich, wenn in Unternehmen die Lizenzverantwortung intern geregelt wird oder Evaluierungen bevorstehen, welche Lizenzfunktionen aktiviert oder benötigt werden.

Eine weitere nützliche Übersicht stellt die **Auflistung aller administrativen Portale** in Microsoft 365 dar, welches über die Seite cmd.ms erfolgt. Derzeit existieren über 20 verschiedene Admin-Center, von denen etwa 16 öffentlich zugänglich und direkt nutzbar sind. Diese verteilten Verwaltungsoberflächen können für Administratoren schnell unübersichtlich werden. Die verlinkte Zusammenstellung bietet daher eine

gute Hilfestellung zur Navigation zwischen den verschiedenen Portalen, z. B. Entra Admin Center, Exchange Admin Center, Defender, Compliance oder Intune.

[cmd.ms] the Microsoft Cloud command line!

Are you tired of clicking around in Microsoft portals to get to a blade?

⚡ Use the power of your browser's address bar to quickly get to your favorite blade in Azure, Microsoft 365, Entra ID, Intune...

Try it out. Open a new tab and type **[command].cmd.ms** using any of the commands or alias from the list below.

Remember to [check out the browser extensions](#) that add support for auto-complete in the address bar.



The screenshot shows a search interface for Microsoft Cloud commands. At the top left is a dropdown menu labeled "All Microsoft Portals". To its right is a search bar with the placeholder "Search commands...". Below the search bar is a table with three columns: "NAME", "COMMAND", and "ALIAS". The table contains three rows:

	NAME	COMMAND	ALIAS
❖	Microsoft Entra	en.cmd.ms	ad,aad,entra
❖	Microsoft Entra for GCC High	eng.cmd.ms	adg,aadg,entrag
❖	Microsoft Entra (Azure Portal)	azad.cmd.ms	

Bild 19: Microsoft Cloud command Quelle: cmd.ms

Kapitel 13: Einrichtung der lokalen Active Directory-Struktur und Vorbereitung der Synchronisierung

Die erste praktische Grundlage für den hybriden Betrieb mit Entra ID ist die Installation und Konfiguration eines **lokalen Active Directory Domain Controllers (AD DS)**. Dieser Schritt bildet die Basis für die spätere Synchronisierung mit Microsoft Entra ID über Entra ID Connect. Die Installation des AD-Rollendienstes ist in den meisten Fällen ein standardisierter Vorgang, der mit wenigen Konfigurationsschritten über den Server-Manager durchgeführt wird.

In der Praxis stellt dieser Installationsprozess zu Beginn einen sogenannten „No-Brainer“ dar – viele Schritte laufen im Stil von *weiter, weiter, fertigstellen* ab. Die Herausforderung liegt eher in der späteren Einrichtung und Konfiguration von Entra ID Connect, die mehr Aufmerksamkeit und Feinabstimmung erfordert.

Vor dem Start empfiehlt es sich, eine kleinere Anpassung vorzunehmen, um die Benutzererfahrung bei der weiteren Einrichtung zu verbessern: die **Deaktivierung der IE Enhanced Security Configuration**. Diese verhindert ständige Sicherheitsabfragen beim Öffnen von Webseiten im Internet Explorer oder Microsoft Edge – was insbesondere beim Download von Setup-Dateien oder beim Zugriff auf Webportale störend sein kann. Die Einstellung findet sich im **Server Manager** unter dem Reiter *Local Server*, mittig im Abschnitt *IE Enhanced Security Configuration*. Für eine reibungslose Einrichtung sollte diese Funktion für Administratoren und Benutzer auf „Off“ gesetzt werden.



Bild 20: Konfiguration

Im Anschluss erfolgt die Vorbereitung der benötigten Installationsdateien. Über den Browser wird zunächst nach dem [Download von Entra ID Connect](#) gesucht. Der offizielle Microsoft-Link liefert hier die passende Version. Ebenso wichtig ist das Herunterladen des Tools [IDFix](#) über das GitHub-Repository. IDFix wird später zur Bereinigung des Active Directory genutzt, um potenzielle Synchronisierungsfehler (z. B. doppelte UPNs oder fehlerhafte SMTP-Adressen) vorab zu identifizieren und zu beheben.

Alternate MSI Installation

If running the ClickOnce application is not desirable or is not possible in your environment, you can install it using one of the MSI's located at: <https://github.com/microsoft/idfix/tree/master/MSIs>

Note that only the ClickOnce application is self-updating to the latest version.

Bild 21:Entra ID Installation

Nachdem diese Vorbereitungen abgeschlossen sind, kann die eigentliche Serverrolle installiert werden. Über den Manage Reiter oben rechts wird „**Add Roles and Features**“ geöffnet. Im Auswahlbereich unter **Server Roles** wird *Active Directory Domain Services* ausgewählt. Sobald diese Rolle hinzugefügt wurde, erfolgt die **Promotion des Servers zum Domain Controller**. Es wird ein neuer Forest mit einem Root-Domain-Namen angelegt. Es sei darauf hingewiesen, dass die Verwendung von .local-Domains in produktiven Umgebungen zunehmend kritisch betrachtet wird – insbesondere in Bezug auf **DNS-Auflösung, Routing und die globale Eindeutigkeit von Domännamen**.

Nachdem diese Vorbereitungen abgeschlossen sind, kann die eigentliche Serverrolle installiert werden. Über den Manage Reiter oben rechts wird „**Add Roles and Features**“ geöffnet. Im Auswahlbereich unter **Server Roles** wird *Active Directory Domain Services* ausgewählt und auf *Add Features* geklickt.

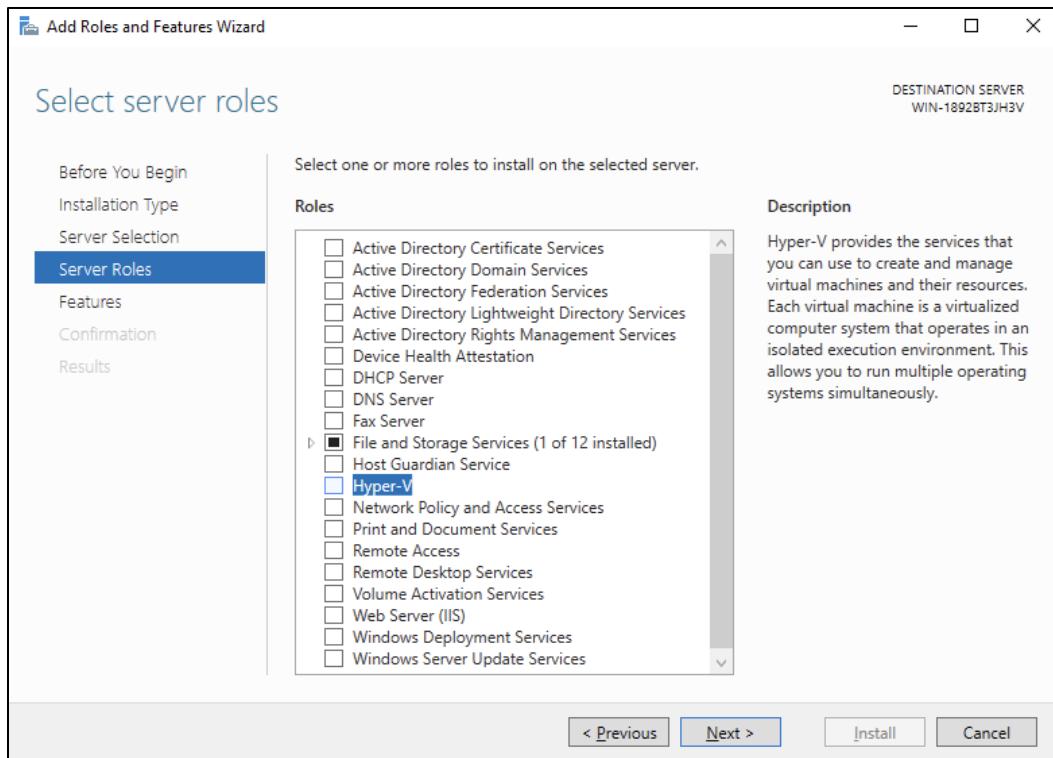


Bild 22: Server roles

Während des Assistentenlaufs erscheint bereits der Hinweis, ob eine **hybride Verbindung zur Cloud** hergestellt werden soll – dies wird später im Rahmen der Entra ID Connect Konfiguration umgesetzt. An dieser Stelle kann jedoch zunächst mit „Next“ fortgefahren werden.

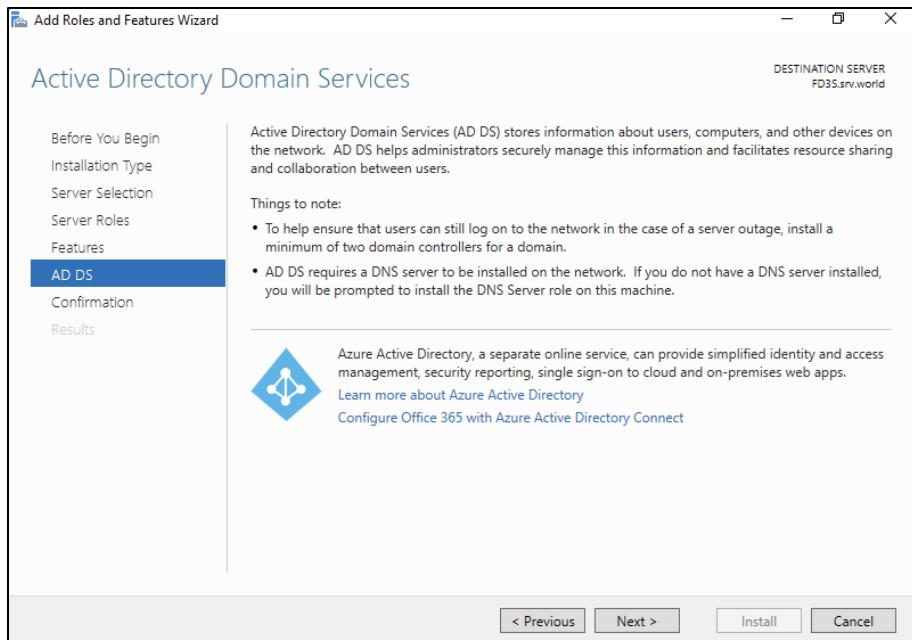


Bild 23: Active Directory Domain Server

Im weiteren Verlauf empfiehlt es sich, den Haken bei „**Restart the destination server automatically if required**“ zu setzen. Dieser Schritt ist notwendig, da der Server im Anschluss an die Rollenzuweisung auch zum **Domain Controller (DC) promotet** werden muss. Der Prozess umfasst somit zwei Phasen: zunächst die Installation der Rolle selbst, anschließend die Promotion und der damit verbundene Neustart des Systems. Sobald diese Optionen gesetzt sind, wird die Installation mit einem Klick auf „Install“ gestartet.

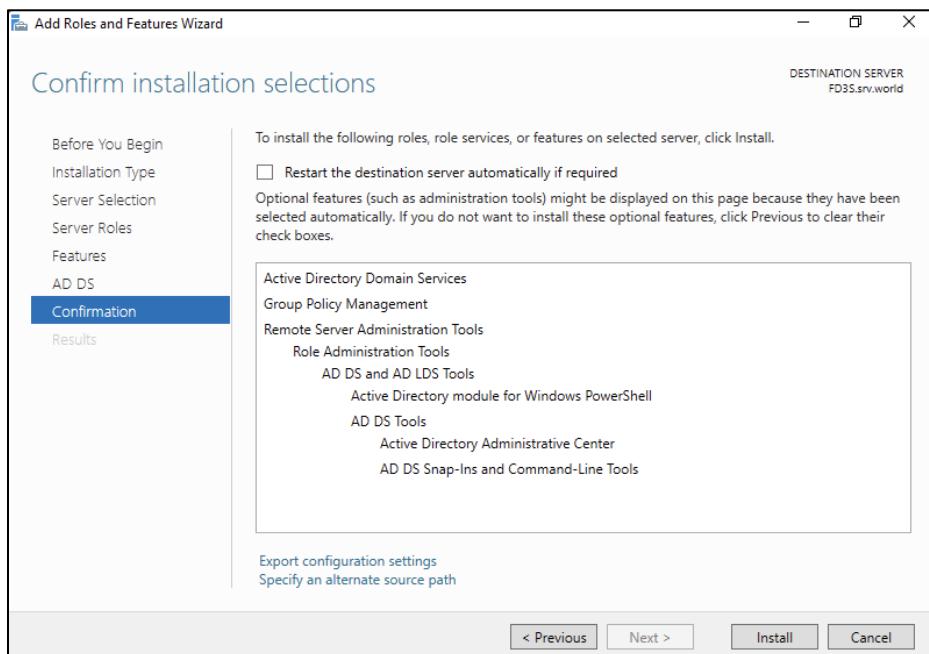


Bild 24: Confirm installation selections

Nach der Installation wird auf **Promote this server to a domain controller** geklickt. Anschließend wird **Add a new forest** ausgewählt. Ein neuer Forest mit einem Root-Domain-Namen wird hier angelegt. Es

sei darauf hingewiesen, dass die Verwendung von .local-Domains in produktiven Umgebungen zunehmend kritisch betrachtet wird – insbesondere in Bezug auf **DNS-Auflösung, Routing** und die **globale Eindeutigkeit von Domainnamen**. Auch wenn diese Konfiguration in Testszenarien häufig verwendet wird, empfiehlt es sich in produktiven Setups eine domainkonforme Benennung mit gültigen, routablen Domain-Endungen.

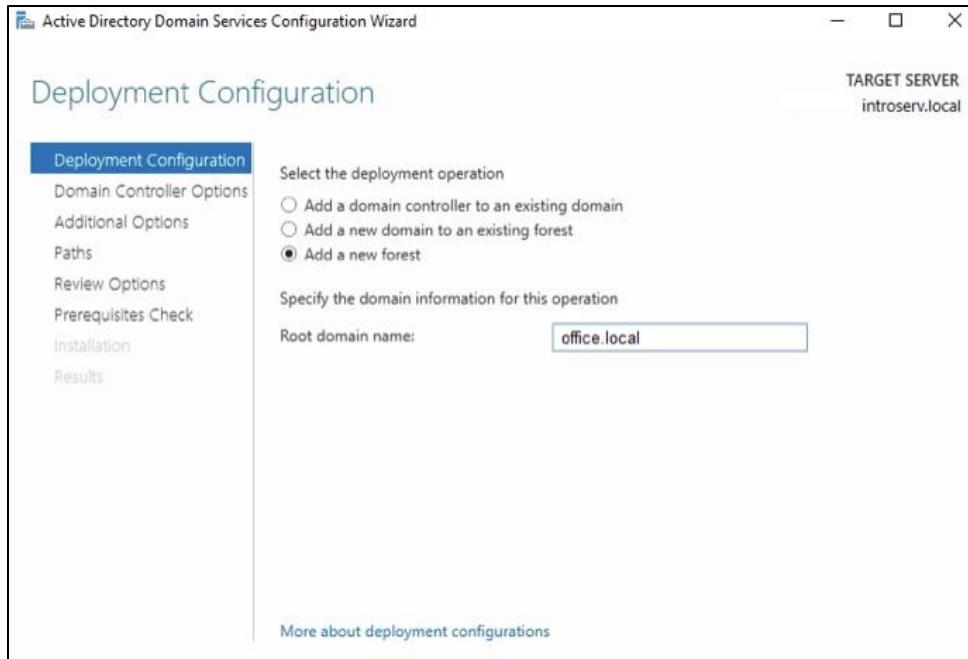


Bild 25: Deployment Configuration

Im Rahmen der Einrichtung wird abschließend ein sicheres Standardkennwort vergeben. Dies gilt sowohl für die Domänenkonfiguration als auch für die später anzulegenden Benutzerkonten. Die restlichen Schritte der Promotion lassen sich mit den Standardeinstellungen abschließen. Nachdem der Domain Controller erfolgreich eingerichtet wurde, erfolgt der Neustart des Servers.

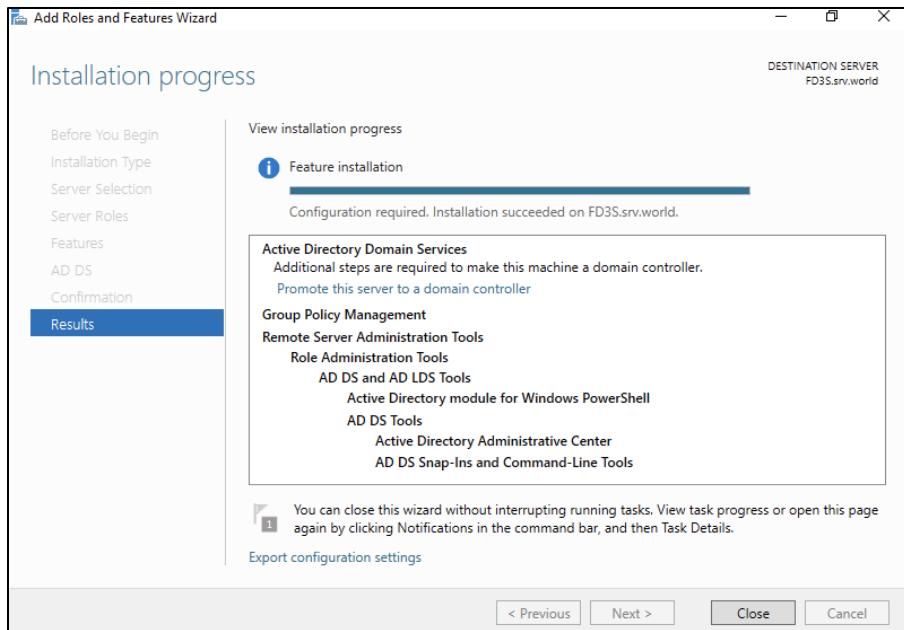


Bild 26: Installation progress

Nach dem Reboot steht die Basisinfrastruktur bereit, um Benutzerkonten zu erstellen und die **hybride Verbindung zu Entra ID** aufzubauen. Die weitere Konfiguration der Synchronisierung erfolgt im Anschluss über Entra ID Connect.

Kapitel 14: Benutzeranlage und Verzeichnisbereinigung mit IDFix

Nach erfolgreicher Einrichtung des Domain Controllers und der Grundkonfiguration der lokalen Active Directory-Umgebung folgt die Anlage der Benutzerkonten, die später mit Microsoft Entra ID synchronisiert werden sollen. Im Rahmen dieses Schulungsszenarios wird zunächst eine neue Organisationseinheit (OU) im Active Directory erstellt. Diese OU dient als logische Gruppierung für Benutzerobjekte, die für die Synchronisation vorgesehen sind.

In dieser OU werden exemplarisch drei Benutzerkonten angelegt. Diese werden im Servermanager unter *Tools* und dann unter *Users and Computers* angelegt. Die Kennwörter werden einheitlich gesetzt, wobei die Option „Kennwort bei nächster Anmeldung ändern“ deaktiviert wird. Ziel ist es, in einem überschaubaren und konsistenten Setup zu arbeiten, das sich für Schulungs- und Testzwecke eignet.

Bevor die Benutzerobjekte mit der Cloud synchronisiert werden, sollte das Verzeichnis überprüft und bereinigt werden. Dazu wird das Tool **IDFix** verwendet. Es dient der Analyse des lokalen Active Directory hinsichtlich Attributfehlern, die bei der Synchronisierung mit Entra ID zu Problemen führen könnten – etwa doppelte UPNs, ungültige Zeichen oder fehlerhafte Top-Level-Domains.

Nach dem Start von IDFix wird über den Befehl **Query** das AD-Verzeichnis analysiert. Das Tool liefert eine Übersicht problematischer Objekte. In diesem Fall weist es auf mehrere Benutzerkonten hin, bei denen der **userPrincipalName (UPN)** auf einer .local-Domäne basiert. Solche Domains sind **nicht routbar** und führen dazu, dass Benutzer in Entra ID automatisch mit einer generischen @onmicrosoft.com-Adresse angelegt werden. Das kann insbesondere bei der Verwendung von Microsoft Teams oder Exchange Online zu Problemen führen.

Beim Durchsehen der IDFix-Ergebnisse fällt auf, dass neben dem **Distinguished Name** (also dem vollständigen Pfad zum Objekt im AD), den **Common Name**, die Objektklasse, das betroffene Attribut angezeigt werden – in diesem Fall der **userPrincipalName**. Das Tool zeigt dabei auch an, wenn es sich um ungewöhnliche oder inkorrekte Objektklassen handelt, auch wenn ein Benutzerobjekt als „Kontakt“ eingetragen ist.

Theoretisch wäre es möglich, dass ein Benutzer sich nicht mit der UPN anmeldet, sondern auch über alternative Attribute wie Straßennamen oder eine Telefonnummer anmeldet. Technisch wird das vom Verzeichnisdienst unterstützt – **praktikabel ist es jedoch nicht**, und **Microsoft empfiehlt ausdrücklich, den UPN als Standardanmeldeattribut zu verwenden**. Diese Empfehlung basiert auf langjähriger Erfahrung in der Cloud- und Hybrid-Administration.

Im konkreten Fall zeigt IDFix den **Fehler „TopLevelDomain“**. Das Value, welches dahinter steht würde zu Problemen führen, weil der UPN die nicht-routbaren Domain **.local** enthält. Wird ein solcher Benutzer in Entra ID synchronisiert, erhält er automatisch eine Cloudadresse mit **.onmicrosoft.com**. Diese ist funktional, aber in der Praxis **nicht benutzerfreundlich oder kommunikationstauglich**, etwa für Teams, Outlook oder SharePoint-Zugriffe. Stattdessen sollte ein **öffentlich registrierter Domänensuffix** verwendet werden.

Zur Behebung dieser Problematik stehen mehrere Optionen zur Verfügung. In einem ersten Schritt kann der UPN einzelner Benutzer direkt in IDFix angepasst werden – beispielsweise durch Umbenennung der Domain. Im gezeigten Beispiel wird daher der Benutzer *Jonas* über die Update-Funktion in IDFix angepasst. Dazu wird der .local-Teil im UPN durch eine passende .com Domain ersetzt und über **Apply** übernommen. Anschließend wird der **Accept** Befehl durchgeführt. Nun steht unter **Action Edit**. Nach einer erneuten Durchführung von **Apply** wurde das **Edit in Complete umgeändert**. Nach einer erneuten Analyse durch IDFix über **Query** verschwindet der Benutzer aus der Fehlerliste – ein Hinweis darauf, dass die Änderung korrekt übernommen wurde.

Im lokalen AD kann nun beim entsprechenden Benutzer unter **Account** der neue **User Loginname** eingesehen werden. Alternativ können auch alle User markiert werden, mit einem Rechtsklick in alle Eigenschaften der User gehen und den Suffix so ändern. Eine weitere Möglichkeit geht über den Servermanager. Hier wird der Reiter **Tools** und anschließend **Domains and Trust** ausgewählt. Mit einem Rechtsklick auf **Active Directory Domains** öffnet sich ein Menü. Hier wird **Properties** ausgewählt und dort kann bei **Alternative UPN suffixes** die passende .com Dmain eingetippt werden. Mit **Add** und anschließend **Apply** kann das Suffix hinzugefügt werden. Dieser kann anschließend für Benutzerkonten ausgewählt werden, um alle betroffenen Objekte konsistent anzupassen.

Die Überarbeitung der UPNs sollte systematisch für alle zu synchronisierenden Benutzer erfolgen. Neben UPN-Fehlern erkennt IDFix auch weitere gängige Probleme, etwa **doppelte SMTP-Adressen, ungültige Zeichen** in Attributwerten oder **nicht unterstützte Objektklassen**, welche zu einem sogenannten **Miss**

Match führen würden. Nach Abschluss aller Anpassungen kann IDFix erneut ausgeführt werden, um sicherzustellen, dass keine kritischen Konflikte mehr vorliegen.

Obwohl viele dieser Korrekturen auch manuell im Active Directory möglich sind, bietet IDFix eine zentrale, übersichtliche Möglichkeit zur Vorabkontrolle und -korrektur. Ursprünglich als **Community-Projekt** gestartet, wurde es später von Microsoft übernommen und offiziell in das GitHub-Repository eingebunden – inklusive Microsoft-Branding, aber weiterhin mit starkem Community-Background.

Die Anwendung von IDFix wird daher als **Best Practice** vor jeder erstmaligen Synchronisierung empfohlen. Sie hilft, potenzielle Fehler frühzeitig zu identifizieren, die Datenqualität zu verbessern und spätere Konflikte mit Entra ID zu vermeiden.

Kapitel 15: Installation und Konfiguration von Microsoft Entra ID Connect

Nach der Vorbereitung der lokalen Active Directory-Umgebung und der Bereinigung durch IDFix folgt nun ein zentraler Schritt im Aufbau der hybriden Identitätsstruktur: die Installation von **Microsoft Entra ID Connect**. Dieses Tool ist das Bindeglied zwischen dem lokalen Verzeichnisdienst (Active Directory) und dem cloudbasierten Microsoft Entra ID.

Ein Blick auf die Installationsdatei zeigt bereits die bestehende Namensinkonsistenz: Während die aktuelle Oberfläche und der Dienst als **Entra ID Connect Sync** erscheinen, trägt die Installationsdatei nach wie vor den Namen „AzureADConnect.msi“. Dieser Umstand ist Ausdruck einer noch nicht vollständig vollzogenen Umbenennung durch Microsoft – Begriffe wie Azure AD und Entra ID werden in Dokumentationen und Tools teils noch synonym verwendet. Für Administratoren bedeutet das: Aufmerksamkeit beim Umgang mit Dokumentation und Pfaden ist weiterhin erforderlich.

Nach dem Start des Installationsassistenten bietet sich zunächst die Möglichkeit, über „**Use Express Settings**“, unten rechts, eine vereinfachte, standardisierte Einrichtung vorzunehmen. Trotz der vermeintlichen Zeitersparnis ist hiervon **dringend abzuraten**. Die Expressinstallation übernimmt alle Objekte ohne Filterung – inklusive Servicekonten, technischer Objekte oder veralteter Einträge – und lässt keinerlei granularen Steuerungsspielraum zu. Aus schulischer wie auch praktischer Sicht sollte stets die Option „**Customize**“ gewählt werden, um die Kontrolle über den Einrichtungsprozess zu behalten.

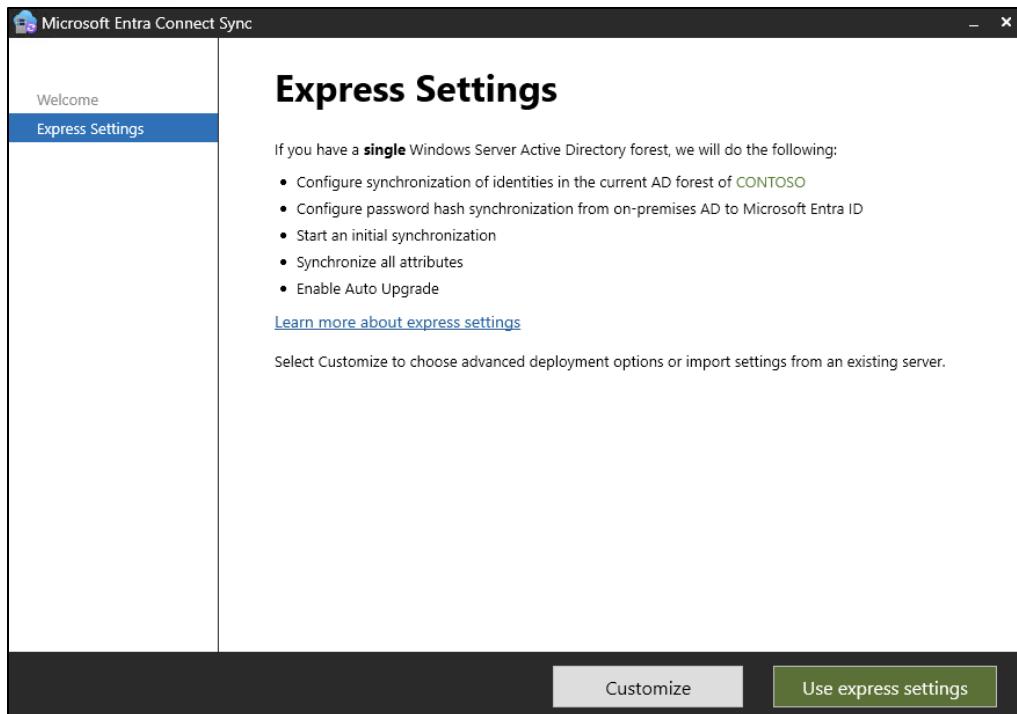


Bild 27: Express Settings

Die benutzerdefinierte Installation bietet mehrere wichtige Installationspunkte:

- **Specify a custom installation location:** Installation in einem abweichenden Pfad, falls gewünscht.
- **Use an existing SQL Server:** Möglichkeit, eine bereits vorhandene SQL-Instanz anstelle der mitgelieferten zu verwenden.
- **Use an existing service account:** Anlegen oder Verwenden eines dedizierten Servicekontos mit Mitgliedschaft in der Gruppe der Unternehmensadministratoren. Die Entscheidung, ein eigenes Servicekonto zu verwenden, hat insbesondere dann Vorteile, wenn im Unternehmen **klare Namenskonventionen oder Richtlinien zur Kontenverwaltung** bestehen. Lässt man das Konto automatisch vom Entra ID Connect-Assistenten erstellen, wird ein technisch generierter Name vergeben, der sich nur schwer in bestehende Verwaltungsschemata einfügt.
- **Specify custom sync groups:** Option zur Verwendung benutzerdefinierter Gruppen oder OUs als Basis für die Synchronisation.
- **Import synchronization settings:** Das ist insbesondere im Zusammenhang mit **Staging-Servern** nützlich ist. Es ermöglicht den Export und die Wiederverwendung bestehender Konfigurationen – etwa für Failover-Umgebungen.

Diese Punkte können auch später bei der Konfiguration vom Entra ID eingerichtet werden.

Besonderes Augenmerk verdient der Punkt **Gruppensynchronisierung**. Microsoft empfiehlt, bei der Synchronisierung über Gruppen 500 Objekte nicht zu überschreiten. In der Praxis funktioniert auch eine höhere Anzahl, jedoch ist dies **nicht offiziell supportet**. Sollte ein Microsoft Support-Fall eröffnet werden, ist mit dem Hinweis zu rechnen, dass die Gruppengröße zuerst zu reduzieren sei.

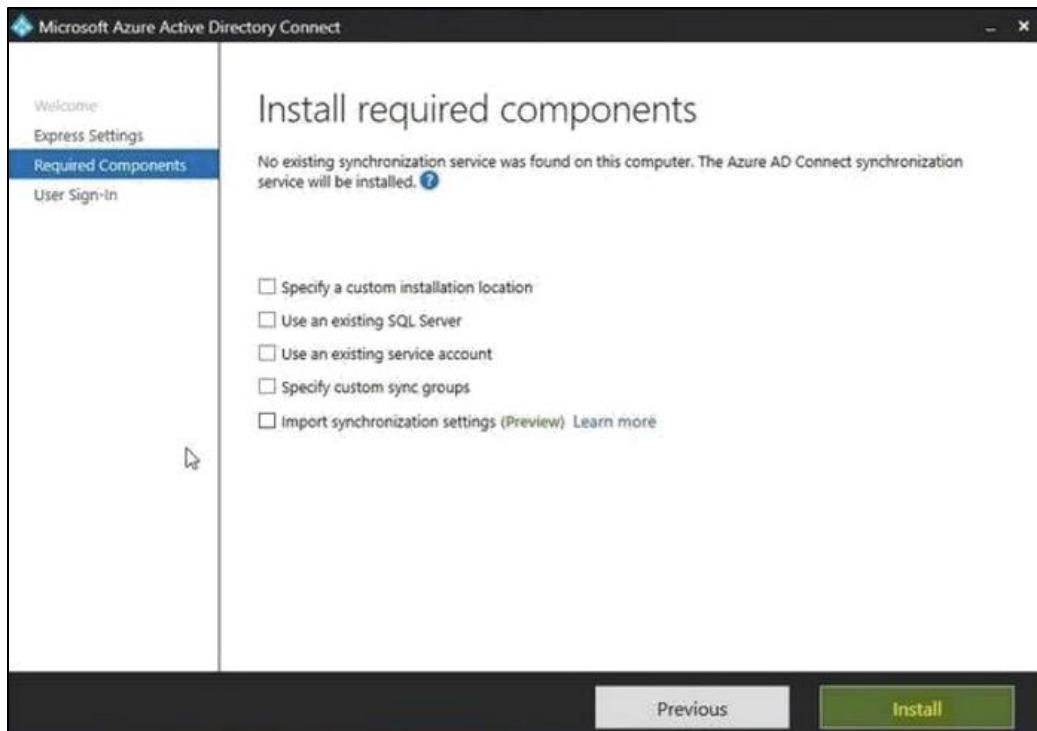


Bild 28: Install required components

Nach Abschluss der Einstellungen erfolgt die Installation. Danach geht die Konfiguration mit dem **User Sign-in** weiter.

Auswahl der Authentifizierungsmethode in Microsoft Entra ID Connect

Nach der grundlegenden Einrichtung von Microsoft Entra ID Connect folgt ein zentraler Punkt in der Konfiguration hybrider Identitäten: die Auswahl der Authentifizierungsmethode. Entra ID Connect stellt dafür mehrere Optionen zur Verfügung, die unterschiedliche Anforderungen an Infrastruktur, Ausfallsicherheit und Verwaltungsaufwand mit sich bringen.

Die Entscheidung, welche Authentifizierungsmethode zum Einsatz kommt, sollte stets mit Blick auf bestehende Systeme, geplante Redundanzszenarien sowie die Verfügbarkeit von Administratoren und Ressourcen erfolgen. Für den Einstieg in die hybride Welt empfiehlt sich in der Regel der **Password Hash Sync (PHS)**, der im Folgenden zuerst behandelt wird.

Password Hash Synchronization (PHS)

Diese Methode stellt den Standardweg dar und wird von Microsoft für die meisten Szenarien empfohlen. Hierbei werden gehashte Passwörter aus dem lokalen Active Directory in regelmäßigen Abständen sicher in die Cloud synchronisiert. Die Anmeldung erfolgt dann direkt gegen Microsoft Entra ID – auch bei temporären Ausfällen des lokalen Netzwerks bleibt der Zugriff möglich.

Vorteile:

Kein zusätzlicher Infrastrukturaufwand
Minimale Abhängigkeit vom lokalen Netzwerk
Einfache Verwaltung und hoher Automatisierungsgrad
Unterstützung für Seamless SSO

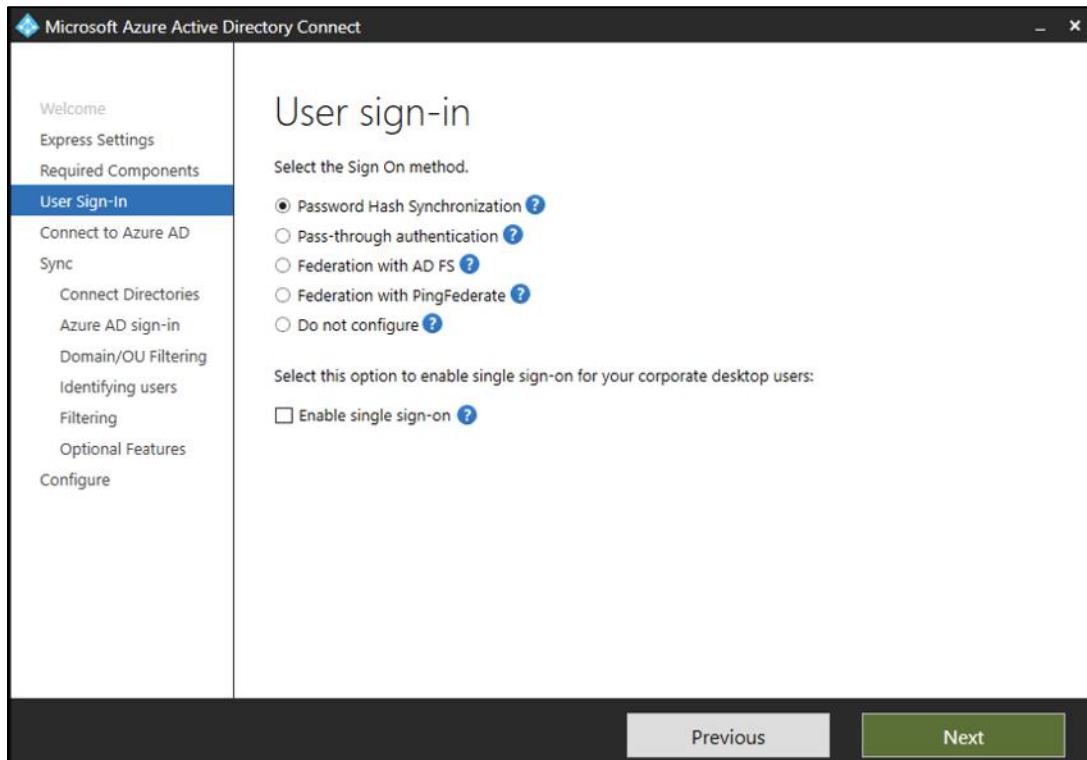


Bild 29: User sign in Password Hash

Pass-through Authentication (PTA)

Hier erscheint zunächst folgender Hinweis: „We recommend that you have a cloud only Hybrid Identity Administrator or Global Administrator account so that you are able to manage pass-through authentication in the event of on-premise failure.“

Bei PTA werden Benutzeranmeldeinformationen nicht in der Cloud gespeichert. Stattdessen wird bei jeder Anmeldung eine sichere Verbindung zum lokalen Netzwerk hergestellt und die Authentifizierung dort durchgeführt. Dies erfolgt über sogenannte **Authentication Agents**, die lokal installiert sind.

Sollte das SSO Konstrukt zusammenbrechen, das Internet fällt aus oder Server ist nicht mehr erreichbar, ist eine Anmeldung über PTA nicht mehr möglich – auch nicht für Administratoren. Daher erscheint hier der Hinweis, dass die administrativen Konten voneinander separiert sein sollten. Eine technische Anforderung, den Agent auf einem separaten Server zu betreiben, besteht nicht – wird aber aus Redundanzgründen empfohlen. Für die Redundanz sollte es nicht auf demselben Server installiert sein wie das Entra ID Connect. Das ist bei der Federation with AD FS anders.

Hinweis für Fortgeschrittene: PTA kann durch mehrere redundante Agents abgesichert werden. Eine technische Anforderung, den Agent auf einem separaten Server zu betreiben, besteht nicht – wird aber aus Redundanzgründen empfohlen.

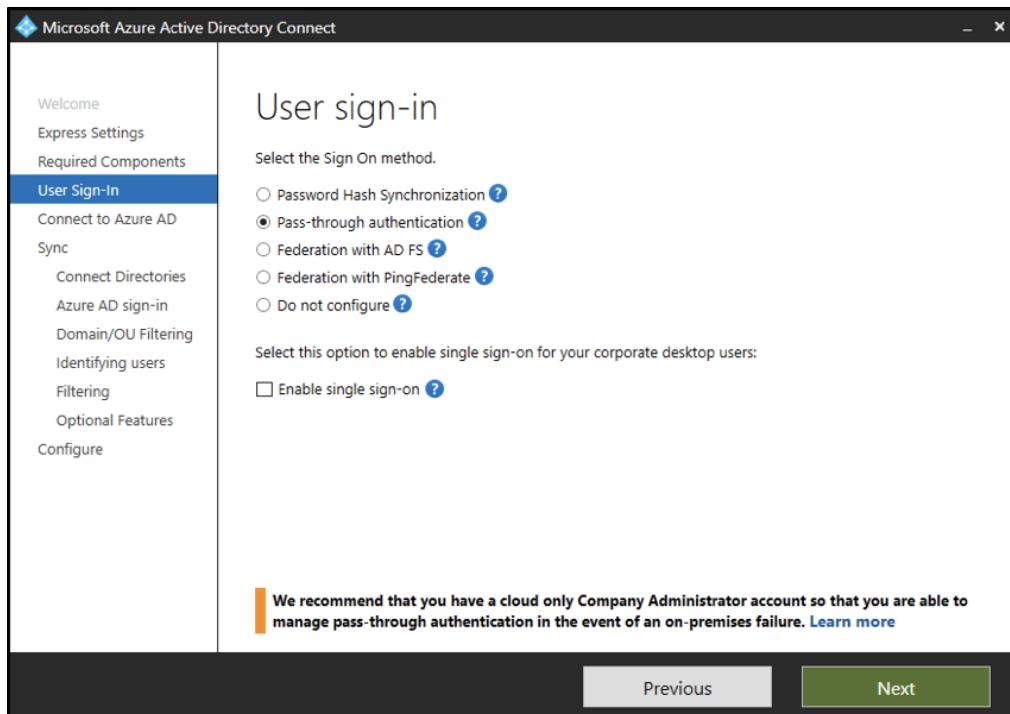


Bild 30: User sign-in Pass-through

Federation with AD FS

Bei dieser Option erfolgt die Authentifizierung über ein lokales Federation-System, meist auf Basis von **Active Directory Federation Services (AD FS)**. Dies ermöglicht komplexere Szenarien wie Multi-Factor Authentication oder Conditional Access auf On-Premise-Basis.

Aufwand und Voraussetzungen:

- Installation eines ADFS-Servers und eines Web Application Proxy (WAP)
- Betrieb, Pflege und Absicherung der ADFS-Infrastruktur
- Erfordert tiefgehende Kenntnisse und Planung

Hier sollte der Aufwand, welcher benötigt wird, nicht unterschätzt werden.

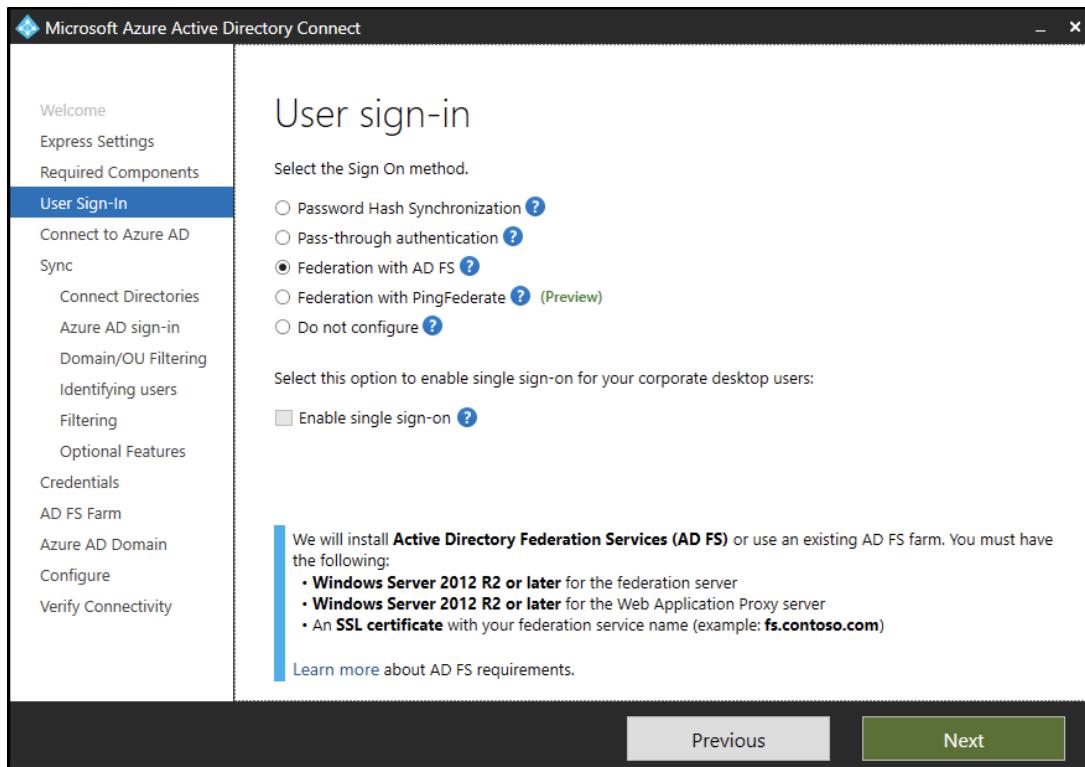


Bild 31: User sign-in Federation with AD FS

Federation with PingFederate

Neben AD FS unterstützt Entra ID Connect auch Federation-Setups mit **PingFederate** – einer kommerziellen Lösung eines Drittanbieters. Der Einsatz dieser Lösung setzt vorhandene Lizenzverträge und entsprechende Kenntnisse voraus.

Die Nennung von PingFederate zeigt exemplarisch, dass Microsoft auch Drittanbieter in die Konfiguration integriert. Die Wahl anderer SAML- oder WS-Federation-Systeme ist ebenfalls möglich, erfordert jedoch manuelle Konfigurationsschritte.

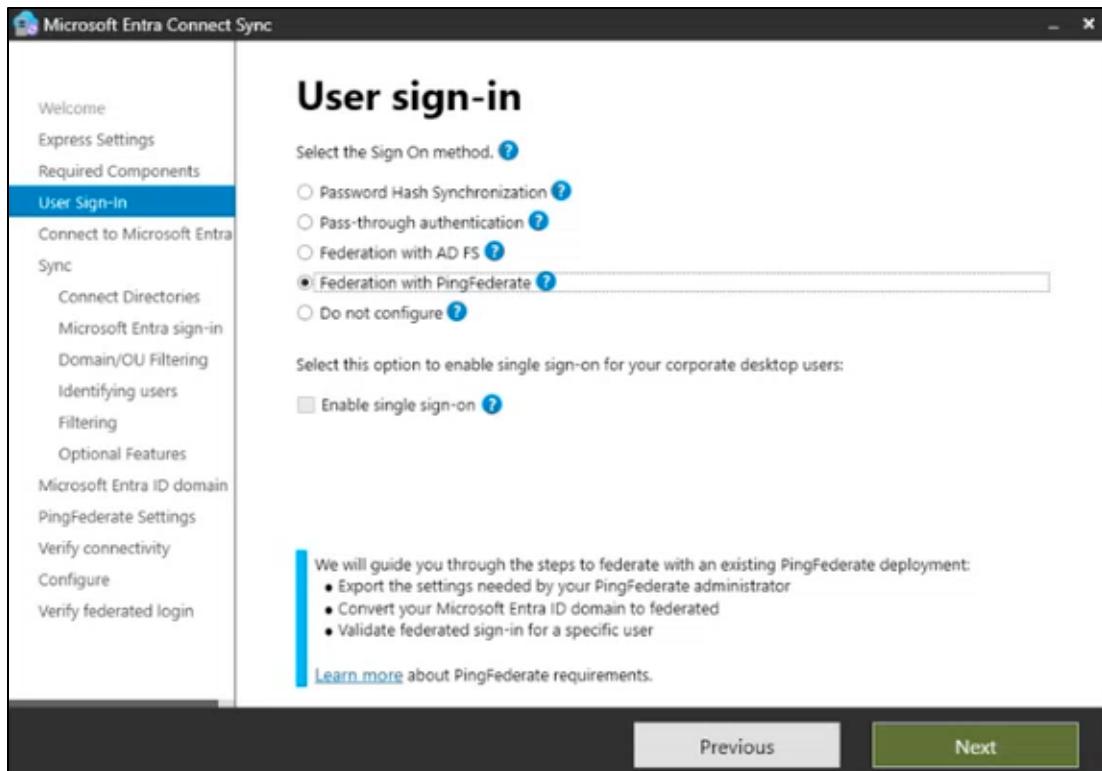


Bild 32: User sign-in Federation with PingFederate

Do Not Configure

Diese Option lässt die Authentifizierungsmethode offen. Das bedeutet: Derselbe Benutzername existiert sowohl lokal als auch in der Cloud – allerdings mit **unterschiedlichen Kennwörtern**. Dies führt fast zwangsläufig zu Verwirrung bei Endanwendern und sollte vermieden werden.

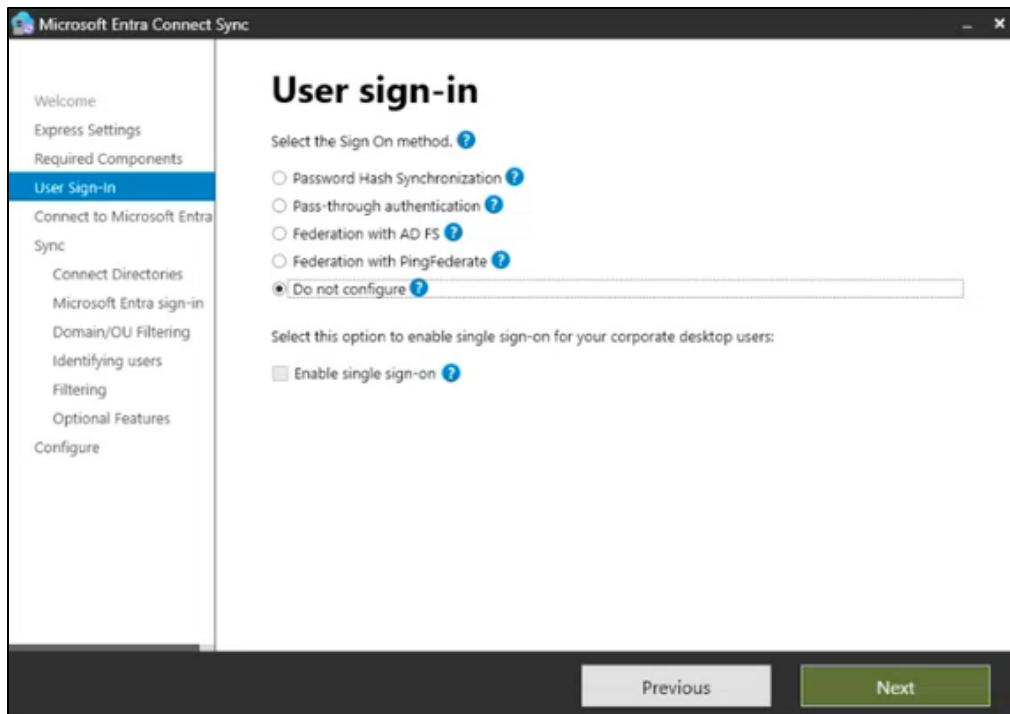


Bild 33: User Sign-in Do not configure

Der Einstieg in die Authentifizierungskonfiguration erfolgt mit der Auswahl der **Password Hash Synchronization**. Diese Methode bietet eine solide Grundlage für die hybride Identitätsverwaltung und ermöglicht den späteren Wechsel zu komplexeren Varianten wie Pass-through Authentication oder föderierten Modellen. Nach Auswahl von *Password Hash Synchronization* wird der Einrichtungsprozess fortgesetzt.

Im Anschluss erscheint der vorbereitete **Benutzer**, der für die Authentifizierung gegenüber Microsoft Entra ID verwendet wird. Die Anmeldung und Authentifizierung mit einem gültigen **Global Administrator-Konto** ist erforderlich, um die Synchronisationseinrichtung abzuschließen und die Integration zwischen lokalem Verzeichnis und Entra ID zu initialisieren.

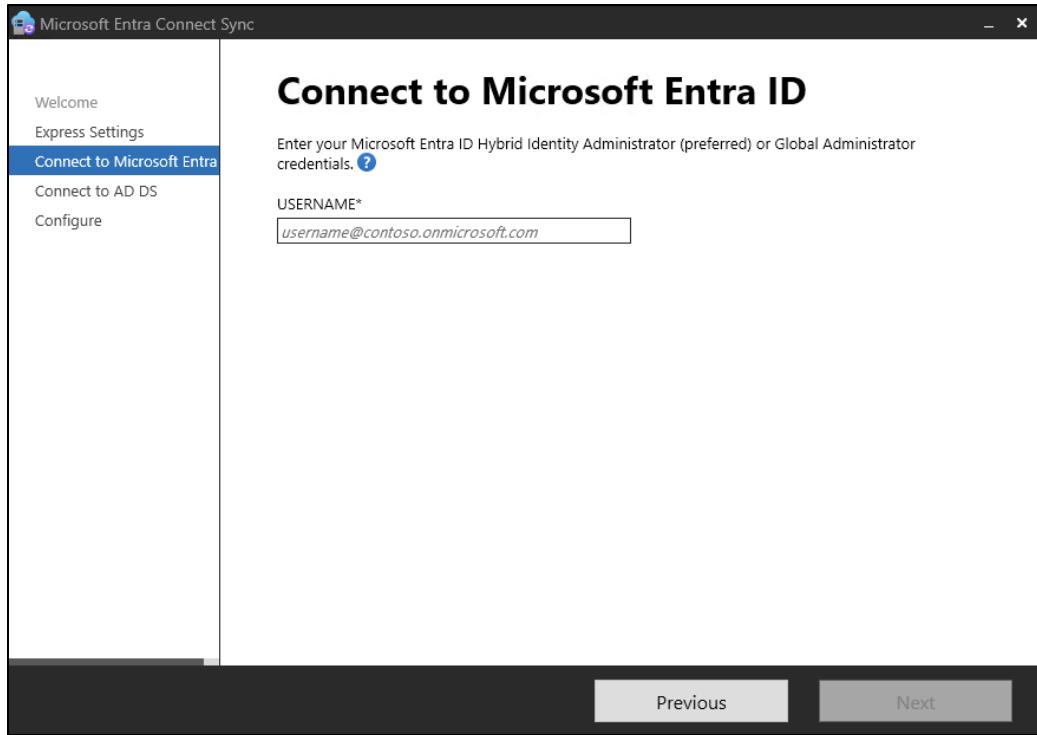


Bild 34: Connect to Entra ID

Im weiteren Verlauf wird der lokale **Active Directory-Forest** eingebunden. Entra ID Connect verlangt dafür Enterprise-Administratorrechte. Nach Eingabe der gültigen Anmeldedaten – in diesem Szenario über Schulungsbenutzername und einem Schulungskennwort – wird die Verbindung zwischen dem lokalen Verzeichnis und Entra ID initial aufgebaut.

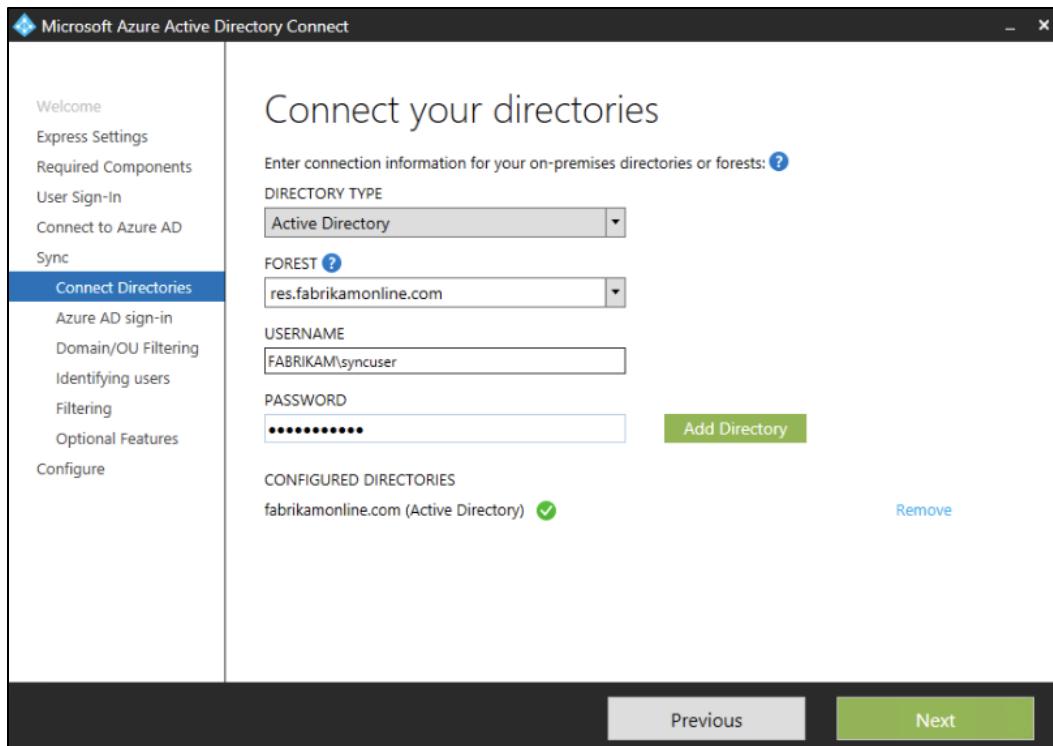


Bild 35: Connect directories

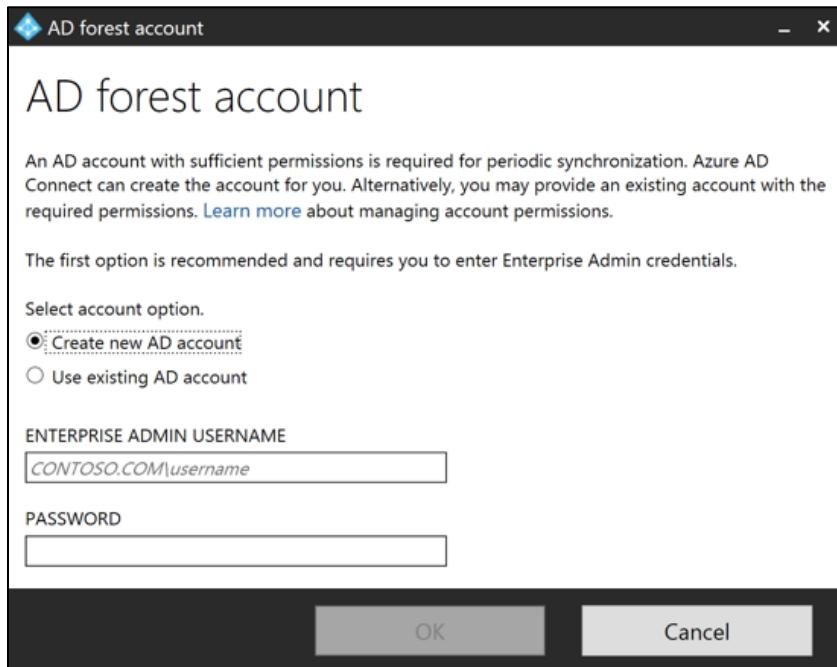


Bild 36: AD forest account

Ein häufiger Fehler in diesem Schritt betrifft den Domainnamen: Wird eine Domäne wie .com in Entra ID Connect nicht angezeigt, liegt das in der Regel daran, dass sie im Microsoft 365 Admin Center noch nicht als **autorisierte Domäne** registriert wurde. Die Konfiguration ist im Admin Center unter **Settings > Domains** vorzunehmen.

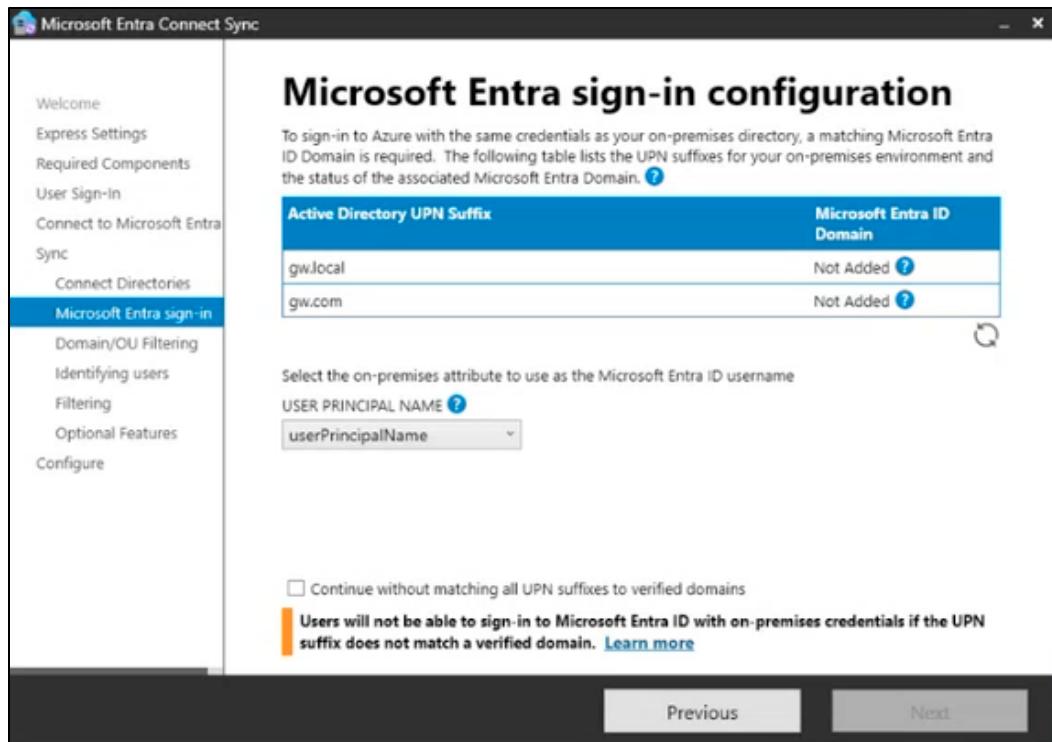


Bild 37: Entra sign-in configuration

Ein weiterer essenzieller Schritt besteht in der Auswahl des Attributs, das zur Identifikation der Benutzer in der Cloud verwendet wird. Standardmäßig ist dies der **User Principal Name (UPN)** – eine Auswahl, die aus Gründen der Usability und Kompatibilität empfohlen wird. Hier gilt auch wieder, dass die Auswahl einmalig vorkommen sollte. Auch wenn andere Attribute wie E-Mail-Adresse oder Telefonnummer theoretisch nutzbar sind, führt dies in der Praxis oft zu Benutzerverwirrung und erhöhtem Supportaufwand.

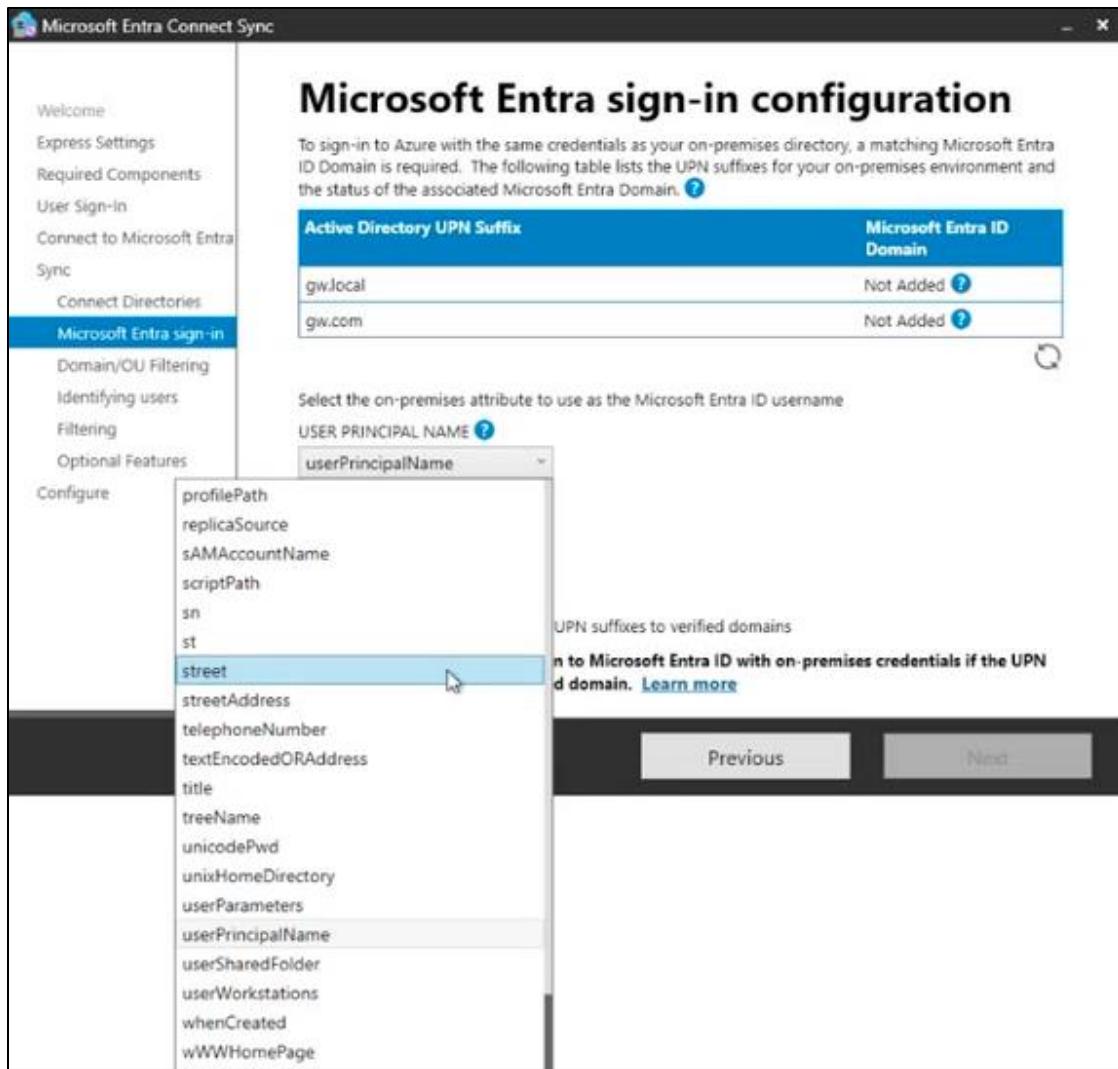


Bild 38: Auswahl

Darüber hinaus können erweiterte Optionen für die Benutzeridentifikation genutzt werden, etwa wenn mehrere Forests angebunden sind und Benutzerobjekte mehrfach existieren. In diesen Fällen bietet Entra ID Connect die Möglichkeit, **benutzerdefinierte Attribute** wie die ms-DS-ConsistencyGuid oder mail als Abgleichskriterium zu verwenden.

Im nächsten Schritt erfolgt die Auswahl der zu synchronisierenden Organisationseinheiten (OUs). Es wird ein Verzeichnis angezeigt und hier kann ausgewählt werden, was synchronisiert werden soll. Bei der Express Installation wird das ganze Verzeichnis genommen. Dies ist besonders wichtig zur Reduzierung des Objektumfangs sowie zur Steuerung, welche Konten, Gruppen oder Geräte wirklich in die Cloud überführt werden sollen.

Besonderes Augenmerk verdient die Konfiguration der Organisationseinheiten (OUs), insbesondere im Kontext von **Microsoft Intune** und **Windows Autopilot**. Soll im weiteren Verlauf beispielsweise ein zentrales Mobile Device Management über Intune realisiert werden, müssen entweder die klassischen **Computer-OUs** oder – je nach Struktur – spezifische, eigens definierte OUs mit entsprechenden **Windows-Fat-Clients oder Notebooks** in die Synchronisation einbezogen werden.

In hybriden Szenarien empfiehlt es sich, die automatisierte Gerätebereitstellung über Windows Autopilot in Kombination mit Entra ID Connect vorzubereiten. Hierzu zählen auch dedizierte Gruppenrichtlinien, die für neu hinzugefügte Geräte gelten und deren Verwaltung über Intune ermöglichen. Nur wenn diese OUs und die enthaltenen Objekte in die Cloud synchronisiert wurden, kann eine reibungslose Integration und Gerätekonfiguration im Rahmen der Endpoint-Verwaltung erfolgen.

Daraufhin folgt der Abschnitt „**Uniquely Identifying Your Users**“. Ist die Benutzerbasis eindeutig, kann hier die Voreinstellung beibehalten werden. Sind Benutzer in mehreren Verzeichnissen verteilt, bietet sich die Auswahl eines spezifischen Attributs an.

Im nachfolgenden Schritt geht es um die eindeutige Zuordnung von Benutzeridentitäten. **Standardmäßig** ist die Einstellung *Users are represented only once across all directories* aktiviert – eine Konfiguration, die für die meisten Umgebungen ausreicht und empfohlen wird, sofern keine mehrfachen Benutzerobjekte über verschiedene Forests hinweg existieren.

In komplexeren Szenarien mit **mehreren Active Directory Forests**, in denen Benutzerobjekte potenziell mehrfach vorhanden sind, bietet Entra ID Connect die Möglichkeit, alternative Matching-Kriterien zu definieren. Hierzu kann unter *Users identities exist across multiple directories* ein **spezifisches Attribut** ausgewählt werden, anhand dessen Benutzer eindeutig zugeordnet werden. Zur Auswahl stehen u. a. **E-Mail-Adresse, ImmutableID, SAMAccountName** oder benutzerdefinierte Attribute. Diese Einstellung erlaubt es, redundante Identitäten zusammenzuführen und ein konsistentes Benutzerabbild in der Cloud zu gewährleisten.

Auch in diesem Schritt bleibt die Empfehlung bestehen, auf Eindeutigkeit und Klarheit in der Benutzerstruktur zu achten. In der Praxis bedeutet dies, die Voreinstellung beizubehalten und den UPN (User Principal Name) als Identifikationsmerkmal zu verwenden – sowohl aus Kompatibilitätsgründen als auch zur Minimierung von Supportaufwand.

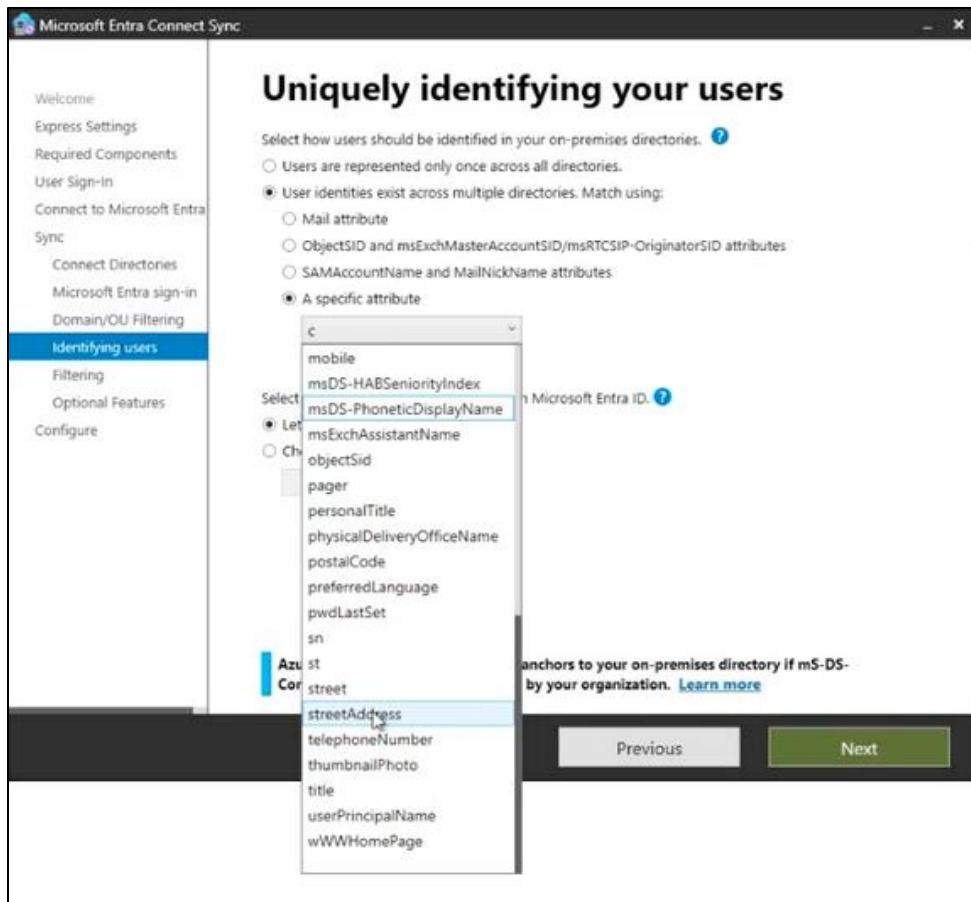


Bild 39: Uniquely identifying your users

Darunter befindet sich die Auswahlmöglichkeit „Select how users should be identified with Microsoft Entra ID“. Wird der hier der 1. Wert „Let Azure manage the source anchor“ ausgewählt, erfolgt die Anmeldung über UPN.

Auch an dieser Stelle bestätigt sich erneut die Bedeutung einer eindeutigen Benutzeridentität. Die Beibehaltung des UPN als primäres Attribut für die Benutzeranmeldung unterstützt ein sauberes und nachvollziehbares Identitätsmanagement in hybriden Umgebungen. Die Konfiguration wird entsprechend übernommen, ohne Änderungen vorzunehmen.

Im Anschluss daran erfolgt die Option zur **Gruppenfilterung**. Diese kann – wie bereits im frühen Verlauf der Installation – auch an dieser Stelle konfiguriert werden. Sie ermöglicht eine gezielte Auswahl synchronisierter Gruppen und dient sowohl der Reduktion der Objektsynchronisation als auch der sauberen Abgrenzung relevanter Verzeichnisobjekte. Die Gruppenfilterung ist somit technisch an zwei Stellen im Assistenten konfigurierbar.

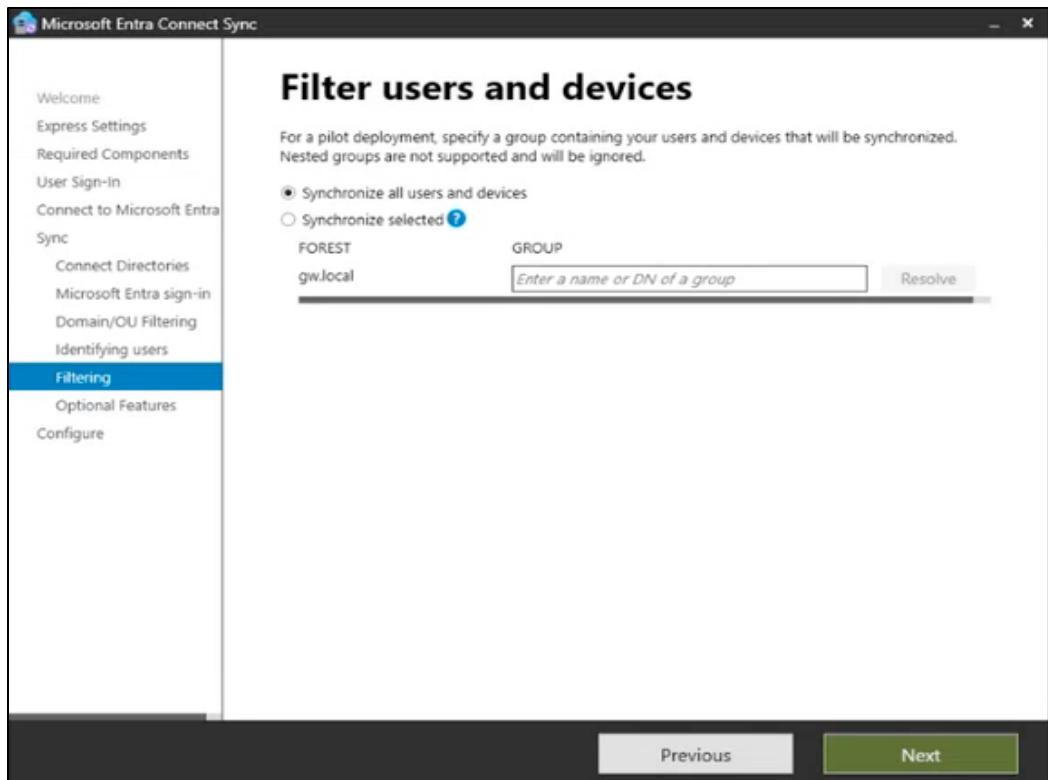


Bild 40: Filter users and devices

Ein weiterer Punkt ist die Aktivierung optionaler Features wie:

Exchange Hybrid Deployment

Device Writeback

Password Writeback

Exchange Hybrid Deployment.

Damit eine reibungslose Migration von einer lokalen Exchange-Infrastruktur hin zu **Exchange Online** möglich ist, müssen bestimmte Exchange-spezifische Attribute im Rahmen der Verzeichnissynchronisation berücksichtigt werden. Diese werden über Entra ID Connect in die Cloud übertragen. Voraussetzung dafür ist, dass entsprechende Häkchen bei den erweiterten Features gesetzt und die Synchronisation dieser Attribute aktiviert wird.

An dieser Stelle wird auch erneut deutlich, dass **Password Hash Synchronization** als Authentifizierungsmethode bereits vorausgewählt ist – ein Indikator dafür, dass diese Methode mit hybriden Szenarien kompatibel ist und auch im Zusammenspiel mit Exchange Online zuverlässig funktioniert.

Die Features **Password Writeback** und **Device Writeback**, ermöglichen eine **bidirektionale Synchronisation** – also nicht nur die Übertragung von Objekten aus dem lokalen Active Directory in die Cloud, sondern auch die Rückführung bestimmter Objekte oder Informationen zurück in die lokale Infrastruktur. Besonders in Szenarien mit **Cloud-First-Strategien**, aber weiterhin bestehender On-Premise-Komponenten, stellt dies einen wichtigen Aspekt für die nahtlose Integration dar.

Im letzten Schritt vor Abschluss der Konfiguration erscheinen zwei besonders wichtige Auswahlmöglichkeiten: „**Start synchronization process when configuration completes**“ sowie „**Enable staging mode**“. Die erste Option sorgt dafür, dass nach erfolgreichem Abschluss der Einrichtung unmittelbar der erste vollständige Synchronisationslauf (**Fullsync**) startet – sämtliche konfigurierte Objekte werden dabei gemäß der gesetzten Filter in die Cloud übertragen.

Die zweite Option, „**Enable staging mode**“, aktiviert einen speziellen Betriebsmodus, in dem zwar alle Konfigurationen und Leseberechtigungen aktiv sind, jedoch **keine Änderungen an Microsoft Entra ID oder dem lokalen Active Directory vorgenommen werden**. Der Modus dient dazu, alternative oder redundante Entra ID Connect-Instanzen bereitzuhalten, etwa für Failover-Szenarien oder Testumgebungen.

Besonders im produktiven Betrieb empfiehlt es sich, bei einem von mehreren vorhandenen Entra ID Connect-Servern diesen Haken **nicht** zu setzen – dieser Server übernimmt dann den Aktiven Part. Auf den übrigen Servern wird der Haken gesetzt und dieselbe Konfiguration angewendet. Diese Server agieren fortan als **staging-instanzbasierte Rückfallebene**, die bei Ausfall der Hauptinstanz ohne erneute Einrichtung aktiviert werden können.

Damit ist sichergestellt, dass eine stabile, hochverfügbare Synchronisationsinfrastruktur aufgebaut wird – eine essenzielle Voraussetzung für hybride Identitätsmodelle.

Sollte ein zweiter aktiver Server konfiguriert werden, um zu testen, was passiert, sollte man vorsichtig sein. Denn in diesem Fall wird die Konfiguration später eine **Fehlermeldung** ausgeben und darauf hinweisen: „**Es gibt bereits einen aktiven Server**“. Die Konfiguration wird in einem solchen Fall nicht erfolgreich abgeschlossen. Das liegt daran, dass nur ein aktiver Server in einer synchronisierten Umgebung für die Datenexporte verantwortlich sein darf – Mehrfachinstanzen im aktiven Modus führen zu Konflikten und verhindern die Synchronisation.

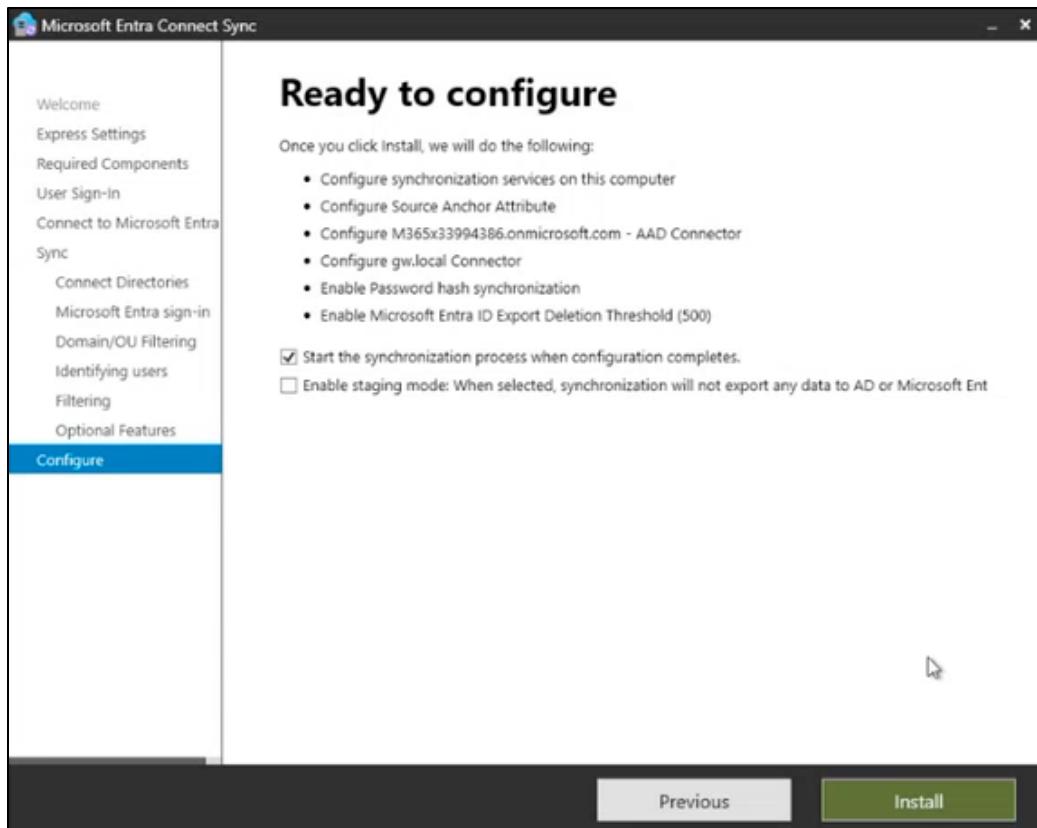


Bild 41: Ready to configure

Checkliste: Entra ID Connect – Installation & Konfiguration

Vorbereitung

Server mit Windows Server 2016 oder neuer bereitgestellt

Lokales Active Directory (AD DS) mit mindestens einem Domain Controller aktiv

Entra ID Connect Setup-Datei (AzureADConnect.msi) heruntergeladen

Optional: IDFix heruntergeladen und Active Directory bereinigt

Domäne in Microsoft 365 / Entra ID als **verifiziert** registriert (z. B. itz-gmbh.de)

Start der Installation

Setup von Entra ID Connect als Administrator gestartet

Option „**Customize**“ anstelle von „Express Settings“ gewählt

Falls gewünscht: benutzerdefinierter Installationspfad festgelegt

Falls vorhanden: vorhandene SQL-Instanz oder Servicekonto eingebunden

Lokales AD Forest korrekt erkannt

Anmeldung & Berechtigungen

Anmeldung mit **Global Admin-Konto** aus Microsoft 365 durchgeführt

Verbindung zum lokalen AD mit **Enterprise Admin-Konto** hergestellt

Synchronisationsoptionen

Password Hash Synchronization aktiviert

Attribut für Anmeldung: z.B. **userPrincipalName (UPN)**

Falls Mehrfachverzeichnisse: Benutzerabgleich über spezifisches Attribut (z. B. mail)

Verzeichnisauswahl

Nur relevante **OUs** zur Synchronisation ausgewählt

Optional: Geräte-OU für Autopilot/Intune berücksichtigt

Benutzerfilterung

Gruppenfilterung nur bei < **500 Benutzerobjekten** aktiviert

Alternativ: Filterung über OU oder Attribute konfiguriert

Optionale Features

Optional: **Exchange Hybrid Deployment** aktiviert

Optional: **Password Writeback / Device Writeback** konfiguriert

Staging-Modus (optional)

Staging-Mode aktiviert für Nicht-Produktivsysteme

Aktivierung des Produktivservers geplant (Staging-Haken entfernen)

Abschluss

„Start Synchronization when configuration completes“ aktiviert

Setup abgeschlossen und Full Sync erfolgreich gestartet

Protokolle und Synchronisationsstatus überprüft (über Synchronization Service Manager)

Tipp: Dokumentiere alle Einstellungen und Konfigurationspfade – vor allem bei mehreren synchronisierten Forests oder im Failover-Fall.

Kapitel 16: Synchronisationsüberwachung und Verwaltung von Gastzugriffen im Entra ID

Nachdem du die Einrichtung von Microsoft Entra ID Connect abgeschlossen hast und der Health-Agent erfolgreich installiert wurde, kannst du nun mit dem **Synchronization Service** einen genaueren Blick auf

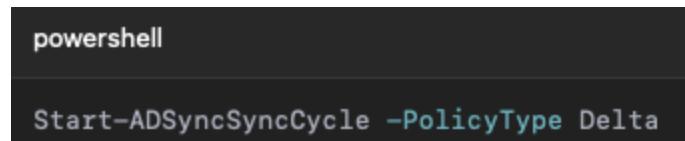
die laufenden Synchronisationsprozesse werfen. Öffne dazu über das Startmenü die entsprechende Anwendung und vergrößere das Fenster zur besseren Übersicht. Dort wirst du sechs Schritte sehen, die für jede Richtung der Datenverarbeitung – aus dem lokalen AD zur Cloud und umgekehrt – ausgeführt werden. Hier wird aufgelistet wann welche Objekte, wie angelegt wurden. Diese Schritte sind wichtig, um im Fehlerfall den Ursprung von Synchronisationsproblemen zu identifizieren und gezielt beheben zu können.

Gehe Schritt für Schritt durch die einzelnen Prozesse: Im zweiten Bereich unter „**Adds**“ kannst du erkennen, welche neuen Objekte im Entra ID angelegt wurden. Hier findest du für jeden angelegten Benutzer z. B. den DistinguishedName, den userPrincipalName und weitere Metadaten. Diese Details helfen dir dabei, die Objekterstellung nachzuvollziehen. Sollte ein Objekt z. B. nicht angelegt oder verändert worden sein, kannst du anhand der Logs erkennen, wo genau der Fehler liegt. Zusätzlich bekommst du Einsicht in den Ablauf der **Full- und Delta-Synchronisationen**, was dir hilft zu überprüfen, wann zuletzt welche Daten verarbeitet wurden.

Standardmäßig erfolgt alle **30 Minuten** ein automatischer Synchronisationslauf. In vielen Fällen ist dieser Intervall ausreichend. Möchtest du jedoch beispielsweise nach Änderungen sofort synchronisieren, kannst du dies manuell anstoßen. Dazu kannst du dich im Synchronization Service durch die einzelnen Schritte manuell durchklicken – aber Vorsicht: Die **richtige Reihenfolge** ist dabei entscheidend. Du musst stets beim lokalen Full Import beginnen und dich dann zur Cloud-Seite weiterarbeiten. Wird die Reihenfolge nicht eingehalten – z. B. wenn du nur die letzten beiden Schritte ausführst – kann es zu **Inkonsistenzen in der Synchronisationspipeline** kommen. In solchen Fällen hilft meist nur noch ein vollständiger Full Sync, um die Abläufe zu stabilisieren.

Um dies zu vermeiden, empfiehlt sich der Einsatz von **PowerShell** – ganz im Sinne eines strukturierten und automatisierten Administrationsprozesses. Mit folgendem Befehl startest du beispielsweise einen **Delta-Sync**:

```
Start-ADSyncSyncCycle -PolicyType Delta
```

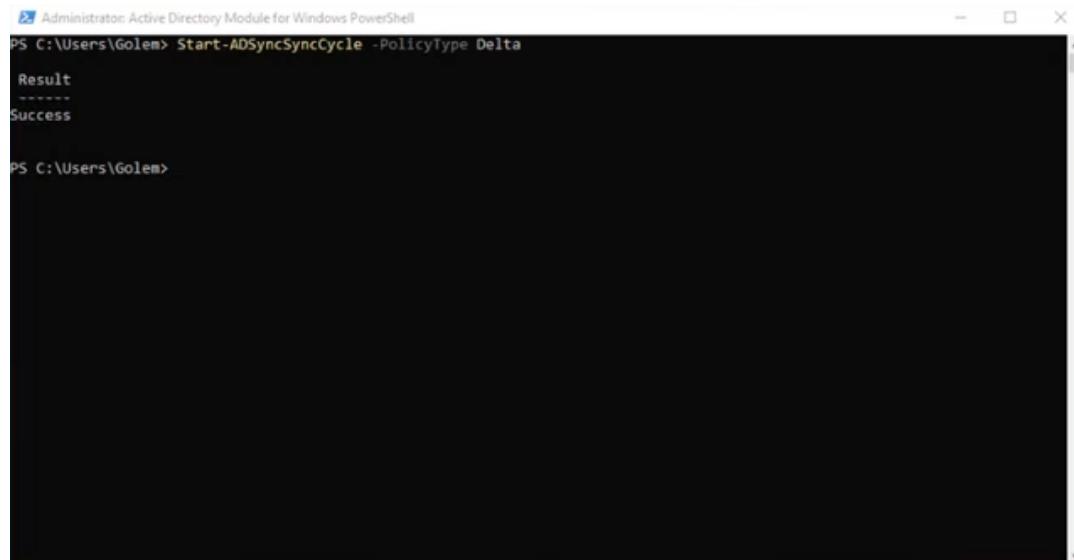


```
powershell
Start-ADSyncSyncCycle -PolicyType Delta
```

Bild 42: PowerShell

Führe diesen Befehl in einer **PowerShell mit Administratorrechten** aus. Sobald du ihn bestätigst, startet der Delta-Sync, der ausschließlich geänderte Objekte verarbeitet. Dies ist ressourcenschonend und schnell – insbesondere in größeren Umgebungen ein großer Vorteil.

In einer Umgebung mit wenigen Objekten erfolgt die Synchronisation meist innerhalb weniger Sekunden. In größeren produktiven Szenarien – mit mehreren Hundert oder Tausend Benutzerkonten – kann ein **Full Sync bis zu 60 Minuten oder mehr** in Anspruch nehmen. Besonders bei Erstkonfigurationen oder nach größeren Umstrukturierungen solltest du dies berücksichtigen.



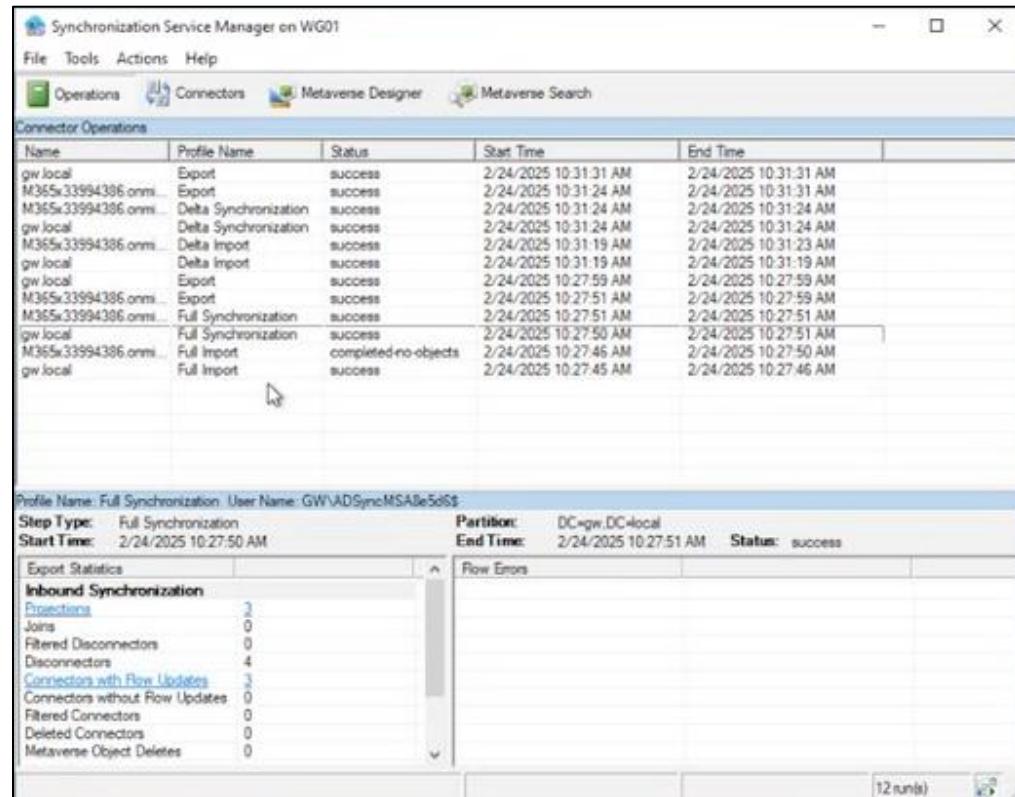
```

Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Golem> Start-ADSyncSyncCycle -PolicyType Delta
Result
-----
Success

PS C:\Users\Golem>

```

Bild 43: PowerShell Befehl



Name	Profile Name	Status	Start Time	End Time
gw.local	Export	success	2/24/2025 10:31:31 AM	2/24/2025 10:31:31 AM
M365x33994386.onmicrosoft.com	Export	success	2/24/2025 10:31:24 AM	2/24/2025 10:31:31 AM
M365x33994386.onmicrosoft.com	Delta Synchronization	success	2/24/2025 10:31:24 AM	2/24/2025 10:31:24 AM
gw.local	Delta Synchronization	success	2/24/2025 10:31:24 AM	2/24/2025 10:31:24 AM
M365x33994386.onmicrosoft.com	Delta Import	success	2/24/2025 10:31:19 AM	2/24/2025 10:31:23 AM
gw.local	Delta Import	success	2/24/2025 10:31:19 AM	2/24/2025 10:31:19 AM
gw.local	Export	success	2/24/2025 10:27:59 AM	2/24/2025 10:27:59 AM
M365x33994386.onmicrosoft.com	Export	success	2/24/2025 10:27:51 AM	2/24/2025 10:27:59 AM
M365x33994386.onmicrosoft.com	Full Synchronization	success	2/24/2025 10:27:51 AM	2/24/2025 10:27:51 AM
gw.local	Full Synchronization	success	2/24/2025 10:27:50 AM	2/24/2025 10:27:51 AM
M365x33994386.onmicrosoft.com	Full Import	completed-no-objects	2/24/2025 10:27:46 AM	2/24/2025 10:27:50 AM
gw.local	Full Import	success	2/24/2025 10:27:45 AM	2/24/2025 10:27:46 AM

Profile Name: Full Synchronization User Name: GW\ADSyncMSAbe5d\$

Step Type: Full Synchronization Partition: DC=wg,DC=local

Start Time: 2/24/2025 10:27:50 AM End Time: 2/24/2025 10:27:51 AM Status: success

Export Statistics		Inbound Synchronization		Row Errors	
Inbound Connectors	3	Projections	3	Row Errors	0
Joins	0	Filtering	0	Row Deletes	0
Filtered Disconnectors	0	Row Updates	3	Row Deletes	0
Disconnectors	4	Row Deletes	0	Row Deletes	0
Connectors with Row Updates	3	Row Deletes	0	Row Deletes	0
Connectors without Row Updates	0	Row Deletes	0	Row Deletes	0
Filtered Connectors	0	Row Deletes	0	Row Deletes	0
Deleted Connectors	0	Row Deletes	0	Row Deletes	0
Metaverse Object Deletes	0	Row Deletes	0	Row Deletes	0

Bild 44: Synchronization Service Manager

Kapitel 17: Verwaltung und Kontrolle von Gastbenutzern

Ein weiteres zentrales Thema, das du nicht vernachlässigen solltest, ist der **Umgang mit Gastbenutzern**. Über das Admin Center gehst du zuerst auf *Alle anzeigen* und anschließend auf *Identität*. Nach dem Ladeprozesse kann nun *Benutzer* und dann *Alle Benutzer* ausgewählt werden. Hier kannst du gezielt nach **Gastkonten** filtern, indem du unter dem Reiter *Filter* den Benutzertyp „Gast“ auswählst. In einer Beispielumgebung mit 110 Benutzern und 65 Gästen ergibt sich ein fast ausgeglichenes Verhältnis – ein möglicher Indikator für **veraltete oder nicht mehr benötigte Gastzugänge**.

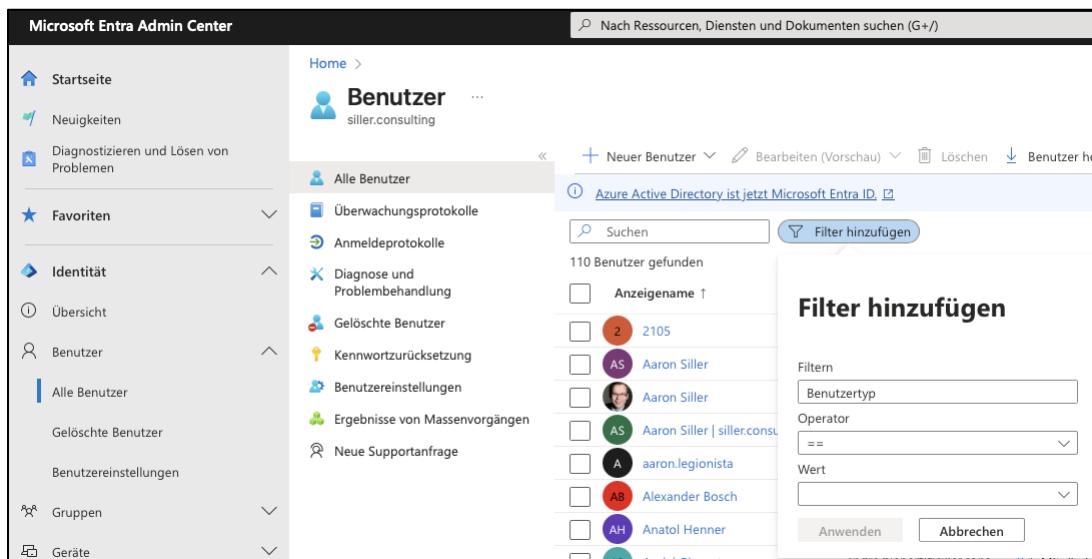


Bild 45: Benutzer

Die eigentliche Herausforderung liegt darin, zu erkennen, **welche Gastbenutzer noch Zugriff benötigen** und welche Zugriffe verwaist sind. In einer idealen Umgebung erfolgt dies durch einen klaren **On- und Offboarding-Prozess**. In der Praxis sieht es jedoch oft anders aus: Jeder interne Benutzer darf Gäste einladen, was langfristig zu einer unübersichtlichen Zugriffslage führt.

Zwei Möglichkeiten stehen dir zur Verfügung, um den Zugriff zu prüfen:

1. Access Reviews (ab Entra ID P2 / Governance Lizenz)

Über Entra ID P2 oder Governance kannst du mithilfe von **Access Reviews** automatisiert prüfen lassen, ob ein Gastzugriff noch notwendig ist.

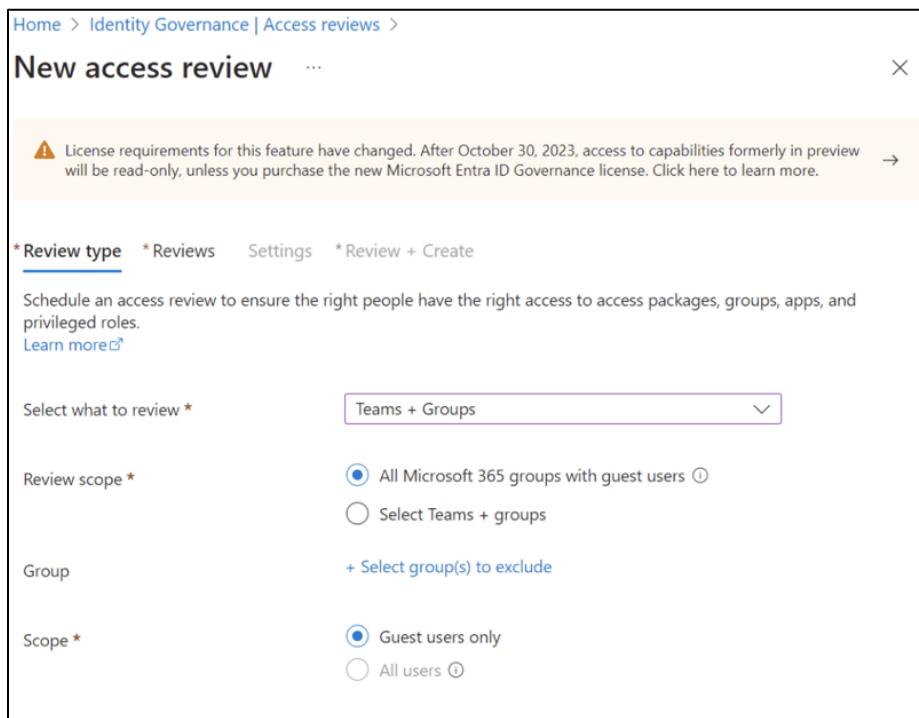
2. Last-Login-Day via PowerShell / Graph API analysieren

Falls dir keine Entra ID P2 Lizenz zur Verfügung steht, kannst du auch über PowerShell oder die **Microsoft Graph API** prüfen, wann sich ein Benutzer zuletzt authentifiziert hat. Das ist ein guter Indikator dafür, ob der Zugriff noch benötigt wird. Benutzer, die sich **in den letzten 90 Tagen** nicht angemeldet haben, sind potenzielle Kandidaten für den Entzug von Rechten.

Access Reviews: Automatische Überprüfung

Das **Entra ID Portal** bietet unter dem Pfad **Identity Governance → Access Reviews** eine strukturierte und teils automatisierbare Oberfläche. Dort kannst du über „**New Access Review**“ gezielt definieren, welche Ressourcen und Benutzerverhältnisse geprüft werden sollen. Das sind auf der ersten Ebene ist das Microsoft Teams + Gruppen und auf der zweiten Ebene SharePoint und OneDrive. Da die meisten externen Benutzer über **Teams** eingebunden werden, empfiehlt es sich, genau hier mit der Validierung zu beginnen.

Bei der Auswahl kannst du entweder einzelne Gruppen gezielt prüfen oder eine globale Überprüfung aller Gruppen mit externen Mitgliedern aktivieren – z. B. über die Option „**All Microsoft 365 Groups with Guest Users**“. Dabei kann ausgewählt werden, ob alle internen Benutzer, oder nur die der **Gastkonten** in den Fokus genommen werden sollen.



The screenshot shows the 'New access review' configuration page. At the top, there's a notice about license requirements changing after October 30, 2023. Below that, the 'Review type' section is selected. It includes tabs for 'Review type' (selected), 'Reviews', 'Settings', and 'Review + Create'. A descriptive text explains the purpose of scheduling an access review to ensure right access. Under 'Select what to review', 'Teams + Groups' is chosen. In the 'Review scope' section, 'All Microsoft 365 groups with guest users' is selected. There's also an option to 'Select Teams + groups'. Under 'Group', there's a link to 'Select group(s) to exclude'. In the 'Scope' section, 'Guest users only' is selected, while 'All users' is available as an option.

Bild 46: Review type

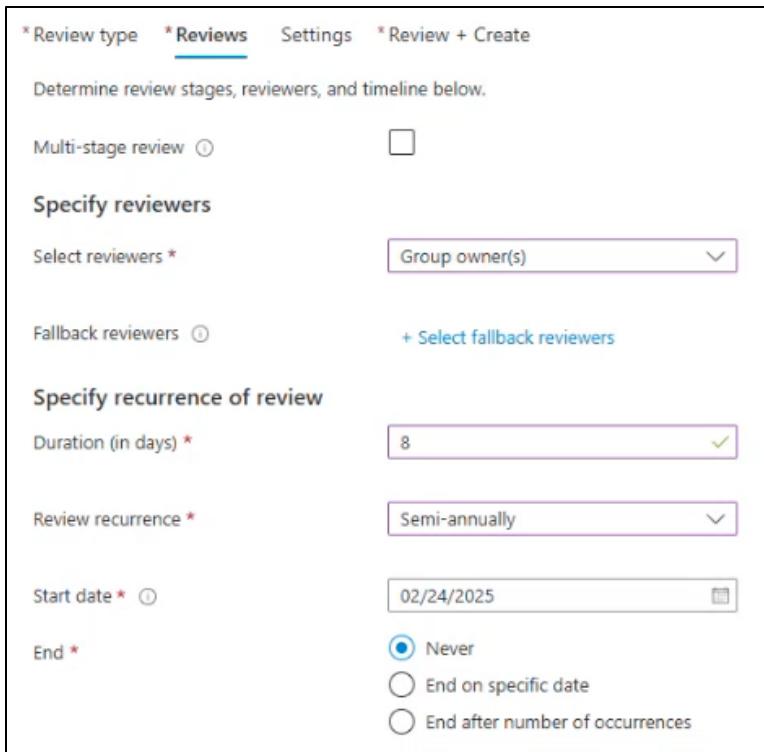
Im nächsten Schritt legst du fest, **wer die Bewertung durchführen soll**. Hier stehen dir mehrere Optionen zur Verfügung: der jeweilige **Gruppenbesitzer**, **der Benutzer selbst oder Gruppen**, der **Manager** (gemäß Attribut im Benutzerobjekt). In der Praxis hat sich meist die Verantwortung beim Gruppenbesitzer bewährt, vor allem im Kontext von Microsoft Teams. **Wichtig:** Eine Microsoft 365-Gruppe – und damit ein Team – sollte **immer mindestens zwei Besitzer** haben, um den Self-Service-Gedanke zu gewährleisten und die IT-Administration zu entlasten.

Sollte es keinen Gruppenbesitzer geben, kannst du zusätzlich sogenannte **Fallback Reviewer** definieren. Diese springen dann für die Bestätigung ein.

Ein weiterer Konfigurationspunkt ist die **Review recurrence**. Du kannst hier zwischen wöchentlich, monatlich, quartalsweise, halbjährlich oder jährlich wählen. Hier muss entschieden werden, wie oft der

besitzer reviewen soll, ob seine Benutzer noch benötigt werden oder nicht. Vorsicht vor der Aussage, dass der Kunde genau weiß, wann welche Gastzugriffe benötigt werden. Dies ist Meistens nicht der Fall. In der Praxis ist eine **halbjährliche Überprüfung (semi-annually)** ein sinnvoller Rhythmus, da er einerseits regelmäßig genug ist, um Relevanz zu behalten, und andererseits nicht zu viel administrativen Aufwand erzeugt.

Zusätzlich bestimmst du den **Startzeitpunkt und die Laufzeit der Überprüfung**.



The screenshot shows the 'Review type' configuration interface. At the top, there are tabs: *Review type, *Reviews (which is selected), Settings, and *Review + Create. Below the tabs, it says 'Determine review stages, reviewers, and timeline below.' There is a checkbox for 'Multi-stage review'. Under 'Specify reviewers', there is a dropdown menu set to 'Group owner(s)'. Below that, there is a section for 'Fallback reviewers' with a link '+ Select fallback reviewers'. Under 'Specify recurrence of review', the 'Duration (in days)' is set to 8, and the 'Review recurrence' is set to 'Semi-annually'. The 'Start date' is set to 02/24/2025. For 'End', the option 'Never' is selected, while 'End on specific date' and 'End after number of occurrences' are unselected.

Bild 47: Startzeitpunkt

Unter **Settings** kann das Verhalten ausgewählt werden, **wenn keine Bewertung erfolgt**. Über die Option „**Auto-apply result to resource**“ kannst du automatisieren, dass wenn ein Feedback kommt, dass auch etwas passiert und nicht nur eine Information im Admin Center erscheint. Unter dem Punkt „**If reviewers don't respond**“ kann ausgewählt werden was passieren soll, wenn keine Antwort kommt. Hier kannst du zwischen den Möglichkeiten *remove access*, *approve access* oder *take recommendations* auswählen. Das letztere sind Empfehlungen, die an dich geschickt werden. Es wird empfohlen den Access zu entfernen.

Im Bereich der erweiterten Einstellungen kannst du u. a. festlegen:

- **No sign-in within 30 days:** Ob ein Benutzer sich in den letzten 30 Tagen nicht angemeldet hat.

New access review

⚠ License requirements for this feature have changed. After October 30, 2023, access to capabilities

* Review type * Reviews Settings * Review + Create

Configure additional settings, including decision helpers and email notifications.

Upon completion settings

Auto apply results to resource

If reviewers don't respond Remove access Take recommendations

⚠ Setting 'If reviewers don't respond' to 'Remove access' or 'Take recommendations' while 'Auto-apply results to resource' is enabled could potentially lead to all access to this resource being revoked if the reviewers fail to respond.

At end of review, send notification to

Enable reviewer decision helpers

No sign-in within 30 days

User-to-Group Affiliation

Advanced settings

Justification required

Email notifications

Reminders

< Previous **Next: Review + Create**

Bild 48: New access review

- **User-to-Group Affiliation:** Ist für die internen Benutzer, als Hinweis, ob du noch in anderen Gruppen bist und Zugriff deswegen benötigt oder eben nicht mehr benötigt wird.

- **Justification required:** Die Entscheidung, die getroffen wird, muss nochmal bestätigt werden.

- **Email notification:** Es geht eine zusätzliche E-Mail-Benachrichtigung raus.

- **Reminders:** Es wird ein Reminder rausgeschickt, innerhalb der ausgewählten Tage. Jeden Tag ein Reminder, solange er keine Antwort gegeben hat.

- **Additional content for reviewer email:** Zusätzlich besteht die Möglichkeit, eine benutzerdefinierte Nachricht zu hinterlegen, die dem Bewertenden angezeigt wird. Das gibt dir die Gelegenheit, Hintergründe oder unternehmensspezifische Hinweise zu kommunizieren.

* Review type * Reviews Settings * Review + Create

Name new access review

Review name * ⓘ Review guest access across Microsoft :✓

Description ⓘ

Confirm access review + create

Resources

Selected resource
All Microsoft 365 groups

Review scope
Guest users

Reviews

Reviewers
Group owner(s)

Frequency
Semi-annually

End
No end

Settings

Auto-apply results to resource

< Previous Create

Bild 49: Create review

Abschließend vergibst du einen **Review-Namen**, definierst Start und schließt den Prozess mit „**Create**“ ab. Wichtig: Die Zählung beginnt ab dem Startdatum, eine rückwirkende Gültigkeit gibt es nicht.

Solltest du (z. B. mangels Lizenz für Entra ID P2) keinen Zugriff auf Access Reviews haben, kannst du ein eigenes System über PowerShell aufbauen. Hierbei lässt sich z. B. die Shell ins **Azure Log Analytics Workspace** hochladen, der dann alle 30, 60, 90 Tage durchläuft und eine Mail rauschickt. Auch wenn diese Lösung weniger komfortabel ist, stellt sie dennoch eine funktionale Alternative zur Verfügung – und ist deutlich besser als auf eine Überprüfung vollständig zu verzichten.

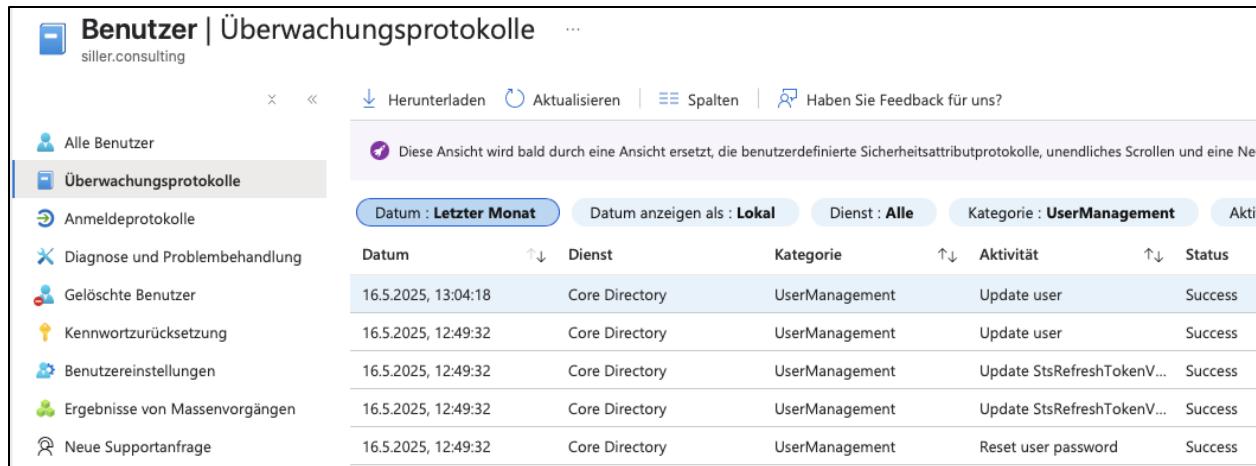
Kapitel 17: Protokollanalyse und Sicherheitskonfigurationen im Microsoft Entra ID

Ein häufiger Wunsch in der Praxis ist es, die **letzte Anmeldung eines Benutzers zu filtern**, etwa um inaktive Benutzer oder veraltete Gastkonten zu identifizieren. Solche Filter sind im Entra Admin Center jedoch nur

eingeschränkt möglich. Aktuelle Anmeldeereignisse sind in der Weboberfläche auf **maximal 30 Tage** begrenzt sichtbar mit dem *Sign-in Logs*. Für darüberhinausgehende Auswertungen musst du auf die PowerShell oder die **Microsoft Graph API** zurückgreifen. Alternativ kann auch das **Microsoft Purview Compliance Center** genutzt werden, um umfassendere Audit-Daten zu durchsuchen.

Ein zentraler Bestandteil bei der Analyse und Überwachung von Aktivitäten im Microsoft Entra ID ist das Verständnis der beiden Protokollarten: **Überwachungsprotokolle (Audit Logs)** und **Anmeldeprotokolle (Sign-in Logs)**. Beide liefern dir wichtige Informationen, jedoch mit unterschiedlichen Schwerpunkten.

Beginnen wir mit den **Überwachungsprotokollen**. Diese erfassen alle durchgeführten **administrativen Aktionen** bei den Identitäten. Der Hinweis darauf, was administrativ am Benutzerobjekt durchgeführt wurde. Die Protokolle geben dir Auskunft darüber, **wer** eine Änderung vorgenommen hat, **welches Zielobjekt** betroffen war, **wann** die Änderung erfolgte und **ob** sie erfolgreich war.



Datum	Dienst	Kategorie	Aktivität	Status
16.5.2025, 12:49:32	Core Directory	UserManagement	Update user	Success
16.5.2025, 12:49:32	Core Directory	UserManagement	Update user	Success
16.5.2025, 12:49:32	Core Directory	UserManagement	Update StsRefreshTokenV...	Success
16.5.2025, 12:49:32	Core Directory	UserManagement	Update StsRefreshTokenV...	Success
16.5.2025, 12:49:32	Core Directory	UserManagement	Reset user password	Success

Bild 50: Überwachungsprotokolle

Die **Anmeldeprotokolle** hingegen dokumentieren die **Authentifizierungsversuche** einzelner Benutzer gegenüber Microsoft-Diensten. Hier wird festgehalten, welcher Benutzer sich wann aus angemeldet hat, ob die Anmeldung erfolgreich war, welcher Dienst betroffen war.

Zur besseren Unterscheidung:

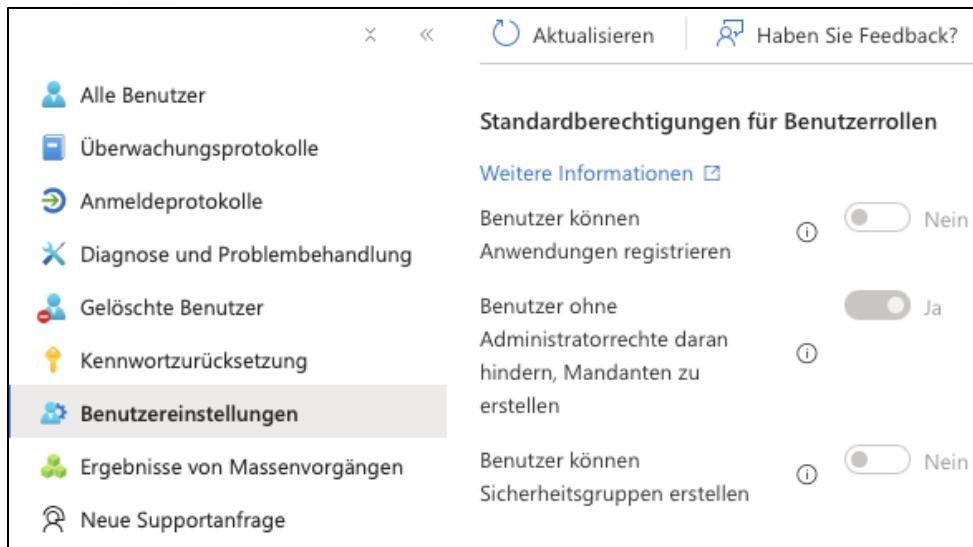
- **Audit Logs (Überwachungsprotokolle):**

→ Was wurde administrativ an Benutzer- oder Gruppenobjekten geändert?

- **Sign-in Logs (Anmeldeprotokolle):**

→ Wer hat sich wann, wie und wo authentifiziert – und war der Login erfolgreich?

Im nächsten Schritt wechselst du im linken Menü des Microsoft Entra Admin Centers zu den **Benutzereinstellungen**. Dieser Bereich enthält mehrere sicherheitsrelevante Konfigurationsoptionen, die du unbedingt überprüfen und ggf. anpassen solltest – idealerweise direkt in einem Test-Tenant, um die Auswirkungen vorab beurteilen zu können.



The screenshot shows the 'Standardberechtigungen für Benutzerrollen' (Standard permissions for user roles) page in the Microsoft 365 Admin Center. On the left, there's a sidebar with various options like 'Alle Benutzer', 'Überwachungsprotokolle', etc. The 'Benutzereinstellungen' option is selected and highlighted in grey. On the right, there are three settings listed:

- Benutzer können Anwendungen registrieren**: A toggle switch is set to 'Nein' (No). There is a help icon (info sign) next to the switch.
- Benutzer ohne Administratorrechte daran hindern, Mandanten zu erstellen**: A toggle switch is set to 'Ja' (Yes). There is a help icon next to the switch.
- Benutzer können Sicherheitsgruppen erstellen**: A toggle switch is set to 'Nein' (No). There is a help icon next to the switch.

Bild 51: Standardberechtigungen

Beginnen wir mit der Einstellung „**Benutzer können Anwendungen registrieren**“. Diese Option erlaubt es standardmäßig, dass Benutzer über die Plattform myapps.microsoft.com eigene Anwendungen im Verzeichnis registrieren können. Die Registrierung neuer Anwendungen im Tenant sollte ausschließlich durch autorisierte Administratoren erfolgen. Hier soll eine Schatten-IT verhindert werden.

Die zweite relevante Einstellung lautet „**Benutzer ohne Administratorrechte daran hindern, Mandanten zu erstellen**“. Auch hier empfiehlt sich eine restriktive Konfiguration – setze diese Option auf „Ja“. Hintergrund: Ein „Mandant“ (Tenant) ist die übergeordnete Verwaltungseinheit im Microsoft-365-Ökosystem. Es besteht die Gefahr, dass die unternehmenseigenen Domänen mit neuen Tenants verknüpft werden, was zu Sicherheits- oder Verwaltungsproblemen führen kann. Der Aufbau von Test- oder Entwicklungsumgebungen sollte daher ausschließlich durch die IT verantwortet werden.

Die dritte Einstellung „**Benutzer können Sicherheitsgruppen erstellen**“. Auch hier lautet die Empfehlung: deaktivieren. Sicherheitsgruppen sollten zentral durch Administratoren verwaltet werden, um Klarheit über deren Zweck, Berechtigungen und Gültigkeit zu behalten. In der Praxis legen Endnutzer ohnehin eher Microsoft 365 Gruppen an – oft automatisch beim Anlegen von Teams. Genau deshalb solltest du auch darüber nachdenken, die Teams-Erstellung zu zentralisieren, um die Kontrolle über Gruppen und deren Ressourcen zu behalten.

Ein weiterer zentraler Punkt in den Benutzereinstellungen betrifft den **Gastbenutzerzugriff**. Standardmäßig ist dieser so konfiguriert, dass Gastbenutzer einen eingeschränkten Zugriff auf Eigenschaften und Mitgliedschaften von Verzeichnisobjekten haben. In der Praxis bedeutet das beispielsweise, dass ein externer Guest, über die Suchfunktion die sogenannte „Enterprise Search“ möglicherweise auch andere Teams oder SharePoint-Seiten sehen könnte, sofern keine Einschränkungen greifen.

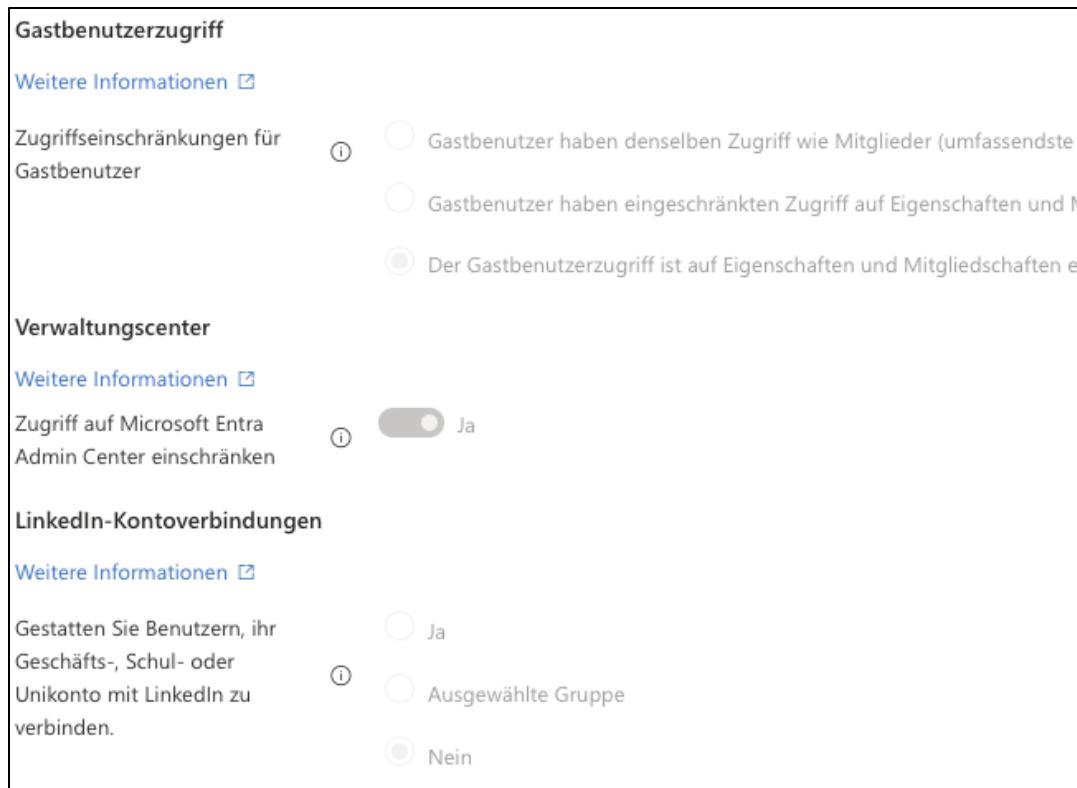
Dieses Verhalten ist aus sicherheitstechnischer Sicht in den meisten Fällen nicht wünschenswert. In der Regel sollen Gastbenutzer ausschließlich auf jene Ressourcen zugreifen können, zu denen sie explizit eingeladen wurden – also beispielsweise auf Dateien in einem bestimmten Team oder einer SharePoint-Bibliothek, nicht aber auf andere Verzeichnisobjekte.

Daher empfiehlt es sich, die Option „**Der Gastbenutzer ist auf Eigenschaften und Mitgliedschaften eigener Verzeichnisobjekte beschränkt**“ zu aktivieren. Das ist die restriktivste Einstellung und stellt sicher, dass Gastnutzer nur ihre eigenen Informationen sehen können.

Zusätzlich solltest du auch den Punkt „**Zugriff auf das Microsoft Entra Admin Center einschränken**“ aktivieren. Nur Benutzer mit explizit zugewiesenen Adminrollen sollen Zugang in das Entra ID Admin Center erhalten. Andere User ohne Adminberechtigung, die sich auch in den anderen Admin Centern nicht bewegen dürfen, sollten auch keinen Lesezugriff auf das Entra Admin Center haben.

Hier ist ein wichtiger Hinweis aus der Praxis angebracht: Gebe einem Geschäftsführer von einem Unternehmen nur aus dem Grund, weil er der Geschäftsführer ist, keine globalen Administratorenrechte zu geben. Das kommt in der Praxis öfters vor, dass der Geschäftsführer dies fordert. Aus Sicht der IT-Sicherheit ist dies jedoch nicht zu empfehlen.

Abschließend gibt es noch die Einstellung zur **LinkedIn-Kontoverknüpfung**. Diese ist standardmäßig erlaubt, stellt aber weniger ein Sicherheitsrisiko als vielmehr ein **Compliance-Thema** dar. Durch die Verknüpfung des geschäftlichen Microsoft-Kontos mit einem privaten LinkedIn-Konto können Metadaten ausgetauscht werden. Dies folgt dem Prinzip der **Datensparsamkeit (DSVGO-Annäherung)**, das besagt: So wenige Informationen, wie möglich nach außen geben.



The screenshot shows the 'Guest User Access' configuration page. It includes sections for 'Guest User Access', 'Administrative Center', and 'LinkedIn Account Connections'. In the 'Guest User Access' section, the 'Restrict guest access to properties and group memberships of their own directory objects' option is selected. In the 'Administrative Center' section, the 'Restrict access to the Microsoft Entra Admin Center' option is enabled. In the 'LinkedIn Account Connections' section, the 'Allow users to connect their work or school LinkedIn account to their Microsoft account' option is disabled.

Gastbenutzerzugriff	
Weitere Informationen	
Zugriffseinschränkungen für Gastbenutzer	<input type="radio"/> Gastbenutzer haben denselben Zugriff wie Mitglieder (umfassendste)
	<input type="radio"/> Gastbenutzer haben eingeschränkten Zugriff auf Eigenschaften und N
	<input checked="" type="radio"/> Der Gastbenutzerzugriff ist auf Eigenschaften und Mitgliedschaften e
Verwaltungszentrum	
Weitere Informationen	
Zugriff auf Microsoft Entra Admin Center einschränken	<input checked="" type="checkbox"/> Ja
LinkedIn-Kontoverbindungen	
Weitere Informationen	
Gestatten Sie Benutzern, ihr Geschäfts-, Schul- oder Unikonto mit LinkedIn zu verbinden.	<input type="radio"/> Ja
	<input type="radio"/> Ausgewählte Gruppe
	<input checked="" type="radio"/> Nein

Bild 52: Gästebenutzerzugriff

Im Laufe der Jahre hat sich Microsoft 365 von einem eher geschlossenen zu einem sehr offenen System entwickelt. Während früher Funktionen zunächst deaktiviert waren und man sie als Administrator aktiv einschalten musste, hat sich dies mittlerweile grundlegend geändert. Heute ist es häufig so, dass bestimmte Einstellungen direkt **standardmäßig aktiviert** sind.

Das bedeutet für dich als Administrator, dass du zunehmend entscheiden musst, **welche Funktionen wirklich benötigt werden** und welche du gegebenenfalls bewusst **deaktivieren** solltest, um den Schutzbedarf deiner Umgebung zu erfüllen.

In der Entra ID-Verwaltung ist die Frage, **wer Zugriff auf das Microsoft Entra Admin Center erhalten darf** – insbesondere im Kontext von Benutzerrollen mit begrenzten Rechten. Auf den ersten Blick wirkt es widersprüchlich, dass selbst bei aktivierter Zugriffsbeschränkung einzelne Benutzer weiterhin Zugang erhalten können, sofern ihnen entsprechende Rechte zugewiesen wurden.

In der Praxis geht es hier um eine bewusste Abwägung: **Sollen privilegierte Benutzer – etwa mit Leserechten oder über zeitlich begrenzte Rollen aus einem Privileged Identity Management (PIM) – Zugriff auf administrative Funktionen des Entra Admin Centers erhalten, obwohl sie keine permanente Administratorrolle besitzen?**

Früher war der Zugriff auf das Entra Admin Center zunächst standardmäßig für alle berechtigten Benutzer freigegeben. Erst in späteren Updates hat Microsoft die **Standardkonfiguration geändert**. Idealerweise sollte es so sein, dass wenn du ein globaler Admin bist oder ein limitierter Administrator hast, dann der **Zugriff auf das Entra Admin Center funktioniert**.

Damit stellst du sicher, dass keine sogenannten „Poweruser“ oder über Privileged Identity Management – also noch nicht Administratoren – hinzugefügt werden.

Microsoft verändert auch regelmäßig Standardkonfigurationen in seinen Produkten. Solche Änderungen gehen bei Administratoren unter Umständen unter oder erfahren erst verzögert davon.

Die beste Informationsquelle ist dabei Microsoft selbst. Im **Nachrichtencenter im Entra Admin Center**, kannst du **E-Mail-Benachrichtigungen zu relevanten Services aktivieren**, etwa für Entra, Microsoft Teams oder Exchange. Über die **Einstellungen lässt sich gezielt auswählen**, zu welchen Themen du informiert werden, willst. So lässt sich die Informationsflut zumindest eingrenzen und fokussiert auf deine IT-Umgebung ausrichten.

Alternativ bieten auch externe IT-Dienstleister – wie im Beispiel die Regio IT aus Aachen – **monatliche Update-Sessions** an, in denen die wichtigsten Änderungen zusammengefasst vorgestellt werden. Je nach Bedarf kannst du also zwischen automatisierter Microsoft-Kommunikation und kuratierten Drittanbieter-Updates wählen.

Einstellungen

Benutzerdefinierte Ansicht E-Mail

Sie können anpassen, welche Nachrichten in der Liste angezeigt werden, indem Sie entweder den Dienst oder das Tag auswählen.

Nachrichten für diese Dienste anzeigen

- Allgemeine Ankündigung
- Basic-Mobilität und Sicherheit
- Dynamics 365-Apps
- Exchange Online
- Microsoft 365 Apps
- Microsoft 365 Copilot
- Microsoft 365 für das Web
- Microsoft 365-Suite
- Microsoft Bookings

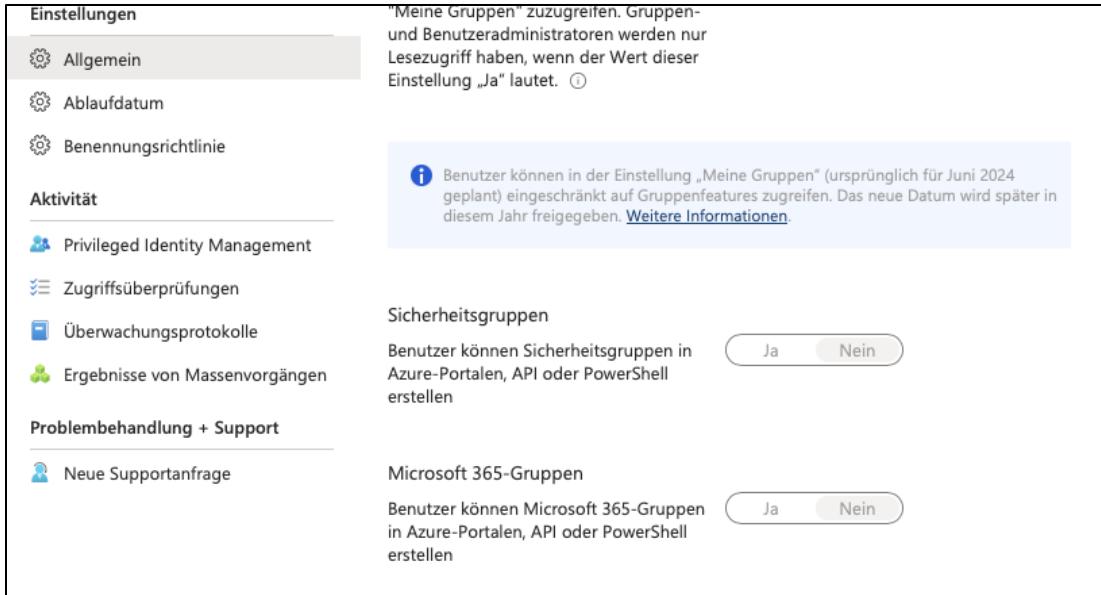
Bild 53: Nachrichten

Kapitel 18: Gruppenverwaltung, Berechtigungen und Lifecycle Management in Microsoft Entra ID und Microsoft Teams

Als nächstes geht es um die zentrale Verwaltung von Gruppen in Microsoft Entra ID. Beginne zunächst mit einem Blick in den Bereich „**Gruppen**“ > „**Übersicht**“ im Microsoft Entra Admin Center. Dort erhältst du eine kompakte Aufstellung, wie viele Gruppen aktuell im Tenant existieren – unterteilt in Sicherheitsgruppen, Microsoft 365 Gruppen sowie dynamische Gruppen. Diese Übersicht ist dabei hilfreich, um das aktuelle Gruppenkonstrukt besser einschätzen zu können.

Ein besonderer Fokus liegt auf den beiden Optionen in den **Gruppeneinstellungen** unter „Allgemein“:

- „Benutzer können Sicherheitsgruppen in Azure-Portalen, API oder PowerShell erstellen“
- „Benutzer können Microsoft 365 Gruppen erstellen“



The screenshot shows the 'Einstellungen' (Settings) section of the Microsoft 365 Groups settings. Under 'Allgemein' (General), it says: "Meine Gruppen" zuzugreifen. Gruppen- und Benutzeradministratoren werden nur Lesezugriff haben, wenn der Wert dieser Einstellung „Ja“ lautet. ⓘ". A note below states: "Benutzer können in der Einstellung „Meine Gruppen“ (ursprünglich für Juni 2024 geplant) eingeschränkt auf Gruppenfeatures zugreifen. Das neue Datum wird später in diesem Jahr freigegeben. [Weitere Informationen](#)". Under 'Sicherheitsgruppen' (Security groups), it says: "Benutzer können Sicherheitsgruppen in Azure-Portalen, API oder PowerShell erstellen" with a 'Ja' (Yes) button. Under 'Microsoft 365-Gruppen' (Microsoft 365 Groups), it says: "Benutzer können Microsoft 365-Gruppen in Azure-Portalen, API oder PowerShell erstellen" with a 'Nein' (No) button.

Bild 54: M365 Gruppen

Beide Einstellungen sollten aus administrativer Sicht auf „**Nein**“ gesetzt werden. Warum? In der Praxis ist es sinnvoll, wenn ausschließlich IT-Verantwortliche Gruppen erstellen, zur Gewährleistung einheitlicher Standards. Beachte: Das Deaktivieren der M365-Gruppenerstellung verhindert noch nicht automatisch, dass Nutzer Teams anlegen können – dies betrifft nur die Gruppenanlage direkt.

Teams-Besitzer und deren Bedeutung

Im nächsten Schritt wechselst du in das **Microsoft 365 Admin Center** und dort in den Bereich **Teams** → In der Teamsübersicht wieder auf **Teams** → **Teams verwalten**. Nun erscheint eine Auflistung der verschiedenen Teams. Achte hier besonders auf die Spalte „**Besitzer**“. Es zeigt sich häufig, dass viele Teams nur einen Besitzer haben. Im Sinne vom **Self-Service-Gedanke** ist es allerdings empfehlenswert, dass **jedes Team mindestens zwei Besitzer** hat. Außerdem solltest du den Umfang der aktiven Teams prüfen. Wenn du z. B. 156 Teams bei 264 Benutzern findest, lohnt sich eine kritische Prüfung: Welche davon sind überhaupt noch aktiv und notwendig?

Um dem Einhalt zu geben ist es wichtig zu entscheiden, wer darf Teams anlegen, aber auch sich Gedanken darüber zu machen, wie du mit dem Lifecycle Management umgehst.

Lifecycle Management aktivieren

Ein besonders effektives Werkzeug zur automatisierten Pflege deiner Gruppen- und Teamstruktur ist das **Lifecycle Management** in Entra ID, das dir ab der **Entra ID P1 Lizenz** zur Verfügung steht. Du findest die entsprechende Funktion unter „**Einstellungen**“ > „**Ablaufdatum**“.

Mit dieser Funktion kannst du definieren, wie lange ein Microsoft 365 Team (bzw. die zugrundeliegende Gruppe) **aktiv bleiben darf**, ohne dass eine Benutzeraktivität erfolgt. Eine Aktivität kann sein:

Ein gesendeter Chat (auch ein Leerzeichen reicht),
Eine Datei wurde geändert oder hochgeladen,

Ein neuer Guest wurde hinzugefügt.

Sobald innerhalb der definierten Lebensdauer (z. B. 365 Tage) keine Aktivität erfolgt, wird der Team-Besitzer **automatisch 30, 15 und 1 Tag vor Ablauf** per E-Mail gewarnt und kann die Gruppe auf Knopfdruck verlängern. Reagiert er nicht, wird das Team gelöscht – kann aber **innerhalb von 30 Tagen** wiederhergestellt werden. Diese Funktion hilft nicht nur, ungenutzte Altlasten zu identifizieren und zu bereinigen, sondern auch sensible Informationen besser abzusichern. Das Ablaufdatum auf 1 Jahr einzustellen, ist dafür eine gute Empfehlung.

Hinweis: Nicht jeder User braucht eine P1 Lizenz. Es reicht hier aus, dass nur eine P1 Lizenz vorhanden ist, um das technisch bereit zu stellen. Allerdings ist das für die Gruppen nicht mehr lizenkonform. Microsoft hat die Prüfung der Lizenzen in den letzten Jahren stark runtergefahren, es kann trotzdem zu einer Nachlizenzierung kommen.

Es wird auch empfohlen ein Sammelpostfach anzulegen.

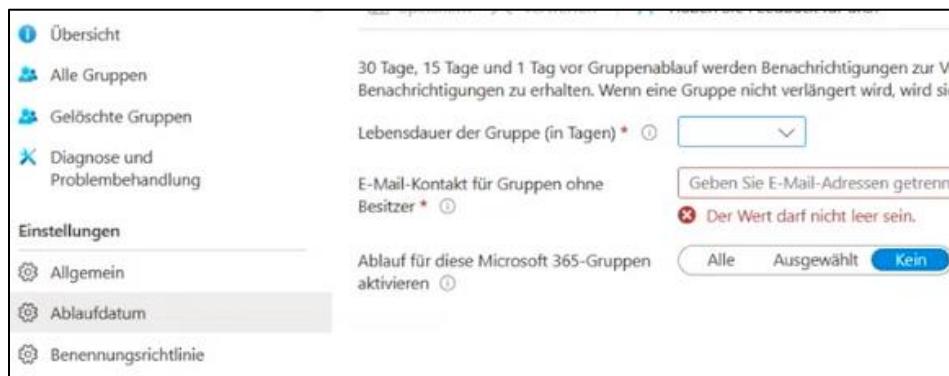


Bild 55: Sammelpostfach

Ein häufiges Anliegen in der Praxis ist die Frage, was eigentlich passiert, wenn Benutzer keine Berechtigung mehr zur Gruppen- oder Team-Erstellung haben. In der Regel wird der entsprechende Menüpunkt im Portal einfach ausgeblendet, ohne dass eine direkte Information oder Fehlermeldung erscheint. Das bedeutet: Benutzer sehen die Option nicht mehr, können aber nicht direkt erkennen, warum. Daher empfiehlt es sich, begleitend eine Kommunikationsstrategie aufzusetzen, z. B. durch interne Anleitungen oder Hinweise im Intranet, die auf den zentralisierten Bereitstellungsprozess verweisen.

Teams-Onboarding gezielt steuern

Ein weiterer wichtiger Aspekt in der Verwaltung von Microsoft Teams ist die **Kontrolle darüber, wer überhaupt neue Teams anlegen darf**. Das lässt sich **nicht über die grafische Benutzeroberfläche**, sondern ausschließlich über **PowerShell** steuern. In einem früheren Blogartikel mit dem Titel „[Teams erstellen einschränken](#)“ habe ich diesen Prozess einmal ausführlich dokumentiert.

Die Vorgehensweise ist dabei wie folgt:

Zunächst legst du eine **dedizierte Sicherheitsgruppe** an, deren Mitglieder zukünftig die Berechtigung erhalten sollen, Teams zu erstellen. Anschließend wird über einen **PowerShell-Befehl** festgelegt, dass **nur Mitglieder dieser Gruppe** zur Erstellung neuer Microsoft Teams berechtigt sind. Alle anderen Benutzer

werden entsprechend daran gehindert. Die Teams Erstellung einschränken, kann auch nur über die Shell erstellt werden und nicht über die GUI.

Dies funktioniert **lizenzenabhängig** – also auch mit **Microsoft 365 Business Standard** – und bietet eine schlanke, effektive Möglichkeit, das Teams-Onboarding in einem Unternehmen zu regulieren.

Wenn du bestimmte Berechtigungen im Tenant einschränkst – etwa für das Erstellen von Gruppen oder das Einladen von Gastbenutzern – stellt sich schnell die Frage: **Wie wirkt sich das eigentlich auf die Nutzererfahrung aus?** Was passiert, wenn ein Benutzer versucht, eine Aktion auszuführen, die ihm durch die neuen Richtlinien nicht mehr erlaubt ist?

Die Antwort lautet: **Die entsprechenden Optionen werden im Frontend schlicht ausgeblendet.** Das heißt, der Menüpunkt, z. B. „Team erstellen“, ist für den betroffenen Benutzer gar nicht mehr sichtbar. Ein aktiver Hinweis oder eine Fehlermeldung nach dem Motto „*Bitte wenden Sie sich an den Administrator*“ erscheint allerdings nicht.

Daher solltest du sicherstellen, dass deine Benutzer über **interne Kommunikationskanäle** oder durch **Hilfeseiten** informiert werden, wie sie bei Bedarf neue Teams, Gruppen oder Zugriffsberechtigungen beantragen können. Denn nur so wird gewährleistet, dass Einschränkungen zwar wirksam, aber dennoch nutzerfreundlich umgesetzt werden.

Noch ein kleiner Hinweis in eigener Sache: Ich veröffentliche regelmäßig Inhalte – auch zu Themen wie Conditional Access – auf meinem [YouTube Kanal](#). Wenn dich das interessiert, kannst du dir den Link abspeichern. Je nach Arbeitsumgebung bekommst du dort weitere praktische Einblicke, die du für deine Umgebung nutzen kannst.

Kapitel 19: Geräteverwaltung im Microsoft Entra ID – Best Practices und Konfiguration

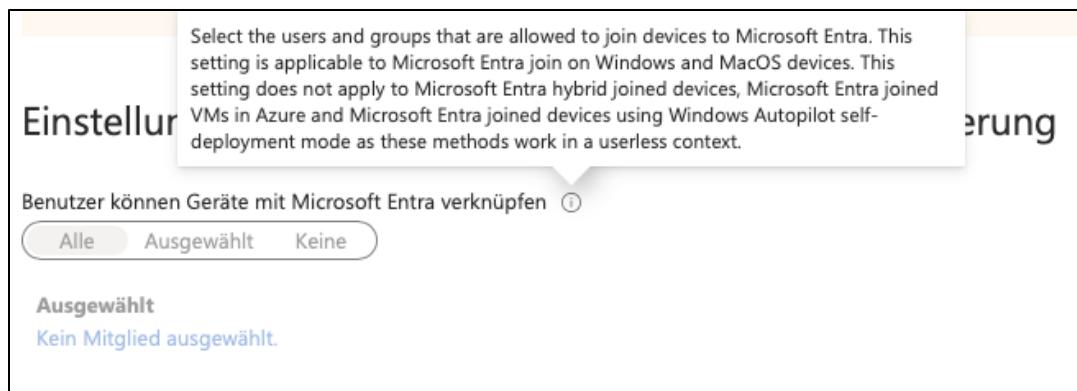
Im nächsten Schritt wechselst du im Microsoft Entra Admin Center in den Bereich „**Geräte**“ und klickst anschließend auf „**Übersicht**“, um dir einen Überblick über die aktuell registrierten Geräte im Tenant zu verschaffen. Hast du zum Beispiel etwa 509 Geräte bei rund 100 aktiven Benutzerkonten ist dies eine Zahl, die auf den ersten Blick recht hoch erscheint. Rechnet man jedoch mit durchschnittlich zwei Geräten pro Benutzer, käme man auf etwa 200–250 Geräte. Terminalserver und weitere gemeinsam genutzte Systeme, können diese Zahl jedoch schnell deutlich nach oben treiben. Wichtig ist hier: Die alleinige Anzahl an Geräten ist nicht entscheidend – vielmehr zählt, wie du die Registrierung und Verwaltung dieser Geräte kontrollierst und absicherst.

Um das zu steuern, wechselst du links in den Bereich „**Geräteeinstellungen**“. Der erste zentrale Punkt dort lautet:

„**Benutzer können Geräte mit Microsoft Entra verknüpfen**“.

Ein Klick auf das kleine (i) neben dem Eintrag zeigt dir wichtige Details. „*Select the user and groups that are allowed to join devices to Microsoft Entra. This setting is applicable to Microsoft Entra Join and MacOS*

devices. This setting does not apply to Microsoft Entra hybrid joined devices, joined VMs and autopilot devices.“



Select the users and groups that are allowed to join devices to Microsoft Entra. This setting is applicable to Microsoft Entra join on Windows and MacOS devices. This setting does not apply to Microsoft Entra hybrid joined devices, Microsoft Entra joined VMs in Azure and Microsoft Entra joined devices using Windows Autopilot self-deployment mode as these methods work in a userless context.

Benutzer können Geräte mit Microsoft Entra verknüpfen ⓘ

Alle Ausgewählt Keine

Ausgewählt
Kein Mitglied ausgewählt.

Bild 56: Geräteeinstellung

In dieser Einstellung geht es darum, ob ich als User mein Gerät selbst joinen kann – nicht jedoch hybrid-joined Devices, Azure VMs oder Autopilot-Geräte. Das bedeutet: Aktivierst du diese Funktion für alle Benutzer, kann jeder Mitarbeitende eigenständig Geräte mit dem Tenant verknüpfen – etwa über die Anmeldung in Teams, Office oder Drittanbieter-Apps. Ein User sollte nicht die Möglichkeit besitzen, seine Geräte selbst zu joinen. Stichwort: BYOD. Viele Unternehmen gehen von BYOD weg, da es mehr Arbeit hinter sich birgt, als es einen Mehrwert bietet.

Solche **ungewollten Registrierungen** führen zu einer aufgeblähten Geräteverwaltung, die kaum kontrollierbar ist. Deshalb solltest du in Erwägung ziehen, diese Option auf „**Keine**“ oder zumindest „**Ausgewählte Benutzergruppen**“ zu setzen. Will ein Benutzer dann dennoch ein Gerät registrieren, kann er sich an dich als Administrator wenden, und du kannst die Freigabe temporär aktivieren. Dieses Vorgehen erhöht die Kontrolle erheblich und reduziert Risiken – insbesondere im Kontext von BYOD-Szenarien (Bring Your Own Device), die zunehmend kritisch betrachtet werden.

Der nächste Punkt betrifft die Geräte-Registrierung in Microsoft Entra. Diese Option ist für die Business-Standard- oder -Premium-Lizenzen deaktiviert. Stattdessen läuft die Registrierung über Intune, wo du Steuerungsmöglichkeiten über Richtlinien und Conditional Access erhältst.

Als Nächstes siehst du die Einstellung:

„Multifaktor-Authentifizierung zum Registrieren oder Beitreten von Geräten bei Microsoft Entra erforderlich“.

Auch hier lautet die Empfehlung: **Setze den Wert auf „Nein“**. Microsoft selbst weist in der Beschreibung darauf hin, dass dieser Mechanismus durch **bedingten Zugriff (Conditional Access)** besser gesteuert werden kann. Die Geräteeinstellungen sind tenantweit gültig, da sie Legacy-Einstellungen sind und bieten daher nur eingeschränkte Steuerung. Über Conditional Access kannst du hingegen deutlich flexibler und sicherer arbeiten

Scrollst du weiter nach unten, erreichst du eine weitere zentrale Einstellung:

„Maximale Anzahl von Geräten pro Benutzer“.

Hier kannst du zwischen 5, 10, 15, 20 (empfohlen), 50 und 100 wählen. Früher war der Microsoft-Standardwert auf 50 Geräten pro Benutzer. Inzwischen hat Microsoft selbst diesen Wert auf **20** reduziert und gibt dies auch als Empfehlung an. Realistisch betrachtet ist das jedoch immer noch sehr großzügig bemessen. Die wenigsten Benutzer benötigen mehr als drei Geräte, die auf ihren Namen registriert sind. Meine Empfehlung: **Setze den Wert auf fünf**. Sollte ein User bereits 5 Geräte registriert haben, kann er dieser auch weiterhin nutzen, er kann dann nur kein weiteres Gerät registrieren.

Wichtig zu verstehen ist dabei: Diese Grenze betrifft nicht die Anzahl der Geräte, an denen sich ein Benutzer anmeldet, sondern jene, die **explizit auf seinen Namen registriert sind** – also als primärer Benutzer im Entra ID eingetragen sind. Eine Anmeldung auf Poolgeräten oder Terminalservern ist davon nicht betroffen.

Bevor du Änderungen vornimmst, kannst du intern evaluieren, ob es in deiner Umgebung begründete Ausnahmen gibt. Grundsätzlich gilt: **Weniger ist mehr**, wenn es um die Anzahl der verwalteten Geräte pro Benutzer geht – sowohl aus Sicherheits- als auch aus Verwaltungsgründen. Sobald die Umgebung Intune-gestützt arbeitet, kannst du zusätzliche Schutzmechanismen wie Gerätezustandsrichtlinien oder Compliance-Richtlinien einführen.

Häufig tauchen Geräte in Entra ID auf, die man gar nicht dort drin haben möchte oder sein sollten. Oft liegt das daran, dass sich Nutzer z. B. in **Microsoft Teams** oder der **Office-Suite** anmelden – oder auch in Drittanbieter-Apps, die Entra ID zur Authentifizierung und Anmeldung nutzen. Dabei wird ein bestimmtes Dialogfenster angezeigt, das viele vermutlich kennen, aber selten bewusst wahrnehmen.

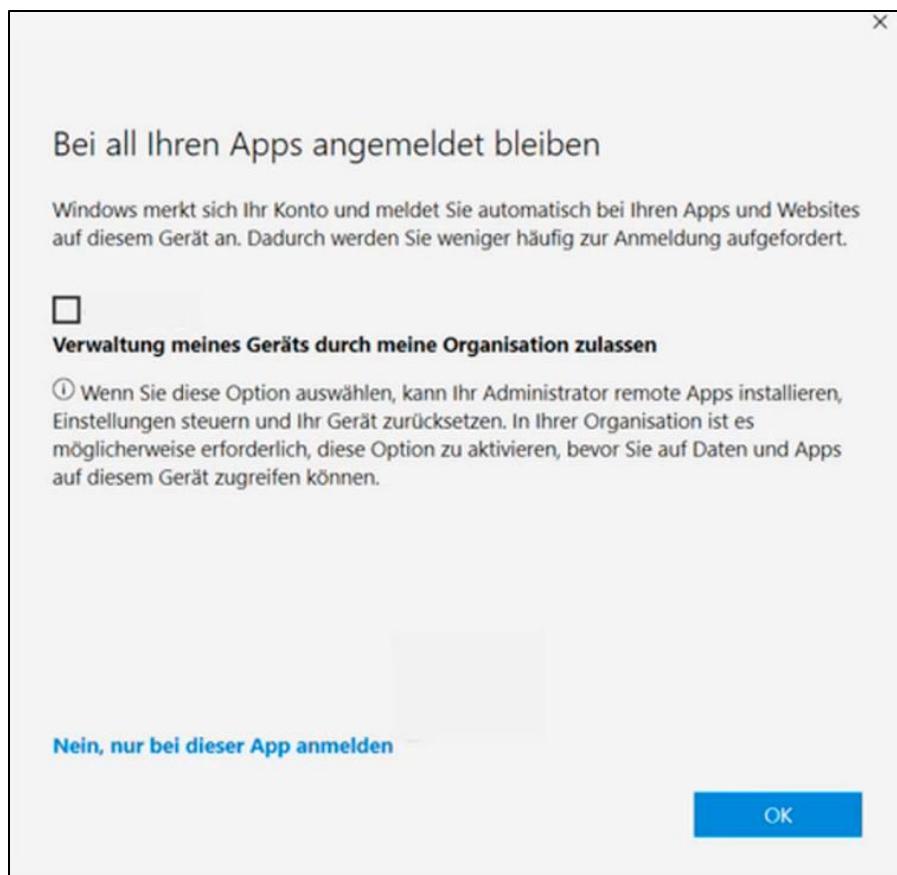


Bild 57: Meldung Registrierung

In diesem Fenster ist standardmäßig ein Haken gesetzt: „**Verwaltung meines Geräts durch meine Organisation zulassen**“. Die meisten klicken hier gedankenlos auf „OK“. Was passiert? Das Gerät wird automatisch **in Entra ID registriert**. Microsoft hat zwischenzeitlich einen erklärenden Hinweis ergänzt, der informiert, dass Administratoren mit dieser Option etwa **Apps installieren, Einstellungen verwalten oder Geräte zurücksetzen** können – aber das greift natürlich nur, wenn eine **Intune-Lizenzerierung** vorhanden ist.

Ohne Intune bedeutet das: Das Gerät ist zwar in Entra ID sichtbar, aber es lässt sich nicht wirklich verwalten. Es liegt also als Objekt im Verzeichnis – aber mehr auch nicht.

Microsoft hat zwar den Erklärtext in das Fenster eingefügt, jedoch den Haken standardmäßig drin gelassen. Somit führt es zum gleichen Ergebnis, wie vorher, dass viele Geräte registriert werden.

Eigentlich sollte an dieser Stelle die Option „**Nein, nur bei dieser App anmelden**“ ausgewählt werden. Mit der kommenden **Windows 11-Version (voraussichtlich ab 25H2)** wird Microsoft das Dialogfenster überarbeiten. Künftig soll dort eine gezieltere Auswahl möglich sein:

Privates Gerät registrieren

Unternehmensgerät

Keine Registrierung

Das gibt Hoffnung, dass ungewollte Registrierungen künftig seltener vorkommen.

Wie du ungewollte Registrierungen unterbindest

Für **Unternehmensgeräte**, die du direkt verwaltet, lässt sich dieses Verhalten per **Registry Key** unterbinden. Damit wird das Dialogfenster zur Geräteverwaltung komplett deaktiviert.

Bei **persönlichen Geräten**, auf die du keinen direkten Zugriff hast, brauchst du ein Zusammenspiel aus:

Organisationseinstellungen in Microsoft 365

Intune

Conditional Access

Nur mit diesem Dreiklang lässt sich zuverlässig verhindern, dass private Geräte automatisch in Entra ID registriert werden.

Vielleicht hast du dich auch schon mal gefragt, warum in Entra ID plötzlich **Hunderte Geräteobjekte** auftauchen – obwohl du dich doch bewusst **immer gegen die Registrierung entscheidest** und bei der Anmeldung den Haken bei „Verwaltung meines Geräts durch meine Organisation zulassen“ entfernst.

Die Antwort: **Es gibt mehr als nur diese eine Stelle**, an der ein Gerät in Entra ID registriert werden kann.

Jede Anwendung, die sich über Entra ID authentifizieren lässt, kann potenziell zur **automatischen Registrierung** führen. Dazu zählen unter anderem:

Office-Programme

Der Microsoft Store

Xbox-Dienste (z. B. Game Pass unter Windows)

Änderungen in den **Kontoeinstellungen** von Windows

SaaS-Applikationen mit Entra ID-Integration

Diese Prozesse laufen meist im Hintergrund ab – du bekommst als Nutzer oft gar nicht aktiv mit, dass eine Registrierung erfolgt ist. Das erklärt, warum trotz bewusster Auswahl immer wieder neue Geräte in Entra ID auftauchen.

Ein Registry Key als Schutzmaßnahme

Um das gezielt zu unterbinden, kannst du einen **Registry Key setzen**, der diese automatische Registrierung deaktiviert. So lässt sich das Verhalten auf Unternehmensgeräten zentral steuern und eindämmen.

Achtung bei Terminalservern und Mehrfachanmeldungen

Auch bei **Terminalservern** kann es schnell passieren, dass mehrere Registrierungen erzeugt werden – insbesondere, wenn sich viele verschiedene Nutzer darauf anmelden. Bei solchen Systemen ist das teilweise noch nachvollziehbar. Auf **normalen Clients** hingegen sollte es eher die Ausnahme sein, dass ein Gerät mehrfach auftaucht.

Wichtig zu wissen: **Entra ID macht keinen Unterschied**, ob ein Gerät einmal oder zehnmal registriert ist. Für jede neue Benutzeranmeldung kann ein weiteres Geräteobjekt erzeugt werden – selbst wenn es sich technisch gesehen um denselben physischen Rechner handelt.

Wenn also viele doppelte oder unnötige Geräte in deiner Entra ID auftauchen, ist das ein klarer Hinweis darauf, dass **Konfigurationsoptimierungen** sinnvoll wären – sei es über Registry, Intune oder Conditional Access.

Geräteeinstellungen in Entra ID – Sicherheit durch klare Konfiguration

Wenn du ins **Microsoft Entra Admin Center** gehst, findest du unter den Geräteeinstellungen einige Optionen, die du unbedingt im Blick behalten solltest – gerade im Hinblick auf Sicherheit und Verwaltungsaufwand.

Ein guter erster Schritt ist, die **maximale Anzahl an registrierten Geräten pro User herunterzusetzen**. Ein besonderes Augenmerk solltest du auf die **lokalen Administrator-Einstellungen** legen. Seit einiger Zeit gibt es die Option, dass ein Benutzer bei einem manuellen Join automatisch in die Gruppe der **lokalen Administratoren** aufgenommen wird. Auch Cloud-Administratoren können hier standardmäßig Adminrechte auf den Geräten bekommen.

Eine klare Empfehlung lautet hier: **Deaktiviere beide Optionen!**

Ein klassischer User sollte niemals lokale Adminrechte erhalten.

Auch deine globalen Admins sollten nicht automatisch lokale Admins auf jedem Gerät sein – das birgt ein enormes Risiko: Wird dieses Konto kompromittiert, sind potenziell alle Geräte betroffen.

Stattdessen solltest du dir die Option „**Aktivieren der lokalen Microsoft Entra Administratorkennwortlösung (LAPS)**“ ansehen. Die Einrichtung kannst du entweder über **Microsoft Intune** oder direkt lokal umsetzen.

Auch wenn du aktuell noch **keine Gerätesynchronisierung mit Entra ID Connect** aktiviert hast – was völlig in Ordnung ist –, solltest du dennoch die Grundlagen hier sauber konfiguriert haben. Gerade bei künftiger Skalierung oder dem Einsatz von Intune spielt das eine zentrale Rolle.

Tipp: Falls du LAPS bereits im Einsatz hast, auch in der „Legacy“-Variante, ist das immer noch ein Fortschritt gegenüber der automatischen Aufnahme in Admin-Gruppen. Die moderne Microsoft Entra LAPS-Lösung ist jedoch empfehlenswert für mehr Kontrolle und Sicherheit.

Wenn du alle Einstellungen wie gewünscht gesetzt hast, **vergiss nicht, oben auf „Speichern“ zu klicken** – sonst gehen die Änderungen verloren.

Kapitel 20: Microsoft 365 Installationsoptionen

Vielleicht hast du oder deine User schon einmal eine bestimmte Fehlermeldung im Zusammenhang mit Gerät-Registrierungen gesehen und dich gefragt, woher sie kommt. Die Ursache kann unter anderem in einer eher unscheinbaren Einstellung im **Microsoft 365 Admin Center** liegen – genauer gesagt bei den **Installationsoptionen für Microsoft 365 Apps**.

So findest du die relevante Einstellung

1. Melde dich im Microsoft 365 Admin Center an.
2. Navigiere in der linken Menüleiste zu **Einstellungen** und anschließend zu **Organisationseinstellungen**.
3. Scrolle nach unten bis zu den **Microsoft 365 Installationsoptionen**.
4. Wähle dann den Reiter **Installation** aus.
5. Dort findest du die Option: „**Apps für Windows und mobile Endgeräte bereitstellen**“

Diese Einstellung erlaubt es jedem Benutzer, sich zum Beispiel über **office.com** mit seinem geschäftlichen Benutzerkonto anzumelden und die Microsoft 365 Apps **auf beliebigen Endgeräten zu installieren** – darunter auch private PCs, Laptops oder Smartphones.

Was auf den ersten Blick praktisch klingt, hat jedoch ernsthafte Konsequenzen:

Geräte werden automatisch registriert – auch private.

→ Dadurch entstehen Einträge in der Entra ID, die weder erwünscht noch kontrolliert sind.

Unternehmensdaten gelangen auf unverwaltete Geräte.

→ Beispielsweise landet geschäftliche E-Mail in einer Office-Installation auf einem privaten Gerät.
→ Es gibt keinerlei Absicherung, ob dieses Gerät sicher, verschlüsselt oder überhaupt geschützt ist.

Berechtigte Sicherheitsbedenken:

→ Daten können versehentlich oder absichtlich weitergegeben, kopiert oder gespeichert werden.
→ Du verlierst als IT-Verantwortlicher die Kontrolle über deine Datenumgebung.

Um das zu verhindern:

Deaktiviere diese Option in den Organisationseinstellungen.

Entferne dazu den Haken bei „Apps für Windows und mobile Endgeräte bereitstellen“.

Ergänzend kannst du über Conditional Access Policies gezielt steuern, auf welchen Geräten sich

Benutzer anmelden dürfen, und Downloads oder App-Installationen auf nicht verwalteten Geräten blockieren.

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)

Bild 58: Auswahl App-Installation

Wenn jemand auf dich zukommt und sagt: „*Ich brauche unbedingt die Office Suite*“, dann sollte das nicht bedeuten, dass jeder uneingeschränkt Zugriff bekommt. Stattdessen: Lasst euch kurz Bescheid geben – ihr könnt die Installation dann entweder selbst übernehmen oder den Zugriff zeitlich begrenzt freigeben. Wichtig ist: Diese Option sollte **nicht dauerhaft aktiv** sein, denn sonst öffnet ihr die Türen für unkontrollierte Installationen auf privaten Geräten. Und genau das wollt ihr im Unternehmenskontext vermeiden.

Wichtig: Diese scheinbar kleine Einstellung kann ein echtes Einfallstor für Schatten-IT und Datenabfluss sein. Behalte sie deshalb unbedingt im Blick – und stelle sicher, dass deine Geräte- und Datenrichtlinien wirklich greifen.

Gerätezugriff über Intune einschränken

Es gibt noch einen alternativen Weg, wie du die Registrierung von Geräten unterbinden kannst: über Intune. Das funktioniert auch, **wenn ein Gerät noch gar nicht in Intune eingebunden ist**. Du kannst bestimmte Konfigurationen im Vorfeld so setzen, dass eine ungewollte Registrierung gar nicht erst möglich ist.

Dazu gehst du ins Intune-Portal.

Hinweis: Diese Funktion steht nur zur Verfügung, wenn ihr Microsoft 365 Business Premium im Einsatz habt. Mit dem Business Standard-Plan funktioniert das leider nicht.

Type	Platform
Android Enterprise (work profile)	<input type="button" value="Allow"/> <input type="button" value="Block"/>
Android device administrator	<input type="button" value="Allow"/> <input type="button" value="Block"/>
iOS/iPadOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>
macOS	<input type="button" value="Allow"/> <input type="button" value="Block"/>
Windows (MDM) ⓘ	<input type="button" value="Allow"/> <input type="button" value="Block"/>

Sobald du in Intune bist, klicke auf „**Geräte**“ und dann auf „**Registrierung**“. In diesem Bereich findest du „**Geräte-Plattform einschränkungen**“. Öffne diese und wähle die Option „**Alle Benutzer**“ aus. Unter den **Eigenschaften** kannst du anschließend „**Plattformmeinstellungen bearbeiten**“.

Bild 59: Persönliches Eigentum

Was du hier siehst, sind alle aktuell zugelassenen Plattformen für eine Geräteeinbindung. Rechts findest du den Abschnitt „**Persönliches Eigentum**“ – und genau hier solltest du ansetzen. Blockiere die Registrierung privater Geräte über diesen Weg.

Ob ein Gerät als geschäftlich oder privat gilt, hängt maßgeblich davon ab, **wie** es registriert wurde. Wenn ein Gerät über das bekannte Anmeldefenster – etwa beim ersten Start oder über office.com – eingebunden wird, handelt es sich in der Regel um einen **privaten Registrierungsweg**.

Anders sieht es aus, wenn die Registrierung über **Gruppenrichtlinien (GPOs)**, **Autopilot**, oder direkt in den **Windows-Einstellungen** unter „Arbeits- oder Schulkonto hinzufügen“ erfolgt. Diese Methoden gelten als **unternehmensgesteuerte bzw. geschäftliche Wege**.

Kurz gesagt: Die Art und Weise der Registrierung entscheidet darüber, ob ein Gerät als verwaltetes Unternehmensgerät oder als privat registriertes Gerät geführt wird.

Nachdem du gespeichert hast, kehre zurück zu Entra ID. Klicke dort links auf „**Geräte**“ und dann auf „**Übersicht**“.

Gehe nun auf „**Gesamtanzahl der Geräte**“. Hier kannst du anhand des Verknüpfungstyps Microsoft Entra Registered erkennen, dass der private Registrierungsweg genommen wurde.

Verknüpfungstyp
Microsoft Entra reg...

Bild 60: Verknüpfungstyp

Klick oben auf „**Aktivität**“, sortiere dann von alt nach neu. Auch wenn das Aktivitätsdatum nicht 100 % zuverlässig ist, bekommst du einen ersten Anhaltspunkt, welche Geräte registriert sind.

Nimm dir ruhig ein paar Minuten Zeit, geh die Liste durch und prüfe, ob Geräte dabei sind, die dir unbekannt vorkommen, offensichtlich privat genutzt werden oder schlichtweg Altlasten sind.

Falls du dich entscheidest, ein Gerät aus der Liste zu entfernen, passiert Folgendes: Wenn das Gerät **noch aktiv im Einsatz** ist, bekommt der betroffene Nutzer eine Meldung wie: „*Ihr Administrator hat dieses Gerät gelöscht. Bitte wenden Sie sich an Ihre IT.*“ – und das regelmäßig alle 30 Minuten. Das Gerät bleibt zwar funktionsfähig, aber der Nutzer wird ständig daran erinnert. Erst

wenn er es neu registriert, verschwindet der Hinweis. Ist das Gerät jedoch nicht mehr aktiv, hat das Löschen **keine weiteren Auswirkungen**.

Kurzum: Diese Übersicht ist ein gutes Tool, um alte oder verdächtige Registrierungen zu bereinigen und die Sicherheit eurer Umgebung deutlich zu verbessern.

Gerätebereinigung und automatisierte Entfernung veralteter Objekte

Ein oft unterschätzter, aber enorm wichtiger Aspekt in der Entra ID Verwaltung ist der Umgang mit veralteten Geräten. In der Geräteübersicht im Microsoft Entra Admin Center kannst du schnell feststellen, wie viele Geräte sich im Tenant befinden und wann diese zuletzt aktiv waren. Wenn du über das Menü „**Geräte > Übersicht**“ navigierst, wirst du unter anderem einen Bereich finden, der explizit „**Veraltete Geräte**“ listet. Die Definition hierfür lautet: Geräte, die sich seit über sechs Monaten nicht mehr synchronisiert oder gemeldet haben.

Ein solcher Zeitraum sollte – je nach Anwendungsfall – mit Vorsicht betrachtet werden. Du solltest daher nicht pauschal alle, als „veraltet“ markierten Geräte löschen. Stattdessen ist es empfehlenswert, diese Liste zunächst **vorsichtig zu filtern und zu bewerten**. Nutze sie als Indikator für eine anschließende Analyse und spreche ggf. mit betroffenen Teams oder Benutzergruppen, bevor du Entscheidungen über die Entfernung triffst.

Es gibt auch noch eine alternative Methode zur Verwaltung. Ein praktischer Ansatz ist hier die Nutzung eines **PowerShell-Skripts**, das automatisiert Geräte entfernt, die sich seit einer bestimmten Anzahl von Tagen nicht mehr gemeldet haben. Dieses Skript ist unter dem Begriff „**Automated Stale Device Removal**“ bekannt.

Mit dem Skript lässt sich flexibel definieren, welche Geräte zu entfernen sind – zum Beispiel alle, die seit **30, 60, 90 oder 120 Tagen** keine Rückmeldung mehr geliefert haben. Das Tool liefert dir eine schnelle, skalierbare Möglichkeit, die Geräteverwaltung effizient zu automatisieren – insbesondere dann, wenn du vorher eine saubere Bestandsaufnahme durchgeführt hast.

```

Code Blame 16 lines (13 loc) · 491 Bytes

1 $dt = (Get-Date).AddDays(-90)
2 $params = @{
3     accountEnabled = $false
4 }
5
6 $Devices = Get-MgDevice -All | Where {$_.ApproximateLastSignInDateTime -le $dt}
7 foreach ($Device in $Devices) {
8     Update-MgDevice -DeviceId $Device.Id -BodyParameter $params
9 }
10
11 $dt = (Get-Date).AddDays(-120)
12 $Devices = Get-MgDevice -All | Where {($_.ApproximateLastSignInDateTime -le $dt) -and ($_.AccountEnabled -eq $false)}
13 foreach ($Device in $Devices) {
14     Remove-MgDevice -DeviceId $Device.Id
15 }
16

```

Bild 61: Shell Skript

Empfehlung für die Praxis: Führe zunächst ein manuelles Cleanup durch, um Klarheit über das vorhandene Gerätelayout zu erhalten. Danach kannst du mit einem festen Stichtag und dem Script arbeiten, um kontinuierlich für Ordnung zu sorgen. Damit stellst du sicher, dass dein Entra ID nur die tatsächlich relevanten und genutzten Geräte enthält.

Kapitel 20: Kontrolle über Benutzereinwilligungen und Applikationsberechtigungen

Weiter geht es mit dem Umgang mit Benutzerberechtigungen und der Verwaltung von Einwilligungen bei Applikationen. Um diese Einstellungen zu prüfen, navigierst du im Microsoft Entra Admin Center zu „Anwendungen“ > „Unternehmensanwendungen“ und anschließend auf der linken Seite zu „Einwilligung und Berechtigungen“.

In der hier dargestellten Umgebung war bereits eine Vorkonfiguration vorgenommen worden: Benutzer dürfen selbstständig Applikationen registrieren – allerdings nur solche, die sogenannte „schwach eingestufte Berechtigungen“ anfordern. Klickst du auf diese Berechtigungsliste, werden dir fünf spezifische Berechtigungen angezeigt, die automatisch freigegeben werden. Neue Applikationen installieren sollten die Administratoren machen und nicht der User selbst.



Verwendete API	Berechtigungen	Beschreibung
Microsoft Graph	profile	Grundlegendes Profil von Benutzern anzeigen
Microsoft Graph	email	E-Mail-Adresse von Benutzern anzeigen
Microsoft Graph	openid	Benutzer anmelden
Microsoft Graph	User.Read	Anmelden und Benutzerprofil lesen
Microsoft Graph	offline_access	Zugriff auf Daten beibehalten, für die Sie Zugriff erteilt haben

Bild 62: Berechtigungen

Als Administrator solltest du daher prüfen, ob dieses Verhalten in deinem Tenant tatsächlich gewünscht ist. Du solltest diesen Mechanismus deaktivieren, um unkontrollierte App-Registrierungen zu vermeiden.

Du kannst diese Konfiguration ändern, indem du auf „Einstellungen für die Benutzereinwilligung“ zurückgehst und dort die Einstellung „**Benutzereinwilligung nicht zulassen. Für alle Apps ist ein Administrator erforderlich.**“ auswählst. Damit erreichst du, dass Benutzer bei der Nutzung oder Installation neuer Applikationen, die bestimmte Berechtigungen benötigen, eine **Genehmigungsanfrage an einen globalen Administrator** senden müssen.

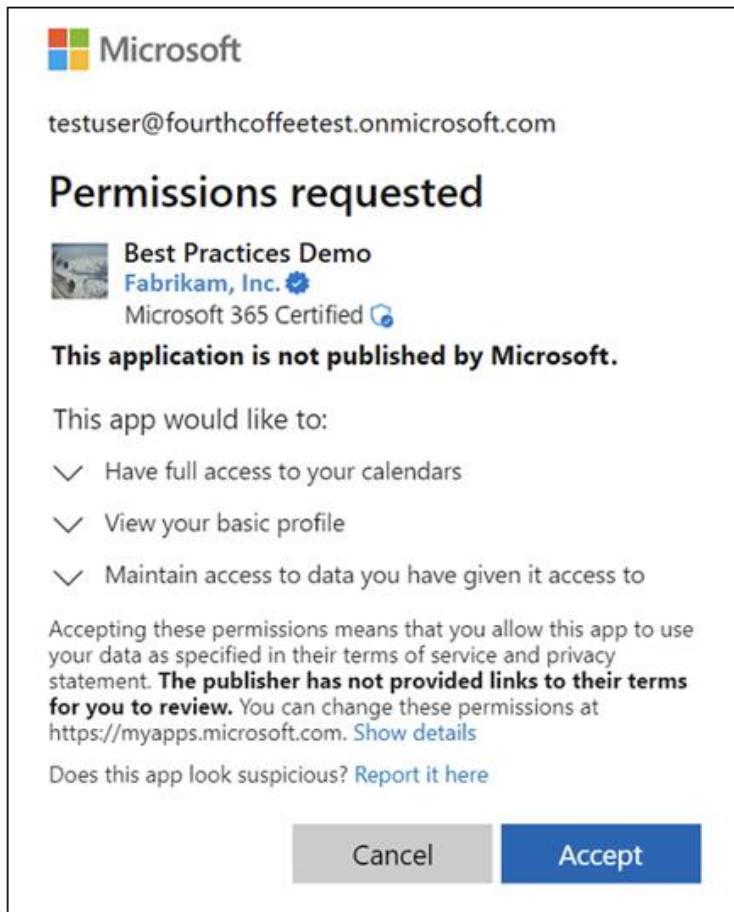


Bild 63: Permission requested

Wenn dieser Fall eintritt, sieht der Benutzer in der Oberfläche eine sogenannte „**Permission Request**“-Anzeige – eine Anforderungsmaske, die klar signalisiert: Nur ein globaler Administrator kann diesen Zugriff genehmigen. Dadurch wird automatisch verhindert, dass Applikationen ohne dein Wissen tiefgreifende Rechte im Tenant erhalten. Besonders bei OAuth-basierten Cloud-Anwendungen ist das entscheidend, da über entsprechende Berechtigungen Zugriff auf E-Mail-Inhalte, Kalender, Kontakte oder sogar auf alle Dateien im OneDrive oder SharePoint erfolgen kann.

Ein zusätzlicher Best Practice: Mache vor Änderungen unbedingt einen **Screenshot der aktuellen Konfiguration**, um bei Bedarf auf die vorherigen Einstellungen zurückgreifen zu können oder diese zu dokumentieren.

Im weiteren Verlauf dieses Schritts solltest du dir nun die Übersicht der bereits registrierten Unternehmensanwendungen ansehen. Navigiere dazu zu „**Unternehmensanwendungen**“ > „Übersicht“. Dort siehst du alle Applikationen, die in deinem Tenant im Einsatz sind – unabhängig davon, ob sie aktiv verwendet werden oder lediglich registriert wurden. Nimm dir Zeit und gehe die Liste durch. Häufig fallen hier bereits **verdächtige oder unerwartete Applikationen** auf.

Name	↓	Objekt-ID	Anwendungs-ID	URL für Startseite	Erstellt am
D	DfMGraphApp	002de6b4-a450-49bd-96...	380e9762-7111-490b-80...		13.1.2024
D	DirectoryLookupS...	0061f2cf-589e-4b11-9afb...	9cd0f7df-8b1a-4e54-8c0...		18.9.2020
AC	Azure Communicati...	00b12d97-ace5-4f72-8f6...	1fd5118e-2576-4263-813...		3.5.2021
N	Networking-MNC	0227152a-f46a-42d7-8c4...	6d057c82-a784-47ae-8d...		17.3.2020
HM	Hubble Media Ser...	0246e059-505e-42e9-88...	84a0e9dd-6e58-4aad-82...		6.9.2024
MD	Microsoft Defende...	02827144-2652-4ea7-b6...	0c7668b5-3260-4ad0-9f5...		31.5.2022
IG	Intune Grouping a...	02c0a017-7c16-4c01-8da...	fd14a986-6fe4-409a-883...		12.5.2022

Bild 64: Anwendungen

Es tauchen zum Beispiel Anwendungen wie „**Miro**“, „**Awork**“ oder auch „**Samsung Mail**“ auf. Letztere wurde wahrscheinlich durch die Nutzung eines mobilen Endgeräts mit vorinstallierter Samsung-Mail-App autorisiert. Solche Einträge sind zwar nicht per se verdächtig, sollten aber im Rahmen eines vollständigen Überblicks dokumentiert und bewertet werden.

Mache nun weiter mit dem Aufruf der jeweiligen Anwendung und navigiere zunächst zum Abschnitt „**Besitzer**“. Hier kannst du feststellen, ob überhaupt ein Besitzer für die Applikation eingetragen ist. Ist das nicht der Fall, gehst du weiter auf „**Benutzer und Gruppen**“, um zu prüfen, ob die App aktuell noch mit einem Benutzerkonto verknüpft ist. Falls keine Benutzer mehr zugeordnet sind oder die hinterlegte Person nicht mehr aktiv ist, könnte das bereits ein Hinweis darauf sein, dass die Anwendung obsolet ist.

Im nächsten Schritt öffnest du den Bereich **Aktivitäten und** anschließend „**Anmeldeprotokolle**“. Um eine aussagekräftige Auswertung zu erhalten, filterst du hier idealerweise nach dem Zeitraum „**Letzter Monat**“. Wenn keine Anmeldungen im definierten Zeitraum erfolgt sind, ist es sehr wahrscheinlich, dass die Applikation aktuell nicht mehr genutzt wird.

Klicke auf Eigenschaften und nun hast du zwei Optionen: Entweder du **löscht die Anwendung sofort**, oder du **deaktivierst zunächst die Anmeldung** zur App. Sollte sich nach der Deaktivierung ein Benutzer melden und auf die Applikation zugreifen wollen, kann der Zugriff jederzeit wieder aktiviert werden. Meldet sich hingegen niemand, lässt sich die App zu einem späteren Zeitpunkt endgültig entfernen. Wichtig ist, vor dem Löschen in Zweifelsfällen Rücksprache mit dem betroffenen Benutzer zu halten.

Dieses Vorgehen lässt sich systematisch auf alle Anwendungen im Tenant anwenden. Im Beispiel wurde unter anderem „**Samsung Mail**“ geprüft – eine Anwendung, die oft durch mobile Endgeräte registriert wird. Bei solchen Apps empfiehlt es sich, neben der Prüfung der Anmeldeaktivitäten auch über den Einsatz von **App-Schutzrichtlinien in Intune** nachzudenken. Mit diesen Richtlinien lassen sich Sicherheitsmaßnahmen wie das Unterbinden von Screenshots oder das Kopieren von Inhalten aus geschäftlichen Apps umsetzen. Voraussetzung dafür ist allerdings, dass die entsprechenden Geräte über **Intune verwaltet** werden.

Durch diesen strukturierten Prüfprozess und die Anpassung der Benutzereinwilligungsrichtlinien stellst du sicher, dass keine unkontrollierten Applikationen im Hintergrund mitlaufen und gleichzeitig neue Registrierungen nur unter administrativer Kontrolle erfolgen. So reduzierst du effektiv potenzielle Sicherheitsrisiken und behältst die Kontrolle über deinen Applikationsbestand.

Kapitel 21: Externe Identitäten und Zusammenarbeit sicher steuern

Ein zentraler Aspekt in der Verwaltung von Microsoft Entra ID ist der kontrollierte Umgang mit **externen Identitäten** – insbesondere im Kontext der **Gasteinladung**. Du beginnst die Konfiguration im Entra Admin Center unter „**Externe Identitäten**“, indem du zunächst zur **Übersicht** navigierst. Dort findest du den Punkt „**Einstellungen für externe Zusammenarbeit**“. Der oberste Punkt **Gastbenutzerzugriff** wurde bereits in einem früheren Kapitel im Zusammenhang mit Benutzereinstellungen kurz angeschnitten wurde.

Der nächste Punkt beantwortet folgende Frage: **Wer darf überhaupt externe Benutzer einladen?** Standardmäßig erlaubt Microsoft, dass **Mitglieder, Gastbenutzer mit Mitgliederrechten sowie Benutzer mit bestimmten Administratorrollen** neue Gäste hinzufügen dürfen. Diese Voreinstellung ist in vielen Organisationen problematisch, da sie unkontrolliert zu einer wachsenden Zahl externer Konten führen kann – häufig ohne sinnvolle Dokumentation oder Überprüfung.

Als IT-Administrator solltest du daher in Betracht ziehen, diesen Prozess zu **zentralisieren**. Idealerweise führst du einen **strukturierten Onboarding-Prozess** ein, in dem ausschließlich autorisierte Administratoren oder ausgewählte Personengruppen – etwa Projektleiter – berechtigt sind, externe Gäste einzuladen. So behältst du die Kontrolle über alle externen Identitäten im Tenant und kannst gleichzeitig sicherstellen, dass jede Einladung dokumentiert, gerechtfertigt und revisionssicher ist.

Die Empfehlung lautete: Entwickle in Abstimmung mit dem Endkunden **klare Richtlinien**, wer Gäste einladen darf und unter welchen Voraussetzungen. Das betrifft nicht nur technische Einstellungen, sondern auch betriebliche Absprachen und Kommunikationsprozesse mit betroffenen Abteilungen.

Den Punkt **Einstellungen für das Verlassen von externen Benutzer** sollte auf „**Ja**“ eingestellt sein. Ein weiterer Punkt ist die **Einschränkung von Einladungen nach Domänen**. Standardmäßig erlaubt Microsoft, dass **Einladungen an beliebige externe Domänen** gesendet werden können. Hier bietet dir Entra ID die Option, nur Einladungen an vorher **freigegebene Domänen** zuzulassen. Sobald eine bestimmte Domäne freigegeben ist, dürfen Benutzer mit einer E-Mail-Adresse aus dieser Domäne eingeladen werden. Alle anderen Anfragen würden abgelehnt.

Einstellungen für das Verlassen von externen Benutzern

Externen Benutzern erlauben, sich selbst aus Ihrer Organisation zu entfernen (empfohlen) [\(i\)](#)

Weitere Informationen

Ja Nein

Einschränkungen für die Zusammenarbeit

⚠️ Mandantenübergreifende Zugriffseinstellungen werden auch beim Senden einer Einladung angewendet.

Senden von Einladungen an beliebige Domäne zulassen (inklusive Einstellung)
 Einladungen für die angegebenen Domänen verweigern
 Einladungen nur für die angegebenen Domänen zulassen (restriktivste Einstellung)

Bild 65: Externe Benutzer

Während du dich im Bereich der externen Identitäten und der Gastkonfiguration bewegst, kann schnell die Frage auftreten, wie sich diese Einstellungen im Vergleich zum Microsoft Teams Admin Center verhalten.

Die Antwort: **Beide Bereiche greifen ineinander, adressieren aber unterschiedliche Ebenen.** Im Entra ID Admin Center geht es um **die übergreifende Steuerung für sämtliche Microsoft-365-Dienste**, bei denen Gäste eingebunden werden können – also nicht nur Teams, sondern auch SharePoint, OneDrive und weitere Applikationen. Das Teams Admin Center beschränkt sich dagegen auf die spezifischen Einstellungen innerhalb von Microsoft Teams. Das Entra ID Portal bildet somit die **tenantweite Steuerungsebene** für die externe Zusammenarbeit.

Ein praktisches Feature in diesem Zusammenhang ist das **Zulassen spezifischer Domänen**. Wenn du auf die entsprechende Einstellung klickst, kannst du festlegen, mit welchen externen Domänen dein Tenant kollaborieren darf.

Kapitel 22: Gasteinstellungen in SharePoint und OneDrive sinnvoll konfigurieren

Navigiere dazu im **Microsoft 365 Admin Center** zum Menüpunkt **Einstellungen der Organisation**. Unter dem Abschnitt findest du anschließend den Eintrag **SharePoint**.

Es gibt vier zentrale Varianten, wie du das Teilen von Inhalten regeln kannst:

1. **Nur Personen in Ihrer Organisation:** Dies ist die restriktivste Variante. Mit ihr ist keine externe Freigabe von Inhalten mehr möglich – alles bleibt strikt innerhalb der eigenen Organisation.
2. **Nur vorhandene Gäste:** Dies ist eine deutlich restriktivere Einstellung. In diesem Modus kann nur mit Benutzern geteilt werden, die bereits im Entra ID Tenant als Guest hinterlegt sind. Möchte ein Mitarbeitender beispielsweise eine Datei an dich senden und du bist noch nicht als Guest vorhanden, muss er sich zunächst an die IT wenden. Diese legt dich dann manuell als Guest an,

woraufhin du eine Einladung erhältst und dich registrierst. Diese Methode bietet eine bessere **prozessuale Nachvollziehbarkeit**.

3. **Neue und vorhandene Gäste:** Mit dieser Option kann ein Benutzer eigenständig Gäste in den Tenant eingefügt. Diese Gäste erhalten dann eine E-Mail-Einladung, über die sie den Zugriff bestätigen. Diese Einstellung bietet ein **besseres Maß an Kontrolle** gegenüber der anonymen Freigabe, ist aber dennoch weit offen.
4. **Jeder (anonyme Benutzer):** Diese Einstellung erlaubt die sogenannte „**anonyme Authentifizierung**“. Das bedeutet, dass ein freigegebener Link beliebig weitergegeben werden kann. Dabei ist keine Authentifizierung erforderlich, was die **Nachverfolgbarkeit nahezu unmöglich macht**.

SharePoint

i Sie sind nicht berechtigt, Änderungen zu speichern. [Weitere Informationen](#)

Wählen Sie aus, wie Ihre Benutzer SharePoint-Sites teilen können, die in Ihrer Organisation erstellt wurden.

Benutzer können teilen mit:

- Nur Personen in Ihrer Organisation – kein externes Teilen zulässig
- Nur vorhandene Gäste – Nur Gäste, die bereits im Verzeichnis Ihrer Organisation vorhanden sind.
- Neue und vorhandene Gäste – Gäste müssen sich anmelden oder einen Prüfcode angeben.
- Jeder – Nutzer können Dateien und Ordner über Links freigeben, für die keine Anmeldung erforderlich ist

Erweiterte Optionen für externes Teilen

Schränken Sie die externe Freigabe nach Domäne ein, lassen Sie die externe Freigabe nur für angegebene Sicherheitsgruppen zu, und vieles mehr im SharePoint Admin Center. [Zum SharePoint Admin Center wechseln](#)

Bild 66: SharePoint

Kapitel 23: Mandantenübergreifende Zugriffseinstellungen – Kontrolle über eingehende und ausgehende Einladungen

Navigiere zunächst im **Microsoft Entra Admin Center** zum Punkt **Einstellungen für externe Zusammenarbeit** und öffne dort die **mandantenübergreifenden Zugriffseinstellungen**. Diese Funktion ist eines der zentralen Werkzeuge, um externe Identitäten in deinem Tenant sicher zu verwalten. Klicke dann auf **Standardeinstellungen**, um die allgemeinen Richtlinien für alle anderen Microsoft-Tenants zu konfigurieren.

B2B-Zusammenarbeit	Direkte B2B-Verbindung	Zunächst werfen wir einen Blick auf die eingehenden Zugriffseinstellungen . Diese bestimmen, ob externe Benutzer aus anderen Microsoft-Tenants überhaupt Zugriff auf Ressourcen deines Tenants erhalten dürfen. In kritischen Situationen – etwa bei Auffälligkeiten oder Sicherheitsvorfällen – kannst du hier den Zugriff sofort blockieren und sämtliche externe Zugriffe unterbinden. Diese Maßnahme ist eine Art Notbremse, mit der sich ein potenzielles Eindringen externer Benutzer schnell unterbrechen lässt.
B2B collaboration inbound access settings lets you set up self-service sign-up so they can request access.		Weitere Informationen ↗
<u>Externe Benutzer und Gruppen</u>	Anwendungen	
Zugriffsstatus	Bild 67: Zugriff blockieren	
<input checked="" type="radio"/> Zugriff zulassen <input type="radio"/> Zugriff blockieren		
Gilt für		
<input checked="" type="radio"/> Alle externen Benutzer und Gruppen		

B2B-Zusammenarbeit Direkte B2B-Verbindung

Die Einstellungen für den ausgehenden B2B Collaboration sind die Standardeinstellungen, die für alle externen Microsoft Anwendungen gelten. Sie bestimmen, welche externen Anwendungen sie zugreifen können.

[Weitere Informationen ↗](#)
Benutzer und Gruppen
Externe Anwendungen

Zugriffsstatus

 Zugriff zulassen

 Zugriff blockieren

Gilt für

Bild 68: Zugriff

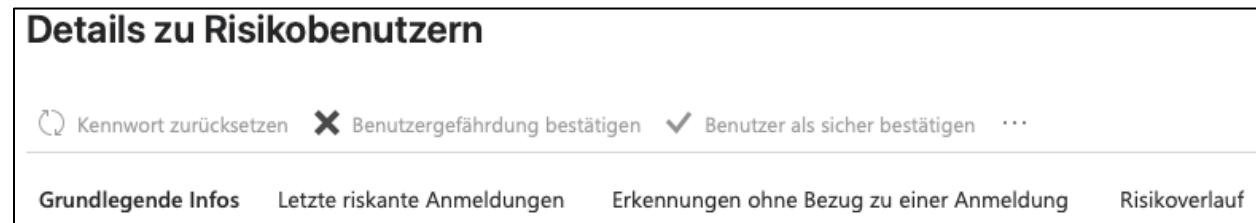
Standardmäßig ist es so eingestellt, dass jeder Benutzer von externen Organisationen eingeladen werden kann. Doch genau hier setzt eine wichtige Überlegung an: In vielen Unternehmen ist es nicht notwendig, dass sämtliche Benutzer Einladungen von außen annehmen können. Eine sinnvolle Maßnahme wäre, den Zugriff nur bestimmten Benutzergruppen zu gestatten. Du kannst eine dedizierte Sicherheitsgruppe anlegen und in den Richtlinien unter „Zugriff zulassen für bestimmte Benutzer oder Gruppen“ genau diese Gruppe angeben. So sorgst du dafür, dass nur Mitglieder dieser Gruppe Einladungen von außen annehmen dürfen.

Kapitel 24: Identity Protection und Sicherheitsbewertung – Risikoanalysen verstehen und nutzen

Starte dafür im Microsoft Entra Admin Center im Bereich **Identitätsschutz**. Der volle Zugriff kann nur mit einer P2 Lizenzierung genutzt werden. Jedoch stehen bei den anderen Lizenzierungen die Berichte zur Verfügung. Die Identity Protection ist ein KI-gesteuerter Mechanismus. Dieser Mechanismus erkennt von wo aus sich User anmelden, von welchen Geräten, wie häufig sich User anmelden, ob es fehlerhafte Anmeldungen gab und kategorisiert, und validiert diese dann.

Um die Berichte einzusehen, klicke unter **Berichte auf riskante Anmeldungen**. Wähle im Datumsfilter den Zeitraum „**Letzter Monat**“, um dir einen Überblick darüber zu verschaffen, ob im vergangenen Monat verdächtige oder anomale Anmeldeversuche registriert wurden. Mit einer P2 Lizenz erhältst du automatische Warnung. Hast du diese nicht ist es wichtig, dir einen internen Reminder zu setzen – etwa wöchentlich oder mindestens zweiwöchentlich –, um diesen Bereich manuell zu überprüfen. Ein monatlicher Check wäre an dieser Stelle eher zu spät, wenn es um präventive Sicherheit geht.

Details zu Risikobenutzern



The screenshot shows a user interface for managing risk users. At the top, there are three buttons: a circular arrow for password reset, a red X for confirming user risk, and a checkmark for marking users as safe. Below this is a horizontal menu bar with four items: "Grundlegende Infos" (underlined), "Letzte riskante Anmeldungen", "Erkennungen ohne Bezug zu einer Anmeldung", and "Risikoverlauf".

Bild 69: Risikobenutzer

Besonders relevant ist hier auch der Bericht über **riskante Benutzer**. Dieser zeigt dir Konten, bei denen in der Vergangenheit verdächtige Anmeldeaktivitäten festgestellt wurden. Öffne dafür den gleichnamigen Punkt und wähle einen Benutzer aus. Dort findest du unter „**Letzte riskante Anmeldungen**“ einen Einblick, ob und wann Auffälligkeiten vorlagen. Sollten alte Anmeldungen vorliegen empfiehlt es sich in solchen Fällen, die Anmeldung als **sicher zu bestätigen**, um keine unnötigen Blockierungen im System aufrechtzuerhalten – vorausgesetzt, der Benutzer ist legitim bekannt.



The screenshot shows the Microsoft Identity Security Score dashboard. At the top, there's a navigation bar with a search bar, a 'Weitere Informationen' button, and a 'Haben Sie...' button. Below the navigation, there are several sections: 'Erste Schritte', 'Diagnose und Problembehandlung', 'Schützen' (which includes 'Bedingter Zugriff', 'Identity Protection', and 'Security Center'), and 'Verwalten' (which includes 'Identitätssicherheitsbewertung' and 'Benannte Standorte'). The main area displays a large orange trophy icon next to the text '90.91%' in a large, bold font. Below the score, it says 'Letzte Aktualisierung: 24.2.2025, 01:00:00' and a link to 'Microsoft-Sicherheitsbewertung anzeigen'. A note at the top right says 'Eine neue Sicherheitsbewertungsoberfläche ist verfügbar.'

Bild 70: Identitätssicherheitsbewertung

Im Anschluss kannst du einen Blick auf die **Identitätssicherheitsbewertung** werfen. Diese findest du ebenfalls im Bereich **Identitätsschutz**. Den Microsoft Defender findest du im Microsoft 365Admin Center → Sicherheit. Im Microsoft Defender Portal unter **Gefährdungsverwaltung** → **Sicherheitsbewertung** findest du Maßnahmen, die du im Tenant konfigurieren solltest, um das Sicherheitsniveau von deinem Tenant hochzustufen.

Neben einem gewissen „Gamification-Effekt“ bietet er dir eine sehr detaillierte Liste von Maßnahmen, die du umsetzen kannst, um dein Sicherheitsniveau zu erhöhen. Klicke im Defender Portal auf **Empfohlene Maßnahmen**, um eine Übersicht dieser Konfigurationsvorschläge zu erhalten. Hier kannst du einmal durchgehen, welche Maßnahmen für dich in Frage kommen und welche nicht.

Beachte jedoch: Viele der Maßnahmen bauen direkt auf Microsoft 365 Services auf, etwa **Defender for Identity**, **Defender for Endpoint**, **Defender for Office 365** oder **Microsoft Defender for Cloud Apps**. Wenn du alternative Sicherheitslösungen im Einsatz hast – zum Beispiel von Drittherstellern – ist der Score nur bedingt aussagekräftig. Das kann zu Irritationen führen, da dir dann potenziell niedrige Scores angezeigt werden, obwohl du technisch längst abgesichert bist.

Zurück im Entra ID: Die dortige **Identitätssicherheitsbewertung** ist von dem Microsoft Secure Score abgekapselt. Ein Wert im 90% Bereich ist sehr gut. Nutze diese Bewertung als Orientierungshilfe und prüfe, ob einzelne Empfehlungen für deinen Tenant sinnvoll sind – oder ob du das Risiko bewusst akzeptierst, weil du bereits andere Schutzmechanismen etabliert hast.

Kapitel 25: Einstieg in den Bedingten Zugriff (Conditional Access)

Jetzt beginnen wir mit dem **bedingten Zugriff** (Conditional Access). Ziel dieser Funktion ist es, kontextbasierte Richtlinien zu erstellen, die z. B. abhängig vom Standort, Gerätetyp oder Benutzerstatus Zugriff erlauben, verweigern oder absichern – etwa durch eine Multi-Faktor-Authentifizierung (MFA).

Wenn du zum ersten Mal in den Bereich **Bedingter Zugriff > Richtlinien** navigierst, wirst du feststellen, dass noch keine Richtlinien angelegt sind. Du startest also auf einer **grünen Wiese** – ein guter Moment, um dir ein sauberes, durchdachtes Regelwerk aufzubauen. Falls du bereits Mandanten betreust, in denen Conditional Access im Einsatz ist, lohnt sich der Blick auf bestehende Richtlinien.

Namenskonventionen

Ein elementarer Bestandteil von Conditional Access ist eine **klare Benennung deiner Richtlinien**. Du solltest auf einen Blick erkennen können, was eine Richtlinie bewirkt, für wen sie gilt und in welchem Szenario sie greift. Viele Admins wählen Namen wie „MFA intern“ oder „Block Legacy“ – das kann schnell unübersichtlich werden.

Eine professionelle **Namenskonvention** sieht beispielsweise so aus:

```
CA001-AllUser-AllResources-ExceptAdmins&UA_Users-BlockLoginFromSpecificCountries  
CA002-AllUser-AllResources-ExceptAdmins-BlockLegacyAuthentication  
CA003-AllUser-AllResources-ExceptAdmins-BlockUnsupportedDevices  
CA004-AllUser-AllResources-ExceptAdmins-BlockDeviceCodeFlow
```

Bild 71: Beispiel Namenskonvention

CA001–AllUsers–AllResources–Except<Gruppe XY>BlockLoginfromspecific countries

Dieser Aufbau zeigt sofort: Es handelt sich um Richtlinie Nr. 1, sie gilt für alle Benutzer, auf alle Ressourcen – mit einer definierten Ausnahme –, und sie blockiert den Zugriff aus bestimmten Ländern. Welche Richtlinien du einfügen ist, hängt mit deiner Lizenz zusammen. Nicht jede Funktion steht dir zur Verfügung. Allerdings kannst du auch mit wenigen Richtlinien die Sicherheit von deinem Tenant hochstufen.

1. Richtlinie: Zugriff aus bestimmten Ländern einschränken

Ein klassischer Einstieg für eine Sicherheitsrichtlinie ist das **Blockieren von Zugriffen aus nicht benötigten Ländern**. Hierzu stellt sich die Frage: Von wo aus arbeiten deine User?

In den meisten Unternehmen sitzen die meisten Mitarbeitenden in Deutschland. Dann gibt es hin und wieder auch Mitarbeitenden die aus dem Ausland arbeiten. Hier muss klar sein, ob diese per VPN arbeiten

– was den Zugriffspunkt wieder nach Deutschland verlagern würde – oder ob die mobilen Endgeräte (etwa Smartphones mit Exchange Online) direkt kommunizieren.

Ein sinnvoller Ansatz wäre daher: **Standardmäßig nur Zugriffe aus Deutschland erlauben**, weitere Länder jedoch gezielt zu **whitelisten**, falls ein Bedarf besteht. Gerade für mobile Geräte ohne VPN ist das wichtig, da diese sonst keine Verbindung mehr aufbauen könnten.

Übrigens: Wenn ein Gerät per VPN über die Firmenzentrale verbunden ist, wird es als Zugriff aus Deutschland erkannt, auch wenn sich der User physisch im Ausland befindet.

Um zu prüfen, von welchen geografischen Standorten aus sich ein bestimmter Benutzer in der letzten Zeit angemeldet hat, begibst du dich im Microsoft Entra Admin Center in die **Anmeldeprotokolle** der User. Dort stellst du zunächst den **Zeitraum** auf „letzter Monat“ ein, um einen erweiterten Überblick über alle erfolgten Anmeldungen im zurückliegenden Zeitraum zu erhalten.

Anschließend nutzt du die Funktion „**Filter hinzufügen**“ auf der rechten Seite des Bildschirms. Scrolle in der Liste der verfügbaren Filteroptionen nach unten, bis du die Einstellung „**Standort**“ findest. Diese Auswahl erlaubt es dir, Anmeldeereignisse nach geografischen Kriterien wie Region oder Bundesland zu segmentieren.

Nachdem du den Standortfilter aktiviert hast, lässt du die Ergebnisse kurz laden. In diesem Fall zeigte sich, dass nur wenige Standorte im Protokoll vermerkt waren. Die erwartete automatische Auflistung durch die Oberfläche blieb jedoch aus. In solchen Situationen kann es hilfreich sein, das Filterfenster zu schließen und die Einträge manuell von oben nach unten zu überfliegen, um einen Eindruck darüber zu gewinnen, **aus welchen Regionen tatsächlich auf das System zugegriffen wurde**.

Technische Umsetzung: 1. Richtlinie Länderblockierung

Um eine neue Richtlinie anzulegen, gehst du dafür in das **Entra ID → Condition Access → Neue Richtlinie**.

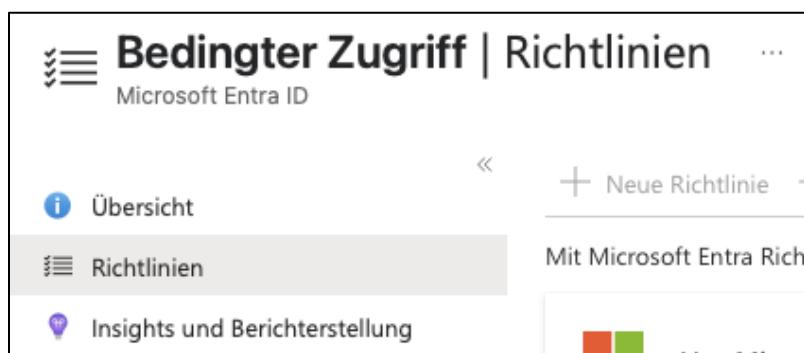


Bild 72: Neue Richtlinie

1. Richtlinie:

CA001–AllUsers–AllResources–ExceptBreakingGlassAccount–BlockLogin from specific countries

Im Normalfall sollte es eine „**AnyAny**“ Richtlinie geben im Condition Access. Das heißt alle Benutzer **außer**. Im ersten Schritt definierst du den Namen der Richtlinie. Dafür nutzt du „**AllUser**“ und „**AllResources**“ und schließt dann gezielt Ausnahmen aus – beispielsweise für einen „*Breaking Glass*“-Account oder *Notfall-Admin*. Falls bereits ein dedizierter Admin-Account existiert, kann dieser als Ausnahme definiert werden. Alternativ empfiehlt es sich, eine eigene **Gruppe** für ausgenommene Benutzer anzulegen. Anschließend folgt noch die Info, was passieren soll z.B., dass der Login von bestimmten Ländern geblockt werden soll.

Einschließen <hr/> <input type="radio"/> Kein <input checked="" type="radio"/> Alle Benutzer <input type="radio"/> Benutzer und Gruppen auswählen	Ausschließen <hr/> <p>Wählen Sie die Benutzer und Gruppen aus, die von der Richtlinie ausgenommen werden sollen.</p> <input type="checkbox"/> Gastbenutzer oder externe Benutzer ⓘ <input type="checkbox"/> Verzeichnisrollen ⓘ <input type="checkbox"/> Benutzer und Gruppen
--	--

⚠️ Sperren Sie sich nicht aus! Diese Richtlinie wirkt sich auf alle Benutzer aus. Wir empfehlen, eine Richtlinie zunächst auf eine kleine Gruppe von Benutzern anzuwenden, um sicherzustellen, dass sie sich wie erwartet verhält.
[Weitere Informationen ⓘ](#)

Bild 73: Einschließen/Ausschließen

Als nächstes klickst du auf **Benutzer** und wählst bei Einschließen **Alle Benutzer** aus.

Unter Ausschließen wählst du deinen Breaking Glas Account aus oder eine Benutzergruppe. Alles, was über eine einzelne Person hinausgeht, sollte grundsätzlich gruppenbasiert konfiguriert werden.

Der Aufbau einer Condition Access Richtlinie ist immer gleich. Es wird zuerst definiert, wer von der Richtlinie überhaupt betroffen ist. Danach entscheidest du bei welchen Ressourcen die Richtlinie greifen soll.

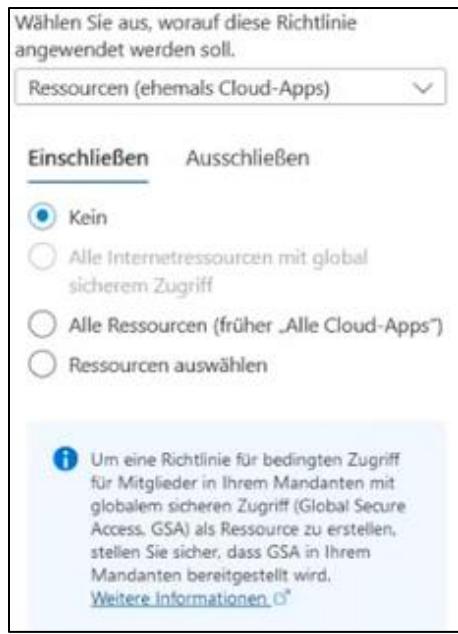


Bild 74: Ressourcen

Im nächsten Schritt wählst du unter „**Zielressourcen**“ die Option „**Alle Ressourcen**“, um sicherzustellen, dass die Regel sämtliche Microsoft-365-Dienste umfasst – darunter Teams, SharePoint, Outlook, Intune, Word und andere. Die Zugriffssteuerung soll für sämtliche Zugriffsversuche auf die Microsoft-Ressourcen gelten.

Bis hierin wurde definiert, dass alle User auf irgendeine Ressource im Microsoft 365 zugreifen dürfen oder eben nicht.

Konfigurieren ⓘ

Ja Nein

Einschließen Ausschließen

- Beliebiges Netzwerk oder beliebiger Standort
- Alle vertrauenswürdigen Netzwerke und Standorte
- Alle konformen Netzwerkstandorte
- Ausgewählte Netzwerke und Standorte

Info: Um eine Richtlinie für bedingten Zugriff zu erstellen, die sicherstellt, dass die Mitglieder Ihres Mandanten aus ihrem konformen Netzwerk stammen, stellen Sie sicher, dass der globale sichere Zugriff (Global Secure Access, GSA) bereitgestellt und die adaptive Zugriffssignalisierung im GSA in Ihrem Mandanten aktiviert ist. Weitere Informationen zur Vorgehensweise [adaptive GSA-Zugriffssignalisierung aktivieren.](#)

Anschließend definierst du unter dem Punkt „Netzwerk“ von welchem Standort aus sich die User anmelden dürfen. Aktiviere hier die Option Konfigurieren auf „Ja“ und wähle „**Ausgewählte Netzwerke Standorte**“.

Bild 75: Netzwerk

Mit dem „Block Login from specific countries“ arbeitest du mit einem Blacklisting. Das heißt du musst definieren, von wo du den Zugriff erlaubst und von wo aus nicht. Dies wird mit einer separaten Auflistung gemacht, die erstellt wird.

Gehe hierfür in das Entra Admin Center unter den Punkt Schutz → Bedingter Zugriff → Verwalten → Benannte Standorte → Länder/Regionen. Wähle nun zuerst alle Länder aus, indem du neben Namen in das Kästchen klickst und wählst die Länder ab von denen der Zugriff nicht blockiert werden soll.

Achte darauf, nur die Länder freizugeben, aus denen wirklich ein legitimer Zugriff notwendig ist. Diese Einstellung gilt nicht für den Admin, da dieser aus der Richtlinie ausgenommen ist. Wenn alle Mitarbeiter über ein Firmen-VPN mit deutschem Exit arbeiten, reicht es möglicherweise, ausschließlich Deutschland

zuzulassen.

Die Standorteinstellungen kannst du jederzeit auch anpassen, wenn sich etwas im Unternehmen ändern sollte. Gib einen sprechenden Namen für die Standorte ein z. B. „**BlockLoginExceptGermany**“. Es sollte ein Name sein, bei dem alle verstehen um was es geht.

Sobald die Standortdefinition abgeschlossen ist, kehrst du zur Richtlinie zurück und wählst unter „Netzwerk“ das passende Netzwerk also zum Beispiel die eben angelegte Standorteinstellung aus. Damit wird jeder Anmeldeversuch aus nicht freigegebenen Ländern automatisch unterbunden – außer natürlich von den explizit ausgenommenen Konten.

Zielressourcen ⓘ

Alle Ressourcen (früher „Alle Cloud-Apps“)

Netzwerk **NEU** ⓘ

1 eingeschlossen

Ausgewählte Netzwerke und Standorte

Auswählen

BlockLoginExceptGermany

Bild 76: Germany Except

Sobald die Netzwerkdefinition abgeschlossen ist, wählst du unter „**Zugriffskontrolle**“ die Aktion „**Blockzugriff**“. Damit wird jeder Anmeldeversuch aus nicht freigegebenen Ländern automatisch unterbunden – außer natürlich von den explizit ausgenommenen Konten. Im Anschluss klickst du nur noch auf Erstellen und deine erste Richtlinie ist eingefügt.

CA001-AllUser-AllRessources-ExceptAdmins&UA_Users-BlockLoginFromSpecificCountries

Bild 77: 1. Richtlinie

Ein Hinweis zur Sicherheit: Vergewissere dich, dass der aktuell angemeldete Benutzer (mit dem du arbeitest) nicht von der Blockregel betroffen ist, bevor du die Richtlinie aktivierst. Andernfalls könntest du dich versehentlich selbst aussperren. Daher empfiehlt es sich, die Richtlinie zunächst im Berichtmodus zu belassen.

Ein wichtiger technischer Aspekt, betrifft das Zusammenspiel zwischen Geräte-Registrierung, Gruppenrichtlinien (GPOs) und der Synchronisation mit Microsoft Entra ID. Wenn du in deiner Umgebung die automatische Registrierung von Geräten über den bekannten Dialog deaktivierst (etwa über eine Gruppenrichtlinie), dann können neue Geräte ohne zusätzliche Maßnahmen zunächst nicht mehr automatisch in Entra ID auftauchen, sofern du sie nicht auch in die Synchronisation aufnimmst. Diese Beobachtung wurde von Torsten korrekt angemerkt und von Aaron bestätigt.

Sobald du aber Geräte sowohl in den Sync aufnimmst als auch die GPO konfigurierst, wird der Hybrid-Join ermöglicht. Dabei unterscheidet Entra ID zwischen folgenden Join-Typen:

1. Microsoft Entra ID Join: Cloud-only Registrierung, typischerweise bei Intune oder Autopilot.
2. Microsoft Entra ID Registered: Geräte sind registriert, jedoch nicht domänengebunden – häufig bei BYOD oder manueller Anmeldung über Office-Produkte.
3. Hybrid Azure AD Join: Geräte sind sowohl lokal im AD als auch in Entra ID eingebunden – ideal für Unternehmensgeräte mit zentraler Verwaltung.

Der empfohlene Ablauf sieht vor, zunächst die GPO auszurollen und dann parallel die Gerätesynchronisation zu aktivieren. Beide Schritte sind notwendig, um den Hybrid-Join erfolgreich durchzuführen. Vorab sollte eine Gerätebereinigung durchgeführt werden, um redundante Objekte im Verzeichnis zu vermeiden. Denn: In der Praxis kommt es gelegentlich vor, dass ein und dasselbe Gerät mehrfach (z. B. als "Registered" und als "Hybrid Joined") in Entra ID erscheint – was unter anderem durch fehlerhafte oder überlappende Registrierungsprozesse entstehen kann.

Microsoft erkennt zwar theoretisch den Wechsel des Join-Typs und ersetzt den alten Eintrag, dies funktioniert jedoch **nicht immer zuverlässig**. Ein Gerät kann in Entra ID mehrmals auftauchen – auch mit identischem Namen, aber unterschiedlichen Join-Typen – ohne dass Microsoft diesen Zustand automatisch konsolidiert.

Die praktische Auswirkung, wenn der Registrierungsdialog deaktiviert und gleichzeitig keine Gerätesynchronisation aktiv ist: In diesem Fall kann sich ein User weiterhin ganz normal **an Office 365 oder Teams anmelden**, jedoch wird das Gerät **nicht** in Entra ID als Objekt registriert. Für den User ist das Verhalten auf dem Endgerät **nicht wahrnehmbar anders**. Erst auf Verwaltungsebene fehlen die Einträge, was insbesondere für Compliance, Gerätemanagement oder Conditional Access relevant ist.

Vor der Aktivierung der GPO sollte die Synchronisation mit Entra ID konfiguriert werden, um eine unterbrechungsfreie Verwaltung sicherzustellen. Die Reihenfolge dieser beiden Schritte (GPO vs. Sync) ist **nicht zwingend entscheidend**, solange am Ende beide Voraussetzungen erfüllt sind.

Technische Umsetzung: 2. Richtlinie Legacy Authentication

2. Richtlinien:

CA002–AllUsers–AllResources–ExceptBreakingGlassAccount–Block LegacyAuthentication

Nun wird eine 2. Richtlinie erstellt. Zunächst beginnst du, wie bei der vorherigen Richtlinie, mit dem Erstellen einer neuen Richtlinie über Entra ID → Bedingter Zugriff → Neue Richtlinie. Du kannst die Richtlinie kopieren, einfügen und gegebenenfalls anpassen.

Du wählst „Alle Benutzer“ aus und schließt anschließend die Administratorengruppe aus, sodass sie nicht von der Richtlinie betroffen ist. Als nächstes bestimmst du die betroffenen Ressourcen. Bei der Legacy Authentication unerheblich ist, ob der Zugriff z. B. über Outlook, SAP oder andere Dienste erfolgt – der Authentifizierungsmechanismus steht im Fokus, nicht der Dienst selbst.

Zuweisungen		Nicht konfiguriert	Bild 78: Bedingungen
Benutzer	Alle Benutzer eingeschlossen und bestimmte Benutzer ausgeschlossen	Client-Apps	Der entscheidende Schritt bei dieser Richtlinie liegt im Setzen der Bedingungen. Du öffnest dazu den Bereich „Bedingungen“ und klickst auf „Client-Apps“.
Zielressourcen	Alle Ressourcen (früher „Alle Cloud-Apps“)	Nach Geräten filtern	
Netzwerk	NEU Nicht konfiguriert	Authentifizierungsflows	
Bedingungen	0 Bedingungen ausgewählt		

Client-Apps

Steuern Sie den Benutzerzugriff für bestimmte Clientanwendungen, die keine moderne Authentifizierung verwenden.
[Weitere Informationen](#)

Konfigurieren ⓘ

Wählen Sie die Client-Apps aus, auf die diese Richtlinie angewendet wird.

Clients mit moderner Authentifizierung
 Browser
 Mobile Apps und Desktopclients

Legacy-Authentifizierungsclients
 Exchange ActiveSync-Clients
 Andere Clients ⓘ

Hier ist eine Unterteilung zu sehen. Einmal die **Clients mit moderner Authentifizierung und Legacy-Authentifizierungsclients**. Anschließend aktivierst du die Konfiguration und wählst dort gezielt nur die Legacy-Authentifizierungsprotokolle aus. Typische Legacy-Protokolle, die geblockt werden sollen, sind z. B. POP3, IMAP oder SMTP ohne OAuth – sie gelten heute als unsicher und unterstützen keine Multi-Faktor-Authentifizierung.

Bild 79: Client Apps

Du solltest dir bewusst darüber sein, ob solche Protokolle in eurer Umgebung überhaupt verwendet werden. Falls ja, könnten durch das Blockieren Funktionseinschränkungen auftreten. In solchen Fällen musst du ggf. gezielt mit Ausnahmen arbeiten.

Zum Schluss definierst du im Abschnitt „Zugriffskontrolle“, was passieren soll, wenn die zuvor gesetzten Bedingungen erfüllt sind. In diesem Fall lautet die Aktion: „Zugriff blockieren“. Damit ist sichergestellt, dass jede Authentifizierung über Legacy-Protokolle unterbunden wird – außer für Benutzer in der definierten Ausnahmegruppe.

Diese Richtlinie stellt sicher, dass sich alle Benutzer – ausgenommen eure definierten Admins – nicht mehr über unsichere Authentifizierungsprotokolle anmelden können. Das ist ein zentraler Sicherheitsmechanismus in modernen Microsoft-365-Tenants und sollte zu den grundlegenden Richtlinien in jeder Umgebung gehören.

Es gibt gegeben falls Einschränkungen durch die Lizenzierung – beispielsweise bei der Nutzung von Risiko-basierten Sign-In-Einstellungen, die nur mit einer E5-Lizenz verfügbar sind.

CA002-AllUser-AllRessources-ExceptAdmins-BlockLegacyAuthentication

Bild 80: 2. Richtlinie

Technische Umsetzung: 3. Richtlinie Unsupported Devices

3. Richtlinien:

CA003-AllUsers-AllResources-ExceptBreakingGlassAccount-BlockUnsupportedDevice

Die nächste Conditional-Access-Richtlinie ist die: „**CA003 – Block Unsupported Device**“. Ziel dieser Richtlinie ist es, den Zugriff auf Microsoft-365-Ressourcen von nicht unterstützten Plattformen aus zu blockieren. Auch hier gilt: Alle Benutzer sind von der Richtlinie betroffen – mit Ausnahme der Administratorengruppe.

Geräteplattformen ⓘ	
Nicht konfiguriert	
Standorte ⓘ	
Nicht konfiguriert	
Client-Apps ⓘ	
Nicht konfiguriert	
Nach Geräten filtern ⓘ	
Nicht konfiguriert	
Authentifizierungsflows ⓘ	
Nicht konfiguriert	

Die Konfiguration beginnt mit der bekannten Basis: **alle Benutzer, außer Admins**. Bei den Anwendungen werden erneut alle Ressourcen ausgewählt. In diesem Fall wird über die **Geräteplattformen** weitergearbeitet

Bild 81: Geräteliste

Geräteplattformen

Wenden Sie die Richtlinie auf ausgewählte Gerätelisten an.

[Weitere Informationen ⓘ](#)

Konfigurieren ⓘ

Einschließen Ausschließen

- Jedes Gerät
- Gerätelisten auswählen
 - Android
 - iOS
 - Windows Phone
 - Windows
 - macOS
 - Linux

Bild 82: Auswahl Geräteliste

Diese Richtlinie ist vor allem dann relevant, wenn bestimmte Plattformen – etwa **Windows Phone**, **MacOS** oder **Linux** – im Unternehmen **nicht offiziell eingesetzt oder verwaltet** werden. In solchen Fällen sollte der Zugriff von diesen Geräten aus unterbunden werden, um die Angriffsfläche zu minimieren.

Besonders wichtig: In Unternehmen ohne Intune-Integration **kann nicht über Konformitätsregeln** gearbeitet werden. Das bedeutet: Es ist **nicht möglich**, beispielsweise bei iOS-Geräten sicherzustellen, dass nur gemanagte oder aktuelle Versionen Zugriff haben. Entsprechend bleibt nur die pauschale Entscheidung **für oder gegen eine Plattform**.

Eine Entscheidung über iOS hängt auch mit der internen BYOD-Strategie zusammen: Wenn **keine Firmen-iPhones** vergeben werden, könnten iOS-Zugriffe theoretisch blockiert werden. Bedenke jedoch, dass z. B. über Webmail häufig auch private Mobilgeräte auf Unternehmensdaten zugreifen, sodass eine Einschränkung pragmatisch überlegt sein sollte.

Hinweis: Auf unterstützten Plattformen kann **dann eine Zugriffskontrolle auf Basis der Gerätekonformität** sinnvoll sein – also z. B. „Nur wenn das Gerät im Intune verwaltet wird“. Statt **auszuschließen**, müssen die **nicht erlaubten Plattformen (z. B. Windows Phone, MacOS, Linux)** unter „**Einschließen**“ ausgewählt werden. Denn: Nur die Geräte, die explizit **eingeschlossen sind**, werden in die Bedingung einbezogen – und somit vom späteren **Block-Zugriff** auch wirklich erfasst.

Abschließend wird die **Zugriffskontrolle gesetzt**: „**Blockzugriff**“ für alle Anfragen, die von den definierten, nicht unterstützten Plattformen stammen. Die Ausführung der Richtlinie erfolgt **nicht sofort produktiv**, sondern zunächst im „**Bericht**“-Modus, um mögliche Seiteneffekte zu erkennen und rechtzeitig zu korrigieren.

Ein wichtiger Aspekt für die Validierung und spätere produktive Umsetzung ist das Testen der Richtlinien.

[CA003-AllUser-AllRessources-ExceptAdmins-BlockUnsupportedDevices](#)

Bild 83: 3. Richtlinie

Technische Umsetzung: 4. Richtlinie Device Code Flow

4. Richtlinien:

[CA004-AllUsers-AllResources-ExceptBreakingGlassAccount-BlockDeviceCodeFlow](#)

Nun kommt die nächste wichtige Conditional-Access-Richtlinie, die aus zwei Komponenten besteht: Der Blockierung des sogenannten **Device Code Flows** und der Konfiguration einer **verkürzten Session-Lifetime**, also einer regelmäßigen Reauthentifizierung.

Wie bei den vorherigen Richtlinien gilt auch hier der Standardaufbau:

Alle Benutzer sind betroffen,
alle Ressourcen werden berücksichtigt,
Administratoren sind explizit ausgenommen.

Der **Device Code Flow** ist eine moderne Authentifizierungsmethode von Microsoft, die standardmäßig aktiviert ist. Dieser Flow ermöglicht es, Geräte **ohne grafische Oberfläche**, über die Kommandozeilen in das Entra ID zu bringen.

Solche Gerätearten sind in der Regel in klassischen Unternehmensumgebungen **nicht im produktiven Einsatz**. Daher empfiehlt es sich, den Device Code Flow **grundsätzlich zu blockieren**, es sei denn, ein konkreter Anwendungsfall – wie etwa die Einbindung eines Konferenztelefons – macht ihn erforderlich. Auch aus **Phishing-Sicht** ist diese Maßnahme empfehlenswert, da missbräuchliche Token über diesen Weg einfacher erzeugt werden könnten.

Zielressourcen ⓘ	Nach Geräten filtern ⓘ
Alle Ressourcen (früher „Alle Cloud-Apps“)	Nicht konfiguriert
Netzwerk NEU ⓘ	Authentifizierungsflows ⓘ
Nicht konfiguriert	Nicht konfiguriert
Bedingungen ⓘ	
0 Bedingungen ausgewählt	

Bild 84: Authentifizierungsflows

Authentifizierungs... ×

Steuern Sie, wie Ihre Organisation bestimmte Authentifizierungs- und Autorisierungsprotokolle und -zuweisungen verwendet. [Weitere Informationen](#)

Konfigurieren ⓘ

Ja

Übertragungsmethoden

- Gerätancodeflow
- Authentifizierungsübertragung

Der Device Code Flow wird in den **Bedingungen** aktiviert und die Option „**Blockzugriff**“ in den **Zugriffskontrollen** ausgewählt.

Bild 85: Übertragungsmethode

Besondere Aufmerksamkeit erhält an dieser Stelle Geräte wie z. B. **Konferenztelefonen**, **Besprechungsraum-Endgeräten**, **Smart-TV's** oder **Teams-Telefonie-Geräten**. Wenn diese eine URL über die Kommandozeile abrufen können, zählen diese Geräte ebenfalls in die Richtlinie mit rein.

CA004-AllUser-AllRessources-ExceptAdmins-BlockDeviceCodeFlow

Bild 86: 4. Richtlinie

Technische Umsetzung: 5. Richtlinie Session Lifetime

5. Richtlinien:

CA005—AllUsers—AllResources—ExceptBreakingGlassAccount&DeviceAccounts—IncludeWindows_MacOS—SessionLifeTimeLimit7Days

Auch bei dieser Richtlinie erfolgt der Einstieg wie gewohnt: Sie betrifft **alle Benutzer, alle Ressourcen**, mit Ausnahme der **Administratoren**.

Device Accounts ist ein wichtiger Punkt zu Beginn dieser Richtlinie: Solltest du beispielsweise Geräte oder sogenannte **Service-Konten** im Einsatz haben – wie es etwa bei Konferenzräumen mit **Fernsehern** oder **Konferenztelefonen** der Fall ist – bei denen ein **Benutzer dauerhaft hinterlegt** ist, müssen diese idealerweise **ausgenommen** werden. Denn: Wenn sich jemand über ein solches Gerät anmeldet, wird im Hintergrund eine sogenannte **Session ID** – ein Authentifizierungs-Cookie – erzeugt. Diese Session ID ist bis zu **90 Tage gültig**.

Wird diese ID kompromittiert, hätte ein Angreifer potenziell drei Monate Zeit, sich mit genau dieser Information Zugriff zu verschaffen. Daher lautet die Empfehlung: Die Lebensdauer dieser Sitzung auf **deutlich weniger Tage zu reduzieren**, in der Regel auf **5 bis 14 Tage**. **Sieben Tage** ist hier ein guter Mittelwert. Das bedeutet: Nach dieser Zeit muss ein Benutzer sich **erneut authentifizieren**, etwa in **Word, Excel, PowerPoint, Outlook** oder über **office.com**.

Für reguläre Benutzer ist das problemlos umsetzbar. Für **Service-Konten**, etwa an **Konferenztelefonen, Empfangsarbeitsplätzen** oder vergleichbaren Szenarien, ist das hingegen **unpraktisch**, da dort ein manueller Re-Login organisatorisch schwierig wäre. Solche Konten solltest du daher **explizit ausschließen**.

Die Umsetzung erfolgt über die **Zugriffskontrollen**, genauer gesagt über den Bereich „**Sitzung**“. Hier wird die Option „**Anmeldehäufigkeit**“ aktiviert und auf **7 Tage** eingestellt. Dadurch werden Benutzer in Word, Excel, PowerPoint, Outlook, Office.com usw. spätestens nach einer Woche erneut zur Anmeldung aufgefordert.

Um die Geräte von der **Teams-Telefonie** nicht auszuschließen, musst du eine Gruppe dafür erstellen. Diese Gruppe wird in der Richtlinie **ausgeschlossen**. Die Geräte müssen dafür weder im Intune noch im Entra ID vorhanden sein. Der reine Login auf Basis der Benutzeridentität reicht dafür bereits aus.

Du kannst auch eine **dynamische Gerätegruppen** erstellen. Diese Funktion erfordert eine **Entra ID P1 Lizenz**.



Bild 87: Geräteplattform Auswahl

Als Plattform für die Richtlinie wird zunächst **Windows** eingeschlossen, da diese Systeme im Unternehmen genutzt werden. Eine Frage ergibt sich um **Android- und iOS-Geräte**. Es wird empfohlen, diese **nicht** einzuschließen, um zu vermeiden, dass reguläre Benutzer auf Smartphones zu häufig zur Reauthentifizierung gezwungen werden.

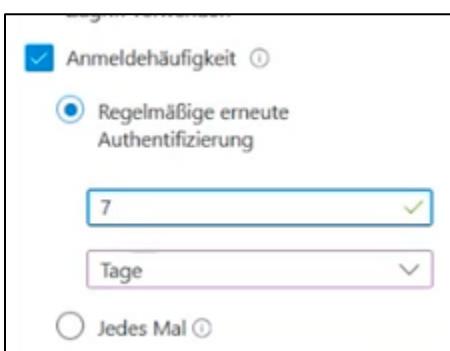
Sitzung

Steuern Sie den Zugriff basierend auf Sitzungssteuerelementen, um in bestimmten Cloudanwendungen eine eingeschränkte Funktionalität zu ermöglichen.

[Weitere Informationen ⓘ](#)

- Von der App erzwungene Einschränkungen verwenden ⓘ
- ⓘ Dieses Steuerelement kann nur mit unterstützten Apps eingesetzt werden. Aktuell sind Office 365, Exchange Online und SharePoint Online die einzigen Cloud-Apps, die von einer App erzwungene Einschränkungen unterstützen.
[Weitere Informationen ⓘ](#)
- App-Steuerung für bedingten Zugriff verwenden ⓘ
- Anmeldehäufigkeit ⓘ
- Beständige Browsersitzung ⓘ
- Fortlaufende Zugriffsevaluierung anpassen ⓘ
- Standardwerte für Resilienz deaktivieren ⓘ
- Sicherheitsprofil für globalen sicheren Zugriff verwenden ⓘ

Bild 88: Sitzung



The screenshot shows the 'Anmeldehäufigkeit' (Login Frequency) configuration. It includes a checked checkbox for 'Anmeldehäufigkeit' (Login Frequency), a selected radio button for 'Regelmäßige erneute Authentifizierung' (Regular re-authentication), a dropdown menu showing '7 Tage' (7 days) with a checkmark, and an unselected radio button for 'Jedes Mal' (Every time).

In den **Zugriffskontrollen** wird nicht auf „Zugriff gewähren“ gesetzt, sondern auf „**Sitzung**“. Dort aktivierst du die „**Anmeldehäufigkeit**“ und legst fest, dass sich Benutzer alle **sieben Tage neu authentifizieren** müssen. Der Standardwert bei Microsoft liegt bei **90 Tagen** – durch diese Richtlinie wird er auf ein **sicherheitsoptimiertes Maß reduziert**.

Bild 89: Anmeldehäufigkeit

Dies erfordert, dass User sich alle x Tage neu bei Microsoft authentifizieren, dass dieser Token sich nach x Tagen erneuert.

Der **Defaultwert von Microsoft** liegt bei 90 Tagen – mit dieser Richtlinie wird er für alle nicht ausgenommenen Benutzer aktiv auf **x Tage** runterreduziert.

CA005-AllUser-AllRessources-ExceptAdmins&DeviceAccounts-IncludeWindo...

Bild 90: 5. Richtlinie

Technische Umsetzung: 6. Richtlinie Require MFA Member

6. Richtlinien:

CA006-AllUsers-AllResources-ExceptBreakingGlassAccount-RequireMFAForMembers

Wie immer beginnt auch diese Richtlinie mit dem gewohnten Einstieg: **Alle Benutzer, alle Ressourcen – ausgenommen die Administratoren.**

Die Richtlinie „**CA006 – Require MFA for Members**“ verfolgt das Ziel, für **alle Standardbenutzer eine Multifaktor-Authentifizierung (MFA)** zu erzwingen. Das erhöht das Sicherheitsniveau im Tenant erheblich, denn die Kombination von Benutzername und Passwort allein gilt längst nicht mehr als ausreichend.

Du gehst in die **Zugriffskontrollen**, dann auf den Punkt „**Gewähren**“ und aktivierst dort die Option „**Multi-Faktor-Authentifizierung erfordern**“.

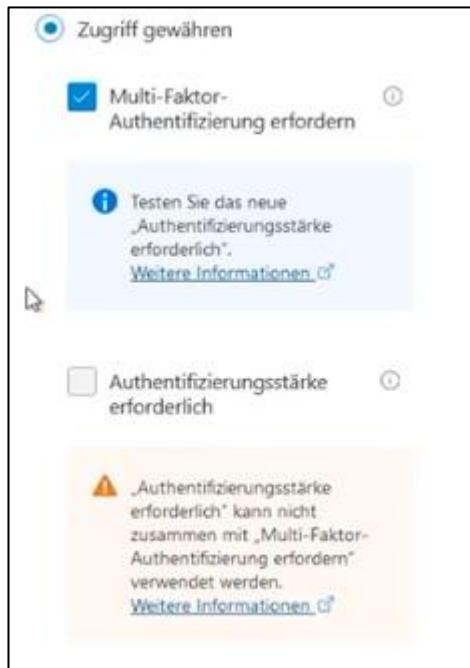


Bild 91: MFA

Jetzt triffst du die Entscheidung: Statt lediglich einen **beliebigen zweiten Faktor** zu erlauben (was auch **SMS** oder **Telefonanrufe** umfasst), wählst du gezielt eine stärkere Methode aus. Denn obwohl diese einfachen Faktoren immerhin rund **91 % aller Credential-Angriffe verhindern**, gelten sie heute als **nicht mehr ausreichend sicher**.

Besonders empfohlen wird der Einsatz **kennwortloser MFA-Verfahren** wie:

Number Matching über die Authenticator-App
Token-basierte Methoden
Zertifikatsbasierte Authentifizierung

Dadurch wird ausgeschlossen, dass sich Benutzer mit **unsicheren Methoden wie SMS oder Telefonanruf anmelden** können – und genau dasstellst du mit dieser Richtlinie sicher.

Abschließend klickst du auf „**Erstellen**“, um die Richtlinie zu aktivieren. Damit ist ein weiterer wesentlicher Baustein für die Absicherung deiner Entra-Umgebung umgesetzt.

CA006-AllUser-AllRessources-ExceptAdmins-RequireMFAForMembers

Bild 92: 6. Richtlinie

Technische Umsetzung: 7. Richtlinie Require MFA Device

7. Richtlinien:

CA007–AllUsers–ExceptBreakingGlassAccount– RegisterOrJoinDevice -RequireMFAForDeviceRegistration

Wie gewohnt beginnt auch diese Richtlinie mit dem Grundgerüst: **Alle Benutzer**, mit der Ausnahme der **Administratoren**.

Mit der siebten Richtlinie – **CA007** – wird ein besonders sicherheitskritischer Punkt adressiert: **die Registrierung oder das Einbinden von Geräten** in die Microsoft Entra ID. Ziel ist es, die Geräteeinbindung zusätzlich mit **Multi-Faktor-Authentifizierung (MFA)** abzusichern.

Es wird darauf hingewiesen, dass es sich um eine **Benutzeraktion** handelt, nicht um den Zugriff auf eine klassische Zielressource wie eine Anwendung oder ein Dienst.

1. Du wählst im Bereich „**Zielressourcen**“ den Menüpunkt „**Benutzeraktionen**“ aus.
2. Dort setzt du den Haken bei „**Gerät registrieren oder einbinden**“.
3. Der Hinweis erscheint: „In Richtlinien, die für die Benutzeraktion „Geräte registrieren oder einbinden“ erstellt wurden, kann nur „Multi-Faktor-Authentifizierung erfordern“ festgelegt werden.“

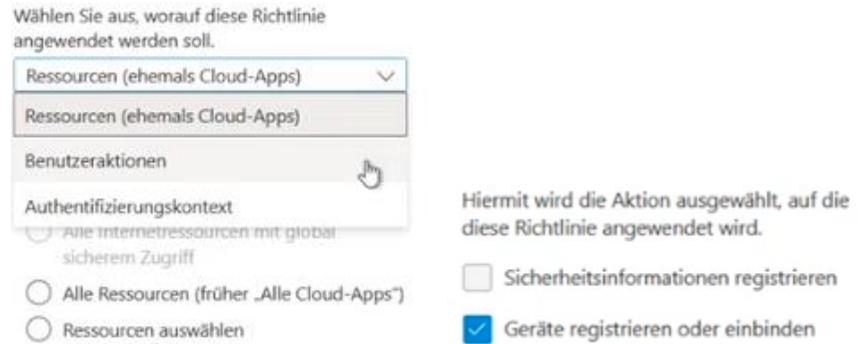


Bild 93: Benutzeraktionen

Das ist genau das, was du machen willst – also geht es weiter mit dem nächsten Schritt.

4. Du klickst auf „**Zugriffskontrollen**“ und gehst dort auf „**Gewähren**“.
5. Hier wählst du aus, dass **MFA erforderlich** ist.

CA007–AllUser–ExceptAdmins–RegisterOrJoinDevice–RequireMFAForDeviceR...

Bild 94: 7. Richtlinie

Überprüfung von Richtlinien mit „What-If“ und Anmeldeprotokollen

Nun stellt sich die Frage: **Wie kannst du überprüfen, wann und wie diese Richtlinien greifen?**

Zunächst gehst du in den Bereich der **bedingten Zugriffsrichtlinien**. Oben im Menü findest du neben „Neue Richtlinie“, „Richtlinie aus Vorlage“ und „Richtliniendatei hochladen“ auch die Option „**What If**“ – und genau dort klickst du drauf.



Bild 95: What if

1. **Wähle einen beliebigen Benutzer** aus deinem Tenant aus.
2. Unter **Cloud-Apps** wählst du z. B. „Office 365“.
3. Du kannst zusätzlich Bedingungen wie Standort oder Plattform definieren, aber das ist optional.
4. Klicke unten auf den blauen Button „**What If**“.

Nach kurzer Ladezeit erscheint eine Übersicht, in der du klar sehen kannst:

- **Welche Richtlinien angewendet werden würden**, und
- **welche nicht angewendet würden** – mit Begründung.

Anzuwendende Richtlinien	Nicht anzuwendende Richtlinien
<input type="button" value="Suche"/>	
Richtliniename ↑	Steurelemente zur Rechteerteilung ↑↓
CA001-AllUser-AllResources-ExceptIBL-Admins-Blnckl nonFromSpecificCountries	Zugriff blockieren
CA002-AllUser-AllResources-ExceptAdmins-BlockLegacyAuthentication	Zugriff blockieren
CA003-AllUser-AllResources-ExceptAdmins-Blnckl InsunsupportedDevices	Zugriff blockieren
CA004-AllUser-AllResources-ExceptAdmins-BlockDeviceCodeFlow	Zugriff blockieren
CA005-AllUser-AllResources-ExceptAdmins-FxceptAdmins&DeviceAccounts-IncludeWindows	
CA006-AllUser-AllResources-ExceptAdmins-RequireMFAForMembers	Authentifizierungsstärke - Passwordless MFA

Bild 96: Angewandte Richtlinien

Ein Beispiel: Die Richtlinie „**CA007 – Require MFA for Device Registration**“ wird nicht angewendet, wenn der Benutzer lediglich eine App nutzt, da es sich **nicht um eine Geräteeinbindung**, sondern um einen Applikationszugriff handelt. Solche Informationen helfen dir, deine Richtlinien präziser zu verstehen und Fehlerquellen frühzeitig zu identifizieren.

Ein zweiter Weg zur Analyse führt über die **SignIn Logs**.

1. Navigiere im linken Menü zu **Benutzer**.
2. Entweder wählst du einen **konkreten Benutzer** oder du gehst auf „**Alle Benutzer**“.

3. Dann klickst du auf „Anmeldeprotokolle“.
4. Wähle dort eine beliebige Anmeldung aus.
5. Klicke auf die **drei Punkte** (Kontextmenü) rechts neben dem Eintrag.
6. Wähle „Nur Bericht“.

Aktivitätsdetails: Anmeldungen

Grundlegende Infos	Standort	Geräteinformationen	Details zur Authentifizierung	Bedingter Zugriff	...
Datum	20.5.2025, 10:49:45			Grundlegende Infos	
Anforderungs-ID	77abbcad-2be2-48fd-ac85-85cb48012700			Standort	
Korrelations-ID	5ec788a5-9faf-4b80-acc3-fc8232cb6144			Geräteinformationen	
Authentifizierungsanforderung	Multi-Faktor-Authentifizierung			Details zur Authentifizierung	
Status	Erfolg			Bedingter Zugriff	
Fortlaufende Zugriffsevaluierung	Nein			Nur Bericht	
Zusätzliche Details	MFA requirement satisfied by claim in the token			Authentifizierungsergebnisse	
				Zusätzliche Details	

Bild 97: Aktivitätsdetails

An dieser Stelle wird dir angezeigt, **welche Richtlinien bei dieser Anmeldung gegriffen hätten** – und welche nicht. Bedenke: Es kann eine Weile dauern, bis die Richtlinien in den Logs sichtbar werden.

Diese beiden Methoden – „What If“ und die Anmeldeprotokolle – bieten dir zwei solide Werkzeuge, um deine Richtlinien im Betrieb **effektiv zu testen und zu überwachen**.

Kapitel 26: Hybrid Azure AD Join & MFA bei Geräteregistrierung

Zu Beginn solltest du verstehen, wann eine MFA-Anforderung beim Geräteeintritt sinnvoll ist. In der Praxis geht es hierbei um zwei Szenarien:

1. **Manuelle Registrierung von Geräten**, beispielsweise durch Benutzer im Rahmen von Bring Your Own Device (BYOD), wenn die Registrierung über die Registry Keys (noch) nicht deaktiviert wurde.
2. **Nicht über die Hybrid-Synchronisation eingebundene Geräte**, die z. B. direkt über die Systemeinstellungen mit der Cloud verbunden werden.

In beiden Fällen greift eine Conditional Access Richtlinie, die MFA verlangt. So wird sichergestellt, dass eine zusätzliche Sicherheitsprüfung erfolgt, selbst wenn sich ein Benutzer versehentlich oder absichtlich mit einem privaten Gerät anmeldet. Zwar lässt sich das Verhalten technisch nicht vollständig unterbinden, doch durch MFA wird die Sicherheit erheblich gesteigert und gleichzeitig Awareness beim Benutzer geschaffen.

Wenn deine Umgebung auf **Hybrid Azure AD Join** setzt, greift diese MFA-Richtlinie *nicht*, da die Join-Prozesse über die Synchronisation abgesichert und automatisiert ablaufen.

Vorbereitung für Hybrid Azure AD Join

Die technische Umsetzung eines Hybrid Joins erfordert mehrere vorbereitende Schritte:

1. OU-Auswahl in Entra ID Connect (früher Azure AD Connect)

Stelle sicher, dass die gewünschten Computer-Organizational Units (OUs) für die Synchronisation aktiviert sind. Nur so gelangen Geräte aus der lokalen AD in die Entra ID.

2. Geräteoptionen konfigurieren

Starte die Entra ID Connect-Konfiguration und wähle die Option „Geräteoptionen konfigurieren“ aus. Melde dich mit einem administrativen Konto an.

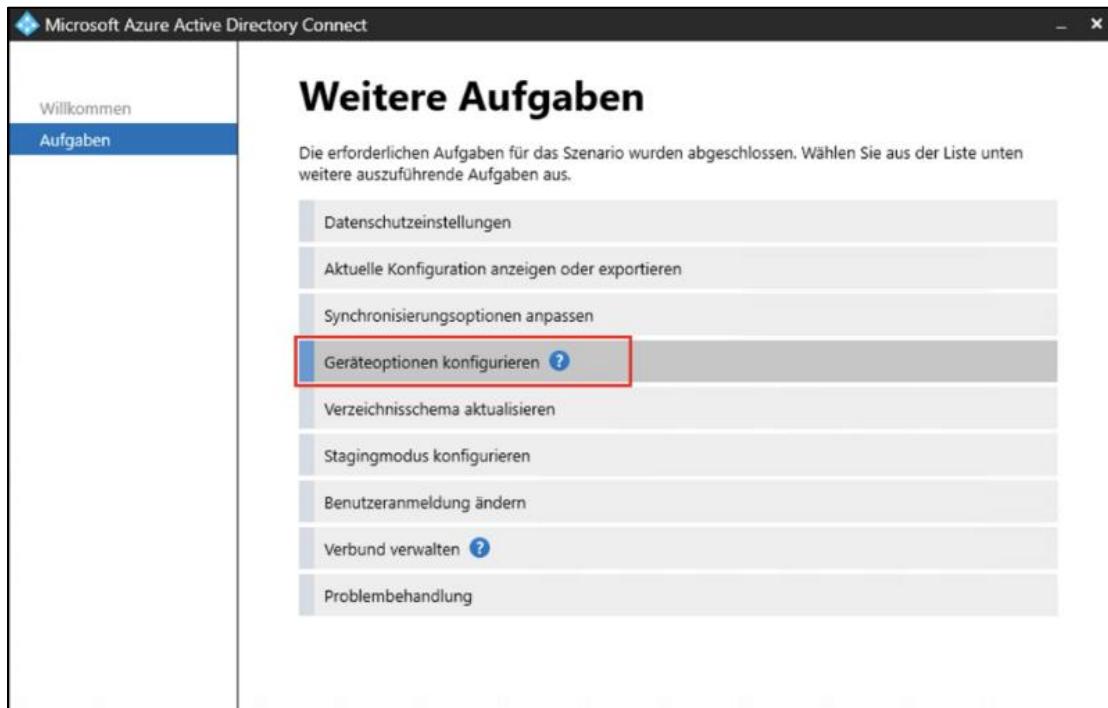


Bild 98: Geräteoptionen

3. Hybrid Azure AD Join aktivieren

Im nächsten Schritt aktivierst du die Option „*Hybrid Azure AD Join für Windows 10 oder höher*“. Setze das Häkchen im Forest-Bereich und hinterlege ein Unternehmenskonto mit administrativen Rechten.

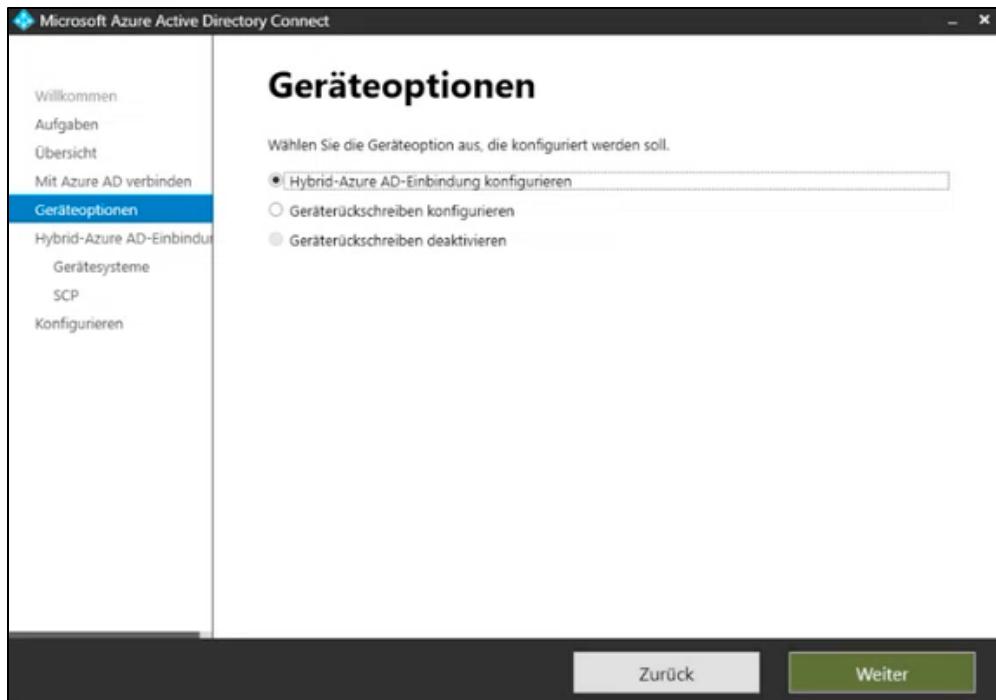


Bild 99: Hybrid Azure AD Einbindung

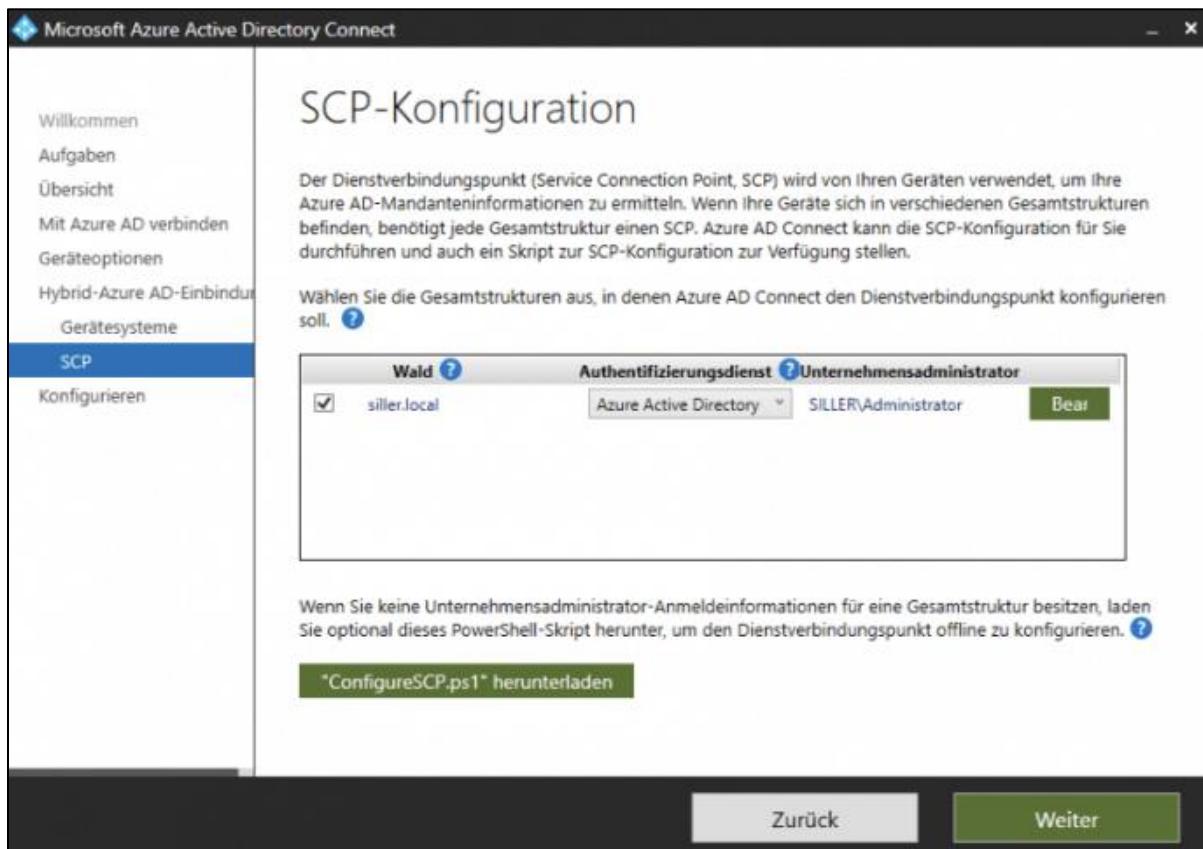


Bild 100: SCP-Konfiguration

Richtlinie: Gruppenrichtlinie zur automatischen MDM-Registrierung (MDM-Join)

Nachdem du die Konfiguration der Hybrid Azure AD Join-Funktion abgeschlossen hast, stellt sich häufig die Frage, ob Geräte zusätzlich auch automatisch bei Microsoft Intune registriert werden sollen. Diese Registrierung kann durch eine Gruppenrichtlinie ausgelöst werden, die speziell für diesen Zweck erstellt wird.

Voraussetzungen

- Die Grundkonfiguration von **Hybrid Azure AD Join** muss abgeschlossen sein.
- Die betroffenen Geräte müssen sich in einer synchronisierten **Organisationseinheit (OU)** befinden.
- Die Umgebung ist nicht zwingend Intune-vorkonfiguriert – eine Registrierung löst keine Konfiguration aus, solange keine Richtlinien im Intune bereitstehen.

Schritt-für-Schritt-Anleitung zur Erstellung der MDM-Join-GPO

1. Lokale Gruppenrichtlinie öffnen

Öffne die Gruppenrichtlinienverwaltung.

2. Neue GPO erstellen

Erstelle eine neue Gruppenrichtlinie und gib ihr einen sinnvollen Namen – z. B. MDM-Join.

3. Richtlinie bearbeiten

Klicke auf die Gruppe und wähle bearbeiten aus. Anschließend klickst du auf **Computerkonfiguration → Richtlinien → Administrative Vorlagen → Windowskomponenten → MDM**

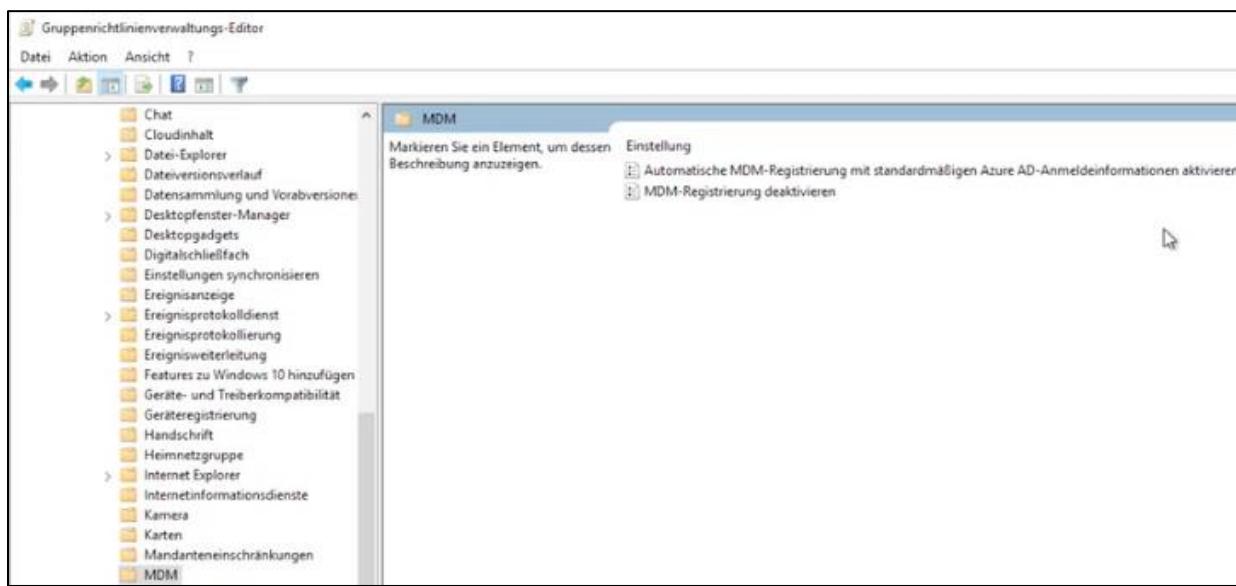


Bild 101: Gruppeneinrichtung

4. MDM-Auto-Registrierung aktivieren

Aktiviere die Richtlinie:

„Automatische MDM-Registrierung mit standardmäßiger Azure AD-Anmeldung aktivieren“

Diese Einstellung sorgt dafür, dass Geräte, die sich hybrid bei Azure AD anmelden, auch direkt für Intune registriert werden – ohne Benutzerinteraktion.

5. Synchronisation der OU sicherstellen

Stelle sicher, dass die OU, in der sich die betroffenen Geräte befinden, per **Azure AD Connect** mit Azure synchronisiert wird.

6. Optionale Validierung am Clientgerät

Um zu prüfen, ob die Registrierung erfolgt ist, führe auf dem Gerät folgenden Befehl aus:

dsregcmd /join

Hier kannst du unter anderem lokal auf dem Gerät sehen, ob das Gerät bereits **gejoined** ist.

Hier entscheidet es sich auch, ob die Geräte auch direkt in Intune aufgenommen werden sollen oder nicht.

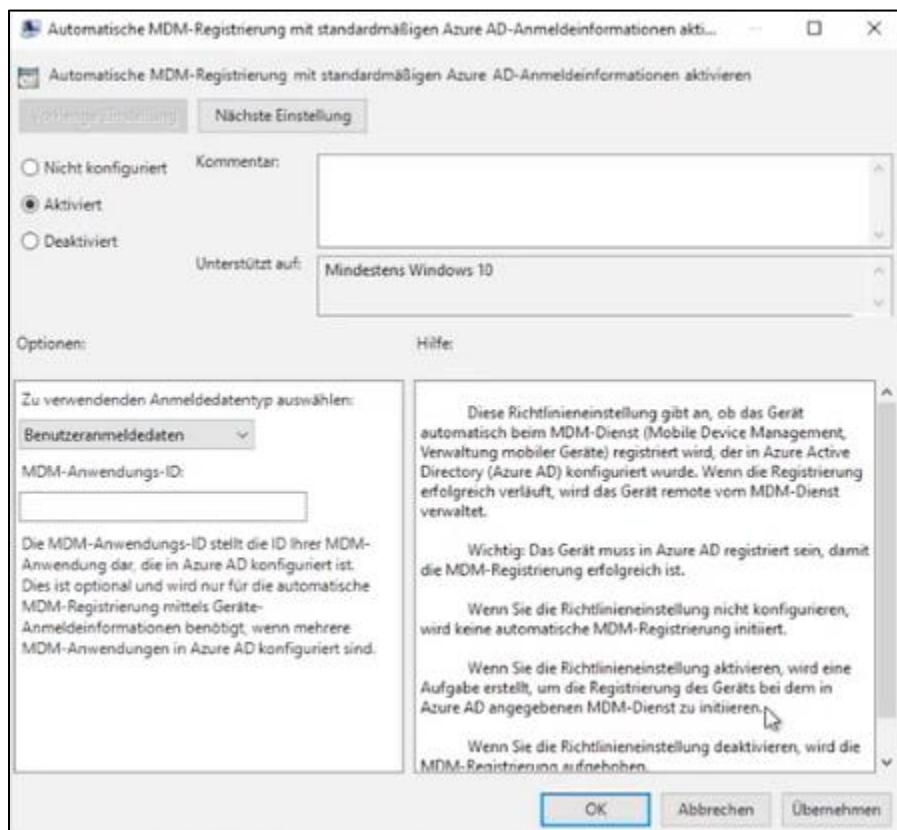


Bild 102: MDM Registrierung

Weitere Hinweise und Best Practices

- **Testgruppe verwenden:**

Es wird empfohlen, die neue Richtlinie zunächst nur auf eine kleine **Testgruppe von Geräten** anzuwenden. Legt hierfür z. B. eine Sicherheitsgruppe an.

- **Hinweis für Benutzer:**

Sobald die GPO greift, erhalten betroffene Nutzer ein Hinweisfenster in der Windows-Taskleiste:

„Wir registrieren Ihr Gerät im Intune“

- **Keine automatische Konfiguration:**

Standardmäßig werden bei der Intune-Registrierung **keine Konfigurationsrichtlinien angewendet**, sofern in Intune nichts definiert ist. Es erfolgt lediglich die Aufnahme in die Verwaltung.

- **Hinweis zur Authentifizierungsmethode:**

Für eine erfolgreiche Registrierung ist es erforderlich, die Authentifizierungsmethode auf **Benutzerobernahmedaten** umzustellen, falls das Gerät auch ins Intune übernommen werden soll. Es wird keine zusätzliche Anwendungs-ID mehr benötigt – diese wird inzwischen automatisch bezogen. Wichtig ist lediglich, dass der Benutzer, der sich am Gerät anmeldet, eine entsprechende Lizenz für Microsoft Intune besitzt und für den Dienst freigeschaltet ist. Das Gerät wird beim Join unter dem Namen dieses Benutzers in Intune registriert.

Erste Tests und Join-Vorgang

Du kannst im Intune sehen, ob das Gerät aufgenommen wurde oder ein Fehler vorliegt. Gehe hierfür in das **Microsoft Intune Admin Center** → **Geräte** → **Geräte verwalten** → **Konfiguration**. Ist hier nichts zu sehen wird nichts angewendet. Um zu sehen, ob die automatische Registrierung aktiv ist, klickst du dafür unter **Geräte-Onboarding** auf **Registrierung** → **Automatische Registrierung**.

Microsoft Intune

MDM Benutzerbereich ⓘ

Keine Einige Alle

MDM URL der Nutzungsbedingungen ⓘ

`https://portal.manage.microsoft.com/TermsofUse.aspx`

MDM Ermittlungs-URL ⓘ

`https://enrollment.manage.microsoft.com/enrollmentserver/discovery.svc`

URL für MDM-Konformität ⓘ

`https://portal.manage.microsoft.com/?portalAction=Compliance`

[Standard MDM URLs wiederherstellen](#)

Windows Information Protection (WIP) Benutzerbereich ⓘ

Keine Einige Alle

WIP URL der Nutzungsbedingungen ⓘ

`https://wip.mam.manage.microsoft.com/Enroll`

WIP Ermittlungs-URL ⓘ

`https://wip.mam.manage.microsoft.com/Enroll`

URL für WIP-Konformität ⓘ

`https://wip.mam.manage.microsoft.com/Enroll`

Bild 103: Geräte Aktivierung

Join manuell testen:

1. Melde dich als lizenzierte Benutzer am Testgerät an.
2. Öffne eine administrative Eingabeaufforderung (CMD).
3. Führe den Befehl `dsregcmd /join` aus.
4. Alternativ kannst du auch `dsregcmd /status` verwenden, um den Status der Registrierung einzusehen.

Hinweis: Der Join-Prozess kann sich bei manchen Geräten über mehrere Tage hinziehen. Grund dafür ist die Token-Authentifizierung, die erst nach Ablauf bestimmter Zeiträume vollständig durchgeführt wird.

Überwachung des Join-Prozesses

Zur Überprüfung, ob das Gerät korrekt registriert wurde, kannst du mehrere Wege nutzen:

- **CMD:** `dsregcmd /status` ausführen

- Achte auf die Werte DomainJoined: YES
AzureAdJoined: YES.
- Ist das der Fall ist das Gerät local und in der Cloud vorhanden und mit dem Konto miteinander verknüpft.
- Hier wird eine ganze Liste mit URL's angezeigt, die zur Verbindung benötigt werden.

```
C:\>dsregcmd /status
```

Bild 104: Shell Befehl

- Ereignisanzeige öffnen:
 - Navigiere zu: Anwendungs- und Dienstprotokolle > Microsoft > Windows > DeviceManagement-Enterprise-Diagnostics-Provider
 - Hier werden nach einiger Zeit Einträge zum Join-Prozess angezeigt.
- Intune Admin Center:
 - Gehe zu Geräte > Registrierungen > Automatische Registrierung, um zu sehen, ob Intune den Prozess erkannt hat.

Vorbereitung der OU-Synchronisation

Falls noch nicht geschehen, müssen auch die relevanten Computer-OUs in die Synchronisation mit Entra ID Connect aufgenommen werden:

1. Öffne den **Entra ID Connect Konfigurations-Assistenten**.
2. Wähle den Punkt **Synchronisierungsoptionen anpassen**.

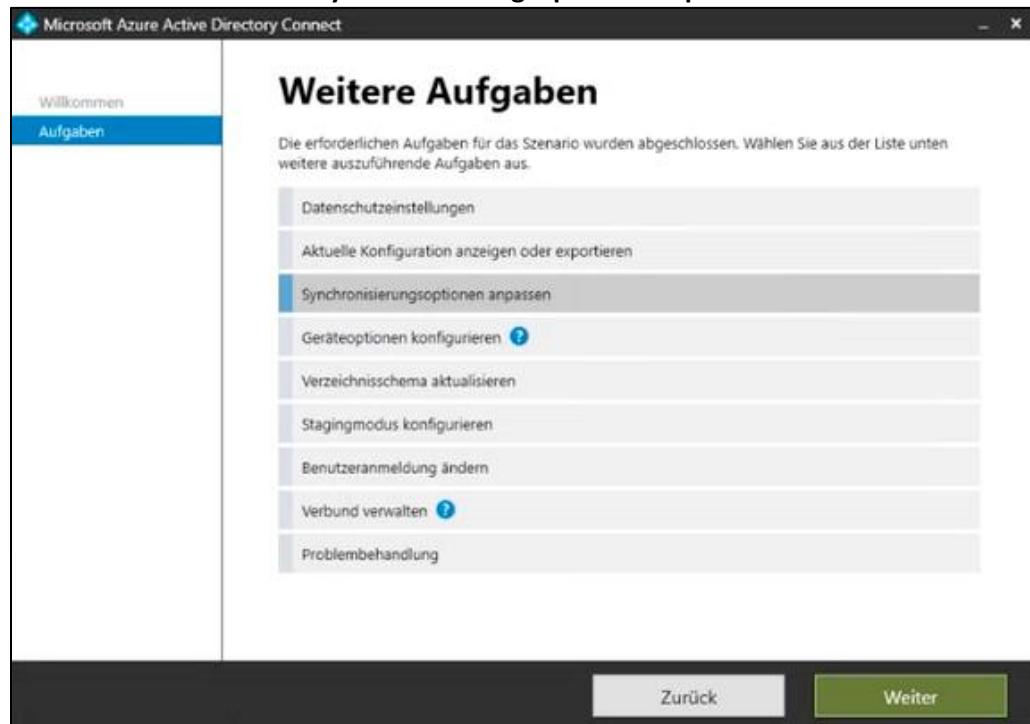


Bild 105: Synchronisierungsoptionen

3. Nimm dort alle OUs auf, die relevante Clientgeräte beinhalten (z. B. auch virtuelle Desktops, falls notwendig).

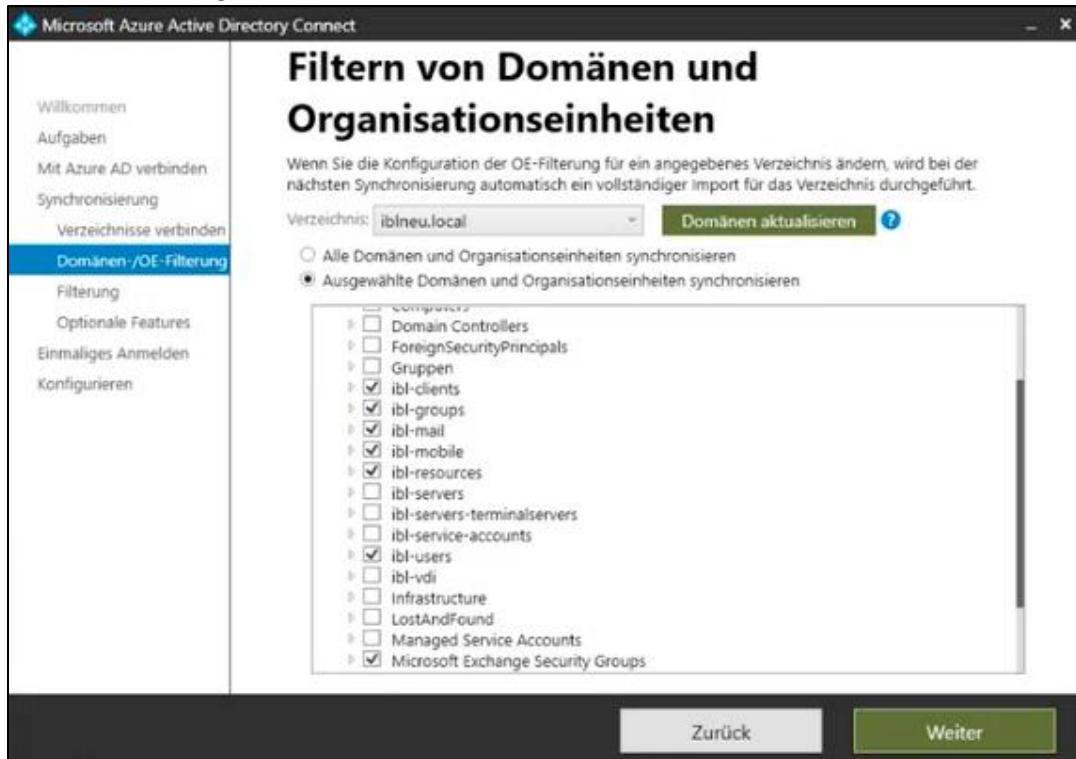


Bild 106: OU Filterung

4. Stelle sicher, dass alle Testgeräte zusätzlich in die Office 365-Gruppe aufgenommen wurden.
Wenn du die Ereignisanzeige öffnest, kannst du unter **Andwenungs- und Dienstprotokolle** → **Microsoft** → **Windows** → **DeviceManagement-Enterprise-Diagnostics-Provider** sehen ob bereits etwas im Ordner vorhanden ist. Ein zweiter Ordner erscheint hier auch noch, der für das Join ist.

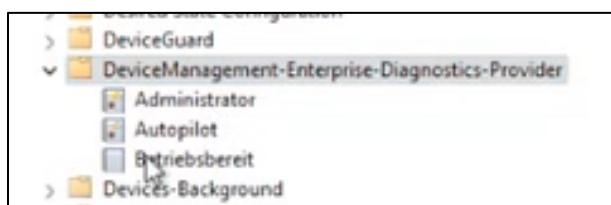


Bild 107: Ordern für Sync

Die vollständige Registrierung und Sichtbarkeit in Intune ist nun eine Frage der Zeit. Manche Geräte erscheinen nahezu sofort, andere benötigen mehrere Stunden oder sogar Tage. Das hängt nicht von einem Fehlverhalten ab, sondern ist systembedingt.

Schlusswort: Dein Weg zu einer sicheren Microsoft 365 Umgebung

Nun weißt du, wie du deine Microsoft 365 Umgebung optimal absichern kannst. Von der Verwaltung deiner Benutzerkonten bis zu den feinen Stellschrauben der Gerätesicherheit – jede Maßnahme trägt dazu bei, Angreifer abzuwehren, Datenverluste zu verhindern und Effizienz zu steigern.

Aber Achtung! Die Arbeit endet hier nicht. Microsoft 365 und Entra ID sind ein dynamisches System, das sich ständig weiterentwickelt. Neue Funktionen und Bedrohungen erfordern regelmäßige Anpassungen. Nutze deshalb die folgenden Prinzipien als Leitfaden.

Kontinuität: Überprüfen regelmäßig deine Sicherheitsrichtlinien und passen sie an aktuelle Anforderungen an.

Automatisierung: Nutze Tools wie Intune oder Defender, um Prozesse zu automatisieren und menschliche Fehler zu minimieren.

Awareness: Schärfe das Sicherheitsbewusstsein deines Teams durch Schulungen und klare Richtlinien.

Am Ende ist Sicherheit kein Zustand, sondern ein kontinuierlicher Prozess. Mit der in diesem Leitfaden vermittelten Basis kannst du nicht nur aktuelle Herausforderungen meistern, sondern deine Umgebung auch zukunftssicher gestalten.

Dein nächster Schritt?

Setze die Maßnahmen schrittweise um. Am besten startest du mit den Bereichen, die den größten Impact haben. Mit jedem Schritt machst du Microsoft 365 Umgebung ein Stück sicherer und effizienter. Jetzt bist du bestens gerüstet, um die Kontrolle über deine Daten und Zugriffe zu behalten – und das Risiko auf ein Minimum zu reduzieren.